



UNIVERSITY
OF
JOHANNESBURG

COPYRIGHT AND CITATION CONSIDERATIONS FOR THIS THESIS/ DISSERTATION



- Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
- NonCommercial — You may not use the material for commercial purposes.
- ShareAlike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

How to cite this thesis

Surname, Initial(s). (2012) Title of the thesis or dissertation. PhD. (Chemistry)/ M.Sc. (Physics)/ M.A. (Philosophy)/M.Com. (Finance) etc. [Unpublished]: [University of Johannesburg](https://ujdigispace.uj.ac.za). Retrieved from: <https://ujdigispace.uj.ac.za> (Accessed: Date).

BioVault: A protocol to prevent replay in biometric systems

By

BOBBY LAUBSCHER TAIT

THESIS

Presented as fulfilment for the degree

D.COM IN ECONOMICS AND MANAGEMENT SCIENCES



In the

FACULTY OF MANAGEMENT

At the

UNIVERSITY OF JOHANNESBURG

PROMOTER: PROF. S.H. VON SOLMS

MAY 2009

“Welcome, and congratulations. I am delighted that you could make it. Getting here wasn’t easy, I know. In fact, I suspect it was a little tougher than you realize. To begin with, for you to be here now trillions of drifting atoms had somehow to assemble in an intricate and curiously obliging manner to create you. It’s an arrangement so specialized, unique and particular that it has never been tried before and will only exist this once, as you...”

Bill Bryson – A short history of everything.

Acknowledgements

1. **My Lord, my Saviour, my guiding Spirit:**

I surrender all I have to my Lord. My Saviour, giving meaning to life, showing me love for all, my guiding Spirit, that gently directs my life onto pathways never thought to be possible – Ek het U lief o Heer!

2. **My parents – Louw and Scotty Tait:**

For your love, always believing in me, and your unwavering support. Thank you for the meticulous attention to the linguistic aspect during proof reading of the thesis. Thank you for giving me the opportunity to study, financial support and more specifically a stable, loving home. This thesis would not have been completed, was it not for your constant encouragement.



3. **Professor Von Solms:**

It was a privilege to have studied under your guidance. Thank you for the opportunity!

4. **My wife – Odelia Tait:**

I love you! You are my shelter, my inspiration!

5. **Professor Ehlers:**

Thank you for your endless motivation and honest advice.

6. **Prof. Danie & tannie Ansie Krige:**

Prof Danie, dankie dat ek in u teenwoordigheid kon vertoef, en u wysheid kon indrink. Tannie Ansie – dankie vir die onbaatsugtige liefde, belangstelling en aanmoediging. Ek is geseënd om julle in my lewe te hê.

7. **William Smith:**

You instilled in me my love for science, physics, and research.
You taught me that if one looks hard enough, a solution is possible!

8. **Frans van der Merwe:**

My loyal friend – I have learned more from you than you will ever know. I humble myself to your knowledge and insight.

9. **Hannes en Stella van Niekerk:**

Oom Hannes en tannie Stella, julle het vorm aan my lewe gegee op 'n baie nodige tyd. Ek is geëerd met jul jare lange bemoëienis met my en julle opregte liefde.

10. **Mev Jantjie Kruger & Mev Loraine Bushney.**

You honestly believed in me in times when few others did. I stand here today, because of the difference you made in my life.

11. **Mr. Klaus König:**

You made my second chance worth the effort! You inspired me to search for deeper understanding.

12. **RAU en UJ:**

RAU, for my first three degrees, and UJ, for the opportunity and funding of the research that led to the development of the BioVault concept.

Table of Contents

Chapter 1

1.1. INTRODUCTION	1
1.2. PROBLEM STATEMENT	6
1.3. OBJECTIVE OF THIS THESIS	7
1.4. SPECIFIC APPROACH	8
1.5. OVERVIEW OF THE THESIS	8
1.5.1. CHAPTER 2 – IDENTIFICATION AND AUTHENTICATION	8
1.5.2. CHAPTER 3 - BIOMETRICS	9
1.5.3. CHAPTER 4: REPLAY	10
1.5.4. CHAPTER 5: TOKEN DUPLICATION	10
1.5.5. CHAPTER 6: SYMMETRY AND ASYMMETRY	11
1.5.6. CHAPTER 7 – THE IMPORTANCE OF IDENTIFICATION & AUTHENTICATION	11
1.5.7. CHAPTER 8 – BIOVAULT VERSION 1.0	11
1.5.8. CHAPTER 9 – BIOVAULT VERSION 2.0	12
1.5.9. CHAPTER 10 – BIOVAULT VERSION 3.0	13
1.5.10. CHAPTER 11 – BIOVAULT, BIOMETRIC ENCRYPTION	13
1.5.11. CHAPTER 12 – BIOVAULT, BIOMETRIC SIGNATURES	13
1.5.12. CHAPTER 13 – CONCLUSION	14
1.5.13. CHAPTER 14 – RESEARCH RESULTS	14
1.5.14. CHAPTER 15 – REFERENCES	14
1.6. SUMMARY OF CHAPTER	14

Chapter 2

2.1. INTRODUCTION	16
2.2. BACKGROUND	16
2.3. IDENTIFICATION AND AUTHENTICATION	18
2.3.1. OPEN OR CLOSED ENVIRONMENTS	18
2.4. IDENTIFICATION	19
2.4.1. IDENTIFICATION IN THE INFORMATION TECHNOLOGY ENVIRONMENT	19
2.4.1.1. Computers	19
2.4.1.2. Electronic devices	21
2.4.1.3. Objects	22
2.4.1.4. Humans	23
2.4.1.5. Conclusion	24
2.5. AUTHENTICATION	25
2.5.1. SECRET PARAMETERS	27
2.5.1.1. Something secretly known	27
2.5.1.1.1. Password considerations	29
2.5.1.1.2. Subverting passwords	30
2.5.1.1.3. Conclusion	35
2.5.1.2. Some unique possession	36
2.5.1.2.1. Subverting Tokens	39
2.5.1.2.2. Conclusion	41
2.5.1.3. Something the user is	42
2.5.1.4. Multi factor authentication	43
2.6. CONCLUSION	44



UNIVERSITY
OF
JOHANNESBURG

Chapter 3

3.1. INTRODUCTION	47
3.2. BACKGROUND	48
3.3. ENROLLMENT	49
3.4. KEY ELEMENTS OF A BIOMETRIC SYSTEM	50
3.4.1. DATA ACQUISITION	51
3.4.2. TRANSMISSION CHANNEL	52
3.4.3. SIGNAL PROCESSING	53
3.4.4. DECISION POLICY	54
3.4.4.1. The False Acceptance Rate (FAR)	55
3.4.4.2. The False Rejection Rate (FRR)	57
3.4.4.3. Crossover rate	58
3.4.5. TEMPLATE STORAGE	59
3.4.5.1. Local storage	59
3.4.5.2. Network storage	59
3.4.5.3. Portable device storage	60
3.5. TYPES OF BIOMETRICS	61
3.5.1. FINGERPRINT	61
3.5.2. MINUTIAE	65
3.5.3. LEVELS OF FINGERPRINT DETAIL	66
3.5.4. ELEMENTARY MECHANISM OF A FINGERPRINT SCANNER	67
3.5.5. FINGERPRINT CAPTURING TECHNOLOGIES	68
3.5.6. TEMPLATE EXTRACTION	68
3.5.7. VULNERABILITIES OF FINGERPRINT BIOMETRICS	71
3.5.7.1. Forcing a false match	72
3.5.7.2. Masking the fingerprint to avoid a biometric match	72
3.5.8. FINGERPRINT CONCLUSION	73
3.6. IRIS SCANNING	74
3.7. CONCLUSION	77

3.8. LIVENESS TESTING	78
3.8.1. LIVENESS TEST CATEGORIES	80
3.8.1.1. Intrinsic properties of a living body	80
3.8.1.2. Involuntary signals generated by a living body	80
3.8.1.3. Responses to stimuli (Challenge-response)	81
3.8.2. STRONG AND WEAK LIVENESS TESTS	82
3.8.3. PROBLEMS WITH LIVENESS TESTS	82
3.9. CONCLUSION	84



Chapter 4

4.1. INTRODUCTION	86
4.2. REPLAY	87
4.2.1. ACQUISITION OF A PASSWORD	87
4.2.2. REPLAY OF AN ACQUIRED PASSWORD	88
4.2.3. PASSWORD REPLAY COMMENTS	89
4.2.4. ACQUISITION OF BIOMETRIC DATA	90
4.2.5. REPLAY OF BIOMETRIC DATA	93
4.2.6. BIOMETRIC DATA REPLAY COMMENTS	95
4.3. CONCLUSION	95



Chapter 5

5.1. INTRODUCTION	97
5.2. MANUFACTURED TOKENS	98
5.2.1. CREDIT CARD SKIMMING [88]	99
5.2.1.1. Credit card skimming conclusion	102
5.2.2. BIOMETRIC CHARACTERISTIC DUPLICATION	102
5.2.2.1. Method 1	103
5.2.2.2. Method 2	104
5.3. CONCLUSION	105



Chapter 6

6.1. INTRODUCTION	108
6.2. SYMMETRY	109
6.2.1. PASSWORDS	109
6.2.2. TOKENS	112
6.2.3. SYMMETRY CONCLUSION	114
6.3. ASYMMETRY	115
6.3.1. ASYMMETRIC USAGE	116
6.4. CONCLUSION	117



Chapter 7

7.1. INTRODUCTION	119
7.2. BACKGROUND	120
7.3. TYPICAL ONLINE TRANSACTION	122
7.3.1. PAYING FOR A LOCAL SUPPLIER	123
7.3.1.1. A direct bank deposit	123
7.3.1.2. An online payment	123
7.3.2. PAYING AN INTERNATIONAL SUPPLIER	124
7.3.2.1. International bank transfer	124
Problems with international bank transfer:	124
7.3.2.2. Credit card online payment	125
7.3.2.3. Secure Socket layer [107]	126
7.4. INTERNATIONAL MONEY VENDORS	128
7.4.1. HISTORY OF PAYPAL	128
7.4.2. THE PAYPAL MECHANISM	129
Making a payment using PayPal	132
7.4.3. ADVANTAGES OF USING PAYPAL	133
7.4.4. DISADVANTAGES WITH PAYPAL	134
7.5. CONCLUSION	135



UNIVERSITY
OF
JOHANNESBURG

Chapter 8

8.1. INTRODUCTION	138
8.2. USING BIOMETRIC DATA FOR AUTHENTICATION	139
8.2.1. CONCLUSION	141
8.3. SNIFFING NETWORK TRANSMITTED BIOMETRIC DATA	141
8.3.1. CONCLUSION	143
8.4. DETECTING REPLAY OF AUTHENTICATION DATA	144
8.5. USING ASYMMETRY TO DETECT REPLAY	144
8.6. DETECT REPLAY IN AN ASYMMETRIC ENVIRONMENT	145
8.6.1. THE BIO ARCHIVE (BA)	146
8.6.2. THE WORKING OF BIOVAULT VERSION 1.0	147
8.7. REPLAY DETECTION BY BIOVAULT	148
8.7.1. CONCLUSION	154
8.8. EVALUATION OF BIOVAULT VERSION 1.0	155
8.9. CRITICAL LOOK AT BIOVAULT VERSION 1.0	156
8.10. CONCLUSION	157



Chapter 9

9.1. INTRODUCTION	159
9.1.1. BIOMETRIC DATA PROTECTION	160
9.1.2. AVOIDING AN EXACT BIOMETRIC MATCH	160
9.2. LATENT BIOMETRIC CHARACTERISTICS AND BioVAULT	161
9.2.1. BIOMETRIC CHARACTERISTIC ACQUISITION	162
9.2.2. MISUSE OF FAKE BIOMETRIC CHARACTERISTIC	163
9.3. BioVAULT VERSION 2.0	166
9.3.1. THE CLIENT-SIDE BIO-ARCHIVE (CBA)	166
9.3.1.1. CBA storage	167
9.3.2. MECHANISMS OF BioVAULT VERSION 2.0	168
9.3.3. DISCUSSION OF THE BioVAULT VERSION 2.0 APPROACH	172
9.4. CONCLUSION	174



Chapter 10

10.1. INTRODUCTION	176
10.2. BACKGROUND	177
10.3. EXPLOITING BioVAULT VERSION 2.0	179
10.4. USAGE OF SNIFFED INFORMATION	182
10.4.1. FRESH BIOMETRIC DATA FROM THE BIO-PARCEL	182
10.4.2. OLD BIOMETRIC DATA FROM THE BIO-PARCEL	183
10.4.3. CHALLENGE FROM THE AUTHENTICATION SERVER	183
10.4.4. CONCLUSION	184
10.5. BioVAULT VERSION 3.0	184
10.6. SERVER CHALLENGE PARCEL FOR USER	189
10.7. CONCLUSION	192



Chapter 11

11.1. INTRODUCTION	194
11.2. BACKGROUND	195
11.3. ENCRYPTION USING A SECRET KEY OR BIOMETRIC CHARACTERISTIC	196
11.3.1. SECRET KEY ENCRYPTION	196
11.3.2. BIOMETRIC DATA FOR ENCRYPTION	198
11.3.3. CONCLUSION	201
11.4. BIOMETRIC ENCRYPTION	201
11.4.1. BIOMETRIC ENCRYPTION OVERVIEW	202
11.4.2. BIOMETRIC ENCRYPTION DISCUSSION	203
11.4.3. PHASE 1 – REQUEST OF BIOMETRIC DATA	203
11.4.4. PHASE 2: SUBMISSION OF BIOMETRIC DATA OF SAM TO JOHN	206
11.4.5. PHASE 3: ENCRYPTED COMMUNICATION BETWEEN JOHN AND SAM	208
11.5. CONCLUSION	210



Chapter 12

12.1. INTRODUCTION	212
12.2. BACKGROUND	212
12.3. CREATING A MAC USING A SECRET KEY OR BIOMETRIC CHARACTERISTIC	214
12.3.1. SECRET KEY MESSAGE AUTHENTICATION CODE (MAC)	214
12.3.2. BIOMETRIC MAC	217
12.3.3. CONCLUSION	219
12.4. USING BIOMETRICS CHARACTERISTICS TO GENERATE A MAC.	220
12.4.1. PHASE 1 – SIGNED MESSAGE DESTINED FOR SAM	222
12.4.2. PHASE 2: AUTHENTICATION SERVER	225
12.4.3. PHASE 3: SAM REQUESTS THE BIOMETRIC MAC KEY.	227
12.4.4. PHASE 4: CONFIRM SAM’S AUTHENTICITY.	229
12.4.5. BIOMETRIC DATA SUPPLIED TO SAM.	231
12.4.6. PHASE 6: TEST MESSAGE’S INTEGRITY.	234
12.5. CONCLUSION	235



Chapter 13

13.1. OVERVIEW	237
13.1. PROBLEM STATEMENT OF THIS THESIS:	237
13.2. MENTIONED DELIVERABLES OF THE THESIS:	238
13.3. EVALUATION OF THESIS SUCCESS.	238
13.3.1. SOLUTIONS TO PROBLEM STATEMENT	239
13.3.2. DELIVERABLES, DELIVERED	240
13.4. CONCLUSION	242



Chapter 14

14.1. OVERVIEW	243
14.2. INTERNATIONALLY ACCEPTED ARTICLES	243
14.3. PATENT PROPOSAL	244
INTERNATIONALLY ACCEPTED ARTICLES	244
INTERNATIONALLY ACCEPTED ARTICLES	261
INTERNATIONALLY ACCEPTED ARTICLES	270
INTERNATIONALLY ACCEPTED ARTICLES	280
PATENT PROPOSAL	296



Chapter 1: Introduction

1.1. INTRODUCTION

The information age has eliminated almost all communication boundaries. People can communicate with virtually anybody anywhere in the world. Considering that trade is so part of everybody's day to day life, this borderless communication soon gave way to global trade.

In any commercial situation, it is important that the buyer is firmly convinced that he is dealing with the authentic seller and vice versa, that the seller is convinced that he is dealing with the authentic buyer. The buyer wants to be sure that it is the authentic seller of the product and not just any individual masquerading as the seller of a product. On the other hand the seller also needs to be sure that the buyer is authentic and that the buyer has the authority to transfer money from his bank account. The seller wants to be satisfied that this buyer is not a hacker that fraudulently gained access to a bank account, paying for the transaction from this unauthorized bank account.

Previously In a small community people usually knew each other and for this reason trade was a lot easier. However, today people trade globally. Money is transferred globally from buyer to seller. Banks acts as go-betweens, vending money on behalf of their clients. The bank relies on identification and authentication techniques when an instruction is received from a client to transfer money to a seller's account. Confidentiality is paramount throughout the entire transaction - if any information is disclosed, e.g. the client's personal details, account information or a number of other aspects relating to the transaction, privacy can be compromised.

Successful identification and authentication are the gate keepers of the security environment. Von Solms and Eloff [1] describe the five information security services as:

- Identification and authentication,
- confidentiality,
- integrity,
- authorization and
- non-repudiation.

If the identification and authentication phase fails, all other information security services are compromised!

The information security service of identification and authentication is currently enforced by means of a number of technologies. These technologies all aim to provide confirmation that the entity accessing the computer environment is the authentic entity. Unfortunately, all the current technologies are fallible. As an example, a major problem relating to passwords and tokens is the fact that a person using a password or token is only indirectly authenticated. For instance if a password is tested for authenticity, the system will match the presented password with a stored password. If the stored password matches the offered password exactly, the system will conclude that the offered password is authentic. This approach has a major flaw – the person presenting the password was not authenticated - only the password was. The system relies on the premise that the user will keep his password secret. In general this method of authentication is referred to as authentication by means of something that the person **knows**. A person can also be authenticated by something that he **possesses** (e.g. tokens), or something that the user **is** (e.g. biometrics) [2].

Biometrics is part of the physical person. Biometrics represents a particular person. Different examples of biometrics are available, varying in complexity and

industry adaptation. Biometrics is part of the user, and in most instances, if a biometric characteristic is digitized, especially under supervision, the system can be firmly convinced that the user is authentic. The utility of this approach is that the system authenticates the person as the undisputed provider of the biometric characteristic.

There are unfortunately also a number of problems associated with biometrics. First and foremost – if a person's biometric characteristic is stolen or filched, the person is faced with the problem that this compromised biometric characteristic can not merely be replaced as one would replace a compromised password or stolen token. Ease of filching a biometric token depends largely on the type of biometric.

Biometrics can be filched in mainly two ways as illustrated in figure 1.1, along the undesired biometric path.

Firstly as illustrated in figure 1.1, as humans interact with their environment, they leave behind latent biometric images. For example, if a person touches a glass, his fingerprint is left on the glass. If a person drinks from this glass, DNA (found in the person's saliva) is left on the glass. Various studies and research have demonstrated that latent biometric images can be lifted, and used at a later stage to spoof biometric devices [3].

In figure 1.1, the action of generating a fake biometric characteristic from a glass that the user touched, is illustrated. This fake biometric characteristic that the hacker manufactured can then be used to spoof a biometric digitizer.

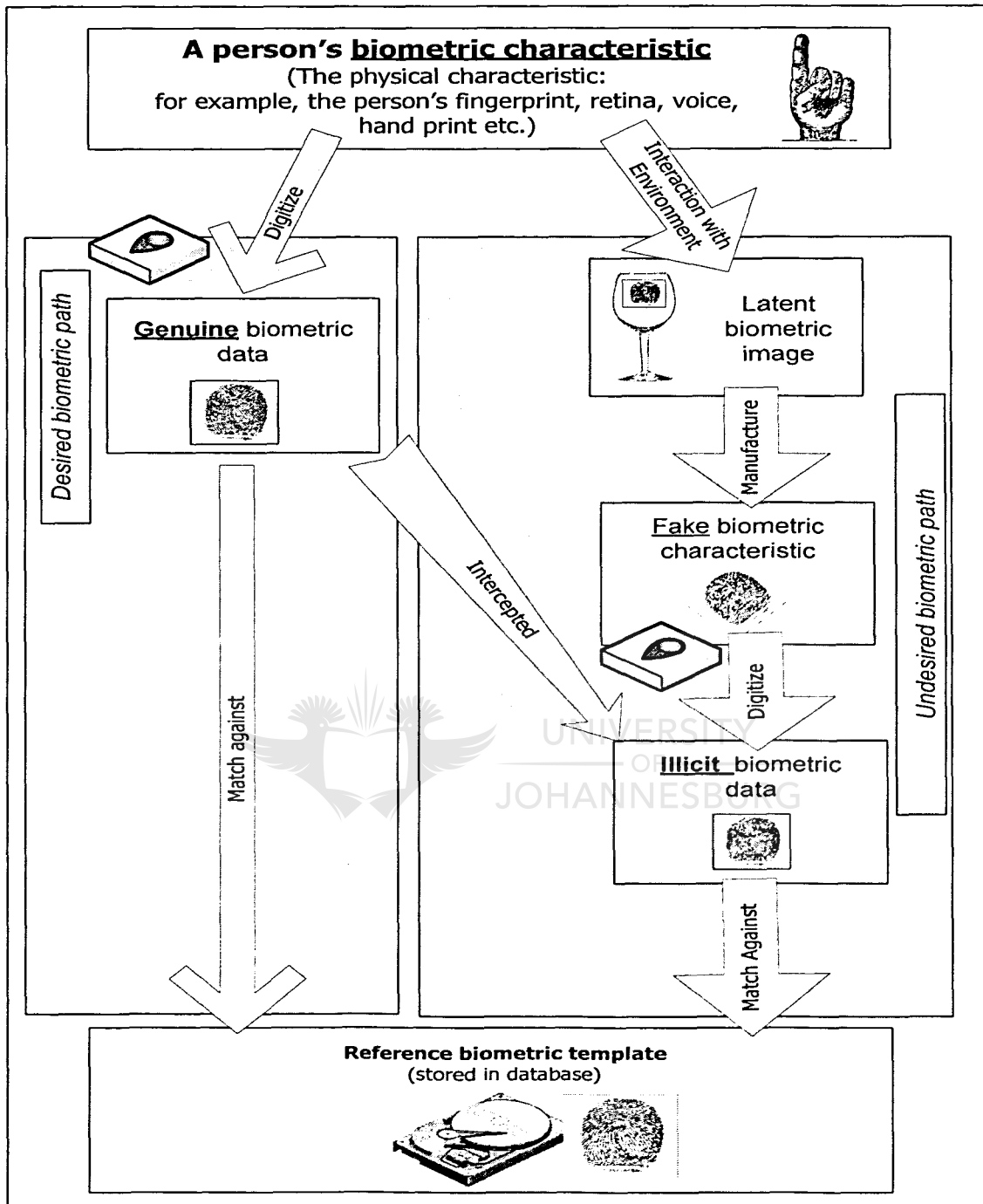


Figure 1.1: Flow diagram for biometric technology.

Secondly, a physical attack on biometrics, as mentioned in the previous paragraph, is not the only concern. Another problem with biometrics is the fact that all biometric characteristics are digitized and changed into an electronic

template. This electronic template is the electronic representation of the biometric.

A reference biometric template is stored in a database and will be used as reference biometric data; all freshly digitized biometric data are compared against the reference biometric template. The electronic biometric data is vulnerable to filching in a number of ways. If the biometric data is stolen in electronic format, as illustrated in figure 1.1, the whole biometric is compromised, and can be replayed for false authentication purposes.

This thesis investigates the problems associated with identification and authentication of the human being. For this reason the thesis focuses mainly on biometrics as a feasible identification and authentication solution.



1.2. PROBLEM STATEMENT

If biometric technology is to be considered as the standard to identify and authenticate persons, the risk of the biometric being stolen is high. As mentioned a biometric characteristic cannot be simply replaced as one would replace a stolen token or password. The following two problems therefore limit the use of biometrics in identification and authentication:

Firstly, biometric data in electronic format can be stolen in various ways and be replayed at a later stage for false identification and authentication. The electronic data of a biometric can be acquired from various sources. For instance, during the capturing phase of the biometric data, during the transmission phase from the biometric device to the terminal, or even when the biometric data is sent over a network – to name only a few.

Secondly, a fake biometric characteristic can be manufactured for a given biometric in order to deceive the biometric matching algorithm into authenticating the manufactured fake biometric characteristic; e.g. a fake latex biometric characteristic can be manufactured from a latent finger print left by a person on a glass.

Due to the mentioned two problems, the wider application of biometrics for identification and authentication – specifically if used for digital signatures – is still hazardous.

In the following paragraph a solution will be proposed that will be discussed in the rest of the thesis.

1.3. OBJECTIVE OF THIS THESIS

Identification and authentication is probably the most important part of electronic commerce. As mentioned in the introduction (section 1.1), if identification and authentication is not irrefutably established, the remainder of the five information security services [1] will fail irrevocably. During an electronic commerce transaction both buyer and seller need to be convinced that the other participant in the contract is beyond any doubt the person or representative of the institution with whom he or she is about to negotiate a deal. Without irrefutable proof of identification and authentication, confidentiality, integrity, authorization and non-repudiation are at stake. The transaction hinges totally on bilateral conviction of identification and authentication. Passwords and tokens are currently used as the preferred technology to assist in identifying and authenticating the person indirectly. Biometrics is a method that authenticates a person directly, but due to the problems associated with biometric data theft, as mentioned in section 1.2, biometric technology is not yet widely usable.

This thesis investigates current identification and authentication technologies, including biometrics. A model, named BioVault, is proposed for an identification and authentication method utilizing biometrics. This model proposes a closed system with a challenge and response approach, utilizing biometrics as the core method for identification and authentication. This model demonstrates that biometrics can be used to identify and authenticate a person over a networked environment, without the risk of biometric data being misused as discussed in section 1.2. This model also allows biometrics to be used as a form of digital signatures.

BioVault is therefore proposed as a solution for the problem statement provided in section 1.2. The following section will cast some light on the approach that will be followed to formulate this model.

1.4. SPECIFIC APPROACH

A number of topics must be considered in order to formulate the model that will solve the problems faced with biometric theft. These topics will be discussed in separate chapters. Each chapter is a different part of the foundation that the model is built upon, and each chapter will introduce different problems and solutions.

The approach that will be followed is to introduce different aspects of the model; each aspect will form the foundation for the next topic. The model will for this reason evolve from a rudimentary solution to a complete all inclusive solution, known as BioVault.

The following deliverables will be presented:

1. A complete system for detecting biometric misuse attempts.
2. A system that will ensure the safe keeping of biometric data during network transmission.
3. A system that will allow users of this model to encrypt sensitive information using biometrics.
4. A system that will allow users of this model to digitally sign electronic documents using biometrics.

The reader will be guided along a path that will eventually lead to the presentation of the complete model.

In the section to follow, the different chapters will briefly be introduced, followed by a brief overview of what the chapter entails.

1.5. OVERVIEW OF THE THESIS

1.5.1. Chapter 2 – Identification and Authentication

Chapter 2 focuses on the security service of identification and authentication. This chapter explains the service of identification and authentication in open and closed environments. Identification is discussed as a separate entity, followed by a discussion of authentication. The three methods of authentication are discussed – something the user knows, something the user owns and something the user is. Mechanisms to enforce authentication for each method are also researched. The chapter also considers problems associated with each mechanism, for example that passwords can be guessed, sniffed, cracked, replayed etc. and that tokens can be falsified, stolen etc.

Chapter 2 will point out that if tokens and passwords are used for identification and authentication, only the password or token is authenticated, and not the person presenting the password or token. This chapter does not discuss the method “Something the user is” in detail, as this aspect of authentication is discussed in depth in Chapter 3.

1.5.2. Chapter 3 - Biometrics

Chapter 3 will consider biometrics as a technology to solve the problems pointed out in chapter 2. This chapter will demonstrate that unlike identification and authentication using tokens and passwords, a person is directly authenticated using biometrics.

The first part of the chapter focuses on the technology of biometrics. Key elements found in all biometric systems are discussed and explained. Aspects like the false acceptance rate, failure to enroll rate and false rejection rate, are graphically illustrated. Even though the eventual model does not rely on any

specific biometric technology, the second part of the chapter focuses on a typical biometric technology like finger prints to demonstrate the typical user interaction with this biometric.

This chapter will demonstrate that a digitized biometric characteristic (biometric data) is just as vulnerable as a password. Thus the biometric data can be sniffed, stolen, and eventually replayed.

The second major problem with stolen biometric data is the fact that the biometric characteristic cannot simply be replaced. Thus if the biometric data from e.g. a thumb print, is copied, the thumb cannot simply be replaced.

The chapter concludes with an overview of the advantages gained using biometrics and the problems found if biometrics is used.

1.5.3. Chapter 4: Replay

This chapter will focus specifically on the problems found relating to any form of replay. The chapter will demonstrate the methods used to acquire biometric data, as well as acquiring passwords, and the methods used to replay this data.

It will be demonstrated that biometrics is just as vulnerable to replay attacks as any other technology

1.5.4. Chapter 5: Token Duplication

This chapter will discuss the problems related to duplicating a man-made token (like a smartcard) and also methods used to duplicate a biometric characteristic (like a finger print). In conclusion this chapter will show that the duplication of a biometric characteristic is a big problem, as the biometric characteristic cannot be replaced like one would replace a man-made token.

1.5.5. Chapter 6: Symmetry and Asymmetry

Chapter 6 will introduce the principle of symmetry and asymmetry. The chapter discusses the fact that passwords and tokens are symmetric authentication technologies and that biometrics is an asymmetric technology. The chapter will demonstrate how asymmetry found in biometrics can be used to identify biometric data uniquely, and then be used as a possible option to detect replay of biometric data.

1.5.6. Chapter 7 – The Importance of Identification & Authentication

This chapter considers the current electronic commerce environment. A typical online transaction is discussed to demonstrate that the current electronic commerce environment relies mainly on passwords and tokens to safeguard the buyer's funds.

If the information in chapters 4 and 5 is considered, it is clear from chapter 7 that the current electronic commerce environment is vulnerable to attack. The chapters following chapter 7 explain the working mechanism of the BioVault model. The BioVault model is designed to safeguard an electronic commerce transaction.

1.5.7. Chapter 8 –BioVault Version 1.0

This chapter illustrates how asymmetry can be used to solve the problem of replay (relating to the first part of the problem statement). This is done with BioVault version 1.0. In order to accomplish this, a Bio-archive is introduced on a trusted server.

The second and even more compelling part of this chapter will demonstrate that electronic sniffing and replay is not the only problem. The chapter will conclude therefore with the problems found with latent finger prints and the manufacturing of false biometric copies.

Chapter 8 concludes with the second part of the problem statement namely:

A fake biometric characteristic can be manufactured for a given biometric in order to deceive the biometric recording device into authenticating a fake biometric characteristic; E.g. a latex biometric characteristic can be manufactured from a latent finger print on a glass, that the person has handled.

BioVault version 1.0 does not address this part of the problem, which is solved in subsequent versions of BioVault.

Chapter 9 will present a basic model to solve the second part of the problem statement.

1.5.8. Chapter 9 – BioVault Version 2.0

Chapter 9 introduces the second version of the BioVault model. This model solves the problem encountered in the second part of the problem statement, namely latent biometric characteristic lifting and fake biometric characteristic manufacturing.

BioVault version 2.0 is introduced in chapter 9 with two major additions to BioVault version 1.0. A Bio-archive on the server as well as the client side, is introduced, and will be known as the client Bio-archive (CBA) and the Server Bio-archive (SBA). These Bio-archives serve as the initial defense line against fake biometric characteristics. Furthermore a challenge and response system is

introduced to assist overcoming the problems associated with fake biometric characteristics.

Chapter 9 concludes with some issues relating to the SBA and CBA, like size of the Bio-Archive (BA), speed, and uniqueness considerations in the BA.

1.5.9. Chapter 10 – BioVault Version 3.0

This chapter starts with a critical evaluation of BioVault version 2.0, considering the major benefits and possible short comings. These led to BioVault version 3.0, in which an improved protocol is introduced. In this protocol, a Bio-parcel is created using XOR technology. Chapter 10 also concludes that there is no need for a full search through the SBA, and that the SBA can include only a limited number of biometric data. Lastly chapter 10 illustrates the mechanism of unique flash drive codes and shared key to protect the contents of the CBA.

1.5.10. Chapter 11 – BioVault, Biometric Encryption

This chapter will illustrate how BioVault version 3.0 can be used to successfully encrypt a message sent over the internet between 2 parties, using biometric data as the secret key for the encryption algorithm,. This method relies on the fact that both sender and receiver are part of the BioVault infrastructure.

1.5.11. Chapter 12 – BioVault, Biometric Signatures

The last application chapter demonstrates the mechanism used to utilize biometric data for the signing of electronic documents. Chapter 12 will illustrate the method that the BioVault environment will follow in order to digitally sign a document, using the biometric data of the person generating the document, and intending to sign the document. This will allow non-repudiation to be enforced. The biometric data that is used to sign the electronic document is thus directly related to the signing party.

1.5.12. Chapter 13 – Conclusion

This chapter considers the aim of this thesis, and shows that each and every aim, as formulated in Chapter 1, has been accomplished successfully.

1.5.13. Chapter 14 – Research Results

Articles emanating from the research are included in this section, as well as a patent application that was discovered during the research of the thesis.

1.5.14. Chapter 15 – References

Chapter 15 includes all sources used during the research of this thesis.

1.6. SUMMARY OF CHAPTER

In conclusion, chapter 1 introduces the various parts that will be discussed in order to formulate the BioVault model. This model will help prevent the usage of filched biometric data, or fake biometric characteristics manufactured from lifted biometric characteristics.

Briefly this chapter points out that:

- Chapter 2 will discuss identification and authentication by means of passwords, tokens and pins, focusing on the shortcomings of these technologies.
- Chapter 3 will discuss biometrics as a possible solution, pointing out the strengths over normal passwords and tokens, concluding that biometrics can also be stolen and replayed.
- Chapter 4 will discuss replay of biometrics and tokens, building the underlying argument for biometric usage.

- Chapter 5 explains the principles of token and biometric duplication and in what way this hinders the acceptance of biometrics for electronic commerce purposes.
- Chapter 6 illustrates the mechanism and usability of asymmetry to identify biometric data.
- Chapter 7 illustrates a typical e-commerce environment found currently, pointing out the strong and weak points of the current environment.
- Chapter 8 will introduce BioVault version 1.0, to solve the problem of biometric data replay using asymmetry. However, chapter 8 concludes with the problem of lifted biometric data and the manufacturing of fake biometric characteristics, subsequently used for false identification and authentication.
- Chapter 9 introduces the BioVault version 2.0 model to demonstrate how the problem of lifted biometric characteristics can be solved.
- Chapter 10 will discuss the BioVault version 3.0 model to ensure client authenticity for biometric identification and authentication.
- The thesis includes two application chapters, chapter 11 and 12, which illustrate how BioVault can be used to digitally sign and encrypt a message using biometric data.
- References, Appendixes and the final conclusion of the thesis are found in chapters 13, 14 and 15.

The following chapter (chapter 2) will discuss identification and authentication using the current methods commonly used in the industry, namely passwords, tokens and pins. These topics will be discussed generally, focusing on their strengths and shortcomings.

Chapter 2: Identification and Authentication

2.1. INTRODUCTION

Identification and authentication is the first information security service as specified by Von Solms and Eloff [1]. This thesis will describe the development of a protocol to assist in the secure usage of biometric identification and authentication. For this reason it is important that the different facets of identification and authentication should be considered. This chapter will discuss the need in a computer environment for identification, followed by a discussion of the factors needed to ensure that an identified person or object is the authentic person or object by means of various authentication techniques. The different types of authentication techniques will be discussed, and the shortcomings of identification and authentication will be considered. In conclusion this chapter will demonstrate that authentication by means of something that a user knows e.g. passwords, or authentication by means of something that the user owns e.g. tokens, do not authenticate a person presenting the password or token, but only authenticates the actual password or token as authentic.

2.2. BACKGROUND

Human beings are masters of identification. They have 5 senses to aid them with identifying virtually everything in their environment. Sight, hearing, touch, smell and taste are jointly used to perceive, identify and even authenticate almost everything in their world. In fact, if something cannot be identified using these 5 senses, it virtually does not exist for that particular person.

Identification is a lifelong learning curve for man, and the ability to identify, educates him / her. If a person is faced with something that was never experienced before, he or she will need to learn from the new experience, and in future, will be able to identify and make decisions based on acquired knowledge. A person cannot describe a taste never tasted, or an odour never smelt before. A person cannot identify a person he has never met.

In a small community, people know everybody that is part of this small community. If somebody calls a person on the telephone, a person will be identified by his way of talking, tone of voice, and even by the type of discussion. A person walking down the street can be identified by the way that he walks, hairstyle and the person's face. A lady entering a shop can even be identified by the perfume that she wears. In this community, identification comes natural, and people are used to identification, without conscious awareness of the process of identification.

Computers must be equipped with 'senses' in order to have the ability to identify. Computers, as with humans, must go through a learning curve in order to successfully identify. A computer is however not as intuitive as a human being, thus if identification parameters are tampered with, the computer has difficulty in making a successful identification.

This chapter will discuss the concepts of identification and authentication. The reader will be introduced to the importance of this security service, and all the aspects relating to identification and authentication. The discussion will mainly focus on the information technology service of identification and authentication. The chapter will conclude with an overview of the importance and relevance of this security service to the information technology environment.

2.3. IDENTIFICATION AND AUTHENTICATION

Identification and authentication ensures that only legal parties are allowed to access an IT system [4].

All forms of identification and authentication assume that there exists a trusted path for secure data transfer between a claimant and a verifier.

Even though identification and authentication is often used as a single concept, this chapter will discuss identification and authentication separately. Identification and authentication as an entity is cited as the first of the five security services [1]. This first service of identification and authentication is of great relevance to this thesis, and will form the core of the developed model.

2.3.1. Open or closed environments

Identification and authentication can be applied in an open or a closed environment [4].



In an open environment, the IT system is not aware of all possible parties. E.g. a website such as Amazon.com [5], allows a new user to choose a unique identifier and password. The Amazon environment has never met the person before and no prior knowledge exists of this particular user. The environment is open for anyone to register to the Amazon environment.

In a closed environment the system is aware of all possible parties that may wish to access the facilities of the environment. This environment is not open to everybody, and registration is not done by the users themselves. For instance, during the registration of the users using the intranet of a company, the network administrator must provide the user with a username and a temporary password for the intranet. Identification and authentication is an important security consideration for both open and closed IT environments. In the rest of the

chapter, attention will first be given to identification, followed by a discussion on authentication.

2.4. IDENTIFICATION

In virtually any environment, if positive identification cannot be established, the risk factor increases, and a possible fraudulent action may occur. As stated in the introduction of this chapter, human beings have a natural ability to identify, and even though they may be fooled, they are not fooled that easily. Unfortunately identification does not come that naturally in the information technology environment. 'Senses' or tools must be supplied to computers to assist them with the ability to identify.

In the information technology environment, a unique identifier (identity) like a username for people or a unique number like a media authentication code (MAC) must be linked to whatever must be identified [6]. One will find that if something needs to be identified by a computer, this item will have one or other unique marking. A barcode is a typical example of a unique marking that assists in the identification of items.

2.4.1. Identification in the information technology environment

In the IT environment, computer devices need to identify a number of objects. Some objects are engineered to work with computers like a USB device, and they will follow a specific convention to ensure that identification of such devices is as simple as possible. A broad outline of a number of the objects that need to be identified in the IT environment will briefly be discussed.

2.4.1.1. Computers

The IT environment must have the ability to identify computer systems. These computer systems are usually a computer terminal running an operating system, with various hardware devices installed on the computer. Computers that need to be identified are linked to a network, and networked computers need to identify each other. Various techniques are used, depending on the type of network being used. As a TCP/IP network is currently the most common type of network [4], the technology to identify a computer in a TCP/IP network will be explained.

To identify a computer connected to the network, a number of methods are utilized:

- 1) Each network card has a unique MAC address (media authentication code) [4] [7], used for network card identification. This MAC allows for direct identification and communication. Each machine is assigned a unique numeric value called a physical address / hardware address for example MAC 01-23-45-67-89-ab.
- 2) Each computer joining the network must also have a unique IP address, this IP address is associated with the MAC of the computer [8] for example 152.106.42.195.
- 3) Lastly a computer can also be identified by the machine's unique universal resource locator (URL) [8], for example: 'csrau.rau.ac.za'.

A computer can identify other computers based on the identifiers associated with the specific computer. The URL is associated with the IP address, and the IP address is associated with the MAC of the computer. Any of these can assist a computer to identify another computer uniquely.

However, in the IT environment, computers are not the only devices needed to be identified. A number of other electronic devices are found that interact with the computer and also have to be identified. These electronic devices are briefly discussed in the next section.

2.4.1.2. Electronic devices

Currently a whole array of electronic devices can be connected to a computer. Previously, the user of a computer had to identify the device on behalf of the computer. The user then had to set various parameters to assist the computer to use the services of the electronic device [9]. Typical example of electronic devices that interact with a computer and that the computer has to identify include:

- USB flash memory for external storage.
- USB devices like printers, external hard drives, cameras, sound cards etc.
- Serial port devices like modems or legacy pointer devices.
- Parallel port printers or scanners.

The above examples show only a few general examples, and as technology has improved, these electronic devices now include unique identifiers for almost all electronic devices that can be attached to a computer [10]. These identifiers are subsequently used by the computer to identify all attached electronic devices. This allows the computer to identify an electronic device and ensure that the device is assigned to the right driver software [10], or to ensure that the correct software is loaded for the specific electronic device.

Computers and electronic devices are manufactured to interact with each other. Computers can identify each other and computers can also identify electronic devices based on unique numbers assigned to these devices. However, computers must also be able to identify items not part of the electronic

environment. For instance, a box of pills is not part of the electronic environment. If we want the computer to identify the box of pills uniquely, the computer must be provided with a 'sense' to assist in this identification. This box of pills is considered as an object that must be identified.

2.4.1.3. Objects

Various methods exist to allow a computer to identify objects that are external to the computer environment. Barcode technology is currently the de-facto standard for identifying virtually any object. Almost all objects have a barcode. A computer can read a barcode on these objects, and this allows the computer to identify the objects.

An Example of a barcode is illustrated in figure 2.1



Figure 2.1: A barcode

Bar code technology is not the only tool available to assist computers to identify objects. Technology such as RF-tags is gaining increasing popularity.

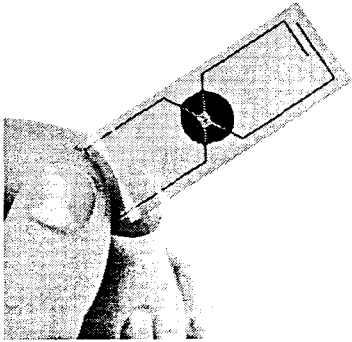


Figure 2.2: A RF-Tag [11]

2.4.1.4. *Humans*

As with objects, humans also reside outside the IT environment, and humans must also be identified by a computer.

In much the same way objects have to be identified by a computer by giving them a unique barcode or a RF-tag, a human must also have an unique identifier associated with the human, in order for the computer to identify the person.

A human will therefore receive a username or user code. This username or user code will usually be a unique name or number linked directly to the user. Ideally nobody else should have the same identifying object in a given IT environment [12]. This unique number or name will assist a computer to identify the user.

A user will be challenged by a secure IT environment to provide his/ her unique identifier; this step is usually part of the logon procedure. A typical logon challenge is illustrated in figure 2.3.

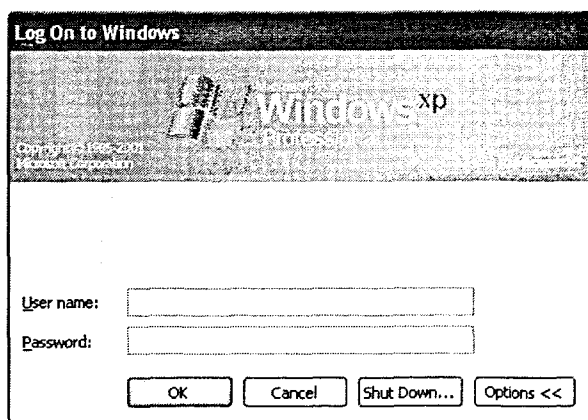


Figure 2.3: Login screen

In the illustration of figure 2.3 the user must supply his / her unique identifier. This allows the computer to identify the user.

2.4.1.5. Conclusion

Identification is the first step in the information security service of identification and authentication. A number of role players interact with a computer, and must be uniquely identified. These role players can be divided into 4 major groups:

- Computers that must identify other computers,
- Electronic devices that must be identified by computers,
- Objects like a box of pills that the computer must identify,
- Humans interacting with a computer must be identifiable.

This unique identifier, regardless of application domain is not covert.

A barcode is always visible and accessible to anyone. A RF tag can be scanned, and the unique number of the RF-tag will be openly displayed. The IP- and MAC address of a computer can effortlessly be found with an instruction such as Ipconfig -all as illustrated in Figure 2.4.


```
C:\WINDOWS\system32\cmd.exe
<> Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Bobby Tait>ipconfig -all

Windows IP Configuration

    Host Name . . . . . : e1232desktop
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . . :
    Description . . . . . : Intel(R) PRO/1000 MT Network Connect
    Physical Address. . . . . : 00-0D-56-C3-9F-65
    Dhcp Enabled. . . . . : No
    IP Address. . . . . : 152.106.42.111
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 152.106.42.240
    DNS Servers . . . . . : 152.106.1.53

C:\Documents and Settings\Bobby Tait>
```

Figure 2.4: Ipconfig in the console window.

The user name of a person can usually be found on the system domain and is not concealed by the system. The system does not obscure this unique identifier. In essence it must be accepted that the name or number used for the purposes of identification in all aspects of the IT environment is not secretive.

Once the computer, electronic device, object or human is identified by a computer, the computer must ensure that whatever was identified is then authentic. In the next section the authentication phase of the identification and authentication security service will be discussed.

2.5. AUTHENTICATION

As discussed in the previous section, identification is the first step in the information security service of identification and authentication. It was mentioned that the methods used for the purpose of identification are not secret, and the names or numbers linked to humans, objects, computers etc, are not covert either. Because of this, it is possible to masquerade as another person merely by responding to a logon challenge as somebody else.

However, humans, computers, and electronic devices are often exclusively authorized to perform certain tasks. Certain privileges are often associated with a specific user. For example, Andy Smith is authorized to change the monthly salaries of employees of a company. Andy will use his identifier e.g. AndySmith to identify himself to the accounting system of the company. The accounting system will then, based on his approved authorization privileges, allow him to alter the monthly salaries of any employee.

In an environment where people are honest, and live with integrity, all would be fine. Unfortunately, this is not the world of today.

A possibility exists that another user, working for this particular company may use Andy's user name to gain access to the authorization privileges awarded to Andy. For example; Mandy feels that the salary she receives each month is insufficient. She will access the accounting software of the company but instead of using her own identifier linked to her, she will enter Andy's identifier. Keep in mind that his identifier is not secret, and people use this identifier daily to identify Andy on the network e.g. AndySmith@CompanyABC.com. Mandy can now masquerade as Andy; she is now identified by the IT environment as Andy, and for this reason she has also acquired all the authorization privileges awarded to Andy. If she chooses to change her monthly salary, she is now authorized to do so.

This presents a number of problems that include (but are not limited to):

- Privacy issues
- Anonymity issues
- Accountability issues
- System integrity issues.

The second step in the IT security service identification and authentication strives to solve the problem of one person, object, electronic device etc. masquerading falsely as something or somebody else. To use only a publicly known identifier that is common knowledge, does not prevent masquerading to take place.

Authentication is the step that endeavors to solve this problem of masquerading. Therefore the service of identification and authentication is a two step process [1]:

- 1) Identification – this is by means of a unique name or number, this is not anonymous and can for this reason be stolen or misused.
- 2) Authentication - verifying that the offered number or name belongs to the offering party, accomplished by certain secret parameters known only to the real owner, or by a unique token only owned by a specific person.

2.5.1. Secret parameters

In order to evaluate the strengths and shortcomings of secret parameters that can be used for authentication, the different secret parameters will be discussed. Each parameter will be discussed briefly, followed by a conclusion that will summarize the strengths and weaknesses of the parameter.

Considering that a user supplies a familiar user-id to the IT environment, a method must be found that will safeguard the identity of the user. Secret parameters are the mechanism that assists in the process of proving authenticity.

These secret parameters come in 4 different forms [12]:

- 1) Something secretly known.
- 2) Some unique possession.
- 3) Something the user is.
- 4) Multi factor authentication.

Each of the secret parameters will now very briefly be discussed.

2.5.1.1. Something secretly known

A secret is often used to authenticate a long lost friend. Many stories are told about friends meeting up after years of separation, and the only way that the friends could prove their identity, is by means of something that they carry knowledge of, and no one else could know about. This is a typical example of proving the identity of a person he alleges to be, by providing knowledge unknown to others.



The earliest computer-based authentication mechanism was established as part of the Compatible Time Sharing System (CTSS) at the Massachusetts Institute of Technology in the early 1960s [13]. The system's designer introduced the notion of a "private code" that students would memorize, much like they memorized the numbers of their combination locks on their student lockers. Today of course, we use the term password to refer to such private codes [14].

Usage of a rudimentary network password is illustrated in figure 2.5:

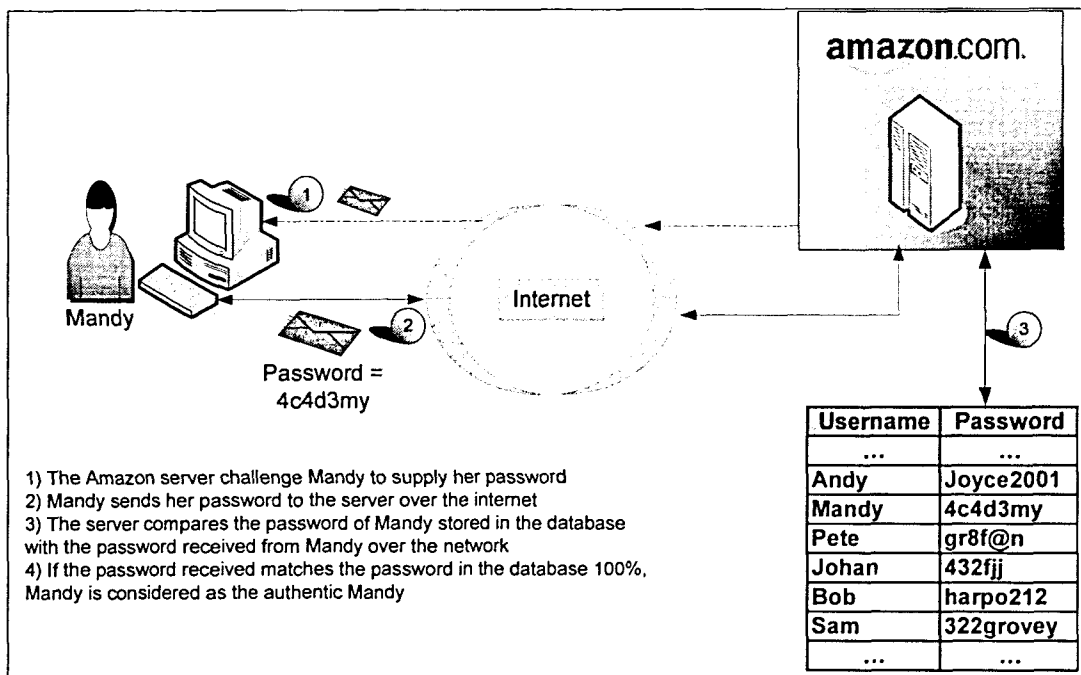


Figure 2.5: Password usage over a network.

Modern life is rife with passwords. They protect everything from children's personal computers to extensive business and financial resources [15].

In theory a password is memorized by a single person, is hard to guess, never written down and is never shared. In practice however, people are constantly violating these expectations. Passwords are often written down, shared with other people, or chosen from a small number of easy-to-guess words. There is an inevitable tug-of-war between choosing a password that is easy to remember and one that is hard to guess. Some systems try to force people to choose hard to guess passwords, and many people then keep a written list of their hard to guess (and hard to remember) passwords. Of course, if this list is copied or stolen, all these passwords provide no protection.

Although passwords are both widely used and easily compromised, they illustrate the fundamental mechanism of automated authentication: the user must provide

some information or input that cannot be provided by someone else. Consider what happens if an authorized user named Sally tries to log in to a server, such as an e-mail server. The server requests a unique identifier from Sally. She will provide her username. The server will then expect Sally to authenticate herself. Sally will for this reason provides a password and transmit the password in an overall trusted environment. She should typically be the only person in the world that knows her password. The server will match the password she provided with a password stored in a database on the server. If the password provided matches the password in the database 100%, the server will accept Sally's authenticity [9]. It must be noted that there is various methods that could be used to gain illegal access to this password entered, however, this aspect is discussed in chapter 4, section 4.2.1.

2.5.1.1.1. Password considerations

The simplest implementations of passwords and personal identification numbers (PINs) yield the simplest of all authentication mechanisms. Sally's memorized password serves as the authenticator. The verification procedure simply performs a character string comparison of the password provided by Sally and a copy of the password stored in the system. The server must verify a 100% match between the password supplied by Sally and the password stored on the server [12].

Passwords work reliably only as long as they are not guessed or otherwise disclosed to potential adversaries through accident, subversion, or intentional sharing. A secret, like a password, becomes easier to steal as it is often shared among more and more people; this reflects the wisdom of the old dictum: "Two people can keep a secret, provided one of them is dead."

2.5.1.1.2. Subverting passwords

A number of ways exist that a password can be discovered. The following section briefly discusses some of these methods.

- *Trial-and-error attempts*

When Jack attempts to bypass an authentication system, the first thing he considers is whether trial-and-error attempts are likely to succeed. Every authentication system is subject to some type of trial-and-error attack. The classic attack on passwords is an interactive attack, in which the attacker simply types one possible password after another, until either the list of possible passwords, or the attacker, is exhausted. Most systems resist such attacks by keeping track of the number of unsuccessful authentication attempts. Once the number of allowed attempts has been reached, the system will resort to a number of options to protect the authentication environment. The administrator of the system will specify that the system must for example, lock the user out for a predetermined time, or lock the user out until the administrator could mitigate the problem.

- *Offline attack*

With the introduction of password hashing and other techniques for obscuring a password cryptographically, a different technique emerged: the offline attack [9]. These attacks take a copy of a cryptographically protected password file and use a computer to try to "crack" it by using a brute force attack on the stored hashes of each password.

The following screen shot illustrates offline attacks executed in LophtCrack [17].

The screenshot shows the LophtCrack 2.5 application window. The title bar reads "C:\Program Files\LophtCrack 2.5\PWFILE.TXT.ic - LophtCrack 2.5". The menu bar includes "File", "Tools", "Window", and "Help". The main area displays a table with the following columns: "User Name", "LanMan Password", "<8", "NT Password", "LanMan Hash", "NT Hash", and "Challenge". The table lists seven users: BillG, Administrator, fredc, twoa, william, threaa, and foura. The "twoa", "threaa", and "foura" entries have an "x" in the "<8" column, indicating they are short passwords. The status bar at the bottom left says "Loaded 7 accounts..." and the bottom right shows "N.M".

User Name	LanMan Password	<8	NT Password	LanMan Hash	NT Hash	Challenge
BillG				5ECD9236D21095C17584248B8D2C9F9E	C04EB42B9F5B114C86921C4163AEB5B1	
Administrator				73CC402BD3E791756C3D3B817E02809D	C7E2622D76D3F001CF08B0753646EBCC	
fredc				3466C2E0487FE39A117EAF50CFAC29C3	80030E356D15FB1942772DCFDD7DD3234	
twoa		x		89D42A44E77140A1A1D3B435B51404EE	C5663434F963BE79C8FD99F535E7AAD8	
william				DEC5E5CBA8028091B79A82610DD89D4C	6B6E0FB2ED246885B98586C73B5BFB77	
threaa		x		1C3A2B6D939A1021A1D3B435B51404EE	E24106942BF38BCF57A6A4E29016E7F6	
foura		x		DCF9CAA6DBC2F2DFAAD3B435B51404EE	FA5664875FFADFOAF61AEF9B097FA46F	

Figure 2.6: LophtCrack

An offline attack usually has a 100% success rate in two cases:

- 1) If the password is short (<8 characters)
- 2) If the password is found in a dictionary.

Firstly, when short passwords (less than 8 characters) are to be cracked the success rate is guaranteed, for this reason, passwords shorter than 8 characters can be cracked even if the password is a non-dictionary word, consisting of non-alphanumeric characters like "\$%^\$#". LophtCrack identifies these short passwords and indicate such passwords with an x [17], [18].

Secondly a password can successfully be cracked when using a brute force dictionary attack [17]. In figure 2.7 LophCrack is executing a dictionary attack.

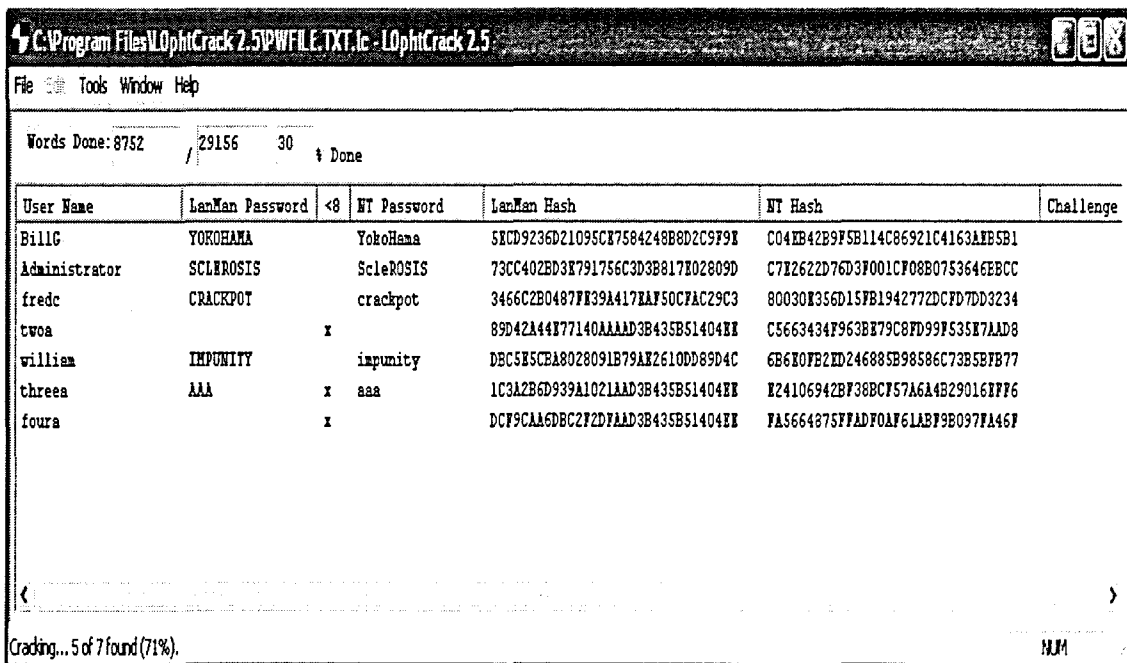


Figure 2.7: LophtCrack executing a dictionary attack.

In fact, dictionary attacks are fast enough that the dictionary contains many unlikely words as well, so that even improbable words will be tested. In studies performed on hashed password files, dictionaries of English words have been successfully used in dictionary attacks to crack between 24.2 per cent and 35 per cent of the file's passwords [19].

If people use short passwords or easily memorized common English terms (such as favorite food dishes), the offline attack can exhaustively check every possible password by comparing its hashed equivalent against the hashed password being cracked.

- *Replication attack*

In this attack, Henry produces a copy of whatever Sally is using to authenticate herself. If Sally has written down her password somewhere, Henry can perform a replication attack by finding the written down password and copying it for his own use. This takes place without Sally's knowledge or intentional co-operation. In practice, such "mouse pad" searches uncover a password between 4 and 39 per cent of the time, depending on the environment [19]. If we characterize a mouse pad search as a single attempted attack, we have an average attack space of as little as 21.

- *Digital Spoofing / Interception*

Also known as a replay attack, this attack takes advantage of the fact that all authentication data are ultimately reduced to zeros and ones (bits) [31]. All passwords are stored in binary. If a password is sent via a communication medium, the electric signals that represent the zeros and ones can be intercepted. If the system expects a particular value for authentication, the attacker intercepts this value while in transit via the communication medium and replays it to masquerade as someone else. The classic example is for Jack to intercept Mandy's password as it travels in bits (binary) from her workstation to the server via the intranet, and is illustrated in figure 2.8.

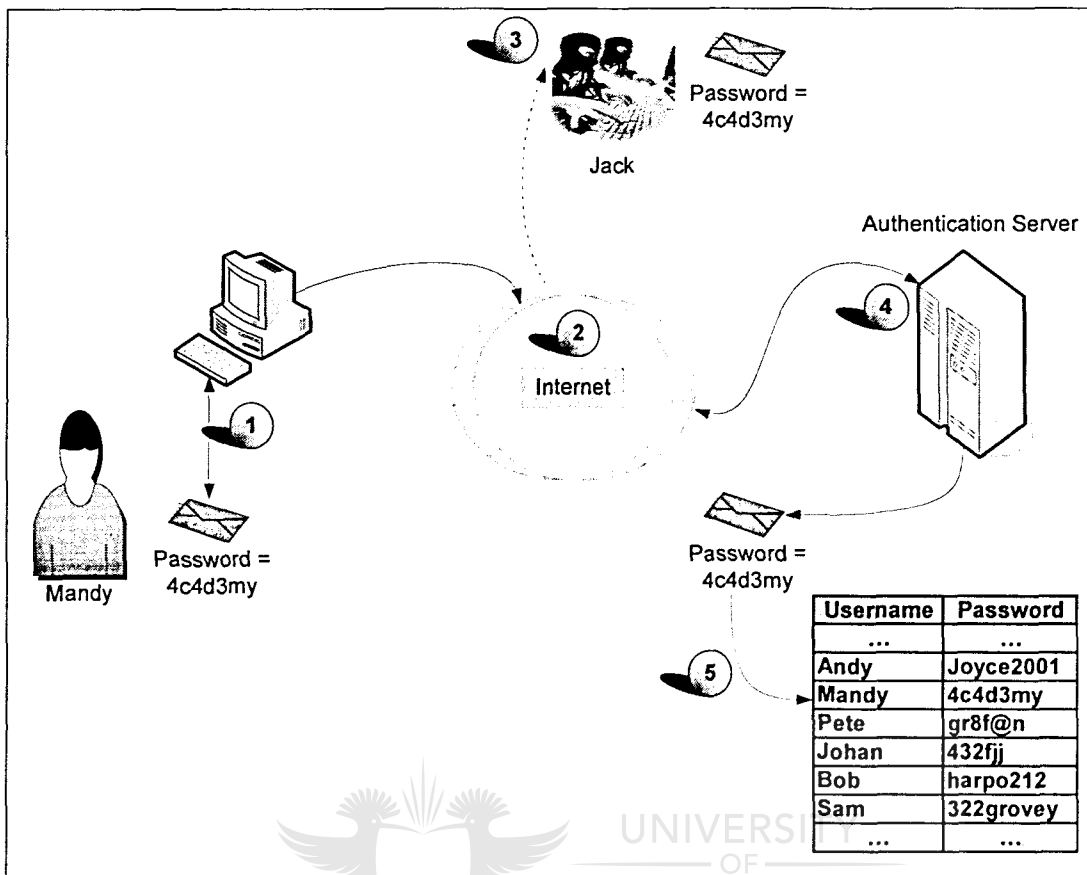


Figure 2.8: Password interception.

Step 1. Mandy would enter her password on her computer.

Step 2. The password is sent via the internet to the authentication server.

Step 3. Jack intercepts Mandy's password.

Step 4. The password arrives at the authentication server.

Step 5. The password received via the internet (from either Mandy or Jack) is compared to the password stored in the password database.

Digital spoofing is an important aspect of this thesis. Virtually all electronic communication today occurs via a shared medium where all information is reduced to zeros and ones. Digital spoofing is a major threat for authentication

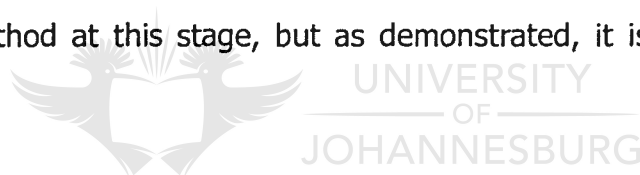
compared to most of the other forms of attacks such as replication attacks or password guessing.

Digital spoofing can be carried out in virtually any area where digital data traverses a communication medium. In depth attention will be given to digital spoofing in Chapter 4, discussing replay.

Interception poses a serious problem for Internet traffic. Telnet and FTP authentication is specifically prone to this type of attack [4]. Cryptographic protection became a standard feature in web browsers since 1994 [20].

2.5.1.1.3. Conclusion

The most common method to ensure authenticity is to provide a user with something that only that user knows – a unique secret. This is the most commonly used method at this stage, but as demonstrated, it is also open to subversion.



The benefits of passwords are [21]:

- Easy to use
- Inexpensive
- Easy to implement
- No special devices are needed
- Easy to manage
- User does not have any physical item than can be stolen or lost (unlike a token).

Unfortunately, passwords also have a number of imperfections [21], [22]:

- Passwords are not resilient against attacks.
- Passwords can easily be subverted using techniques like password guessing, and password cracking.
- Digital spoofing is the technique most relevant aspect to this thesis, and will be discussed in more detail in Chapter 4.
- If a password is compromised the owner is often not aware of the fact that the password is compromised.
- More than one person can use the password (password sharing).
- Most importantly, if a password is used for authentication, the system that checks for authenticity, will only conclude that the password is authentic (as this password will be an exact match with the password database), but the system cannot determine that the person offering the password is in fact the authentic user / owner.

In the following section the second authentication method, some unique possession, will be dealt with.

2.5.1.2. Some unique possession

Physical authentication devices, such as smart cards and magnetic cards, were developed to eliminate certain weaknesses associated with passwords, such as the sharing of passwords [21]. Only one person can be in possession of this unique token, which can therefore not be used simultaneously by more than one party.

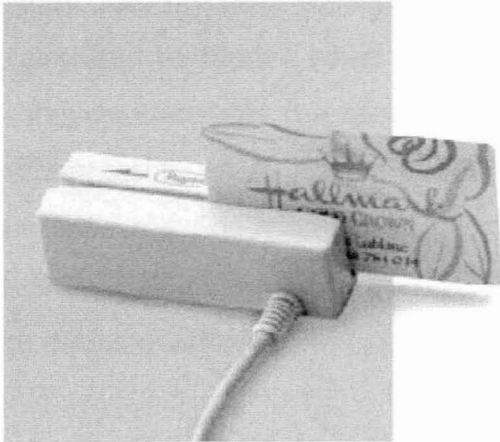


Figure 2.9: Magnetic card and reader [23]

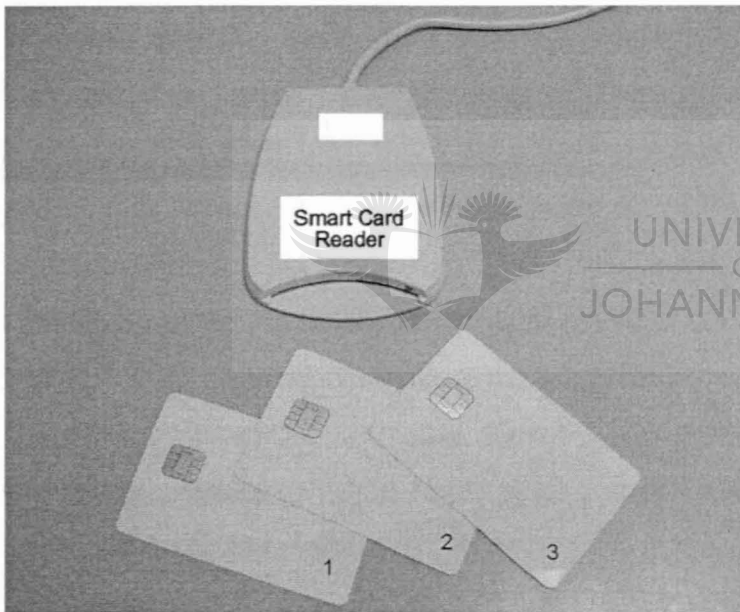


Figure 2.10: Smart card and Reader [24]

A major benefit of cards and tokens is that they cannot be shared with the same freedom as sharing passwords. If Mandy lends her token to someone else, the other person can log in, but Mandy cannot.

In general, these devices store a large base secret /unique identifier (larger, in any case, than typical passwords). Since the token carries the secret identifier,

Mandy does not need to memorize it: she simply has to carry the token and have it available to tender when she logs in. The devices usually contain a special procedure that uses the base secret to generate a hard-to-predict value for the authenticator. When Mandy needs to log in, her device generates the correct authenticator. She then either types the authenticator in, instead of a password, or she relies on a special authentication client to transmit the authenticator to the authentication server [25].

To authenticate Mandy, the authentication server uses a specialized verification procedure designed for the particular device Mandy uses [25]. Usually, however, these procedures would not accept the same authenticator value twice. This increases security since Jack cannot intercept and reuse an authenticator transmitted by Mandy's device. However, it may also inconvenience Mandy if she is able to access her mail only from access points that have the particular device available to accept her token. The appropriate verification procedures usually fall into two categories: Those procedures using secret-key cryptography and those procedures using public-key cryptography [25].

The first password-based tokens, such as a Java card, were implemented using secret-key cryptography. To log in with one of these tokens, Mandy needed to follow the following procedure [26]:

1. Mandy typed her user name.
2. The server replied by displaying a numerical value, called the challenge.
3. Mandy typed the challenge from the server into a keypad of the authentication device.
4. The authentication device used a cryptographic function, often the Data Encryption Standard (DES), to combine the challenge with her base secret, stored inside the token (Java card).

5. The authentication device displayed the result on a digital display; this was called the response.
6. Mandy copied the response into the server's password prompt, using it as the authenticator.
7. Internally, the server combined the challenge it sent with its own copy of Mandy's base secret. If the result matched Mandy's response, the server would allow her to log in.

As these tokens became more sophisticated, they incorporated techniques to generate the challenge value internally. Some vendors produce tokens that use the value from a time-of-day clock as the challenge value, while others use an internal counter, and some combine both. These techniques greatly simplified matters: when Mandy needs to log in, the token simply displays the password she needs to use.

Other devices, notably smart cards and USB tokens [27], use public-key cryptography. If Mandy uses a public-key smart card, Mandy's private key serves as the base secret for authentication, and that key resides on the smart card. When Mandy logs in, most of the authentication process is handled automatically by client software, which performs a challenge-response exchange, similar to what was originally used in tokens. There is an important difference: the verifier is Mandy's public key, not her private key. She never has to divulge her private key to a server to log into it. This reduces the risks to Mandy's base secret, since it does not have to reside anywhere except on her smart card.

Like passwords, authentication devices can be stolen. Unlike passwords, the owner can tell if the device has been stolen. By itself, as with passwords, the authentication system would not be able to verify whether the value offered, comes from a stolen token or not.

2.5.1.2.1. Subverting Tokens

Authentication devices are also subject to interactive and offline attacks, although they are far less likely to succeed.

An *interactive attack* would attempt to generate a legitimate authenticator value. The attack's likelihood of success depends on the size of the authenticator. Since authenticators tend to have at least six digits, the chances of success could be less than one in a million. Moreover, the interactive attempts can be detected by the system receiving them, and the system can then warn the system administrator.

Offline attacks against tokens are more likely to succeed since they cannot be detected. The goal of the attack is to derive the secret stored in the token or smart card. The offline attack begins by collecting a number of authenticators. The attack tries all plausible values for the base secret and tests them against the intercepted authenticators to determine whether a particular base secret value would generate that authenticator. These attacks may be practical against tokens that use the Data Encryption Standard (DES) or other algorithms with similarly short key lengths.

When attacking devices such as tokens or cards, the *replication attack* must duplicate the functionality of the device by either extracting its base secret or by deriving it through a trial-and-error attack [19].

A magnetic card is vulnerable to a *Skimming attack* [28]. Credit card skimming is when a person records the information on a credit or debit card without the owner knowing about it, with the intention of using that credit card information illegally. Skimming most commonly occurs in restaurants, where the card owner loses contact with the card and a purchase is made. It takes about two seconds

to scan a card through a portable reader, and the reader records all the information on the magnetic card. Figure 2.11, illustrates that these portable magnetic card readers are very small and can easily fit into one's pocket. Once this information is received and stored, a hacker can generate new magnetic cards from this information and use this to fraudulently purchase goods without the authentic owner of the magnetic card being aware of this.

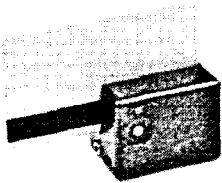


Figure 2.11: The TA-48 portable card reader. [30]

2.5.1.2.2. Conclusion

The second method used for authentication is something that a user owns. This method is a different approach compared to something the user knows. Using passwords, PINs etc. the user must remember something, however, if tokens are used the user does not need to remember anything, the user must only be in possession of the unique token.

Tokens have a number of advantages [21]:

- The person does not need to remember anything.
- Only one person can be in possession of the token.
- If the person does not have the token, the person cannot gain access to the system.
- If the token is stolen or lost the owner will be aware of this fact.
- Can be replaced with a new token, and the old one can be black listed.

However, a number of problems are associated with tokens [22]:

- If the person does not have the token in his possession, the person cannot gain access to the system.
- Considering skimming attacks, tokens can be duplicated without the knowledge of the owner of the token.
- As with passwords the significant problem exists that if a token is used for authentication, the system checking authenticity will only establish that the token is authentic, but the system cannot be sure that the person offering the token is the authentic owner of the token.

Tokens and passwords have one common problem; the system only authenticates the token or password as authentic and not the person presenting the token or password.

In the next section "something that the user is" will be considered, as a possible solution to authenticate the user directly.

2.5.1.3. Something the user is

Biometrics relies on any automatically measurable physical characteristic or personal trait that is distinctive to an individual [29]. Common biometric verification techniques try to match measurements from Mandy's fingerprint, hand, eye, face, or voice to measurements that were previously collected from her during a registration process. For example, if Mandy's system relies on fingerprints, she must place her finger on a fingerprint reader when she logs in. The reader will digitize the fingerprint she provides and try to match it to measurements that were previously collected from her. If the latest measurement matches closely enough, the system acknowledges that Mandy is present and logs her in or grants her access. Mandy has no device to lose or password to forget. She can authenticate herself provided the appropriate physical characteristic or personal trait has not been badly injured or degraded.

As biometrics is the technology used for authentication in the protocol developed as part of this research, biometrics and all biometric considerations will be discussed in depth in the following chapter (Chapter 3).

2.5.1.4. Multi factor authentication

As a general rule, if an authentication system is developed by humans, it can be defeated by humans. Passwords can be intercepted and reused. Password tokens can be stolen. All authentication factors suffer from fundamental weaknesses. Practical systems incorporate at least two factors to neutralize individual weaknesses. Plastic cards for ATMs provide a classic example: Mandy must possess the correct card and she must know the appropriate PIN; otherwise she cannot use the teller machine. Most password tokens incorporate PINs in some fashion, and most biometric systems rely on token-like devices to collect tokens and to protect them cryptographically.

Thus in order to eliminate the weaknesses associated with the various authentication mechanisms, two or more authentication mechanisms are combined in an effort to eliminate the individual weaknesses of each authentication method.

2.6. CONCLUSION

This chapter investigated the methods and technologies to assist the computer environment with identification and authentication. The identification and authentication of humans is of particular interest. A human (computer user) must be identified in a computer environment; this will allow the user to perform certain authorized tasks. Due to the fact that users are specifically authorized to do certain tasks, and can be held accountable for their actions in a computer environment, it is necessary to ensure that the identified user is the actual user and not merely an illicit user masquerading as the authentic user. To ensure that a user is authentic, the computer environment must authenticate the user that is identified.

Authentication can be established by challenging a user to provide a secret, only known by the user, or to provide a token that only the user owns. The user can also provide a biometric token as part of the authentication process.

As illustrated in this chapter, various examples exist to subvert passwords and tokens. It is also clear that passwords are more vulnerable than tokens, but at this stage the usage of passwords outrank the usage of tokens.

Another major problem with passwords and tokens is found in the fact that the system can only authenticate the password, pin or token, as authentic. However the system does not authenticate the user presenting this password, pin or token as the authentic user. Thus the authentication process will confirm the password and token as authentic, but not the user presenting the token or password. This means that the user is only indirectly authenticated.

The argument relies on the fact that the user should be the only person that knows the specific password or the user should be the only person that owns the specific token. If the problems associated with passwords and tokens are considered, it is clear that there is a distinct possibility that the person presenting an authentic token or an authentic password is not the authentic rightful owner of this password or token.

The next chapter will discuss biometrics as a possible solution for identification and authentication. Biometrics is part of the user, and the following chapter will investigate biometrics to determine whether biometrics can be used to authenticate the user presenting the biometric token directly as authentic, instead of only authenticating a presented password or token.



Chapter 3: Biometrics

3.1. INTRODUCTION

In chapter 2 identification and authentication were discussed. The chapter focused on the importance of identification and authentication. Chapter 2 also investigated the various mechanisms used to enforce authentication. It was pointed out that a user can use four distinct mechanisms to be authenticated. These four mechanisms are

- 1) Something that the user **knows** – Like passwords, pass phrases and PINs.
- 2) Something that the user **owns** – Like magnetic cards, smartcards, and RF tags.
- 3) Something that the user **is** – Also known as biometrics.
- 4) Combination of the above mentioned 3 mechanisms.

The previous chapter did not elaborate on biometrics as that will be the focus of this chapter. Biometrics will be the fundamental identification and authentication technology used in a system called BioVault discussed later in this thesis. For this reason the mechanism of biometric models needs to be investigated. This chapter starts with a high level, general discussion of biometric systems, followed by a look at two biometric technologies available today. All currently available biometric technologies are not discussed because the eventual BioVault model does not rely on any specific biometric technology. This chapter will discuss the strengths and weaknesses of biometric technology. The previous chapter elaborated on the core weaknesses of passwords and tokens - if a user uses a password or a token for authentication, only the token or password

presented is authenticated and not the user presenting the password or token. The aim of the chapter is to investigate whether biometrics is more resilient against fraudulent attacks than the authentication mechanisms discussed in chapter 2. This chapter will demonstrate that if a user is authenticated using a biometric token, the user is authenticated directly, not just the offered biometric token.

3.2. BACKGROUND

Biometrics: "(ancient Greek: *bios* ="life", *metron* ="measure") is the study of automated methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits" [35]. Ben Miller, introduced the following definition in 1987 for biometrics: "Biometric technologies are automated methods of verifying or recognizing the identity of a living person based on a physical or behavioral characteristic" [34]. The international biometric industry association defines biometrics as "automated methods for verifying or identifying the identity of a living individual based on physiological or behavioral characteristics" [36].

Verifying our identities and the identities of someone else is part of our daily lives. As stated in chapter 2, reliable identification of virtually everything around us, is important. Humans use 5 senses to assist them to identify objects in their world. From the day humans are born they fine tune their ability to identify. This identification is a lifelong learning process, starting from identifying the sound of one's mother's voice, right through to the ability to identify everything that a human comes in touch with.

Humans use biometrics to identify and authenticate each other. We use all our natural senses to recognize people by their voices, faces, smell, and various other characteristics. An instance of biometric spoofing occurred in the Bible when Jacob fooled his blind, aged father, Isaac, into believing smooth skinned

Jacob was Esau, his hirsute older brother. With the assistance of Rebecca, his mother, Jacob carried off this identity fraud by putting goat's skin on his hands and the back of his neck so that his skin would feel hairy to his father's touch. The book of Genesis [37] explains that Isaac said to Jacob "Come near, that I may feel you, my son, to know whether you are really my son Esau or not". Isaac touched Jacob, and commented "The voice is Jacob's voice, but the hands are the hands of Esau". Isaac should have trusted his voice recognition skills, but succumbed for the biometric spoofing by Jacob.

It is important to realize that humans, even with these natural senses, must go through a learning phase in order to make a successful identification. Humans do not simply have the ability to identify the taste of a strawberry, if the human has never tasted the strawberry before. A human must be introduced to the new taste, and he must learn what a strawberry tastes like.

Computer systems on the other hand, must also go through the same learning phases. Computer systems must also use 'senses' to identify and authenticate a human. The computer system will go through a learning phase to fine tune the ability to identify and authenticate a person.

In the section to follow, the various components forming part of a biometric infrastructure will be discussed. This section is relevant as each sub-section of the biometric environment, as illustrated in figure 3.1, is vulnerable to a security attack.

3.3. ENROLLMENT

Enrollment is the first step for any biometric system [38]. This is the start of the learning phase of the system. During this phase the system is *introduced* to a new user. The user must supply one or more biometric samples for processing

into an acceptable template for future matching. In most instances a user will need to supply a number of samples of the same biometric. Multiple samples are taken as the match performance of most algorithms improves with more samples provided. The eventual template, derived from these multiple samples, and based on an averaging of these samples, is securely stored. Accuracy is important during this process as this will be the primary sample the future samples will be compared to, in order to make a match decision. The lack of a success of enrollment is measured by the failure to enroll rate (FTER) [39].

The FTER is determined by the total number of persons attempting to enroll and those that were unsuccessful to enroll within the thresholds of the enrollment policy.

$$\text{FTER} = \frac{\text{Number of unsuccessful enrolments}}{\text{Total number of persons attempting to enrol}}$$

FTER can be influenced by many factors in the environment (light conditions, humidity, and temperature) or factors relating to the user (occupation, age, and ethnicity).

Once a person is enrolled on a biometric system, a biometric template will be stored for future matching referencing.

It must be noted, for a biometric system to be trusted, all of components of the overall system must be trusted, including the computer systems used as the primary input or verification system. The user, within any biometric scheme is transferring responsibility for authentication to a computer program of which they have no detailed knowledge.

In the following section the key elements, generally found in all biometric systems, are discussed.

3.4. KEY ELEMENTS OF A BIOMETRIC SYSTEM

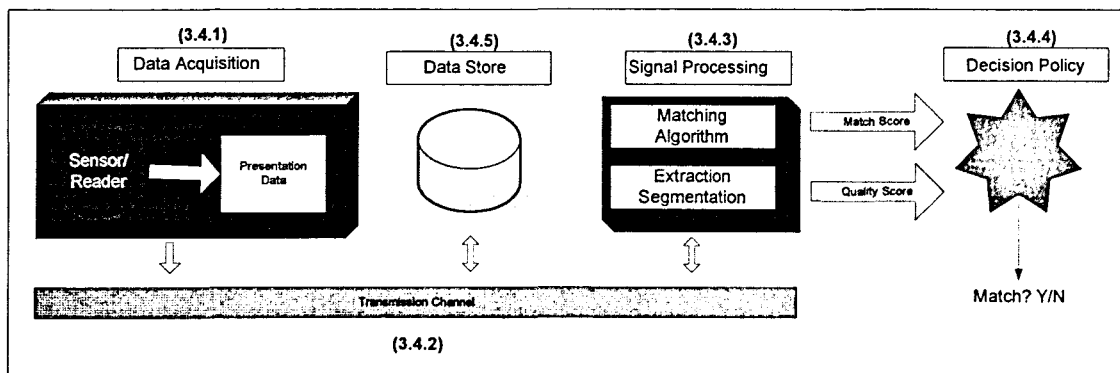


Figure 3.1: Elements of a generic biometric system

3.4.1. Data Acquisition

As illustrated in figure 3.1, the point of data acquisition is whenever a person presents a biometric characteristic to a biometric sensor. This sensor will translate the biometric characteristic into a digital representation, known as biometric data. This step is also known as digitizing of a biometric characteristic. The data acquisition is done using a hardware sensor or reader specifically adapted to record the relevant information from the specific presented biometric. This hardware device is purposely developed for the type of biometric that needs to be digitized. A typical example of a biometric sensor, used for scanning palm geometry is shown in figure 3.2.



Figure 3.2: Biometric Palm Scanner [40]

Biometric devices will translate (digitize) the scanned image into biometric data. Biometric data is the way that the biometric characteristic is presented in electronic format. Biometric data differs between biometric vendors, and differs between different types of biometrics.

The data acquisition phase is the first point of a possible security attack. If a hacker manages to supply a fake biometric characteristic during this stage, the rest of the process will be compromised. Chapter 5 will discuss a method that allows a hacker to generate a fake biometric characteristic. In chapter 5, it is discussed how a gelatin finger is created and subsequently used to spoof a biometric fingerprint reader.

3.4.2. Transmission Channel

Figure 3.1 illustrates the second component of a biometric system, namely the transmission channel. The transmission channel refers to the communication paths between the primary functional components. Some biometric systems are self contained and the transmission channels are internal to the device. Some biometric environments are distributed. In a distributed environment, the transmission channel will carry the information between the various components. It is possible that the database containing enrollment information is located

centrally, with network access, and that the biometric readers are located at the workstations of network users. In this scenario, the transmission channel will transmit all communication between the different components of the biometric system.

The transmission channel is the second aspect of the system that can be attacked. A hacker can for example eavesdrop on the electronic information traversing the communication channel. If this electronic information is compromised by means of a content logger of a computer, the hacker can replay this information (biometric data) at a later stage. The concept of replay is discussed in detail in chapter 4.

3.4.3. Signal processing

Signal processing is sometimes referred to as image processing [36], [41]. Once the biometric sample or biometric characteristic has been recorded and digitized into electronic form as illustrated in figure 3.1, the information will be processed for matching during signal processing.

A number of algorithms will be used to remove irrelevant noise from the data to enhance important biometric features. A biometric sample will undergo a *segmenting* process that will isolate and extract relevant features from the biometric data, and create a reference biometric template. Segmentation will improve the performance of subsequent algorithms, allowing them to more effectively locate and extract relevant biometric features. During this process biometric data will be separated from background information. The reference biometric template is a mathematical representation of the original biometric characteristic.

During the biometric data creation process data *normalization* is also performed. Normalization is the process of adjusting or scaling data to ensure that its range of values always falls within an acceptable, known range. The output of a biometric system's signal processing is generally a *quality score* (to quantify how successful the biometric feature extraction was).

Newly created biometric data is then compared to one or more reference biometric templates by a matching algorithm. The result of the matching algorithm is a *match score*, indicating how similar the newly created biometric data is in comparison with the reference biometric template stored during the enrollment phase.

3.4.4. Decision policy

Matching accuracy is probably the most talked about aspect of a biometric system. As illustrated in Figure 3.1, this is the step that will make the decision between an authentic user and a rejected user. The decision policy considers the output of the signal processing (quality score, and match score as illustrated in figure 3.1) and makes a Boolean (yes / no) final determination whether there is a match or not. Normally empirically determined thresholds are set for the quality score and the match score. If the match score and quality score are above these thresholds, a yes result (authentic) will be given. On the other hand, if any of the two scores does not meet a threshold, a no result (rejection) will be given. The match score and quality threshold can usually be set by the user. Depending on the application domain of the biometric authentication system, different threshold values will be set, resulting in different levels of falsely accepting a user or falsely rejecting a user.

Usually it is easier to maintain higher levels of accuracy using one-to-one matching – also referred to as *verification* or *positive matching*. If a system must

do a one to one match, the system will match received biometric data with specific reference biometric data. This means that the user will first identify him, and then the system will compare the received biometric data from this user with the reference biometric template stored during the enrollment process. In this instance the system matches the biometric data to one and one only reference biometric template.

One-to-many matching, also known as identification is more difficult. All reference biometric templates of the user population database will be searched for a match. If a user presents his or her biometric data to the system, the system will compare the received biometric data with each and every stored reference biometric template in the database. As the database grows, more records need to be compared, requiring more time and resources. Furthermore, larger databases with more records also result in more possible matches.

The uniqueness of a fingerprint in the mathematical sense is difficult (if not impossible) to prove. Until now, no two fingerprints from different fingers have been found to be identical. This is true even for identical twins, between right and left fingers and can be anticipated also for clones (due to the way that a fingerprint is actually formed during a person's fetal development phase).

In a scientific sense, the term "uniqueness" has to be replaced by the probability to find two identical fingerprints from different fingers. This probability may be determined empirically by comparing all fingerprints of a forensic data base against each other. For example, if such a collection contains 100 million fingerprints, a probability of nearly 10-14 should be provable, however, such a large trial has not yet been undertaken to date [38]. Furthermore, the probability for misnaming fingerprints (fingerprints from the same person/finger are filed under different names) is supposed to be much higher. This experience is well

known from experiments with much smaller collections [38]. As a result, the outcome of such a trial becomes questionable.

A scientific investigation of the individuality of fingerprints has been published [38].

Some of the measures of decision policy accuracy include the false acceptance rate (FAR) and the false rejection rate (FRR). The pivot point between the FAR and the FRR is known as the crossover rate [41].

3.4.4.1. The False Acceptance Rate (FAR)

The FAR is also known as the False Match Rate or Type II error [41], and it describes the number of times someone is inaccurately positively matched.

$$(\%) \text{ FAR} = \frac{\text{Number of incidents of false acceptance}}{\text{Total Number of Samples}}$$

The false acceptance rate is an important ratio to consider; as it illustrates the number of times a user will be able to subvert a security system. If the ratio is high, it means that a potential hacker can more easily gain access into a system without having the necessary access rights.

3.4.4.2. The False Rejection Rate (FRR)

The FRR is also known as the False Non-Match rate or Type I error [41]. The FRR refers to the number of times someone, who is supposed to be identified positively, is rejected instead.

$$\text{(\%) FAR} = \frac{\text{Number of incidents of false rejection}}{\text{Total Number of Samples}}$$

It is important to pay attention to the FRR, as this ratio will illustrate the number of times an authorized user will be denied entry into the system. The FRR does not pose a huge security risk, but it will contribute to user irritation with the system, as the system will reject legitimate users [41].

The crossover rate or equal error rate is the intersection of the FRR and the FAR [41]. The lower the crossover rate, the better the rating of the biometric system. The FRR and the FAR in most instances are influenced by threshold settings of the matching algorithm. The security administrator can change these thresholds depending on the type of environment that the biometric system is installed in. From the illustration in figure 3.3, it is clear that the FRR and the FAR have an inverse effect on each other.

3.4.4.3. Crossover rate

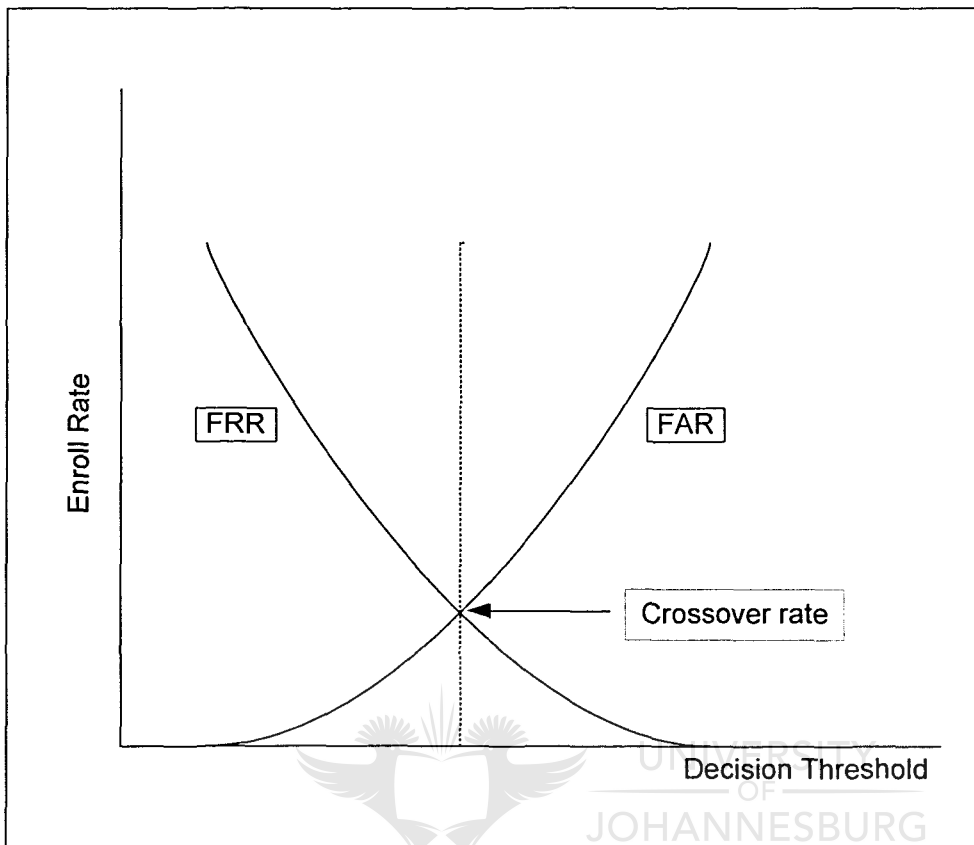


Figure 3.3: Crossover rate.

If a security administrator sets the threshold of the FRR in a way that the users of the system do not get falsely rejected, one would find that there will inversely be many false acceptances.

On the other hand, if the security administrator wants to prevent any possible false acceptances, he would need to set the threshold of the FAR very strict. This would however result in many authentic users being falsely rejected.

3.4.5. Template storage

The last aspect of elements found in the biometric system, as illustrated in figure 3.1, is the storage of biometric data. The storage of biometric data is an important aspect of the environment and is an area that demands security attention. All reference biometric templates must be stored, and if this data is copied, the reference biometric template is compromised. If a hacker manages to get hold of the electronic representation of a biometric characteristic, the hacker can use this biometric data to be falsely authenticated. This problem is discussed in detail in chapter 4. There are three main methods to be considered for reference biometric template storage [42]:

- Local storage.
- Network storage.
- Portable devices storage.

3.4.5.1. Local storage

For local storage all biometric data are stored on the biometric device itself. These types of systems are mainly used for physical access to secure areas. This type of storage is robust as network failure and network compromise is not a major problem, as no data is transmitted over a network. Biometric data management is more difficult since separate user enrollment needs to be done on each access point device. For example, if a Laboratory has 5 entrances, all with devices storing the biometric data locally, the users of this lab will need to register on all 5 devices –local storage can therefore be impractical.

3.4.5.2. Network storage

To store the reference biometric template on a network implies that the biometric data are all stored on a centrally accessible server. A key advantage of

network storage is that enrollment needs only to occur once at a master station, allowing all other devices on the network to access the same reference biometric template. A major drawback of this storage approach is the vulnerability of biometric data traversing the network communication medium. The biometric data can easily be sniffed and replayed at a later stage.

3.4.5.3. Portable device storage

With network and local storage, template size is not a major issue, but with portable devices, template storage might be a bigger concern. A typical smartcard has between 8Kb and 64Kb of storage capacity [43]. In most cases smartcards must also store information other than just the reference biometric template (like user name, password, digital certificates) allowing only about 2Kb to 4Kb for the reference biometric template on the smaller smartcards. Generally, more expensive cards can encrypt information to protect the reference biometric template in case of card loss or theft. Considering that the system places the master biometric template in the hands of users, it is important that the master biometric template storage is secure. If the reference biometric token could be altered, manipulated or replaced, the whole system will be compromised.

One challenge related to interoperability is that reference biometric templates are stored in proprietary formats [42], unique to each biometric vendor [44]. The absence of unique form standards poses a challenge when a company attempts to utilize multiple biometric devices.

This section considered a general approach to biometrics. All biometrics systems will have the above mentioned aspects as part of the biometric environment. In the next section two biometric technologies, namely fingerprint and iris scanning, will be discussed to serve as examples of biometric technologies. A number of

biometric technologies exist. However, fingerprint and iris biometrics will demonstrate the typical mechanism of a biometric, serving as example technologies to be used in this thesis.

3.5. TYPES OF BIOMETRICS

In this section, an overview will be given of two biometric technologies currently in use. There are a number of biometric systems in use, for example, retina scanning, hand geometry, facial recognition, facial thermography, voice recognition and gait, to name only a few, that show a lot of potential. These technologies are not discussed, but only noted. The biometric technologies to be discussed in the next section are in a mature phase of development and usage. The first biometric technology to be investigated is a touch based technology, namely fingerprint biometrics. The second technology is a non-touch technology, namely iris scanning.

3.5.1. Fingerprint



UNIVERSITY
OF
JOHANNESBURG

Fingerprint as a biometric, is the oldest and most widely recognized biometric, they are the impressions of the papillary or friction ridges on the surface of the hand.

Latent impressions that remain on objects humans touch are deposited residue made up of a combination of perspiration, organic solids such as amino acids and inorganic solids such as salts or blood or other susceptible material the finger might have touched recently.

In the 1870s Dr Henry Faulds serving as a missionary doctor in Japan, discovered that artists left their fingerprint impressions on the pottery that they produced. This inspired him to collect fingerprints and study them. He had students working for him, and he went on to collect fingerprints from infants to

determine if fingerprints change as a person grows older [45]. Faulds made a major breakthrough late 1870 by using fingerprints to aid in criminal investigation [45]. A person stole alcohol from Fauld's laboratory. Faulds identified the culprit by matching the fingerprint records on file with the fingerprint left on the bottle. Faulds demonstrated that it is possible to match a latent fingerprint to a specific person. He published an article in *Nature* [45] on fingerprints, the first published article on the subject.

Due to the possibility that fingerprints have enough unique traits to link a person to his fingerprint, police and crime applications were of the first to show serious interest in fingerprint identification technology. Fingerprints were collected from crime scenes and eventually from criminals. This posed a new challenge. It became increasingly necessary to classify the fingerprints in such a way that searches are possible on collected fingerprint samples. The first system was developed for Sir Edward Henry [48]. This classification system became known as the Henry system.

The Henry system classified each individual fingerprint into one of three classes: loop, arch and whorl [46], [47].



LOOP

In a loop pattern, the ridges enter from either side, re-curve and pass out or tend to pass out the same side they entered.



ARCH

In an arch pattern the ridges enter from one side, make a rise in the center and exit generally on the opposite side.



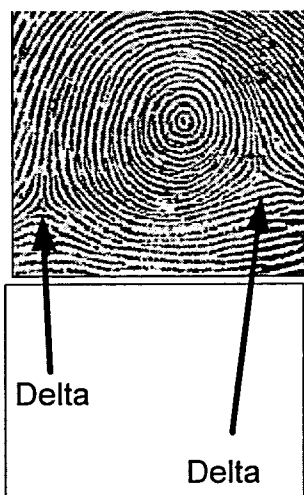
WHORL

In a whorl pattern, the ridges are usually circular.

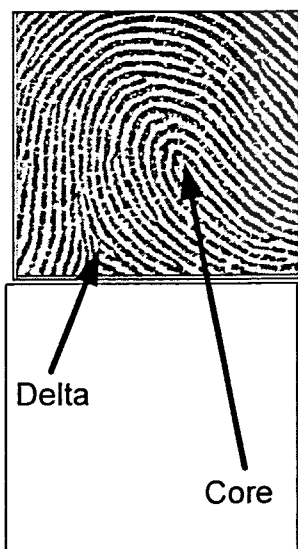
Over the years the FBI and others augmented Henry's system to deal with larger and larger repositories of fingerprints. Each of the above mentioned fingerprint types have specific focal points that assist in the documenting of the fingerprint [47].

A **Whorl** pattern will have two or more deltas. For a whorl pattern, all deltas and the areas between them must be recorded.

In the **loop** pattern there are two focal points: the Core, or the centre of the loop, and the delta. The delta is the area of the pattern where there is a triangulation or a dividing of the ridges.



When fingerprints are recorded, the delta, and the area between the delta and the core must be completely recorded.



The **arch** pattern has no delta or core, but it too must be fully recorded so that its individual characteristics can be readily distinguished.



To deal with searches on large numbers of fingerprints, Law enforcement had two requirements: a classification system that could be used to find similar prints (Henry system) and a way to describe the features that were matched on two fingerprints. In order to distinguish between two fingerprints in the same class, for e.g. two fingerprints from the whorl class, the system had to allow for identification of micro characteristics found in the ridge pattern of an individual print. The National Institute of Standards and Technology (NIST) [49] created a standard for forensic identification and called these micro characteristics *minutia* (singular) or *minutiae* (plural).

3.5.2. Minutiae



Minutiae are a number of small changes in the friction ridges of a fingerprint. These minutiae are recorded and allow for a fingerprint to be uniquely identified. During the classification of a fingerprint, various minutia points will be recorded according to the following types of minutiae commonly found in a fingerprint:

- *Endings*, the points at which a ridge stops.
- *Bifurcations*, the point at which one ridge divides into two ridges.
- *Dots*, very small ridges.
- *Islands*, ridges slightly longer than dots, occupying a middle space between two temporarily divergent ridges.
- *Ponds* or *lakes*, empty spaces between two temporarily divergent ridges.
- *Spurs*, a notch protruding from a ridge.

- *Bridges*, small ridges joining two longer adjacent ridges.
- *Crossovers*, two ridges which cross each other.
- The *core* is the inner point, normally in the middle of the print, around which swirls, loops, or arches centre. It is frequently characterized by a ridge ending and several acutely curved ridges.
- *Deltas* are the points, normally at the lower left and right hand of the fingerprint, around which a triangular series of ridges centre.

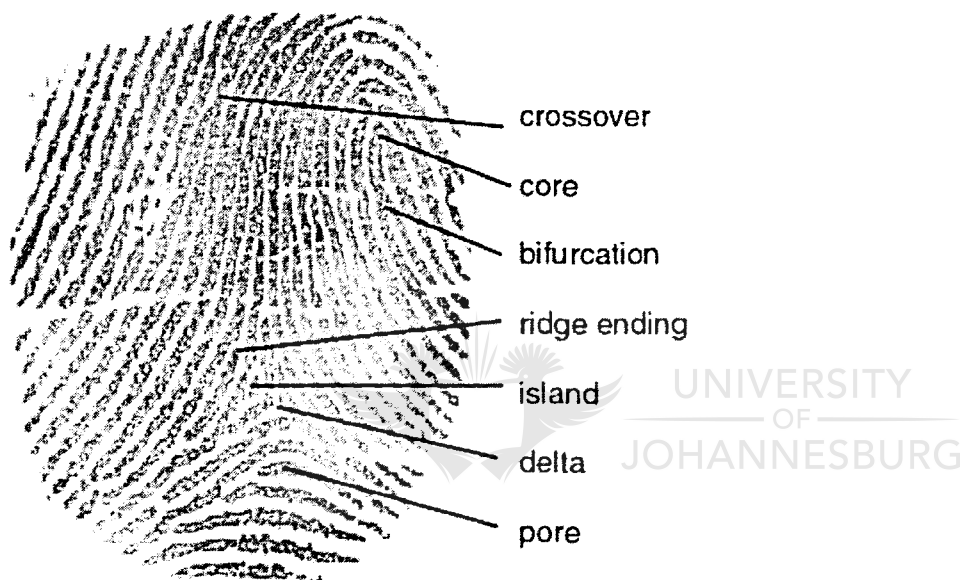


Figure 3.6: Example of Minutiae on a fingerprint [50].

3.5.3. Levels of Fingerprint detail

Over the years, the science of fingerprint examination has matured to a point at which examiners discuss three levels of detail in a fingerprint.

- **Level 1:** Overall appearance of the fingerprint. The pattern, and general ridge flow, classification, ridge count, focal areas, and orientation.
- **Level 2:** Friction ridge detail. The location of major changes in individual ridges, for example, ridge endings, ridge bifurcations, ridge islands, tiny ridges, known as dots, etc. The minutiae system is placed on these

various points on the fingerprint ridges. Furthermore each minutia has an angle of flow relative to the X-axis.

- **Level 3:** Individual ridge details. For example, ridge dimensional attributes that include the edge shape and width, as well as location of sweat pores.

If two fingerprint impressions have the same first level data, and there is general agreement as to the level 2 minutiae points and their relationships with no unexplainable dissimilarities, an examiner can number and mark the minutiae that match to show that the two impressions are from the same finger of the same individual.

3.5.4. Elementary mechanism of a fingerprint scanner

A fingerprint scanner must create a digital picture of a person's fingerprint. This is also known as the sensor, referred to earlier. One of the first systems to digitize a fingerprint was done by Livescan technology [51], to capture ridge detail from a finger to form digital images. This process is illustrated in figure 3.7.

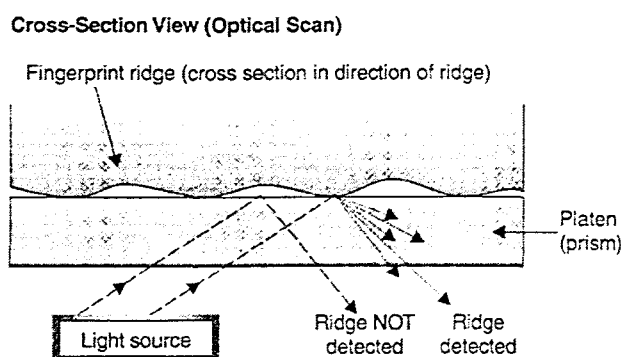


Figure 3.7: Mechanism of Livescan technology [51]

The finger is placed on a glass or plastic translucent surface. Light is scanned from below through the glass or plastic surface. Where a ridge is in contact with the surface, the light rays are prevented from exiting the top of the glass surface and scattered back into the device and focused onto a light sensitive detector. However, where a valley is present, the light is reflected in a focused ray, and a strong signal is detected by the light-sensitive diode.

3.5.5. Fingerprint capturing technologies

Many companies are currently manufacturing fingerprint capturing devices. These devices are typically designed for a few hundred people using an information technology system or application. The majority of these systems rely on minutia based technology to identify fingerprints.

Single-finger flat scanners use mainly the following capture technologies [46]:

- **Optical:** These types of scanners use a light emitting diode (LED) or a flat luminescent panel as a light source, and a Charged Coupled Device (CCD) array for an image capture device.
- **Thermal:** A solid-state device that measures the thermal differences between ridge contact and the air in a valley between ridges is used to form an image of the presented fingerprint.
- **Capacitive:** A solid state device that measures the microvolt differences in potential energy between ridges and valleys is used to form an image of the presented fingerprint.
- **Ultrasonic:** A transducer system that pulses the finger with ultrasonic waves at three wavelengths to locate and measure ridge detail. While the most expensive of the current readers, these devices can “see” through dirt, ink, and other noise, that have an adverse effect on other cheaper models.

3.5.6. Template extraction

To extract the minutiae, the following general process is followed. The images for this section are from a demonstration program developed as part of the BioVault research [52].

The fingerprint is captured in Grayscale, 500ppi 8 bits. This allows for capturing as much as possible to permit accurate ridge location and analysis, and to support manual human fingerprint analysis.

1. **Normalize:** Normalization is the process of adjusting or scaling data such that its range of values always falls within an acceptable, known range.

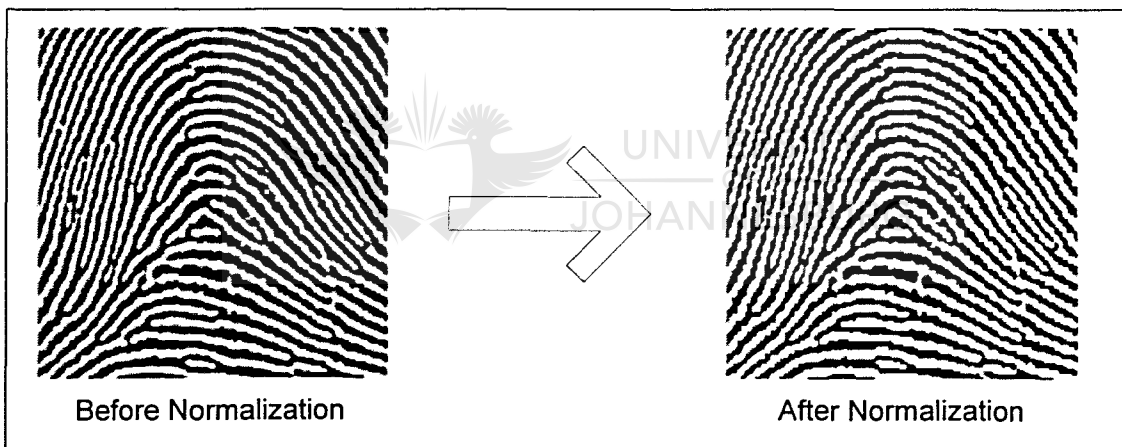


Figure 3.8: Normalization of a fingerprint image.

If close attention is paid to figure 3.8 it will be noticed that the image on the left has a large amount of noise in the picture, due to gray scaling, while the picture after normalization is in black and white only, thus eliminating noise in the picture.

2. **Segmentation:** Segmentation is the process of removing any data or image noise that is not relevant to the captured biometric sample. In

Figure 3.9, the red coloured border around the fingerprint image indicates the segment from the biometric sample that will be considered for further processing.

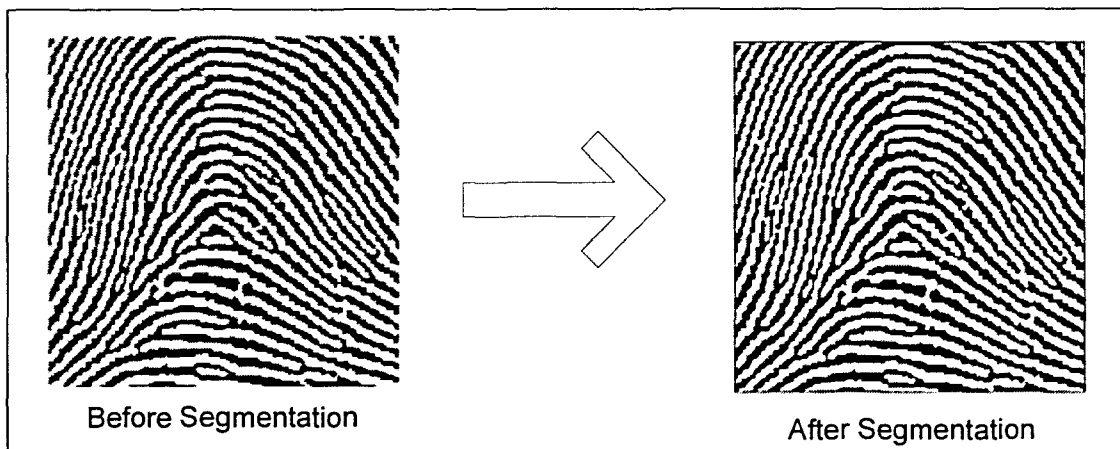


Figure 3.9: Segmentation of fingerprint sample.

3. **Thinning and Binarize:** The fingerprint region is processed to thin the ridges to 1 pixel in width and binarize these thin ridges. The thinned binary image can then in the following step be pruned.

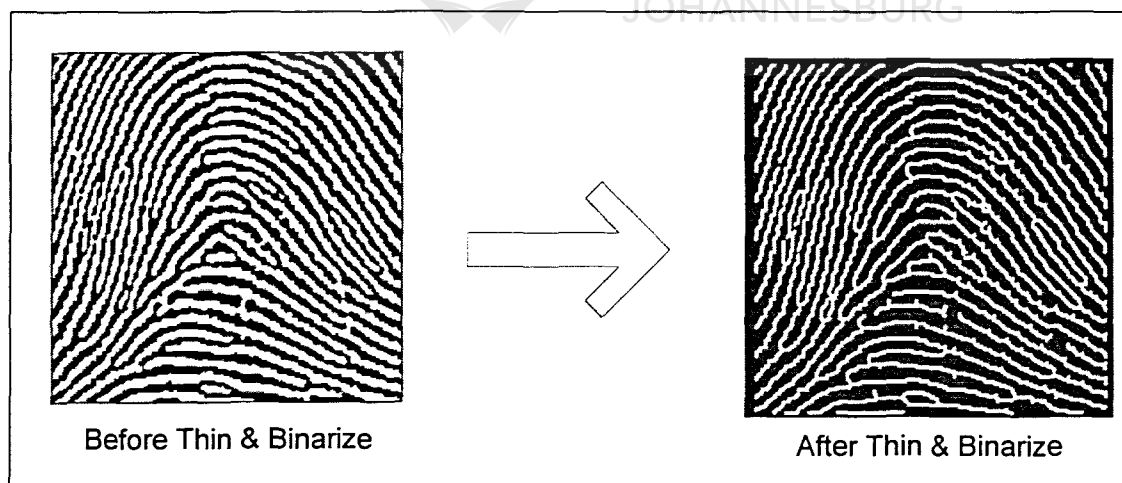


Figure 3.10: Thinning and Binarize of fingerprint sample.

4. **Pruning:** This step involves removing any unnecessary thin lines, caused by the previous processes. This thin, pruned binary image can then be processed to find minutia points.

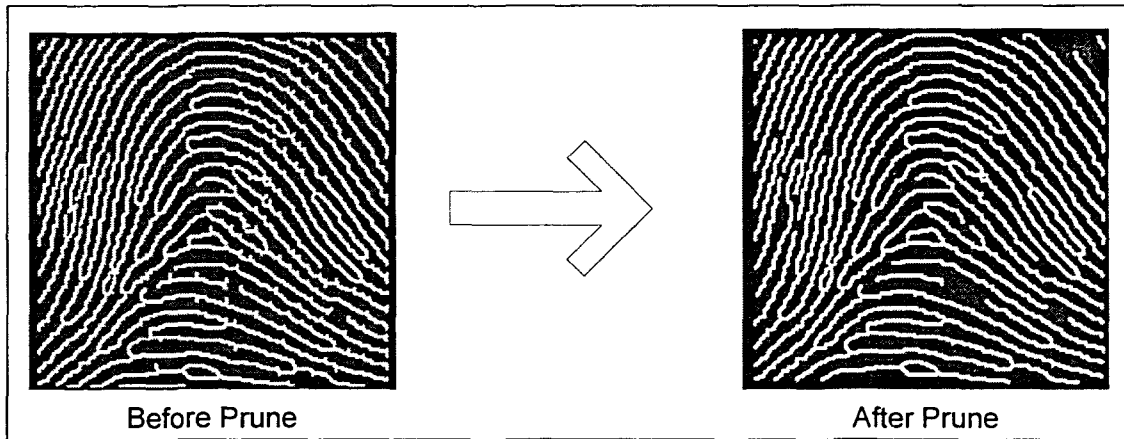


Figure 3.11: Pruning of Thinned Image of Fingerprint sample.

5. **Find Minutiae Points:** This involves the use of Gabor filters [53], [54] that are moved across the image. The calculation shows ridge location and flow direction, as well as ridge endings and changes in direction.

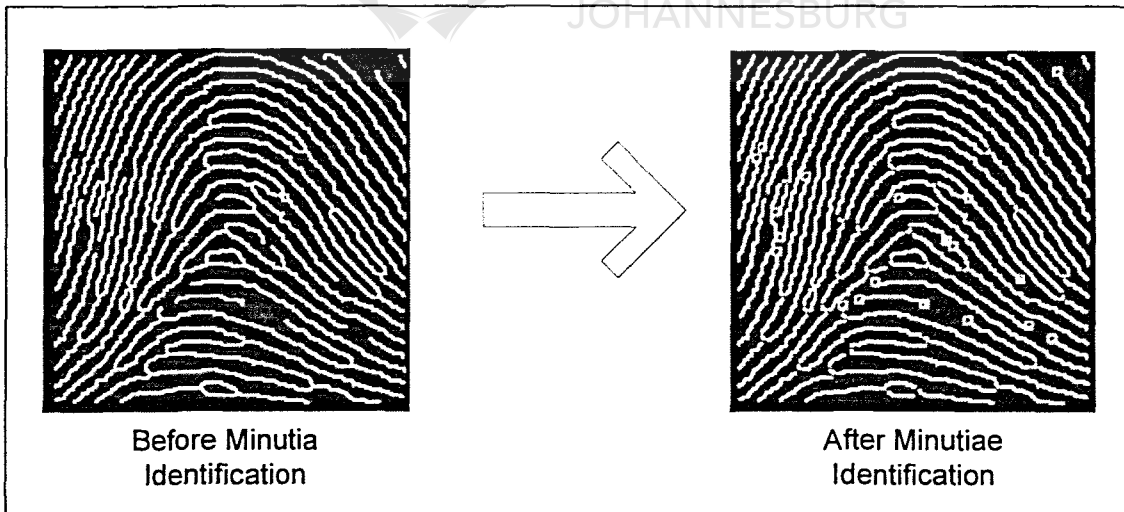


Figure 3.12: Finding Minutiae points on Fingerprint sample

After the minutiae points have been identified, a record averaging around 1000 bytes is created of the minutiae locations in relation to a two dimensional vector plane.

3.5.7. Vulnerabilities of Fingerprint Biometrics

Fingerprint capture devices are susceptible to two types of attacks:

- 1) Force a false match
- 2) Masking the fingerprint to avoid a match.

3.5.7.1. Forcing a false match

Two approaches exist if a hacker wishes to subvert a biometric system in order to force a false match:

1. The hacker could use his knowledge of the internal general mechanism of a biometric system to capture a biometric data in electronic format, and replay this biometric data at a later stage. Replay will be discussed in detail in chapter 4.
2. The hacker endeavors to manufacture a fake biometric characteristic of the person's physical biometric characteristic and use the fake biometric characteristic to be falsely authenticated. This process is illustrated by research conducted by Professor Matsumoto [55], demonstrating how a fake latex fingerprint can be created. This research is discussed in Chapter 5.

Once a finger print is created in latex, this latex finger can then be used to falsely authenticate a person that masquerades as the authentic user. Technical papers have been published of methods to attach thin latex fingerprint pads to a

finger and being successfully verified against the real finger print of the person concerned [55], [56], [57].

3.5.7.2. Masking the fingerprint to avoid a biometric match

A user tries to avoid the biometric device to make a positive match. Cases have been reported in Europe of instances of refugees soaking their fingers in henna (a reddish-brown dye) to avoid ridge detection on cheap optical scanners.

3.5.8. Fingerprint Conclusion

This section discussed and explained the mechanism of fingerprint biometrics as an example of a touch type biometric. In the following chapter, spoofing of biometrics will be investigated among other things. For this reason insight into the internal mechanism as discussed in section 3.5 is important. Fingerprint biometrics is the most mature biometric technology and is widely used [60].

The next biometric technology that will be discussed is iris biometric technology. Iris biometrics is an example of a non-touch type biometric.

3.6. IRIS SCANNING

The intricate nature of the human eye provides access to the most accurate biometrics [61].

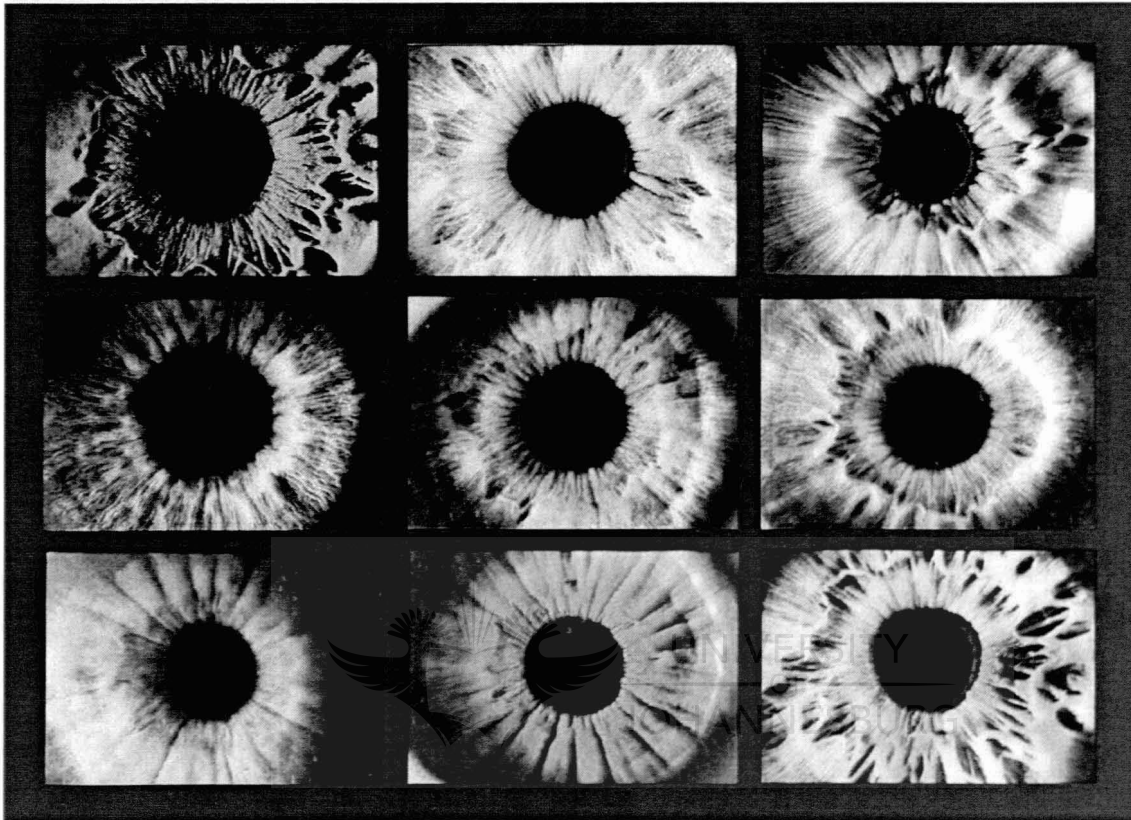


Figure 3.13: Various iris formations

According to Answers [62], the iris is the ring of colored tissue surrounding the pupil. The iris consists of pigmented fibro-vascular tissue known as the stroma [63]. The stroma connects a sphincter muscle, which contracts the pupil, and a set of dialator muscles which open it. The back surface is covered by a two-cell thick epithelial layer, the iris pigment epithelium, but the front surface has no epithelium. The outer edge of the iris, known as the root, is attached to the sclera and the anterior ciliary body. The iris and ciliary body together are known as the anterior uvea. In front of the root of the iris is the region through which the aqueous canal constantly drains fluid out of the eye, with the result that

diseases of the iris often have important effects on intraocular pressure, and indirectly on vision.

The rich textured patterns of the iris, forms the basis for iris recognition. When analyzed, the information density of iris patterns is roughly 3.4 bits per square millimeter [63]. Ophthalmologists first noted the distinctive features of the iris, and observed the patterns to be different between the left and the right eye. The iris is formed before birth, and under normal conditions remains stable until death. Distinctiveness and stability make irises an excellent choice for biometric identification.

Ophthalmologists Leonard Flom and Arin Safir were awarded the patent in 1987 for describing methods and apparatus for iris recognition based on visible iris features [65]. Dr. John Daugman of Cambridge University later developed the algorithms, mathematical methods and techniques to encode iris patterns and compare them in an efficient manner. All applications currently developed utilize Daugman's patented techniques [64].

Iris recognition uses near infra red light. A subject must be co-operative during the capturing phase of the iris. The iris image is captured at close range – roughly 3 to 7 inches (75mm to 175mm). In current systems the scanned image is processed in grayscale, as illustrated in figure 3.16.

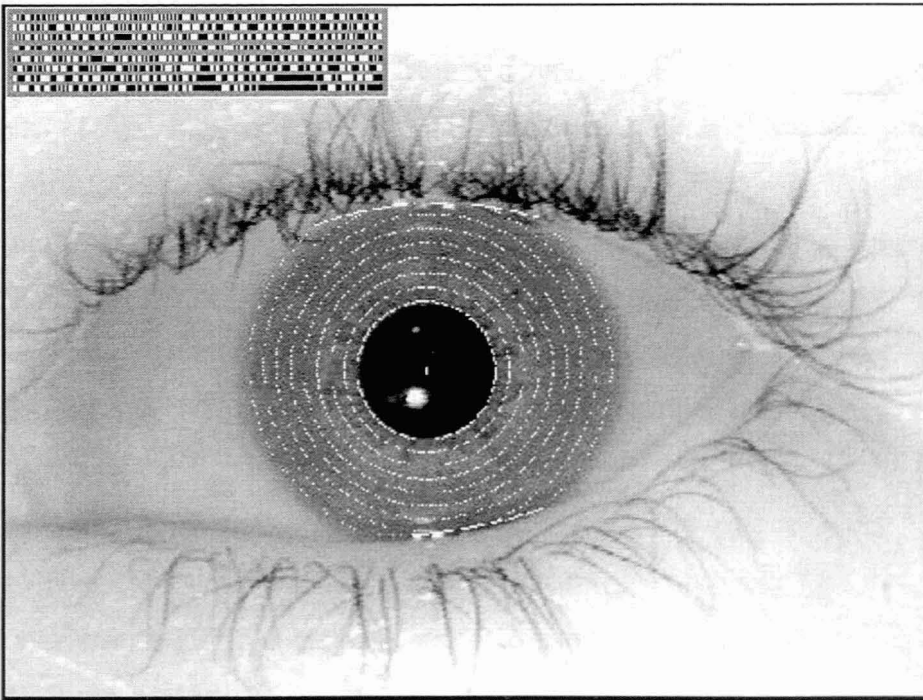


Figure 3.14: Grayscale processing of Iris Image [66]

Size and contrast corrections are performed on the image to counterbalance naturally occurring contractions and expansions of the iris. This result is a size-invariant representation.

Based on Dr. Daugman's initial performance observations with optimized, integer-based code, he estimated a single search engine can perform about 100,000 comparisons per second and also concluded:

"The mathematics of iris recognition algorithms make it clear that databases the size of entire nations could be searched in parallel to make a confident identification decision in about 1 second using parallel banks of inexpensive CPU's, if such large iris databases ever came to exist" [67].

The actual comparison of two iris codes reduces to a series of efficient, low-level XOR operations. Thus the extent to which the iris codes differ is the number of mismatched bits, or the Hamming distance between two iris codes. Hamming difference can be described as the fractional difference between two binary sources of equal length. The original documentation by Dr. Daugman describes a 256 bit Iris Code [67]. However, some changes were made to the header information or changes were made to the process as Iridian now describes a 512 bit Iris Code [68] encrypted to protect the content of the Iris Code.

Dr. Daugman's mathematical analysis of iris code comparisons has shown that iris based technology has a low error rate. The odds of two different irises generating a sufficient similar code to produce a false match are theoretically 1 in 1.2 million [69].

3.7. CONCLUSION

Fingerprint and iris scanning are currently the major role players in the biometric arena [70]. Each of these biometric technologies comprises of certain advantages and disadvantages. Whenever a biometric technology is considered it is important to consider whether the specific biometric technology is intrusive or non-intrusive. For instance, retina scanning is intrusive as a user must allow a light to be beamed into the eye. On the other hand iris technology is not intrusive as a small image is taken of the person's iris. Furthermore, it must be considered to what extent a given biometric can be subverted. Fingerprint biometrics is by far the most common of all biometrics. The majority of attacks at this stage are aimed at fingerprint technology. There are, as will be discussed in the next chapter, several research papers published, investigating the possibility of fingerprint spoofing. Most of the spoofing techniques rely on making a false image of the specific biometric, and for this reason a large amount of research went into liveness testing.

The next section will briefly consider liveness testing.

3.8. LIVENESS TESTING

Recent reports have shown that biometric devices can be spoofed using a variety of techniques [55], [56], [57], [58]. The security provided by biometric devices is diminished if these devices can easily be circumvented. Liveness testing has been suggested to counter the attacks on biometric devices.

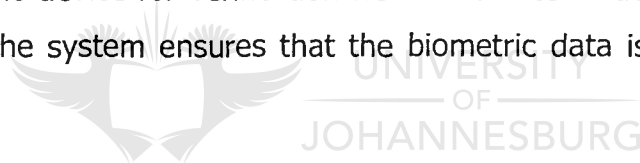
Liveness tests are automated tests to determine whether a biometric sample presented came from a live person. Furthermore liveness testing wants to ensure that the recorded biometric sample came from the person that originally enrolled on the system, thus "the authentic live person".

Considering that a system made by man can be defeated by man, liveness testing serves as an additional level of confidence, that the person is the authentic human.

Often liveness testing is not a sophisticated process. Liveness testing can be as simple as an observer supervising the capturing of biometric samples. A true story, set in South Africa, and published by the East Province Herald newspaper [71] reported: "At first nothing seemed untoward," Postmaster Dawie Bester related. "I was manning the post office counter, which is used to serve illiterate people, when a young man and woman arrived, holding an older man between them" In South-Africa certain pensioners use a fingerprint to claim their monthly pension cheque. The young man and women explained that the older man was their uncle and said "he is very lazy; he cannot be bothered to stay awake to claim his pension. He may be drunk. He is ill." All the same postmaster Bester started to become suspicious when he noticed the old man's eyes are completely

closed and still. Then when he noticed the way the young man was maneuvering the old man's hand on the counter for fingerprint taking, the postmaster told him that pension claimants have to be in full control of their bodies and minds to get their cash, he would summon his supervisor. At that point the couple shouted at the postmaster and abruptly ran off, leaving the old man to fall to the ground. Postmaster Bester explained: "When I got around the other side of the counter, I discovered that the old man was cold and had obviously been dead for many hours, so I called the police. We have had a few people dying while waiting in the queue, but never had a dead person trying to claim".

In the above mentioned example the postmaster was observant enough to notice that the authentic person was not alive. However, if this situation occurred at an unmanned station like an ATM, the outcome might have been different. If a person uses a biometric device for verification from a remote station, it is even more important that the system ensures that the biometric data is from a live authentic person.



One major threat to biometric capture devices is the use of fake or artificial biometric characteristics, for example, fake gummy fingers as manufactured during Prof Matsumoto's [55] research.

It is however important to realize that biometric systems are not more vulnerable than other authentication technologies, for e.g. bar codes, magnetic cards and photo ID cards are all imperfect as well. The advantage that biometric devices have is the fact that something can be done about it – incorporation of automated liveness tests to minimize the effectiveness of artificial simulated biometric specimens.

3.8.1. Liveness test categories

Biometric liveness tests fall into three main categories [61]:

3.8.1.1. Intrinsic properties of a living body

A living body has a number of properties that are observable while the body is alive. The following properties of a living body can be identified:

- Body Fluid – Oxygen, Blood Constituents, DNA.
- Visual – Colour of a live human, opacity, appearance and shape of features.
- Electrical – Capacitance, resistance, impedance, dielectric constant.
- Physical/Mechanical – Weight, density, elasticity.
- Spectral – Fluorescence, transmittance, absorbance, reflectiveness.

3.8.1.2. Involuntary signals generated by a living body

The human body generates a number of involuntary signals while it is alive. The human has no control over these signals, and cannot alter or generate these signals by free will.

- Pulse.
- Heat.
- Body odor.
- Blood pressure.
- Thermal gradients.
- Corpuscular blood flow.
- Skin Exudation.
- Perspiration.
- Transpiration of gases.
- Electric signals generated by the heart (ECG).
- Brainwave signals (EEG).

3.8.1.3. Responses to stimuli (Challenge-response)

In a voluntary challenge-response test the user provides logical responses to a prompt generated by the system. The stimulus can be tactile, visual, or auditory in nature. The user is instructed to do or say something – for example, the system could request from the user to say a specific word or to say words in a specific sequence.

An involuntary challenge-response tests whether the user's body automatically provides the response with a physiological change or as a reaction to a stimulus specific. For instance, if a bright light is projected into a human eye, the eye will automatically contract to reduce the amount of light entering the eye. If a person's eyes are dilated, and do not react at all to light it is usually an indication that the person is dead. To test voluntary and involuntary reaction in a human, the following should be noted:



Voluntary (behavioral)

- Tactile – respond to feeling something.
- Visual – Respond to seeing something.
- Auditory – Respond to a sound.

Involuntary (reflexive)

- Electromyography (EMG).
- Pupil Dilation.
- Body Reflex (striking of the knee).

3.8.2. Strong and Weak liveness tests

A liveness test can be considered as a strong or weak liveness test. Weak liveness tests are tests that are two phased. In phase one the biometric will be recorded and tested, and in the second phase, the system will challenge the human to respond in a way as to prove that he is alive. For example, if the system uses voice recognition to verify the person's identity, in phase one, the person will say a pass phrase. If the system is satisfied that the pass phrase matches the recorded template, the system will in phase two challenge the person to say a few words in a specific sequence. Fingerprint biometrics can also be considered as a weak liveness biometric. In the first phase the system will digitize the fingerprint and compare the minutiae from the fresh print to the minutiae on the template. In the second phase, the system will for e.g. heat the sensor to test for changes in perspiration from the finger. The Sony Fingerprint Identification Unit (FIU 500) tests for liveness by measuring the intrinsic properties of the living finger. The FIU 500 incorporates a sensor that claims to measure the capacitance of the skin [72].

In strong liveness tests, liveness is intrinsic to the biometric. This means that if the human is not alive, the biometric is not measurable (or does not even exist). If brain waves are used as a biometric, it stands to reason that the biometric will not exist if the person is not alive.

3.8.3. Problems with liveness tests

A United States patent entitled "Biometric, personal authentication system" [73] described a system known as 3M Blackstone. The Blackstone used an optical fingerprint sensor and measured electrocardiograph signals (ECG), blood oxygen levels, and pulse rate to verify a person and to test for liveness. On the down

side, the user must hold his finger in place, and with as little movement as possible for around 8 seconds. This is a long time for a person to remain motionless, and is obviously a problem if a high level of throughput is important. With the Blackstone system, the system had to restart the whole process if the user moved or interrupted any of the tests performed by the device. As demonstrated by Blackstone, liveness testing is not easy and usually involves a fairly long delay in the verification process.

Another problem with liveness testing is the lack of open discussion of liveness testing. James Cambier, vice president of research at Iridian technologies Inc, outlines the problem [68]:

“One problem with liveness testing is that most biometric vendors, Iridian Technologies included, do not publicly disclose information about their countermeasures because of the security risk associated with that disclosure. We are not yet to the point in liveness testing where the techniques are so reliable that detailed knowledge of their functionality does not give the hacker an advantage, as is the case with encryption techniques.”

That said all commercially available iris recognition products contain some level of liveness testing.

3.9. CONCLUSION

This chapter focused on the technology of biometrics as a method to authenticate a user. The chapter discussed biometric systems in general, followed by a discussion of two major biometric technologies currently in use. It was pointed out that biometrics is not a magical solution, and also suffers from various problems. However at this stage a large amount of effort goes into research to improve the problems related to biometric spoofing. Liveness testing is one of the current suggestions to assist as a countermeasure against false biometric samples.

Chapter 2 discussed the other methods used for authentication. In Chapter 2 it was pointed out that a system that authenticates a user based on a password or token only authenticates the token as authentic, but not the person presenting the token. This is mainly due to the fact that there is no relation between the user and the token or password other than the secret keeping of the token.

This chapter focused on biometrics. Due to the nature of biometrics there is a direct relationship between the user and the biometric being presented. In essence the problems related to biometric spoofing are far less than the problems related to situations like password sharing or rudimentary passwords.

If a system authenticates a user based on a biometric, the authentication per definition is based on something that the user is. This means that there is a direct relation between the user and the biometric.

If a system authenticates a biometric token, the system is (for the majority of cases) authenticating the user, not merely the presented biometric token.

In the majority of instances, people engage in trade. This is one of the main areas where a person wishes to be identified and authenticated. In the past people would mainly deal with a known person. With the introduction of international trade, spurred on by the internet, it is possible to trade with unknown people on the other side of the world. This makes the demand for secure identification and authentication all the more compelling.

Up to this point, much was discussed about the mechanisms of the technologies used for identification and authentication. Using this knowledge, the following chapter (chapter 4) will discuss the possibility of subverting identification and authentication technologies by means of replay, as well as subverting biometric authentication by means of replay. Replay is one of the major problems in authentication systems, and this chapter will illustrate the various methods of replay found for different authentication technologies.



Chapter 4: Replay

4.1. INTRODUCTION

In the previous two chapters, the technologies at our disposal for identification and authentication were discussed. Chapter 2 focused on-

- something the user **knows**,
- something the user **owns**.

In order to authenticate a person based on what a person knows, passwords and personal identification numbers (PINs) are currently used as the implemented technology. Various token technologies exist to authenticate a person based on what a person owns as discussed in chapter 2.

Chapter 3 introduced the mechanism of biometric technology. This technology is used to implement the authentication service through something the user **is**.

Both the chapters explained the mechanisms of these technologies, and briefly elaborated on some of the vulnerabilities of these technologies.

This chapter will focus on the problem known as "Replay". Replay is a problem relevant to all authentication technologies, and forms a fundamental part of this thesis.

Replay occurs when an authentication mechanism is subverted due to the fact that the electronic representation of the authentication data can be acquired and then replayed at a later stage in its electronic form. This is done in an unauthorized way, in order to force a false match.

In the following section replay will be discussed, followed by a discussion focusing on the various replay approaches available in the different authentication mechanisms.

4.2. REPLAY

When a password or biometric data is compromised, and used by an unauthorized person to force a false authentication, that person replayed that password or biometric data.

The following sections will discuss how passwords and biometric data can be acquired and be replayed in order to force a false authentication.

4.2.1. Acquisition of a password

The first step is to acquire the password of a user. Acquiring a password is illustrated in figure 4.1.

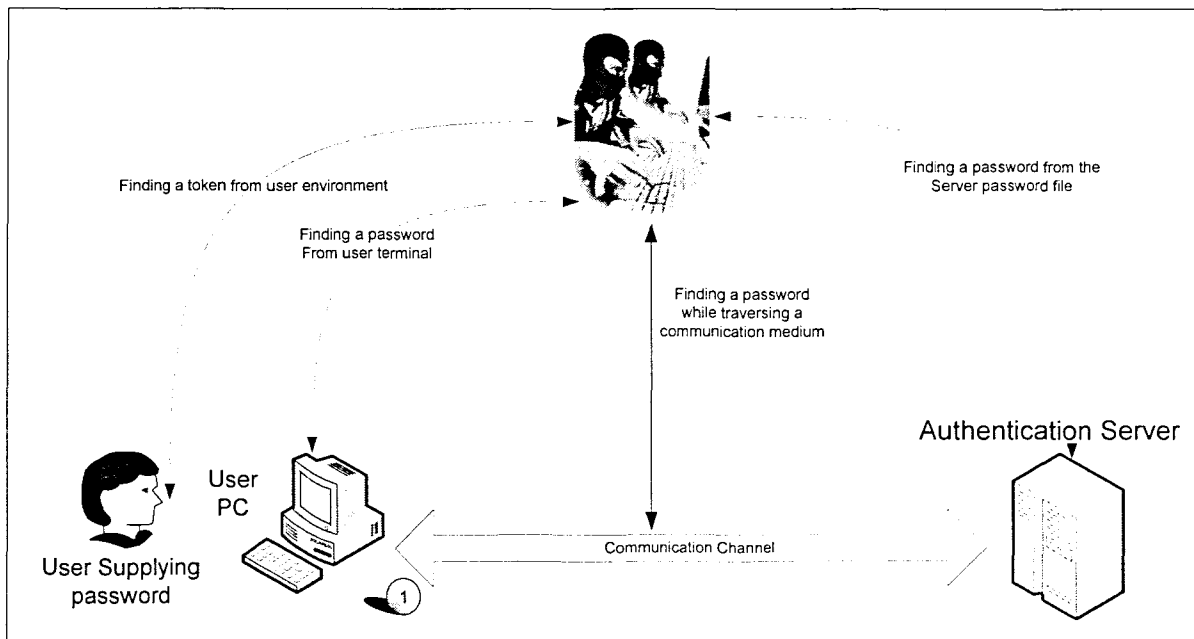


Figure 4.1: Acquisition of a password

As illustrated in figure 4.1, the hacker has several opportunities to acquire the password from a user.

1. As mentioned in Chapter 2, the hacker could simply guess the password, due to the fact that the hacker could do a little research into the personal space of the user.
2. The hacker could peep over the user's shoulder while using the password. Thus the hacker could acquire the user's password simply by observing the user in his environment.
3. The hacker could get the password from the terminal that the user is connected to, by means of key loggers, or searching the terminal for a possible password file.
4. If the password traverses a communication channel such as a network, it is also possible that the hacker could sniff the communication medium using a network sniffer [7].

5. As illustrated in figure 4.1, all passwords are stored on the server. If the hacker could gain physical access to the server, the password file could be copied. Considering that the password file contains all the password hashes of the entire user base, the hacker could crack the hashes using rainbow tables [84], [85] thus acquiring a particular user's password in a fairly short time.

4.2.2. Replay of an acquired password

In the second step the hacker could use the password acquired as explained in section 4.2.1, to be illicitly authenticated by the authentication system. This process is illustrated in figure 4.2.

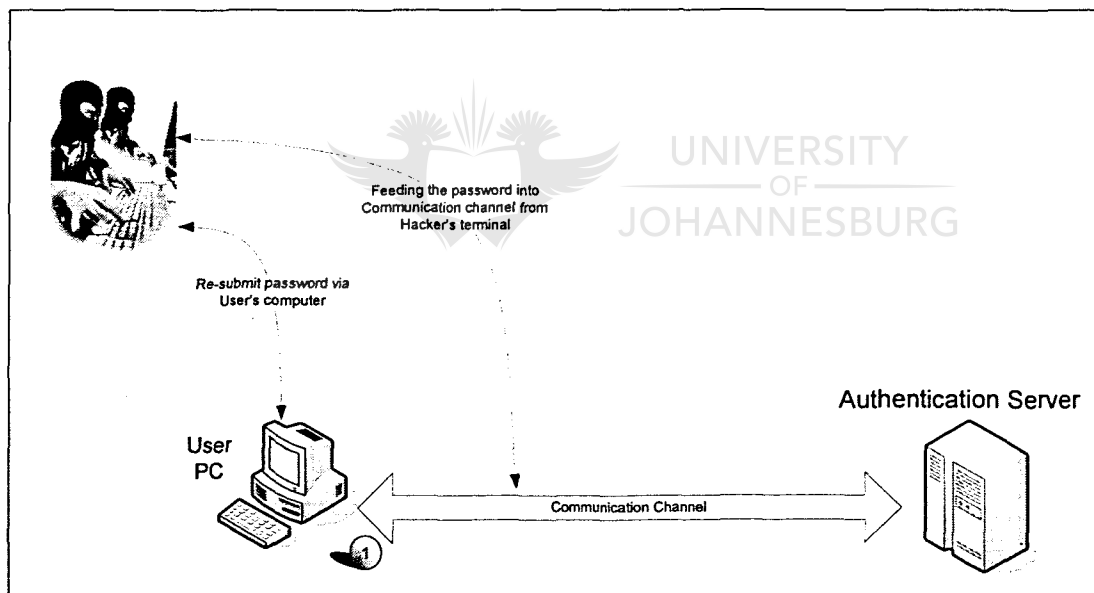


Figure 4.2: Replay of an acquired password

As illustrated in figure 4.2, once the hacker successfully acquired the password of the user, the password could subsequently be used by the hacker to be illicitly authenticated. The hacker could replay this password, by entering it into the

terminal that the user worked on, or submit the password over the communication channel, from his own terminal.

4.2.3. Password replay comments

1. If a password is compromised, and used and replayed at a later stage, it is impossible for the authentication algorithm to determine that the password is being replayed. The internal rules of the algorithm will compare the password received with the password stored in the password file. If the password offered is an exact match with the password stored in the file, the algorithm will accept the presented token as authentic.
2. If a user discovers that his password has been compromised, the user can simply change the password.

The second mechanism that will be investigated for replay vulnerability is biometric technology.



4.2.4. Acquisition of biometric data

Unlike a password, a biometric characteristic is not as readily acquired. If the biometric characteristic, for instance an iris, of a person is required, the hacker may consider in extreme circumstances to remove the user's eye. Other methods, however, are available to obtain a biometric characteristic for replay.

A biometric characteristic, as discussed in Chapter 3, is digitized into an electronic representation (known as biometric data) of the given biometric characteristic. It is possible to intercept this biometric electronic representation (biometric data) just as easy as any other electronic representation of a password can be intercepted.

The biometric system, as illustrated in figure 3.1, has a number of instances, where biometric data can be acquired by a hacker. Figure 4.3, which is based on figure 3.1, illustrates possible sites where the hacker could acquire biometric data of a particular user.

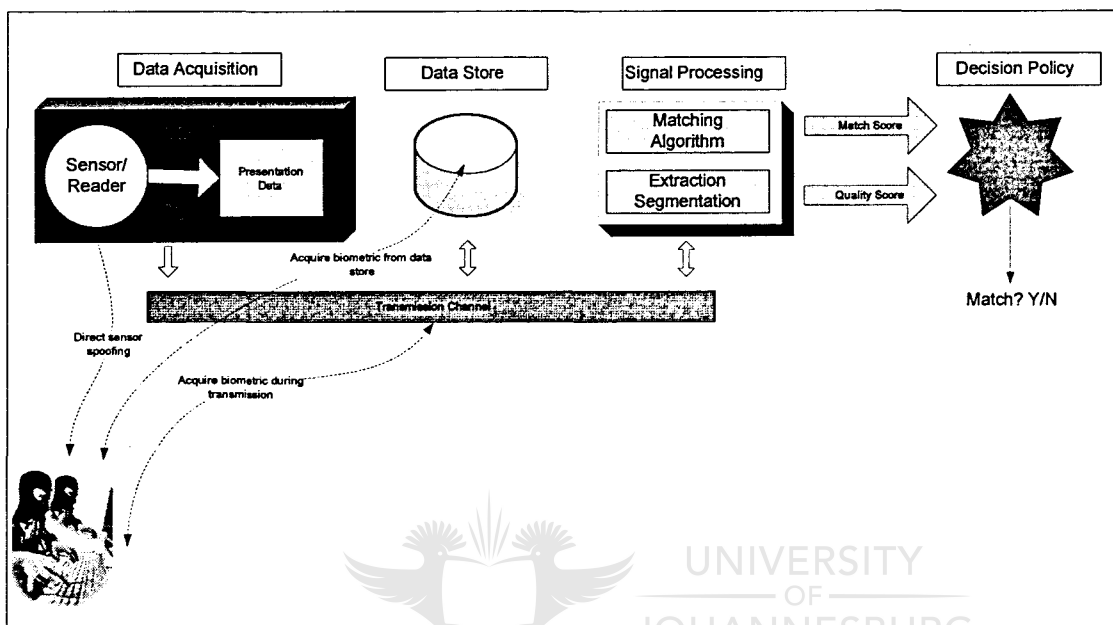


Figure 4.3: Acquisition of biometric data

When a biometric characteristic is presented to a biometric sensor, the device will digitize the biometric characteristic into an electronic representation of the presented biometric characteristic; this electronic representation will be referred to as biometric data.

1. The first site that the hacker could consider to attack is the sensor itself. Once the sensor digitized the biometric characteristic, the hacker could acquire the electronic data directly from the sensor, before it is submitted to the terminal for processing [38].
2. Furthermore, biometric data can be acquired from any section of the internal transmission pathways found in the biometrics environment, as illustrated in figure 4.3. As an example, whenever biometric data is

transmitted between the sensor and terminal, or during transmission between hardware and software, it can be intercepted. This renders the internal biometric transmission channels vulnerable. The hacker can for instance monitor and capture all USB traffic between the biometric sensor and the terminal. Once the biometric sensor sent the digitized information to the terminal, the hacker would have the biometric data of the user's biometric characteristic.

3. The reference biometric data must be stored in a secure data store. If the hacker could gain access to this data store, the hacker would have the electronic representation of the user's reference biometric data.

If a user transmits his biometric data over any network, the biometric data can also be compromised as illustrated in figure 4.4.

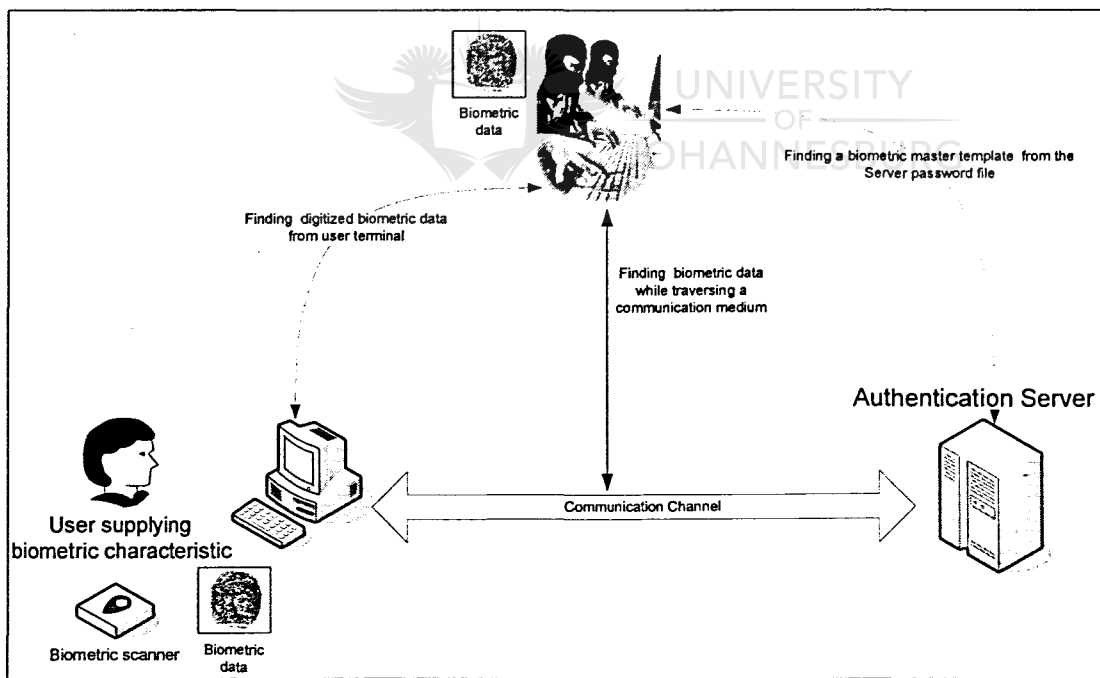
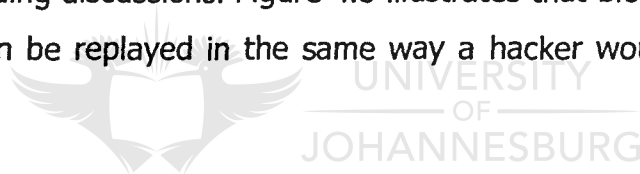


Figure 4.4: Acquisition of biometric data over a network

As illustrated in figure 4.4 the hacker could acquire the biometric data of the user's biometric characteristic from a number of sources. As illustrated in figure 4.4, the hacker could get the biometric data directly from the terminal of the user; the possible places that the hacker can attack the user's terminal are also illustrated in figure 4.3. If the user submits the biometric data over a network communication channel to a remote server, this biometric data can be sniffed and acquired similar to the acquisition of a password. Finally, if the hacker has access to the server, the biometric master template can be acquired directly from the server data store.

4.2.5. Replay of Biometric data

Considering that passwords and biometric data are represented in binary, this binary representation of a password or biometric data can be intercepted as illustrated in the preceding discussions. Figure 4.5 illustrates that biometric data, once compromised, can be replayed in the same way a hacker would replay a password.



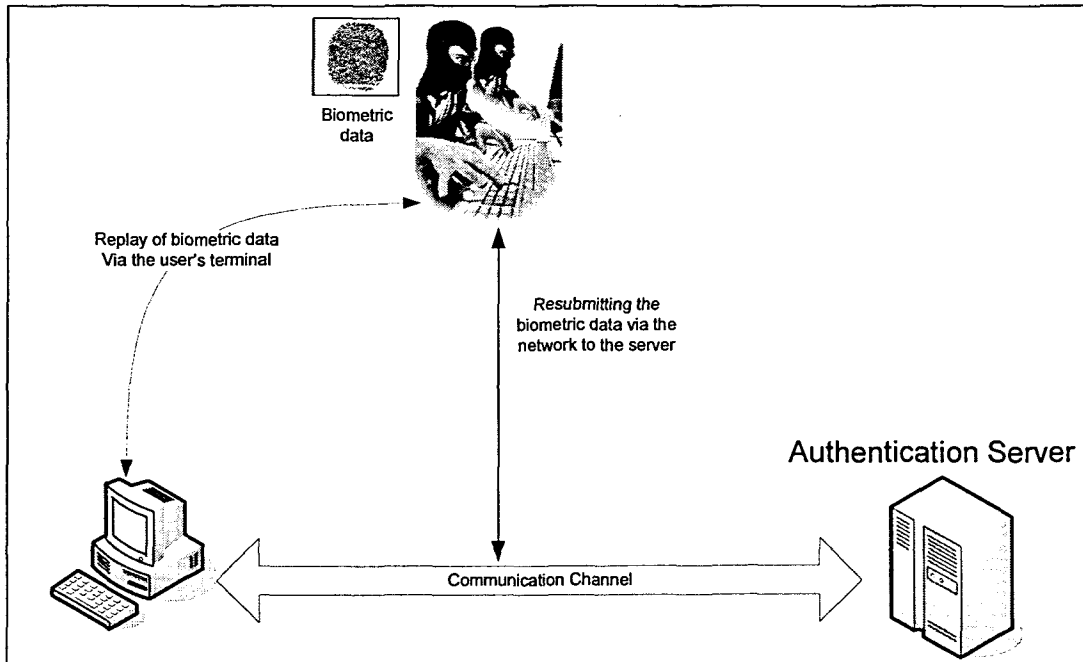


Figure 4.5: Replay of illicit biometric data

Once the hacker has successfully acquired the biometric data the hacker can replay the biometric data. Figure 4.5 illustrates the hacker replaying the biometric data by sending the biometric data through the communication channel to the server, either from the user's terminal, or from the hacker's PC. The server receives the biometric data and compares the biometric data to the stored biometric master template in the data store. If the biometric data falls within the parameters defined by the decision policy, the biometric data will be accepted as authentic. As this is a replay of biometric data that was previously accepted by the decision policy, the hacker can be convinced that the replayed biometric data will be accepted without reservation.

4.2.6. Biometric data replay comments

1. Biometric data is stored and transmitted in electronic form, similar to the manner a password is stored and transmitted in electronic form. If biometric data is acquired by using any specific method, the hacker can replay this biometric data in the same manner a password is being replayed.
2. A user can not merely change a compromised biometric characteristic as a compromised password would be changed. As a user has only 10 unique fingerprints, 2 unique irises and 1 unique DNA, it is imperative that the biometric data needs to be protected in a way that the hacker can not replay this acquired biometric data.

4.3. CONCLUSION

This chapter demonstrated that a biometric characteristic gets converted into an electronic representation. This electronic representation gets stored and transmitted similar to the manner traditional passwords are stored and transmitted. It was pointed out that biometric data and a password can be acquired while in transit via the network or while being processed inside a computer terminal.

Once a password or biometric data is illicitly acquired, a hacker can use this password or biometric data by replaying it, to be illegitimately authenticated.

If a biometric characteristic is compromised, it cannot simply be replaced, unlike passwords and tokens which are easily replaced.

The negative impact of a compromised biometric characteristic in the identification and authentication environment is far greater than that of a compromised password, as biometric characteristics cannot be replaced. Replacement of passwords, however, is almost inexhaustible. Preventing and management of the compromise of biometric characteristics are therefore essential.

In the following chapter (chapter 5), authenticator duplication will be discussed. This is more of a concern if compared to replay, as a duplicated biometric characteristic can be collected from the environment that the user interacts with on a daily basis.

Chapter 5 will demonstrate that tokens and biometric characteristics share the same vulnerabilities relating to duplication and replay.



Chapter 5: Authenticator Duplication

5.1. INTRODUCTION

In the previous chapter it was illustrated that a password can be replayed by supplying the identical password or pin to the authentication server. The password or pin can be acquired from the physical environment of the user, for example, by guessing the password due to the fact that the hacker knows the user well. The password can also be acquired in electronic format, that is, while the password is inside the electronic realm of the IT environment. To illustrate this fact, chapter 4 elaborated on methods that a hacker could exploit to find the electronic version of a person's password, for example, by means of network sniffing or password database hacking.

Another important point, established in the previous chapter, is that biometric data can be acquired in electronic format in a similar fashion a password and pin can be acquired. As a biometric characteristic will be transformed into a reference biometric template of that biometric characteristic, this reference biometric template will be as vulnerable as a password or pin.

Similarly chapter 4 pointed out that biometric data can be replayed as readily as a password or a pin can be replayed.

This possibility of biometric data replay is understandably considered as a major concern [82]. If biometric data is intercepted in electronic format, the biometric characteristic is compromised, and cannot as easily be replaced as a password or a pin can be replaced.

This Chapter will introduce an aspect of more substantial concern. Unlike a commercially manufactured token e.g. a smartcard or special key, which is difficult to forge, a biometric characteristic e.g. fingerprint is readily open to criminal exploitation and forgery. Fresh latent biometric images are left behind as a person interacts with the environment. These are known as latent fingerprints [86].

This chapter will discuss and illustrate how commercially manufactured tokens and biometric characteristics can be forged.

5.2. MANUFACTURED TOKENS

If it is made by man, it can be defeated by man. If the potential gain of stealing a token, or duplicating a token is significant enough, substantial attempts will be made to steal or duplicate a token.

One of the superior advantages cited in favour of a manufactured token is that ideally only one authentic token at any given time should exist [87]. This means that if the token is lost or stolen the owner of the token will be aware of the loss. However, this section will illustrate that it is fairly simple to duplicate a token in order to utilize the token illegitimately without the owner being aware of the compromised token.

In order to illustrate this, credit card skimming [88] will be discussed.

5.2.1. Credit card skimming [88]

A credit card provides the owner of the credit card with the opportunity to authenticate him, based on the fact that he is the only person with that specific unique credit card.

This credit card is authenticated by a number of ways:

- The credit card has a unique number (linked to the owner's credit card account).
- The credit card has an expiry date.
- The credit card is supplied to a specific person, and this name appears on the front of the card.
- The credit card has a specific card verification code (CVC). In the event of a flawed magnetic strip or magnetic card reader on the capturing device, the supervisor can override the magnetic reader to complete the transaction by entering the card number, card expiry date, and the CVC code.
- Lastly a unique magnetic strip containing a number, on the reverse side of the credit card. Payment terminals identify the credit card when the magnetic strip is exposed to the terminal's reader.

The easiest method for a hacker to duplicate the card is to copy the information found on the magnetic strip, on the back of the credit card. A hacking method, known as credit card skimming [88], is currently reported occasionally [89].

The process of credit card skimming is illustrated in figure 5.1.

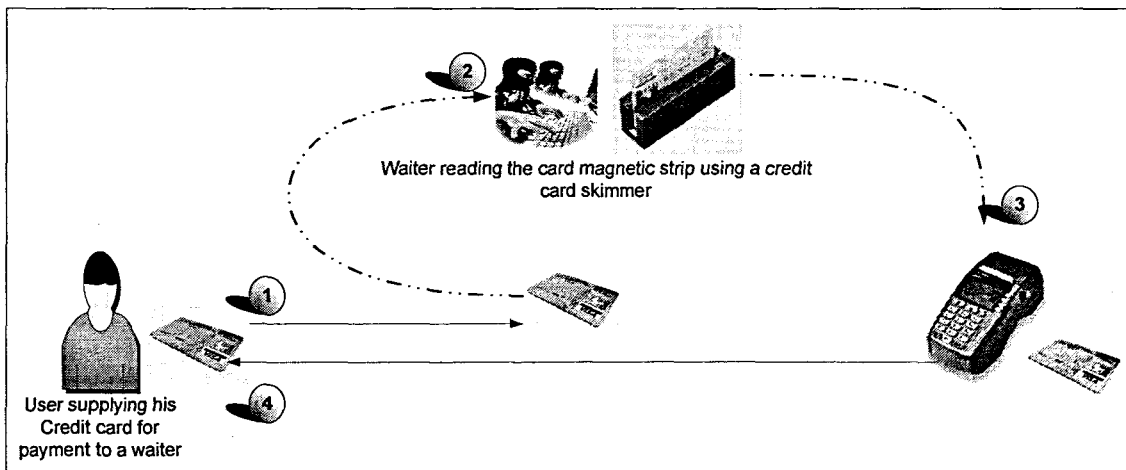


Figure 5.1: Credit card skimming

Figure 5.1 illustrates a typical credit card skimming attempt. In this illustration the credit card is skimmed in a restaurant by a waiter.

1. The owner of the credit card supplies the credit card to the waiter to pay for the bill.
2. The waiter quickly swipes the magnetic strip of the credit card in a magnetic strip reader, as illustrated in figure 5.1. This magnetic reader saves the magnetic strip information.
3. The waiter swipes the user's credit card in the payment terminal. The terminal follows the normal procedure to authenticate the user's card, and check for sufficient funds.
4. Once the transaction is approved, the waiter supplies the card owner with the credit card payment slip, to sign.

At this stage the waiter/ hacker is in possession of the unique number stored on the credit card's magnetic strip. These devices have the ability to store several card numbers, and these stored numbers can then be sold for fraudulent card manufacturing.

The following step of credit card skimming is the manufacturing of fraudulent credit cards, by duplicating the stored magnetic number onto a blank magnetic card. This process is illustrated in figure 5.2.

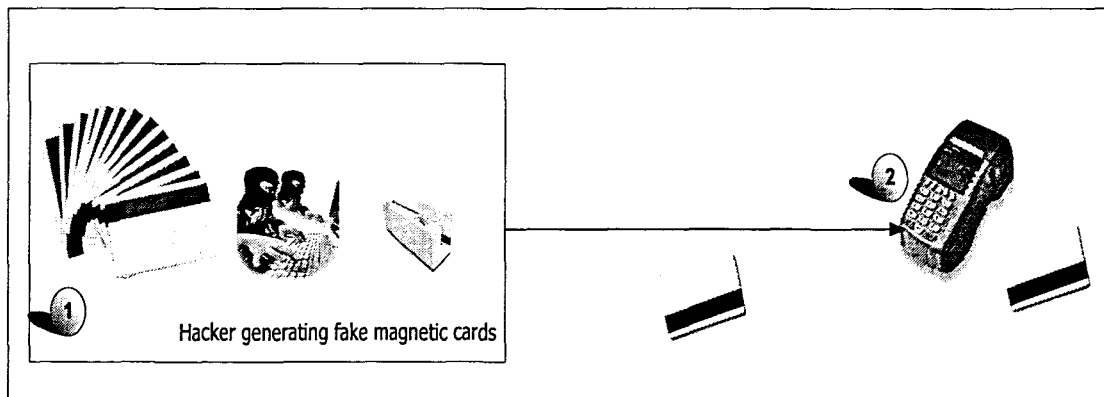


Figure 5.2: Manufacturing of fraudulent credit cards

Once the hacker is in possession of the magnetic strip information, the hacker can manufacture a fraudulent credit card by writing the information stored in the skimming device's memory to the blank magnetic card's magnetic strip. This step is illustrated in step 1 of Figure 5.2. Once the hacker successfully manufactured a fraudulent credit card, this credit card with the authentic magnetic strip information, can be used at a credit card payment terminal to pay for any goods as illustrated in step 2 of figure 5.2. The original token (credit card) now has an exact duplicate.

There is an ongoing war between the companies manufacturing the credit card terminals and the hackers who exploit the vulnerabilities of various magnetic cards being used. In order to combat credit card skimming, the vendors of the magnetic cards now request a few random numbers from the actual card account number, found on the front of the card, to be supplied, before the transaction is approved. This measure temporarily solves the issue found with just skimming the magnetic strip information. It can however be expected that

the criminals will create a new method to duplicate the front of the magnetic card.

5.2.1.1. Credit card skimming conclusion

In conclusion, this section proves that a token can be falsified. If the potential gain from duplicating the token is lucrative enough, a way will be devised to duplicate the token. A constant tug of war will exist between the legitimate users of tokens and hackers that try to exploit the technology. This section illustrated that a token can be copied, and duplicated without the knowledge of the authentic owner of the token.

If an authentic token owner is made aware that his token was compromised, the person will receive a new token, and the compromised token will be blacklisted [89].

In the following section, the creation of fake biometric tokens will be discussed. This section will illustrate that a biometric token is just as vulnerable to being falsified.

5.2.2. Biometric characteristic duplication

As mentioned in chapter 3, biometric characteristics are part of the user. A biometric characteristic cannot be forgotten or stolen, as this type of characteristic is physically part of the user. The user can for example not leave his DNA at home, unlike a credit card or special key.

However, as a user interacts with the environment, latent biometric images are constantly left behind.

This is a significant problem, and is often overlooked. The user will for example leave a latent fingerprint on nearly everything that he touches. If a photo is taken of a person's face, the facial biometric characteristic can be extracted, and using a camera with a high enough resolution, the iris biometric characteristic is also recorded in the picture. Drinking from a cup will undoubtedly leave saliva on the cup, and in this saliva, the DNA biometric characteristic of the person is stored [90]. In essence, as we interact with our environment, we "shed" our biometric characteristics as latent biometric images. These latent biometric images can be lifted, and a false biometric characteristic manufactured.

Prof. Matsumoto illustrated this fact clearly in his research [3], [55], [58].

Professor Tsutomu Matsumoto from Japan's Yokohama National University demonstrated that it is indeed possible to create a biometric specimen from a fake finger print [56]. Prof. Matsumoto demonstrated two methods, both using gelatin to generate a biometric sample. Today, however, latex is commonly available, and can be used as a more durable material than gelatin. The author of this thesis has personally experimented with methods to duplicate fingerprints, and found that latex based fake biometric characteristics, work exceptionally well. Latex based false fingerprints spoofed virtually all devices tested during this research.

5.2.2.1. Method 1

In the first method, Prof. Matsumoto took an image directly from a live finger of a human being, and made a plastic mould of the finger. He poured liquid gelatin into the mould, and allowed the gelatin to harden. He demonstrated that this manufactured gelatin finger can be used as a fake biometric characteristic to spoof both optical and capacitive finger print sensors.

5.2.2.2. Method 2

The second method is more sophisticated and is used to generate a fake biometric characteristic from a latent finger print image that a person left on a glass after touching the glass.

Matsumoto took the glass with the latent fingerprint image, and enhanced it with a type of superglue known as *Cyanoacrylate adhesive*. Once he completed the enhancing of the latent fingerprint image using the superglue, he photographed the enhanced latent fingerprint image on the glass using a digital camera, and used photo editing software to enhance the contrast and quality of the photographed image. He subsequently printed the image on a transparency sheet commonly used for printed circuit board duplication.

At this stage he had an exact copy of the person's fingerprint that he lifted from a glass, on a transparency. This transparency is commonly used to create a printed circuit board (PCB). During PCB creation, the transparency will serve as the blue print of the tracks that must be etched in copper on a PCB. PCB technology has the ability to create ultra fine tracks [91] – similar to the ridges found on a human's finger print. The biometric image etched into copper, resulted in a three dimensional representation of the fingerprint. Finally liquid gelatin is poured on to the PCB to create a gelatin pad from the copper fingerprint "mould".

As mentioned under method 1, once the hacker is in possession of a fake biometric characteristic, this fake fingerprint can be used to spoof biometric fingerprint readers.

5.3. CONCLUSION

This chapter pointed out an important fact. Tokens made by man, can be duplicated without the knowledge of the owner of that token. In the second section the same was pointed out regarding biometric characteristics. As was discussed, the research of Prof Matsumoto, demonstrated that a biometric characteristic can be lifted from the environment the user interacts with, making it possible to create a fake biometric characteristic, without the person being aware of this fact.

This is an important problem, and is subsequently addressed in the BioVault system.

If a person discovers that a commercially manufactured token was duplicated, a new token can be provided. The compromised token will be blacklisted. In the instance that the compromised token is presented for authentication, a warning can be signaled. However, a biometric characteristic cannot simply be replaced.

Chapter 4 discussed the issue of replay, demonstrating that passwords and biometric data are vulnerable to replay of the password or biometric data, in electronic format.

Chapter 5 demonstrated that tokens and biometric characteristics can be duplicated and repeatedly be submitted.

Thus at this stage identification and authentication technologies are vulnerable to the following problems:

		Type of Attack	
		Replay (Chapter 4)	Duplication (Chapter 5)
Type of Authentication mechanism	Password	<input checked="" type="checkbox"/>	
	Pass phrase	<input checked="" type="checkbox"/>	
	Pin	<input checked="" type="checkbox"/>	
	Tokens		<input checked="" type="checkbox"/>
	Biometrics	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Figure 5.3

As illustrated in Figure 5.3, biometric systems are vulnerable to a replay attack of the biometric data as well as a duplication of the biometric characteristic.

The next chapter (chapter 6), titled "Symmetry and Asymmetry", will consider the fact that a biometric characteristic, unlike any of the other authentication technologies, can be uniquely identified. The ability to identify a biometric characteristic uniquely makes it possible to overcome the problems as mentioned up to this point.

Chapter 6 will for this reason be the first chapter proposing an initial solution to the problems faced if biometric authentication is to be used for authentication.

Chapter 6 will form the first step towards formulating the BioVault model, developed in this thesis.



Chapter 6: Symmetry and Asymmetry

6.1. INTRODUCTION

Up to this point identification and authentication were discussed, pointing out that all identification and authentication systems have certain strengths and certain frailties. As chapter 5 concluded, a table was presented to illustrate the various vulnerabilities found for authentication systems, see figure 5.3 on page 104.

These authentication systems rely on proving the authenticity of the user by means of something the user knows, something the user possesses or something the user is. Considering the conclusion in chapter 5 that biometric data can be replayed (when in electronic form) and duplicated (directly from the biometric characteristic, or from a latent biometric image), makes this type of authentication method seem much less attractive if compared to tokens or passwords - biometrics is vulnerable to both replay and duplication attacks!

However, it was already pointed out that in the case of tokens and passwords, only the token or password is authenticated and not the user presenting this password or token. Using biometrics the user is directly authenticated.

At this stage it is clear that passwords, tokens or biometric characteristics can be misused. This was demonstrated in chapter 4 by means of replay, and in chapter 5 by means of duplication.

This chapter will demonstrate that a biometric characteristic has an advantage over passwords and tokens. This advantage is called asymmetry, and asymmetry allows an authentication system to uniquely identify biometric data being reused. This chapter will demonstrate that passwords and tokens are all symmetric authentication mechanisms. For this reason, every offered password will be exactly the same as any previously offered password, thus not allowing each freshly offered password to be uniquely identified and linked to a specific transaction.

6.2. SYMMETRY

In a symmetric system the objects being compared are required to be exactly the same – it implies a 100% match. Symmetric authentication systems are found when using a password or token, as the password supplied by the user needs to be 100% the same as the password stored in the password database. This is discussed in section 6.2.1. If a user supplies a token the information on the token must match the stored information exactly. Tokens, for instance magnetic cards, are discussed in section 6.2.2.

6.2.1. Passwords

Passwords are always symmetric. This means that the password that a user will offer to be authenticated with is always exactly 100% the same password.

An authentication system does a bit-wise comparison between a password supplied by the user and the stored password in the database. This is the most basic approach to password usage and is illustrated in figure 6.1.

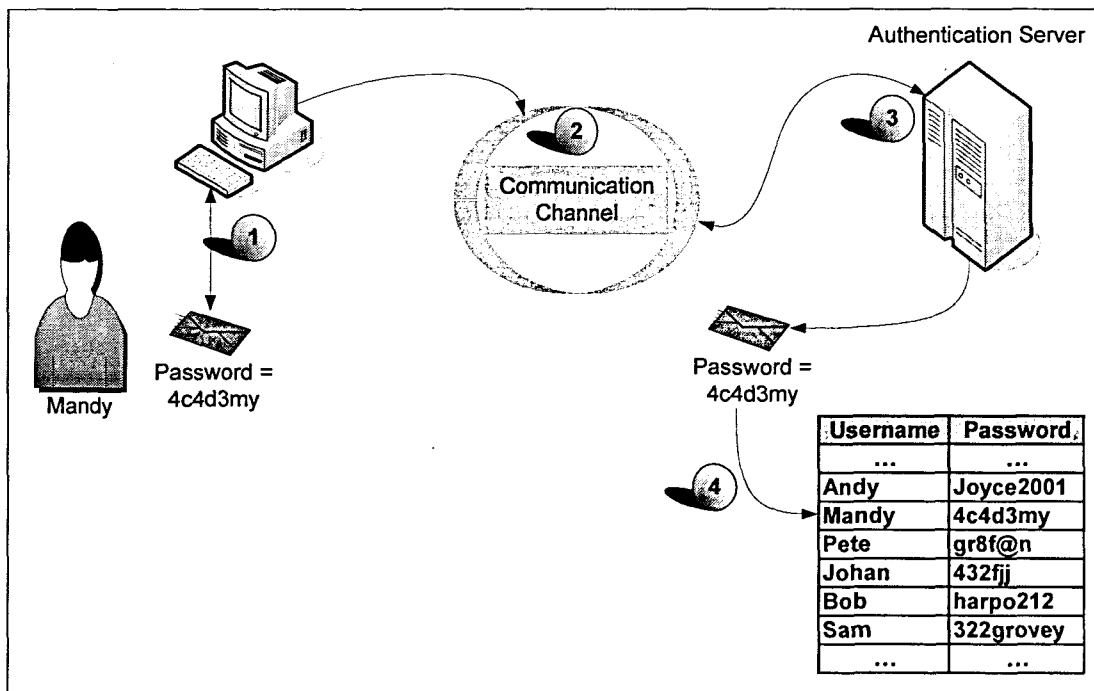


Figure 6.1: Password authentication

In Figure 6.1, the user, "Mandy" must be authenticated, and supplies her password "4c4d3my". In step 2 this password is submitted to an authentication server for authentication. The server receives this password in step 3 and compares the received password with the password in the database in step 4. As the password offered must match the password stored in the database 100%, the offered password is an exact symmetric copy of the stored password.

If the password supplied differs by even one bit from the password in the database, the authentication will not be approved.

In essence a password is compared on bit level. Thus the password "Win" will be translated to the following binary [92], when handled internally by the computer system: 1010111 1101001 1101110. Password comparison is case sensitive; the binary value for a capital w (W) is different if compared to the lower case w [92].

The password stored in the password database is the exact same word (Win), and therefore the word in the database will also translate to the same binary string (1010111 1101001 1101110).

The authentication process will translate the password "Win" received by the user to binary. The password stored will also be translated to binary and compared to the binary of the offered password, as illustrated in figure 6.2.

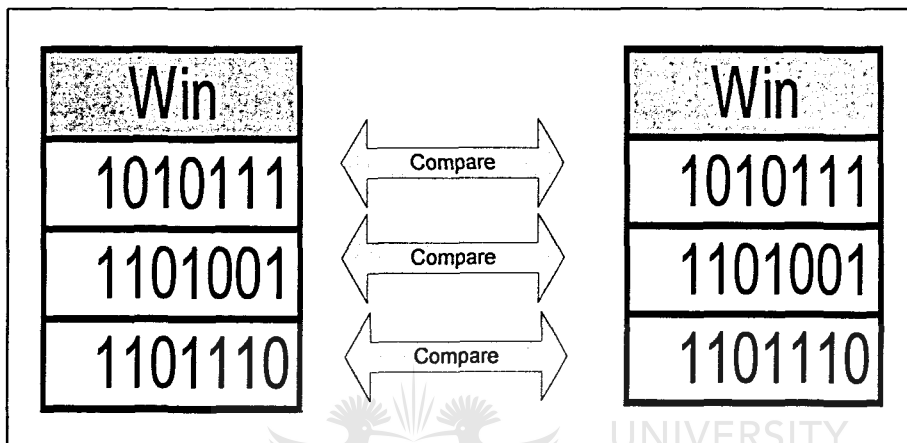


Figure 6.2: Binary comparison

As illustrated in figure 6.2, the offered password "Win" is translated to binary, and compared bit, by bit, to the stored password's binary representation, and if any bit does not match, the authentication process fails.

Figure 6.3 illustrates the difference found between the uppercase "W" in the word "Win" compared to the lowercase "w" in the word "win". The binary difference between these two letters results in an authentication failure.

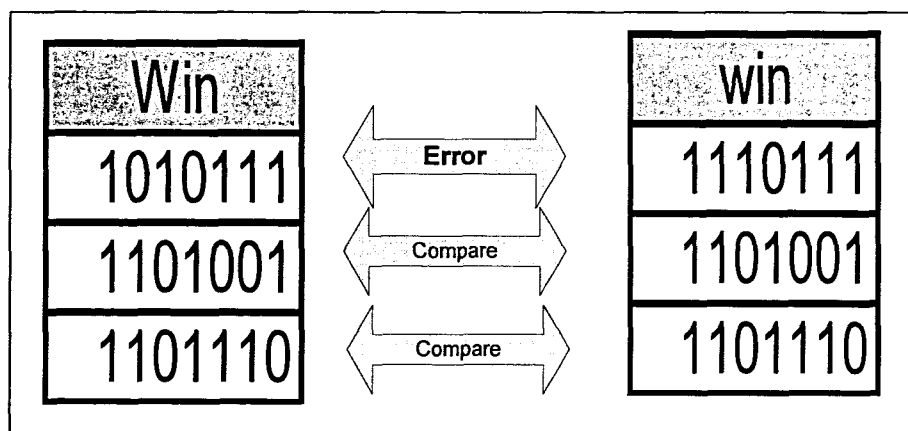


Figure 6.3: Upper and lower case binary comparison

As mentioned, a difference exists between uppercase and lowercase is illustrated in figure 6.3. The password stored in the database is "Win" with an uppercase "W". This letter translates to "1010111". The user supplied the same word, however with a lower case "w". The lower case "w" translates to 1110111". Take note that there is only a 1 bit difference between the two words, but because this system relies on symmetric authentication, the authentication server will not accept the password.

6.2.2. Tokens

If a user inserts a magnetic card into an Automated Teller Machine (ATM) the ATM will read the information from the magnetic strip, and compare it to information supplied by the bank's authentication server. The typical information found on the magnetic strip is defined by the International Standards Organization (ISO) [93] and includes the following fields:

Track one, Format B:

- Start sentinel — one character (generally '%')
- Format code="B" — one character (alpha only)
- Primary account number — up to 19 characters

- Field Separator — one character (generally '^')
- Name — two to 26 characters
- Field Separator — one character (generally '^')
- Expiration date — four characters
- Service code — three characters
- Discretionary data — may include Pin Verification Key Indicator (PVKI, 1 character), Pin Verification Value (PVV, 4 characters), Card Verification Value or Card Verification Code (CVV or CVK, 3 characters)
- End sentinel — one character (generally a '?')
- Longitudinal redundancy check (LRC) — one character.

It is important to take note of the discretionary data stored on the card. This is the data that the authentication server will need to authenticate the card.

The process of using a magnetic card for authentication is illustrated in figure 6.4.

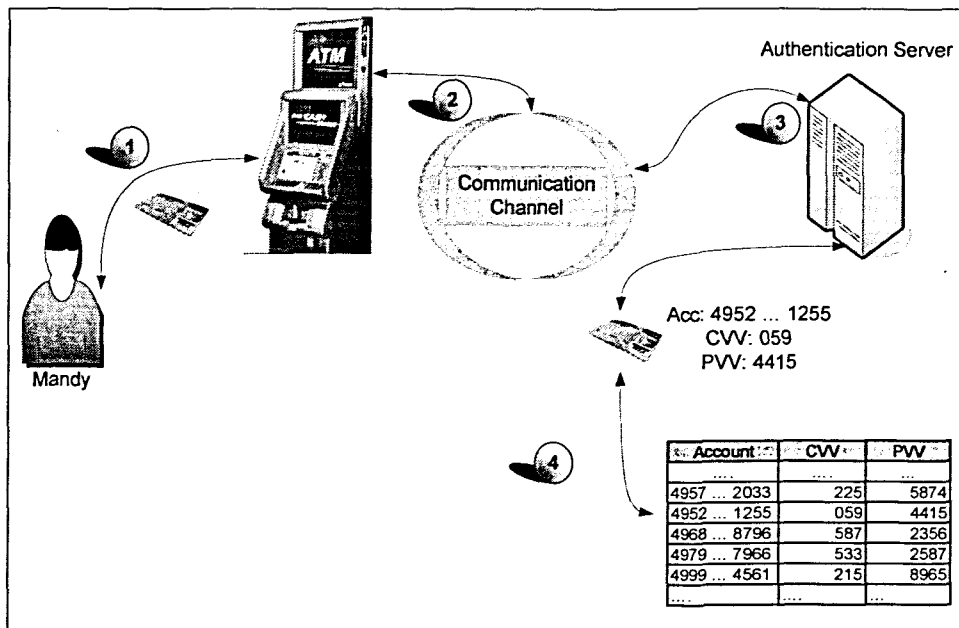


Figure 6.4: Magnetic card based authentication

1. The user inserts the magnetic card into the ATM machine as illustrated. The ATM challenges the user to supply the user's personal identification code (PIN). The ATM extracts the card verification value (CVV) and the Pin verification value (PVV) from the discretionary data field on the card's magnetic strip.
2. This information is transmitted to the authentication server via the network.
3. The authentication server compares the CVV information with the CVV information stored in the database, as well as the PVV code received with the PVV code stored.

As demonstrated in section 6.2.1, this comparison happens on a binary level, and if the CVV supplied is not 100% symmetrical to the CVV stored in the database, the authenticity of the magnetic card is rejected.

6.2.3. Symmetry conclusion

Tokens and passwords are all symmetric authentication systems. The authentication system relies on the fact that the password must match 100% to ensure an authentic match is made. If the codes extracted from a magnetic card do not match the codes stored on the authentication server 100%, authentication is rejected.

This comparison is done on a binary level, and if there is as much as one bit difference between the received value and the stored value, authentication is rejected.

In the next section, attention will be given to asymmetric matching, commonly associated with biometric technology.

6.3. ASYMMETRY

Part of the biometric authentication system, is the important *decision system* that must decide if the user's biometric data is authentic. This decision system was discussed in Chapter 3.

A biometric match is an asymmetric match and for this reason the decision system is incorporated in the biometric authentication environment. This means that a supplied biometric characteristic will virtually never be a 100% exact match of the reference biometric template stored in the biometric data database. Due to a number of factors, freshly recorded biometric characteristics will always be slightly different from the reference biometric template stored in the database.

As an example, the following are some of the factors that cause the fresh fingerprint characteristic to be slightly different to the master biometric template stored during initial enrollment:

- 1) During enrollment an averaged reference biometric template will be stored. This means that the reference biometric template stored during enrollment is the result of an averaged calculation of five or more recorded biometric characteristics.
- 2) Light conditions influence the normalization algorithm.
- 3) Placement of the finger on the digitizing device - the user will not place the finger in the exact same way and on the exact same position on the digital recording device.
- 4) Rotation - the user might rotate the finger on the recording device.

- 5) Pressure - often the user will vary the amount of pressure applied on the device, resulting in a slightly smaller or slightly bigger fingerprint image to be recorded.

The above five points only serve to illustrate that a number of factors influence the process of capturing and recording of a biometric characteristic.

Considering that a newly presented biometric characteristic will for all practical purposes not be a symmetric copy of the reference biometric template stored, a decision policy is needed. This policy will consider the presented biometric characteristic in relation to the reference biometric template, and decide if “enough” similarities are found. If enough similarities are found, the presented biometric characteristic will be considered as authentic. This process is described in Chapter 3.



Some biometric characteristics tend to deviate in a number of ways from the reference biometric template. For this reason, considering the various biometric technologies, the matching algorithms must take these divergences into account, in order to make an authentication decision.

6.3.1. Asymmetric usage

The fact that a biometric characteristic is asymmetric compared to the reference biometric template makes almost all supplied biometric data unique. For this reason all biometric data received from a user is, according to the matching algorithm, unique. Biometric data of a particular user will rarely match 100% with previously received biometric data.

This allows for unique biometric data identification. If an authentication server stored all previously presented biometric data, a test can potentially be done to determine whether newly presented biometric data has been presented to the system in the past.

If the server finds a 100% exact match with any previously presented biometric data, it is possible that the biometric data is biometric data that is being replayed. This replay can be identified due to the improbability of freshly offered biometric data, matching previously presented biometric data exactly (100%).

On the other hand, if a biometric characteristic is used to authenticate a user during a transaction, this biometric data can be stored and linked to the transaction, for auditing purposes.

6.4. CONCLUSION

Passwords and tokens are components of symmetric authentication. For this reason a password or token will always be considered as the identical same password or token. However, as discussed in this chapter, biometric data is asymmetric in nature and for this reason is part of an asymmetric authentication system. Biometric data supplied will rarely match any previously supplied biometric data 100%.

This allows for various applications, and the BioVault system, discussed in the remainder of the thesis, to use symmetry and asymmetry in various ways to overcome problems like replay and duplication of biometric data, as discussed in chapter 4 and chapter 5.

It is however important to realize that the concept of symmetry and asymmetry, as discussed in this chapter, has no direct relationship to similar terminology also found in the encryption systems, known as symmetric key encryption and asymmetric key encryption.

Chapter 7 discusses the importance of identification and authentication, with specific reference to the current e-commerce environment. Chapter 7 illustrates the current technologies used to identify and authenticate a person. However, chapter 7 can be "skipped" without influencing the logical flow of the thesis.



Chapter 7: The Importance of Identification & Authentication.

7.1. INTRODUCTION

The modern world and society revolve around trade and depend on the reciprocity afforded by commerce. Since ancient times dealing amongst people and villages initially consisted mainly of barter trade. Commodity of value, such as gold, eventually was introduced for fixed value determination.

As recently as twenty years ago, trade beyond town and city boundaries was so cumbersome to the individual that agents and merchants were used to acquire products not readily available in the immediate vicinity.

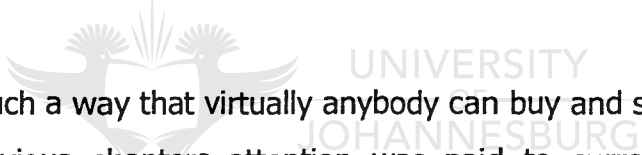
In 1993 a graphical user interface for HTML known as "Mosaic for X" [94] was introduced. This made the internet more accessible to the general public and opened up the possibility of international trade to Tom, Dick and Harry. The internet at first introduced communication between various parties the world over to explore the possibility of international dealing. The internet inevitably became a global trade area.

Companies recognized the opportunity of trade in a previously inaccessible market segment. In 1994 Pizza Hut invited people to place orders on their website [95], [96]. In the same year the first virtual bank – the Cyberbank [97] – opened. Since 1994 online transactions spiraled into a multibillion dollar market with new participants joining the global trading ranks daily.

The previous chapters elaborated on methods of identification and authentication, identifying potential problems using the various methods.

This chapter focuses on an overview of the current on-line trade environment, illustrating the importance of a good identification and authentication system. Electronic commerce is a vast discipline, and many books have been published on the topic. This chapter will summarize electronic commerce. A survey will be made into some of the technologies required for online trade. Considerations like credit card payments and online money vendors will be reviewed. The importance of a proper and trustworthy authentication model will be deliberated. As previously mentioned, this chapter can be skipped without affecting the logical flow of this thesis.

7.2. BACKGROUND



Trade evolved in such a way that virtually anybody can buy and sell merchandise online. In the previous chapters attention was paid to current technologies enforcing identification and authentication. It is necessary to note that these technologies are of vital importance, as they govern the gates of online trade.

With the wealth of information at the disposal of the online user, it is not unusual for a user to find products online and purchase products directly from the manufacturer. This benefits the user, as all information pertaining to the product is supplied by the actual manufacturer. Furthermore it allows the user to cut out a number of middlemen.

A typical example will be a book that is not available at the local bookstore. In the past a person would have needed to place a request for this book at the bookstore. The bookstore would in turn wait for the agent of this book to visit

the store, and place the order for the book. The agent would subsequently have imported the book. After several weeks, the customer would have received a notice that the book had arrived for collection at the book store.

Today most people would pay a visit to Amazon [97] on the internet to confirm the price and the availability of the book, order the book and take delivery shortly thereafter.

A major part of online trade is the payment of goods purchased online. Mechanisms are needed to safely pay for goods purchased.

As a first option, the buyer can pay by means of a direct bank transfer.

Secondly, in the majority of transactions, credit cards are used to purchase online. However this is a high risk option, and will be discussed later in this chapter.

If a user intends to sell merchandise online for example on Ebay [98], he will be expected to identify and authenticate himself to the trading site. Reciprocally, the buyer buying an article online and wishing to pay for this article using the services of a money vendor like Bidpay [99] or PayPal [100], needs to be irrevocably authenticated.

In the section to follow, a typical internet transaction will be demonstrated.

7.3. TYPICAL ONLINE TRANSACTION

The typical online transaction involves the following steps, and is illustrated in figure 7.1:

Step 1 – The user browses the internet in search of the desired product, and a seller wishing to sell the product.

Step 2 – The user finds the product, and enters into negotiations with the seller.

Step 3 – The negotiations will include aspects such as price, handling, shipping, and payment considerations.

Step 4 – The user will then pay the seller using the negotiated method.

Step 5 – Once the seller is sure that the money is safely transferred, the goods will be shipped to the buyer, using the negotiated method of shipping.

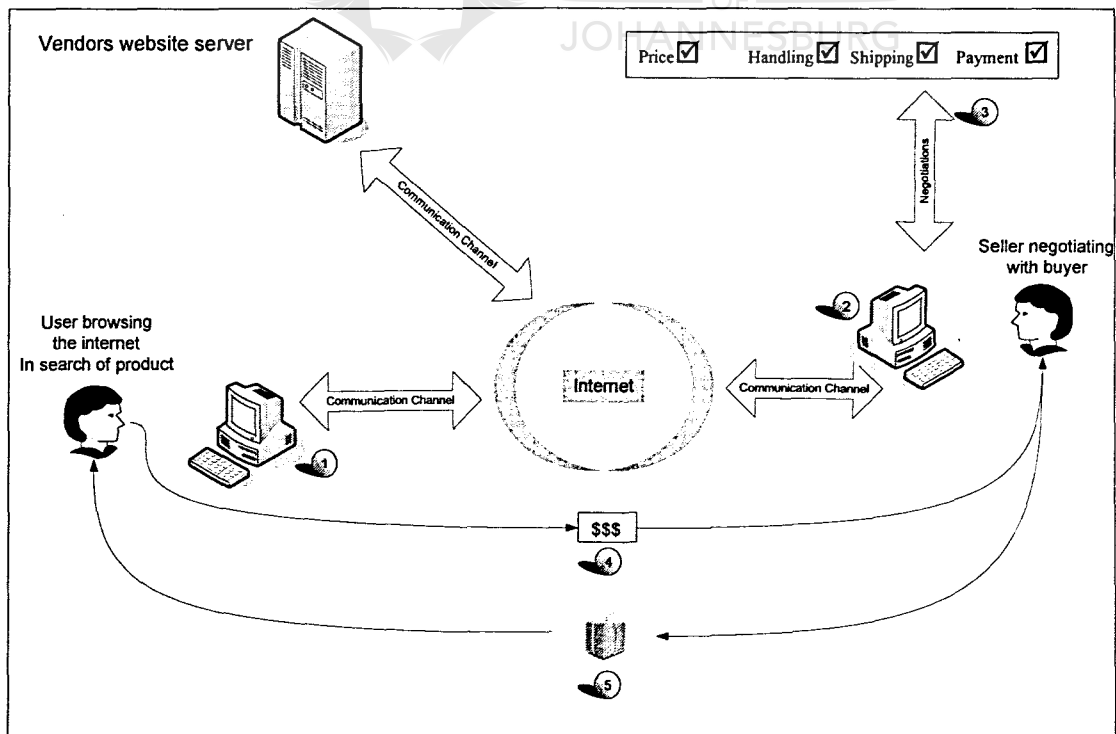


Figure 7.1: Typical online transaction

Payment is a pivotal aspect of the transaction. The seller needs to be convinced that the buyer will pay employing a legitimate method. The buyer needs to keep his identity and details as secret as possible. In order to accomplish this, the seller has a few options available to pay for the transaction.

In the following section consideration is given to the various options available to the buyer, when paying an online supplier.

7.3.1. Paying for a local supplier

If a user purchased a product online from a website or company that resides locally, meaning that the products will not be coming from an international supplier, the buyer can make the payment in one of two ways:

7.3.1.1. *A direct bank deposit*

Money - either as cash or a cheque - can be paid directly into the seller's bank account. Cash payment from the seller's viewpoint is the more desirable method, as it cannot be reversed, once deposited. The buyer's position however is in jeopardy until he has taken possession of the purchased goods. Cheque payment, on the other hand, protects the buyer's position, as payment can be stopped. The seller needs the cheque to be cleared by the buyer's bank before the goods will be released for dispatch. Cash payment needs no authentication. Cheque payment will require a signature.

7.3.1.2. *An online payment*

The buyer uses the online website of his personal bank to make a payment into the bank account of the seller. Making an online payment through the bank is currently protected by the basic identification and authentication methods as

discussed in chapter 2 – thus access to funds transfer is currently protected by means of a username, passwords and often a SMS pin being sent to the buyer via the cell phone network.

7.3.2. Paying an international supplier

If the buyer accessed an international seller's website, the product will be supplied from another country, making the payment more complicated. The following section will consider the options available if a buyer wants to pay for a product purchased internationally.

7.3.2.1. International bank transfer

Due to international regulations a person cannot make a direct (also known as a telex) transfer into an international bank account. This must be requested by the buyer from the buyer's bank. This whole process is conducted off line and is handled by the banking institution.

Paying for products by direct transfer is safe for the buyer as the buyer can be sure that money will only be transferred out of his account once his authenticity was confirmed. The whole process is done at the bank and a buyer paying for his transaction must provide sufficient proof of identity before the transaction will be considered by the banking institution. Direct bank transfers do not reveal any personal details of the buyer's account to the seller. The buyer will be authenticated by producing an identity document to the bank's personnel.

Problems with international bank transfer:

International direct bank transfers, however, are expensive, as the transaction cost for an international bank transfer is approximately R225 (South African Rand) for each transfer [102].

Another major drawback of a bank transfer is the fact that it takes at least 48 hours for the transaction to be processed. All international transfers are handled by the specific bank's head office. Often sellers expect payment within 48 hours.

A seller needs to supply personal information to the buyer's bank, which includes:

- Seller's bank account
- Seller's bank name
- Seller's bank address
- Seller's bank sort code
- Seller's physical address
- Seller's contact number
- Reason for deposit

Sellers often are reluctant to supply this information, as it interferes with privacy issues and anonymity considerations.

7.3.2.2. Credit card online payment

Once the seller and buyer agree on a transaction price, the buyer may consider paying the seller by means of an internationally accepted credit card such as Visa card [103], Master card [104] or American Express [105].

The buyer would be required to provide the following information directly to the seller:

- Credit card number
- Credit card expiry date
- Name on credit card
- Visa / Master / American express

- ☑ Credit card CVC code – the so called Card verification code. As this is the only code that actually protects the card's information, revealing this number should be treated with great circumspection.

Once the seller is in possession of the information, he can process the card transaction electronically. The seller can enter this information into any credit card processing terminal, and draw the funds internationally, directly from the buyer's account.

This option raises the red flag for security concerns as the buyer needs to supply his credit card information to the seller in such a way that the information is unconditionally safe. Should this information be intercepted, it is possible that the card information will be compromised without the buyer being aware of this fact.

In order to protect the security of the credit card, SSL (secure socket layer) is often used to protect the card information during online transmission.

7.3.2.3. Secure Socket layer [107]

The secure socket layer (SSL) protocol was originally developed by Netscape, to ensure security of data transported and routed through HTTP, LDAP or POP3 application layers. SSL is designed to make use of TCP as a communication layer to provide a reliable end-to-end secure and authenticated connection between two points over a network (for example between the service client and the server). Notwithstanding this SSL can be used for protection of data in transit in situations related to any network service. It is used mostly in HTTP server and client applications [106].

If a seller installed SSL as a technology to protect the information during transportation, the buyer can enter the credit card information online. This means that a seller will provide a web-page that is running on a SSL layer, where the buyer can enter his credit card number, credit card expiry date, name on the card and the CVC number. Once the buyer submits this information all communication will be encrypted using SSL.

Risk to consider with direct credit card payments:

A number of risks are apparent when a buyer sends his credit card information directly to a seller.

- 1) The buyer must trust the seller implicitly, that only the agreed upon amount will be withdrawn from the credit card account.
- 2) The buyer must also be convinced that the seller will not withdraw funds from his account at a later stage.
- 3) The buyer also runs the risk that the information will be stored on the database of the seller, and can be compromised if the seller's website is compromised.
- 4) A buyer is submitting his credit card information to a person possibly on the other side of the world, making it difficult to ensure that the buyer is dealing with a serious seller, intending to actually provide a service.

It is preferred that no personal information relating to the buyer should be submitted to the seller.

Because of the risks associated with credit card payment, and issues surrounding direct bank transfer methods for international payments, a number of companies exist that assist an international buyer to pay for purchased goods. The next

section will discuss international money vendors that assist the buyer to securely pay for an international transaction.

7.4. INTERNATIONAL MONEY VENDORS

International money vendors are companies providing a service to international clients to assist in the safe keeping of personal information. If a buyer uses these companies their credit card information is only known to this company (the international money vendor). These international money vendors will usually provide safe online transactions to their clients using SSL.

A whole number of online vendors exist like Bidpay [99], however, in the following section, one of the bigger international money vendors namely PayPal [100] will be discussed.



7.4.1. History of PayPal

Peter Thiel and Max Levchin founded PayPal in 1999 under the name Confinity [108]. The idealistic vision of the company was one of a borderless currency free from governmental controls. However, PayPal's success quickly drew the attention of hackers, scam artists and organized crime groups, who used the service for frauds and money laundering [108]. New security measures stemmed the tide of fraud and customer complaints, but government officials soon stepped in. Regulators and attorney generals in several states, including New York and California, fined PayPal for violations and investigated the company's business practices. Some states, such as Louisiana, banned PayPal from operating in their states altogether. PayPal has since received licenses that allow them to operate in these places [100].

PayPal owes much of its initial growth to eBay buyers who used the service to pay for items and accept payments for their online auctions. PayPal even beat eBay at the online payment business, trumping eBay's in-house payment system Billpoint so thoroughly that in 2002, eBay bought PayPal [109]. eBay phased out Billpoint and integrated PayPal into its services. Sellers with PayPal accounts can place PayPal icons in their auction sites. Buyers can simply click on the PayPal logo to make an immediate payment when the auction is won.

7.4.2. The PayPal mechanism

PayPal is an online payment service allowing individuals and businesses to transfer funds electronically. It allows payments for

- Online auction (e.g. eBay)
- Purchases and services
- Donations
- Transfer of cash for whatever reason to another party.

A basic PayPal account is free. One can send funds to anyone with an e-mail address, whether or not they have a PayPal account. They will get a message from PayPal regarding the funds, and then just have to register their own account, into which the funds can be transferred.

Funds transferred via PayPal stay in a PayPal account until the owner of the funds retrieves them or spends them. If the buyer has entered and verified their bank account information, the funds can be transferred directly into their private bank account. Not all countries allow money to be paid this way. South African citizens can, for this reason, only use PayPal for payment. If money is paid to a South-African citizen, the money will stay in his PayPal account and can be used

for payment of other online transactions. However, the money cannot be paid into a South African citizen's personal bank account. A list of countries that only allows payment from the buyer's account can be found on the PayPal website [100].

Signing up for PayPal is hassle free and does not require one to enter any bank account information, although in various instances a cheque account or credit card is required to use many of PayPal's features. To sign up, on the PayPal homepage, click on the "Sign up Now" button as shown in figure 7.2.



http://www.paypal.com/

Home | Help | Feedback | Previous | Next | Log Out | Copyright | Author

PayPal

[Sign Up](#) | [Log In](#) | [Help](#)

Welcome | **Send Money** | Request Money | Merchant Tools | Auction Tools

Member Log-In

Forgot your Password? [Forgot your Password?](#)


Email Address:

Password:

Join PayPal Today

Now Over 96.2 million accounts

[Learn more about PayPal Worldwide](#)



Go Forward. Go Mobile.

Use your phone to send money and buy things

[Learn more](#)

How PayPal works.

[Learn more](#)

See it. Text it. Buy it. Now.

[Check it out](#)

Buyers

[Send money](#) to anyone with an email address in 55 countries and regions.

PayPal is [free](#) for buyers.

Shop without sharing [financial information](#).

[100% protection](#) against unauthorized payments sent from your account.

eBay Sellers

[Free eBay tools](#) make selling easier.

PayPal works hard to help [protect sellers](#).

PayPal simplifies [shipping and tracking](#).

[Earn cash back](#) with PayPal Preferred Rewards.

Merchants

[Accept credit cards](#) on your website using PayPal.

[Compare our solutions](#) to merchant accounts and gateways.

[Low fees](#) make PayPal the affordable choice.

Learn why PayPal is [good for business](#).

PayPal Mobile

[Learn more](#)

What's New

PayPal Launches Mobile Payments

16 Ways to Promote Your E-Business

Buy or sell worldwide - the safe and easy way

Special Offer

Protect your identity with Equifax

Figure 7.2: PayPal registration

The following pages allow:

1. Choice of account

- Personal, if one intends to utilize it for online purchasing and auctions only
- Business or premier, to accept payments for own business. Upgrade at a later stage is possible.

2. Provision of personal details including security questions in the event one loses one's password.

PayPal provides one with a *.gif (Graphics Interchange Format) picture, with a randomly generated series of letters and numbers which one has to enter. This security step helps prevent fraud and automated fake account generation.

Confirmation of the account by following instructions received by email completes the sign up process.

Buyers and sellers need to be convinced of one's integrity. To achieve this, details of a current credit card with a confirmed statement address are added. This will allow one to utilize PayPal's expanded-use service - such as drawing money directly from the credit card account to pay for auctions.


To utilize the facility to transfer money between one's cheque account and the PayPal account, personal account details are entered, including account and routing numbers. PayPal makes two micro payments (amounting to about \$1) into the account. Unique numbers generated and sent to the private account statement serve as reference numbers to verify the validity of the account. Once the user entered these unique numbers, received on the account statement, the PayPal account is available for payment purposes on the internet.

My Account	Send Money	Request Money	Merchant Tools	Auction Tools	
Overview	Add Funds	Withdraw	History	Resolution Center	Profile

Personal Account Overview

Name: Louw Tait
 Email: paypal@csrau.rau.ac.za (Add email)
 Status: **South African - Verified**

Balance: **\$0.00 USD**

Recent Activity | [All Activity](#) | [Items Won](#) 

Your Recent Activity displays the last day of account activity.

-No New Items-

[Mass Pay](#) | [Referrals](#) | [About Us](#) | [Accounts](#) | [Fees](#) | [Privacy](#) | [Security Center](#) | [Contact Us](#) | [User Agreement](#) | [Developers](#)



[About SSL Certificates](#)

Copyright © 1999-2006 PayPal. All rights reserved.
[Information about FDIC pass-through insurance](#)

Figure 7.3 Verified PayPal Client

Making a payment using PayPal

More than 70 percent of eBay sellers offer PayPal as a payment option, making auctions a major portion of PayPal's business. However, one of the keys to PayPal's success has been its ability to expand beyond the eBay market. One can use it to send money to a friend, donate to a charity, and buy items from online merchants. PayPal has become a major player in driving international electronic commerce.

My Account	Send Money	Request Money	Merchant Tools	Auction Tools
Pay Anyone		Pay for eBay Items		

Send Money Secure Transaction

You can pay anyone with an email address in the 55 countries and regions that accept PayPal.

Recipient's Email:

-OR- Select a recipient

Amount:

Currency: **US Dollars**

Category of Purchase: **- Please Select Type -**

Email Subject (optional):

Note (optional):

Figure 7.4: Making a payment

In order to send money using PayPal, a PayPal client clicks on the **'send money'** tab. In order to send money to a person online, one needs to enter the seller's e-mail address and supply the amount payable (and the currency).

If the buyer's PayPal account has a positive balance the money will be transferred from this account to the seller's PayPal account. In the event of inadequate funds in the buyer's account, PayPal will draw the required amount from the account – credit card or bank account – specified by the buyer during the sign up registration.

After a successful transfer, PayPal will inform the seller by e-mail that the required amount has been paid into his PayPal account.

7.4.3. Advantages of using PayPal

1. Buyer and seller can stay anonymous if they so wish.

2. Neither the buyer nor the seller needs to exchange account information.
3. The process is fast, and the seller will have confirmation of payment for the transaction within minutes.
4. Security is handled by PayPal, and all sessions are encrypted using SSL. Depending on the type of transaction, PayPal forces the seller to supply proof of dispatch or shipping to the buyer.

7.4.4. Disadvantages with PayPal

1. The major disadvantage is the fact that one's PayPal account is only protected by passwords generated by the account holder. The account is at risk of compromise if the passwords fall prey to hacking. Once this occurs, funds in the PayPal account are vulnerable. (Refer to problems relating to passwords discussed in chapter 4.)
2. PayPal acts like a bank, but is not subject to banking regulations. This means that PayPal offers none of the protection registered banks offer, nor is it required to maintain any of the security, customer service or dispute resolution services that banks provide. Similarly, PayPal holds large amounts of customers' money, conducts millions of financial transactions, and even offers credit and debit cards. PayPal was declared not to be a bank by the Federal Insurance Corporation (FDIC) in 2002 as PayPal does not meet the federal definition of a bank, does not hold any physical money, or have a bank charter. PayPal isn't a bank because it doesn't call itself a bank. As a result, most states license PayPal as a "money service."
3. One of the most common problems encountered by PayPal users is the sudden and inexplicable freezing of their accounts. If a PayPal account is frozen, one cannot add or withdraw any funds from the account, and one is required to go through a long, complicated process of identity

verification. Some users claim that PayPal has simply seized their funds and never returned them. Reports by former PayPal employees indicate that this freezing and unfreezing is arbitrary and not subject to serious scrutiny. They claim that company executives view this process as a revenue stream, and that PayPal attempts to recover losses due to fraud by seizing funds from customer accounts [111].

4. Other charges levied against PayPal include [110]:

- A long and confusing Terms of Service Agreement that tricks users into giving up their rights to sue the company and their protections under credit card laws.
- Rude customer service representatives.
- Poor staff appointment practices have led to a number of scams committed as "inside jobs".

Despite these disadvantages, PayPal continues to be the most popular money transfer service for online transactions.

7.5. CONCLUSION

The current electronic commerce environment is protected by passwords and tokens. A buyer needs to be identified to an electronic commerce site (like Amazon, Ebay or PayPal) by means of a user name, and authenticated by means of a password. Once the buyer purchased a product, payment must be effected for this product. A number of options are available to transfer the money to the seller. In all instances the buyer needs to be identified and authenticated, before the money can be transferred.

From this chapter it is evident that if the buyer's username and password are compromised by a hacker, the hacker has access to the buyer's funds.

As mentioned in Chapter 4, all the systems will identify and authenticate the unique username and authenticate the password, provided it is the authentic password. However, the electronic commerce environment can never be assured that the person presenting the username and password is beyond a doubt the authentic user.

The next Chapter will consider the possibility of using biometrics for authentication to overcome the problems associated with passwords and tokens.



Chapter 8: BioVault Version 1.0

8.1. INTRODUCTION

One of the major risks involved in using biometrics for identification and authentication over open public networks is the danger that the biometric data (for instance a fingerprint) can be intercepted and replayed by an unauthorized party. This was successfully demonstrated in Chapter 4. The interception and misuse of biometric data is considered as a major problem; as it is then possible for the hacker to feed the stolen biometric data into the system and become the user masquerading as the user in cyber space, for all practical purposes.

However in chapter 3 it was pointed out that using biometrics can be beneficial for all of the parties involved during identification and authentication, as biometrics are directly related to a person.

Biometrics solves a number of problems related to identification and authentication, but unfortunately introduces additional problems as discussed in chapter 4 and chapter 5. This chapter discusses the first step in solving the problem of biometric data replay.

The reader will be presented with a model known as BioVault that eventually solves a number of problems relating to biometrics, making it possible to use biometrics without the risk of biometric data replay.

The evolution of the different versions of BioVault is covered in Chapters 8, 9 and 10. Each chapter will focus on a different problem related to the problems found in biometric technologies as was discussed in Chapters 4, 5 and 6.

The following table provides an overview of the Chapters that introduced a biometric problem, and the BioVault version that addresses the specific issue.

Biometric issues			BioVault solutions	
Chapter #	Chapter Name	Identified Issue	Chapter #	BioVault version
4	Replay	Biometric data replay	8	Version 1.0
5	Authenticator Duplication	Manufacturing of fake biometric characteristics	9	Version 2.0
5	Authenticator Duplication	Slight altering of biometric data	10	Version 3.0

Table 8.1: BioVault Problem-Solution matrix

This chapter will introduce the first version of BioVault.

8.2. USING BIOMETRIC DATA FOR AUTHENTICATION

If a token or password is used for authentication, only the offered token or password is authenticated. This means that the user presenting this token or password is not directly authenticated. The only reason why the system will consider the user as authentic is because the user was in possession of the authentic token, or because the user knew what the authentic password is.

In order to directly authenticate a user, biometrics will be used in the BioVault system. All practical development on the BioVault system has been done using fingerprint biometrics.

In figure 8.1 it is illustrated how a biometric token can be used for authentication.

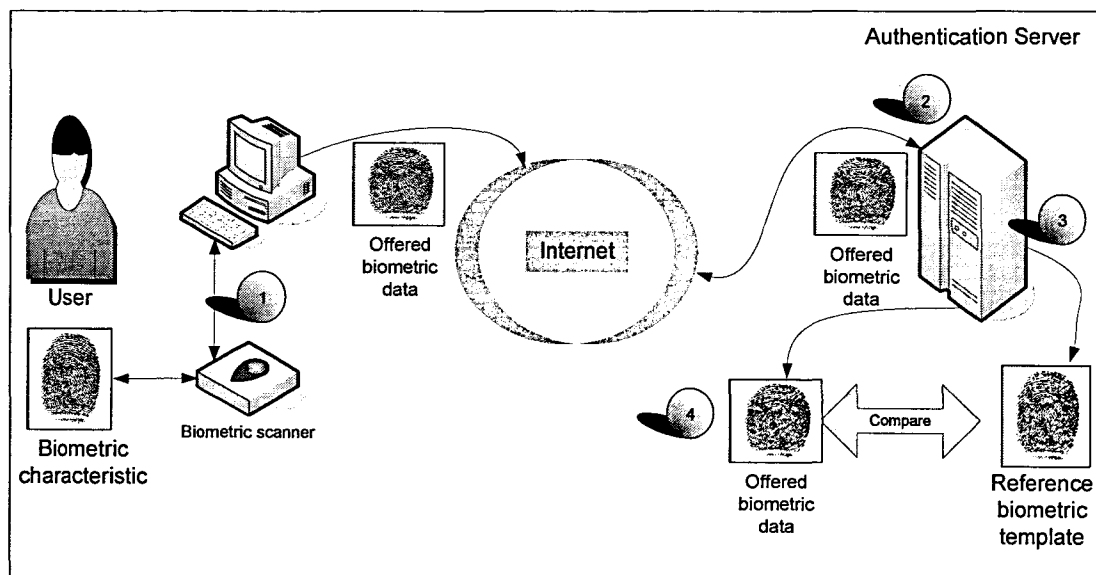


Figure 8.1: Typical network-based biometric authentication.

Step 1

The user offers his fingerprint to the biometric scanner. The scanner will digitize the fingerprint and hand the digitized electronic version of the fingerprint to the driver software of the biometric device.

Step 2

The offered biometric data is submitted via the internet or any networked environment to the authentication server.

Step 3

Once the offered biometric data from the user arrives at the authentication server, the server will fetch the reference biometric template in the user database. The reference biometric template is the template that was stored during the enrollment process.

Step 4

The authentication server will then compare the offered biometric data with the reference biometric template. If the offered biometric data falls within the tolerances defined in the matching algorithm, the system will consider the offered biometric data as the authentic biometric characteristic that was offered. At this stage the authentication server will approve the authenticity of the user.

8.2.1. Conclusion

Biometric data can be used over a networked environment to authenticate a user remotely as illustrated in figure 8.1. However, considering that current network environments rely on Ethernet technology, the biometric data might not be safe during transmission. This possibility is discussed in the next section.

8.3. SNIFFING NETWORK TRANSMITTED BIOMETRIC DATA



If biometric data is sent over a network, the possibility that the biometric data can be successfully sniffed is very high. This scenario is illustrated in figure 8.2.

Step 1

The user offers his fingerprint to the biometric scanner. The scanner will digitize the fingerprint and hand the digitized electronic version of the fingerprint to the driver software of the biometric device.

Step 2

The offered biometric data is submitted via the internet or any networked environment to the authentication server.

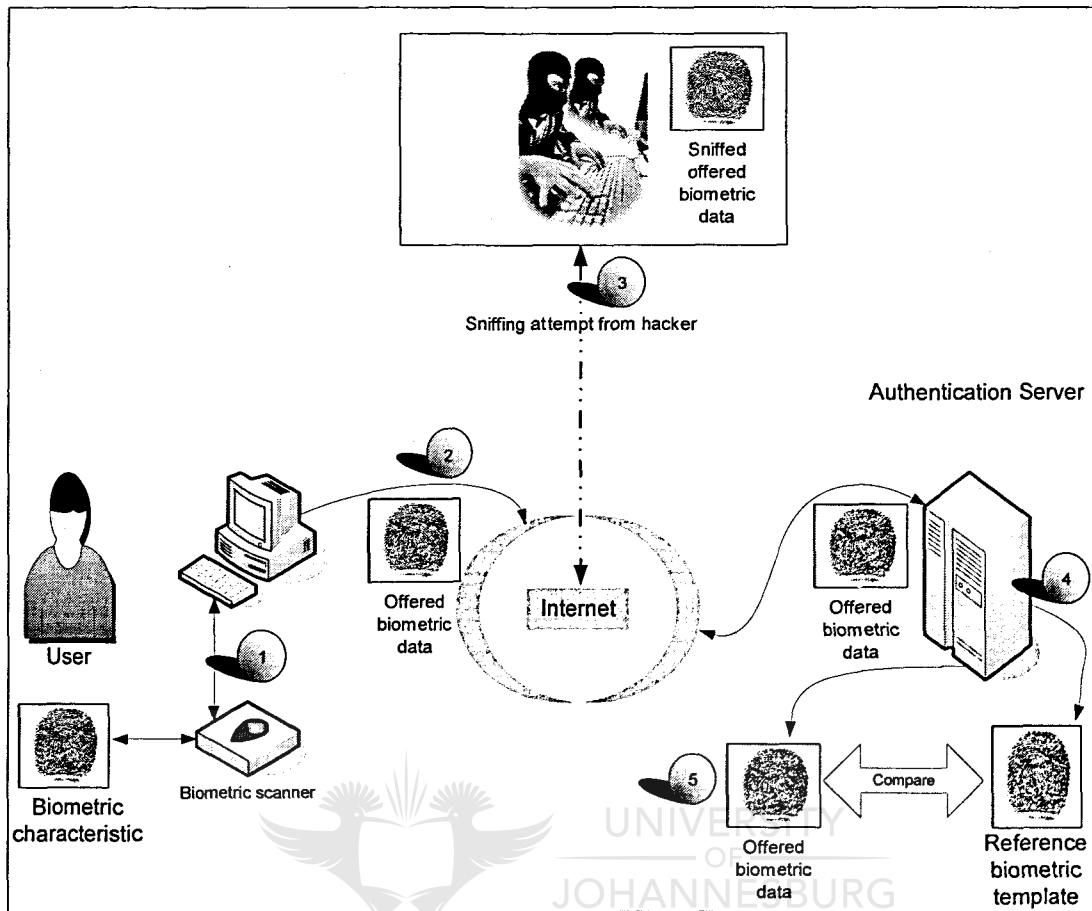


Figure 8.2: Sniffing biometric data transmitted via a network.

Step 3

A hacker monitors the network traffic in promiscuous mode. The hacker collects all the packets submitted by the user, and assembles the network packets. Once the hacker assembled the network packets, he is in possession of the electronic representation of the user's biometric characteristic. However, the hacker did not disconnect the user from the server and for this reason the communication between the user and the authentication server continues as usual in step 4.

Step 4

Once the offered biometric data from the user arrives at the authentication server, the server will fetch the reference biometric template in the user

database. The reference biometric template is the template that was stored during the enrollment process.

Step 5

The authentication server will then compare the offered biometric data with the reference biometric template. If the offered biometric data falls within the tolerances defined in the matching algorithm, the system will consider the offered biometric data as the authentic biometric characteristic that was offered. At this stage the authentication server will approve the authenticity of the user.

8.3.1. Conclusion

If biometric data is used as a method to authenticate a user over a networked environment, it is possible that once the biometric characteristic is converted to electronic data, the biometric data can be sniffed while it traverses the network. In Chapter 4 it was demonstrated that a password can also be sniffed during network transmission.

However, if a password is compromised during a network sniffing attempt, the compromised password can be replaced by a new one. If biometric data is compromised during a network sniffing attempt, this compromised biometric characteristic cannot be merely replaced by a new one.

The fact that a hacker has a copy of the user's biometric data is not the problem as such. The fact that he re-uses this biometric data (replay of this data) is the main problem in this regard.

In order to overcome this problem, a method must be identified to detect replay of biometric data. The first version of BioVault has been developed to detect replay, and is subsequently discussed in the following section.

8.4. DETECTING REPLAY OF AUTHENTICATION DATA

In order to solve the problems faced with the replay of biometric authentication data it would be a beneficial if an authentication server could have the ability to detect replay. Once the server detects replay the server could automatically reject the whole transaction, meaning that money is not lost by the account holder.

8.5. USING ASYMMETRY TO DETECT REPLAY

It was demonstrated in the chapter 4 that in any environment it is possible to gain access to an authentication token and replay it, in order to be falsely accepted as the authentic owner of the given token.

All this is possible for both the symmetric and asymmetric tokens that were discussed earlier. However, this chapter will demonstrate how the authentication server could identify a replay attempt of biometric data.

Passwords and tokens are symmetric authentication mechanisms. Whenever symmetric mechanisms are to be used, the fact remains that a symmetric match must be truly symmetric, thus a 100% correlation is expected between a stored password and a presented password. For this reason it is difficult to discover a possible replay of symmetric authentication mechanisms like passwords and tokens.

On the other hand, if asymmetric technologies like biometrics are considered, it is possible to identify replay. A match between the reference biometric template stored in the database, and the offered biometric data presented by the user, are unlikely to be exactly (100%) the same.

The detection of replay will be discussed in the following section.

8.6. DETECT REPLAY IN AN ASYMMETRIC ENVIRONMENT

The asymmetry of biometric data provides the world with a unique benefit: All biometric data received from a user's biometric characteristic will almost always be unique.

The fact that biometric data is uniquely identifiable is the first principle used by BioVault to prevent the possibility of replay of biometric data.

Thus, this aspect of biometrics provides the environment with the ability to identify all biometric data received. Thus each instance of accepted biometric data can be linked to a given transaction performed by the user. Furthermore it is now possible to record biometric data as it is received from a user, and then check if the same biometric data was ever received before.

In figure 8.3, BioVault version 1.0 is illustrated. This version of BioVault endeavors to solve the problem of replay of an electronic representation of biometric data. A number of components are introduced into the environment of BioVault version 1.0 and is discussed before the mechanism of the model is discussed.

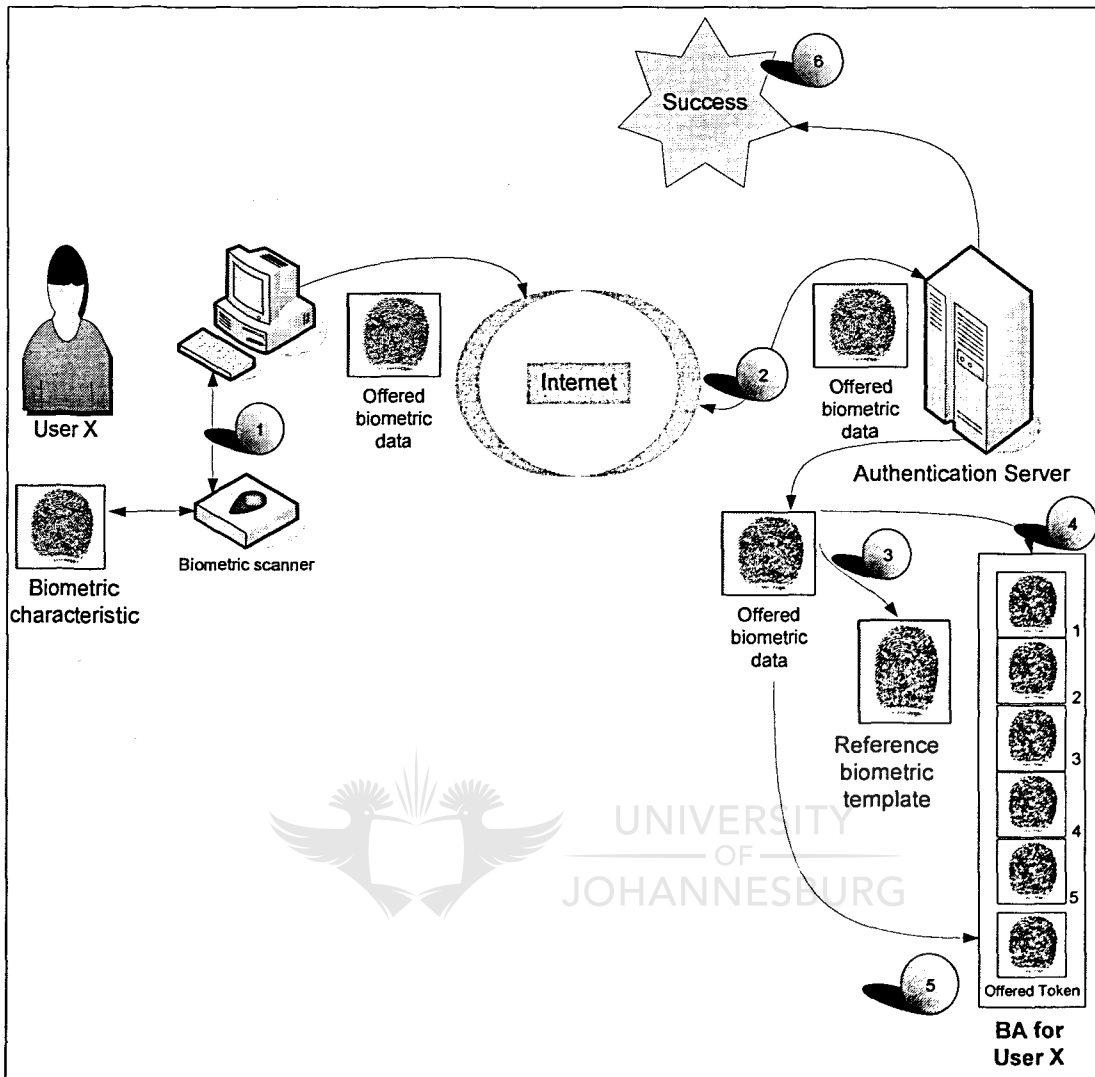


Figure 8.3: BioVault version 1.0

8.6.1. The Bio Archive (BA)

As illustrated in figure 8.3, a BA is introduced for the user on the authentication server. This BA will store previously offered biometric data used by the user, which was successfully authenticated by the matching algorithm. In BioVault version 1, the BA is stored only on the server.

The bio archive will assist in the identification of possible replay attacks. For this reason access to the biometric data stored in the BA must be very fast. To

ensure that specific biometric data inside the BA can be found fast, the BA will be sorted. If the BA is sorted, a binary search algorithm can be used to find biometric data in the BA efficiently.

8.6.2. The working of BioVault version 1.0

Step 1

As illustrated in figure 8.3 the user must offer his fingerprint to the biometric scanner. The scanner will digitize the fingerprint and pass the digitized electronic version of the fingerprint to the driver software of the biometric device.

Step 2

The offered biometric data is submitted via the internet or any networked environment to the authentication server.

Step 3

Once the offered biometric data from the user arrives at the authentication server, the server will fetch the reference biometric template stored in the user database. The reference biometric template is the template that was stored during the enrollment process. The authentication server will compare the offered biometric data with the reference biometric template. If the offered biometric data falls within the tolerances defined in the matching algorithm, the system will accept the biometric data provisionally as authentic, and proceed to step 4.

Step 4

The authentication server will compare the offered biometric data to all previously received biometric data stored in the BA. If an exact match is found between the offered biometric data and any biometric data in the BA, the authentication server will reject the authenticity of the offered biometric data, as a 100% match of

biometric data is highly unlikely, and indicates with high probability, a replay situation.

Step 5

However, if an exact match is not found in the BA, the authentication server will add the newly received biometric data to the user's BA for future usage, as illustrated in step 5 of figure 8.3.

Step 6

Once BioVault version 1.0 is satisfied with the authenticity of the offered biometric data, and also convinced that the offered biometric data is not electronically replayed biometric data (illicit biometric data), the server will send back a "successful" result to the user.

The next section will demonstrate how BioVault version 1.0 will detect replay of sniffed biometric data.



8.7. REPLAY DETECTION BY BIOVAULT

In this section it will be discussed how BioVault will detect replay of illicit biometric data when presented by a hacker. In order to detect replay, symmetry will assist the authentication server to detect the replayed token. This process is illustrated in Figure 8.4.

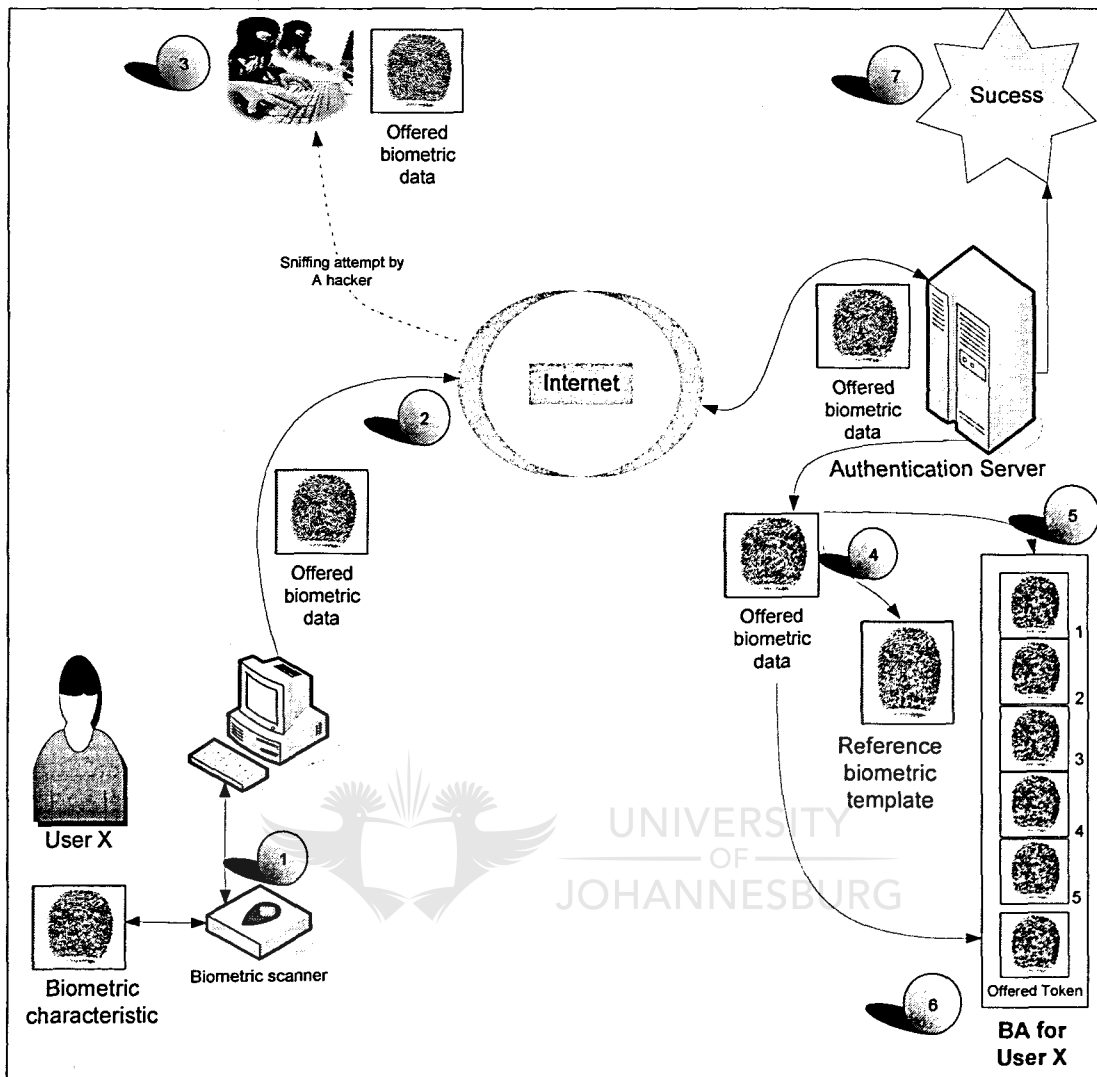


Figure 8.4: Sniffing attempt by a hacker

Figure 8.4 follows the actions of figure 8.3. However in figure 8.4 it is shown that a hacker sniffed the network while the biometric data was sent over the network. The following scenario is illustrated in Figure 8.4.

Step 1

As illustrated in figure 8.3 the user must offer his fingerprint to the biometric scanner. The scanner will digitize the fingerprint and pass the digitized electronic version of the fingerprint to the driver software of the biometric device.

Step 2

The offered biometric data is submitted via the internet or any networked environment to the authentication server.

Step 3

A hacker sniffs all the packets that the user submits over the network, and re-assembles these packets to get the electronic representation of the offered biometric data. However, the hacker does not interfere with the authentication process of the user, and the process continues as normal with step 4.

Step 4

Once the offered biometric data from the user arrives at the authentication server, the server will fetch the reference biometric template stored in the user database. The reference biometric template is the template that was stored during the enrollment process. The authentication server will then compare the offered biometric data with the reference biometric template. If the offered biometric data falls within the tolerances defined in the matching algorithm, the system will accept the biometric data provisionally as authentic, and proceed to step 5.

Step 5

The authentication server will compare the offered biometric data to all previously received biometric data stored in the BA. If an exact match is found between the offered biometric data and any biometric data in the BA, the authentication server will reject the authenticity of the offered biometric data, as a 100% match of biometric data is highly unlikely, and indicates with a high probability, a replay situation.

Step 6

However, if an exact match is not found in the BA, the authentication server will add the newly received biometric data to the user's BA for future usage, as illustrated in step 7.

Step 7

Once BioVault version 1.0 is satisfied with the authenticity of the offered biometric data, and now convinced that the offered biometric data is not electronically replayed biometric data (illicit biometric data), the server will send back a "successful" result to the user.

At this stage, the user has been successfully authenticated. Unfortunately, without the knowledge of the user or the authentication server, a hacker managed to acquire the biometric data during transmission from the terminal to the server. This electronic biometric data is then stored by the hacker and can then be used to be falsely authenticated in the future, by replaying this biometric data.

Fortunately, BioVault version 1.0 has the ability to detect this type of replay attempt, as illustrated in figure 8.5.

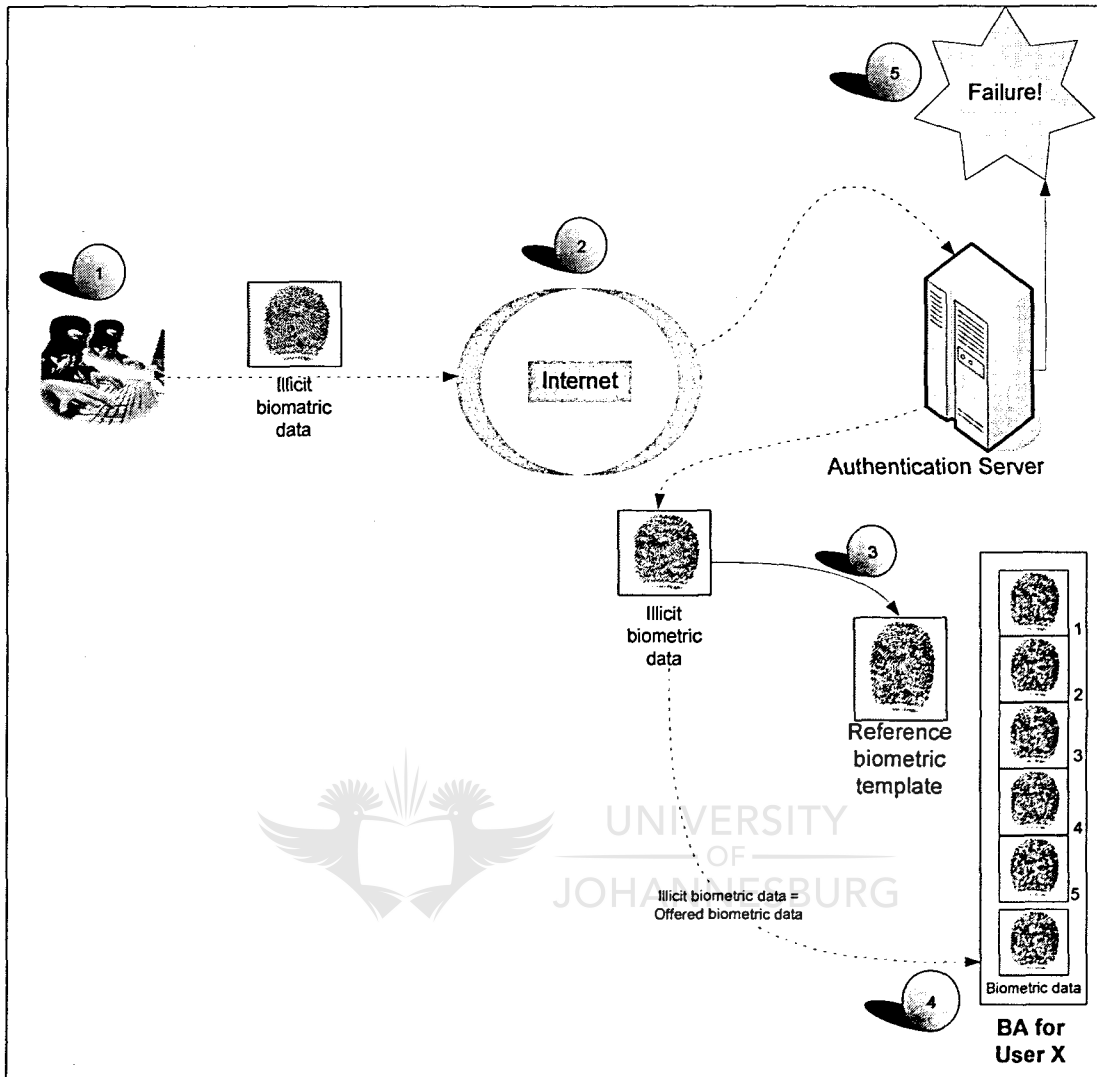


Figure 8.5: Detection of replay

Step 1

The Hacker fetches the stored biometric data and contacts the authentication server.

Step 2

The Hacker replays the illicit biometric data via the internet or networked environment to the authentication server.

Step 3

Once the illicit biometric data from the hacker arrives at the authentication server, the server will fetch the reference biometric template from the user database. The reference biometric template is the template that was stored during the enrollment process.

The authentication server compares the illicit biometric data with the reference biometric template. Considering that the illicit biometric data is 100% the same as the previously offered biometric data, and that it was previously accepted as authentic, the authentication server will once again accept the illicit biometric data provisionally as authentic, and proceed to step 4.

Step 4

The authentication server compares the illicit biometric data to all biometric data stored in the BA. At this stage an exact match will indeed be found in the BA (more specifically in this case, the previously offered biometric data from the user). This will cause the authentication server to suspect a possible replay attempt of biometric data, and reject the illicit biometric data.

Step 5

Considering that an exact match was found in the BA, the authentication server will immediately cause rejection of the illicit biometric data, resulting in an authentication failure.

The fact of the matter remains that there is a small possibility that a 100% match is possible between offered biometric data. To ensure that the user has the opportunity to prove authenticity in the unlikely event of an authentic 100% match, the server will request a fresh biometric token from the user.

8.7.1. Conclusion

Biometrics has the ability to be measured in two distinct ways, not possible with any other authentication approaches.

1. *Firstly, does the biometric data offered, deviate from the reference biometric template found in the server's database?*

If a user presents biometric data, the system will usually determine whether the presented biometric data is within acceptable deviation of the reference biometric data. This means that offered biometric data must fall within the tolerances as defined by the rules governing acceptable FAR and FRR, as discussed in Chapter 3 sections 3.4.4.1 and 3.4.4.2.

2. *Secondly, does the offered biometric data match any previously presented biometric data exactly (100%)?*

Usually biometric data does not get tested for an exact match with the reference biometric template, or even any other offered biometric data that was used in the past. However, as proposed by the BioVault version 1.0, if previously offered biometric data was stored in a database (BA), the system could test if newly presented biometric data matches any previously presented biometric data 100%. If a 100% match is found the possibility of a biometric replay attack is almost confirmed. However, it is possible, but unlikely that freshly offered biometric data might match 100%, mainly due to hardware devices that are not sensitive enough. This is obviously not a major problem. In the unlikely instances that a 100% match is indeed found from authentic fresh biometric data, the server would simply request fresh biometric data to be sent by the user immediately. An authentic user will be able to offer unlimited fresh biometric data without any problem.

8.8. EVALUATION OF BIOVAULT VERSION 1.0

Considering the above mentioned discussion of the initial BioVault, we can conclude that the following observations can be made on the existing authentication approaches that utilize passwords and token technologies:

- 1) Transactions are identifiable; each transaction is linked to specific and unique biometric data.
- 2) It is possible to identify replayed biometric data, because of the asymmetric nature of biometrics. Keep in mind that it is not possible to identify a replayed password – an authentic user actually constantly replays the exact same password.
- 3) Hacker attempts can be noted in a log file as possible hacker attempts and, the biometric data in question can also be placed in a ban list. Thus whenever biometric data is offered, the system will test for a 100% match. If a 100% match is found, this biometric data can be originating from a hacker, and subsequently placed in a ban database, that will monitor further attempts to replay this illicit biometric data.
- 4) Using biometrics, the user is directly authenticated, and not only the token or password being presented.
- 5) If passwords and tokens are used, the system expects a 100% match with the password and token, for authentication to be successful. This makes it impossible to detect the replay of a password or to detect a false token. If the password is exactly the same as the password stored, the system will consider the password as authentic.

8.9. CRITICAL LOOK AT BIOVAULT VERSION 1.0

The BioVault version 1.0 uses symmetry and asymmetry to identify biometric data. This principle is used as an initial starting point to identify possible re-played biometric data.

After the initial development and testing of BioVault version 1.0 the following problems were discovered, and will receive attention in the following chapters:

- 1) It is possible for a hacker to alter the sniffed biometric data just enough to prevent a 100% match with the BA, but still be accepted by the matching algorithm (thus the illicit biometric data does not match 100% with any previously offered biometric data in the BA, but still falls within acceptable tolerances of the matching algorithm).
- 2) The second major problem is the possibility of sourcing a latent biometric image of a person's biometric characteristic. Keep in mind that we constantly interact with our environment, leaving behind much latent usable biometric information. During the research of BioVault, it was demonstrated that for instance fingerprints can be collected from a glass, and a paper-thin latex overlay can be made from the latent fingerprint left on the glass. This is a major problem. It is possible for a hacker to gather biometric information residing outside the BioVault system. This was demonstrated in Chapter 5, relating to authenticator duplication. The classical example is a latex fingerprint used as an overlay on a hacker's finger.

If a hacker creates a fake biometric characteristic (for example a latex fingerprint) from a latent biometric image on a glass, the hacker would have an unlimited supply of biometric data, not yet stored in the BA.

An effort was made in the past by other parties to patent [112] the concept as proposed by BioVault version 1.0 as a possible solution to detect replay. This patent was discovered during a similar patent proposal from the research team that worked on BioVault. Due to the latent biometric images that can be used to generate a fake biometric characteristic, this patent is actually useless. Keep in mind that the hacker now has an unlimited supply of biometric characteristics to generate illicit biometric data that will be unique and not be found in the BA. This fake biometric characteristic would however still be acceptable to the biometric matching algorithm as discussed in chapter 4.

8.10. CONCLUSION

It is clear that it is possible to uniquely identify biometric data by means of their asymmetric nature. This provides an initial step towards assistance in identifying replay attacks. Unfortunately this method, as suggested in the proposed patent [112] and furthermore described as BioVault version 1.0, is not sufficient to solve the problem related to slight biometric data altering or fake biometric characteristics that are generated from latent biometric images outside the BioVault environment (manufacturing a fake biometric characteristic from latent biometric images).

Electronic commerce will only be really secure once biometrics becomes part of the environment. However, a solution is needed to solve problems currently experienced when the use of biometrics in the electronic environment is to be considered. The problems relating to biometric replay were pointed out in chapter 4, and problems relating to biometric authenticator duplication were pointed out in chapter 5.

BioVault version 1.0 successfully solves the problems associated with biometric data replay.

Biometric issues			BioVault solutions		
Chapter #	Chapter Name	Identified Issue	Chapter #	BioVault version	Completed
4	Replay	Biometric data replay	8	Version 1.0	<input checked="" type="checkbox"/>
5	Authenticator Duplication	Manufacturing of fake biometric characteristics	9	Version 2.0	<input type="checkbox"/>
5	Authenticator Duplication	Slight altering of biometric data	10	Version 3.0	<input type="checkbox"/>

Table 8.2: BioVault Problem-Solution matrix, version 1.0

Yet, a number of problems still exist; these problems include altering electronic biometric data to subvert the BA on the server and manufacturing a fake biometric characteristic from the user's environment, to be subsequently used for false authentication.

The next chapter will introduce BioVault version 2.0.

BioVault version 2.0 will focus on solving the problems related to fake biometric characteristics, as discussed in chapter 5.

Chapter 9: BioVault Version 2.0

9.1. INTRODUCTION

Chapter 8 focused on a solution to the problems related to the replay of the electronic presentation of biometric data. As Chapter 8 concluded, electronic replay is the first hurdle on the track of successfully implementing biometrics for authentication.

Biometric issues			BioVault solutions	
Chapter #	Chapter Name	Identified Issue	Chapter #	BioVault version
4	Replay	Biometric data replay	8	Version 1.0
5	Authenticator Duplication	Manufacturing of fake biometric characteristics	9	Version 2.0
5	Authenticator Duplication	Slight altering of biometric data	10	Version 3.0

Table 9.1: BioVault Problem-Solution matrix

One major flaw that is constantly overlooked using biometric technologies when biometrics is considered as an identification and authentication mechanism, is man's interaction with the environment.

This defect in biometric technology was pointed out in chapter 5. Humans leave latent biometrics images behind as they interact with the environment. People leave latent biometrics images behind unintentionally for example, fingerprints on things they touch and hair loss (it is estimated that an individual loses roughly 150 to 200 hair strands daily [113], containing human DNA.) Unless absurd measures are taken to isolate a person from the environment, he/ she is bound to leave latent biometrics images behind. This chapter illustrates how a

newer version of BioVault solves the problems associated with latent biometric images.

9.1.1. Biometric data protection

As pointed out in the previous chapter, if BioVault version 1.0 is to be utilized, the system is capable to detect biometric data being replayed. Due to the asymmetry of biometric data, it is unlikely that any offered biometric data will match any previously offered biometric data totally. This deviation is anticipated, and as such evaluated by the biometric matching algorithm. Depending on the technology used, current matching algorithms will accept a similarity between the reference biometric template and the offered biometric data of 95% to 100% as an adequate match. Although a 100% match is unlikely, currently used algorithms do not consider a 100% match as irregular. BioVault version 1.0 introduced a Bio-archive (BA) to assist in replay detection of previously offered biometric data.



9.1.2. Avoiding an exact biometric match

Chapter 8 concluded that BioVault version 1.0 had two problems that render it fallible.

1. Sniffed biometric data could be altered slightly by a hacker to prevent a 100% match within the BA of the server, but slight enough to stay within the acceptable variance of the matching algorithm. BioVault version 2.0, discussed in this chapter addresses this problem to a certain extent. BioVault version 3.0 amplified in chapter 10, finally solves the debility.
2. Latent biometric images for example fingerprints left on surfaces touched by a user can be lifted and duplicated onto a thin latex mould. During the

research of BioVault it was proved that this overlay can subsequently be used to be illicitly authenticated as the user that left the fingerprint image behind. The fact that the creator of the latex overlay now has the means to supply an unlimited number of illicit biometric data, poses an immense problem. The hacker does not replay any sniffed biometric data of previously offered biometric data from the user. With the fake biometric characteristic at his disposal, the hacker can be authenticated by offering illicit biometric data that will not match any previously offered biometric data in the BA 100%. It was also demonstrated that matching algorithms, will accept the fingerprint digitized from a latex finger as authentic [56], [57]. Considering that the illicit biometric data conforms to the rules of the matching algorithm, BioVault version 1.0 will assume that the fake biometric characteristic is indeed authentic.

Chapter 4 demonstrated that biometric data can be sniffed or acquired in electronic format and then be replayed at a later stage. BioVault version 1.0 as discussed in chapter 8 solved this problem.

This chapter offers a strategy as a first line of defense against biometric characteristic duplication. Chapter 5 focused on authenticator duplication and offered conclusive proof that biometric characteristics can be duplicated as readily as any other manufactured token.

BioVault version 2.0 discussed in this chapter will deal with a solution to circumvent biometric characteristic duplication.

9.2. LATENT BIOMETRIC CHARACTERISTICS AND BIOVAULT

As mentioned in chapter 8, BioVault version 1.0 solved the problem of replay by keeping a Bio-archive (BA) on the server of all biometric data presented by a user. This allowed the system to detect a replay attempt, by simply comparing newly presented biometric data against the previously offered biometric data stored on the authentication server's Bio-archive file.

In the sections to follow, it will be illustrated, how a hacker could subvert BioVault version 1.0, by acquiring a latent biometric image from the user's environment.

9.2.1. Biometric characteristic acquisition

Figure 9.1 illustrates one possible scenario a hacker could pursue to acquire a biometric characteristic from the user's environment. The example presented in figure 9.1, has been personally duplicated and tested by the author. This method was first proposed by Prof T. Matsumoto [3], [55].

The first step in creating a fake biometric characteristic is to acquire a latent biometric image that the user left behind. This is illustrated in figure 9.1.

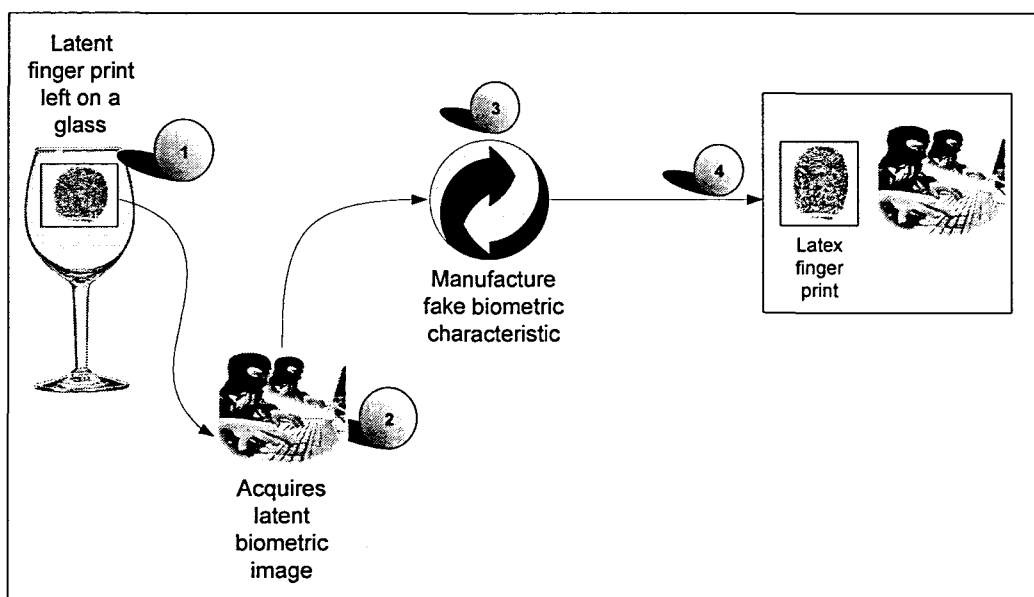


Figure 9.1: Acquisition of latent biometric image

Figure 9.1 illustrates how a hacker could acquire a biometric characteristic that a user left on a glass.



Step 1

The user handles a glass, and leaves a fingerprint on the glass. This is, as already mentioned, referred to as a latent biometric image.

Step 2

The hacker takes the glass and carefully lifts and digitizes the latent biometric image, using the methods discussed in chapter 5, section 5.2.2.

Step 3

Once the latent biometric image has been digitized, the hacker has a number of methods and a number of materials to his disposal to generate a fake biometric characteristic. In this example the hacker generated a latex finger.

Step 4

In the last step, the hacker is now in possession of a latex finger, which can be used to spoof biometric devices whenever needed.

9.2.2. Misuse of fake biometric characteristic

During the research of this thesis and work done by a number of other researchers [55], it was proved that a biometric characteristic can successfully be acquired from the user's environment and subsequently a fake biometric characteristic can be manufactured. This was illustrated in figure 9.1.

The following section will demonstrate how this fake biometric characteristic can be used to subvert the mechanism of BioVault version 1.0

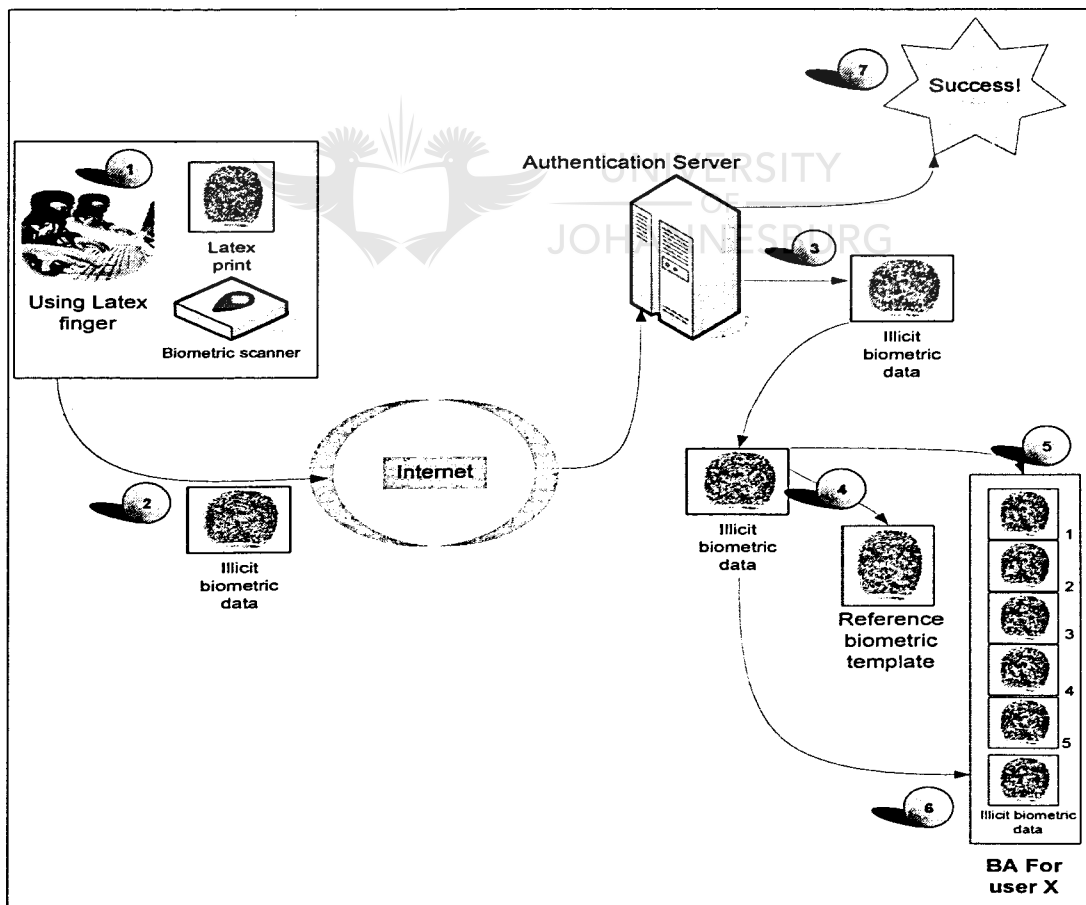


Figure 9.2. Misuse of fake biometric characteristic

Step 1.

The hacker presents the latex finger he created, to the biometric scanner. The scanner digitizes the latex biometric finger, resulting in illicit biometric data, to be prepared for sending to the authentication server.

Step 2.

This illicit biometric data is then sent via the internet to the authentication server running the BioVault version 1.0 system.

Step 3.

Once the illicit biometric data from the user arrives at the authentication server, the server obtains the reference biometric template stored in the user database. The reference biometric template is the template that was stored during the enrollment process.

Step 4.

The authentication server compares the offered, illicit biometric data with the reference biometric template. Considering that the illicit biometric data that was generated from a latent biometric image of user X, are now being compared with the reference biometric template, the system will match the illicit biometric data to the reference biometric template, as was discovered during the research of this thesis. The system will accept the illicit biometric data provisionally as authentic, and proceed to step 5.

Step 5.

BioVault version 1.0 compares the illicit biometric data with all the biometric data stored in the BA of user X. The illicit biometric data is not an electronic replay (as

discussed in chapter 8). BioVault version 1.0 does not find a 100% match in the BA, and adds the illicit biometric data to the BA of user X.

Step 6.

The illicit biometric data accepted by the matching algorithm and a comparison to all the biometric data in the BA of user X, yields a successful authentication response from BioVault version 1.0 as the illicit biometric data passed the checks built into BioVault version 1.0. The hacker has thus, successfully spoofed BioVault version 1.0!

Considering that the hacker managed to subvert BioVault version 1.0, the hacker now has the ability to trade as user X, whenever the need arises. BioVault version 1.0 will not find an exact match in the BA, and the matching algorithm will match the latex biometric print in exactly the same way, the authentic user's biometric data, gets matched.



UNIVERSITY
OF
JOHANNESBURG

9.3. BIOVAULT VERSION 2.0

BioVault version 1.0 can detect electronic replay of the biometric data sent via a network. However biometric devices can be spoofed with a fake biometric characteristic, generated from latent biometric images left by users during interaction with their environment. As demonstrated in section 9.2.2, a hacker can spoof BioVault version 1.0 by employing a fake biometric characteristic. This fake biometric characteristic allows the hacker an unlimited supply of illicit biometric data to be generated, that will be accepted by the biometric matching algorithms.

A second version of BioVault was developed through profound research to protect the environment against biometric data not conforming to the rules established for BioVault version 1.0.

Symmetry and asymmetry, as discussed in chapter 6, play a vital role in the solution, as it allows the system to uniquely identify all offered biometric data. Symmetry and asymmetry are used in conjunction with each other, to protect biometric data.

In chapter 8, the SBA was introduced; the next section considers a new addition to the BioVault system, known as the client-side Bio-archive.

9.3.1. The client-side Bio-archive (CBA)

BioVault version 2.0 introduces the concept of a client-based bio-archive (CBA). At the outset this bio-archive will consist of a limited number of previously used biometric data of the specific user. The larger this bio-archive the more effective the system will be.

Additionally, the biometric data in this CBA is totally random and provided to the CBA by the authentication server. The authentication server will populate the CBA from time to time with different previously offered biometric data of the given user.

During enrollment the authentication server will request a number of biometric data from the user, in order to populate the SBA and CBA for initial utilization by BioVault version 2.0.

Whenever a secure connection is established between the user and the authentication server, the CBA can be updated. However it is expedient that the

CBA is updated under a rigorously controlled environment. In other words, the CBA can be updated by the authentication server, whenever a user visits a bank or ATM machine, as an example.

The server bio-archive will henceforth be referred to as the Server Bio-Archive (SBA), for clarity.

9.3.1.1. CBA storage

The Bio-Archive that the user will use, will store previously offered biometric data. The following can be used to store the CBA:

- 1) A USB flash memory – These tiny appliances like the Micro SD memory, presently offer surprisingly large storage space with storage sizes reaching 64Gb [114], furthermore, no additional equipment will be needed to integrate this technology into the environment.
- 2) A Smart card –These devices however need additional equipment and storage capacity on smartcards is limited.
- 3) A subcutaneous microchip – This technology ensures that a person cannot forget or misplace his CBA, but workable and acceptable solutions are still in development. Storage capacity is limited and technology is controversial [115], [116].

9.3.2. Mechanisms of BioVault version 2.0

BioVault version 2.0 is based on BioVault version 1.0. Consequently it uses the same components as defined in the previous chapter. The only addition to the existing model is a client side bio-archive (CBA). Besides the CBA, BioVault version 2.0 requires a specific methodical procedure, and will now be explained.

Figure 9.3 illustrates the mechanism of the BioVault version 2.0.

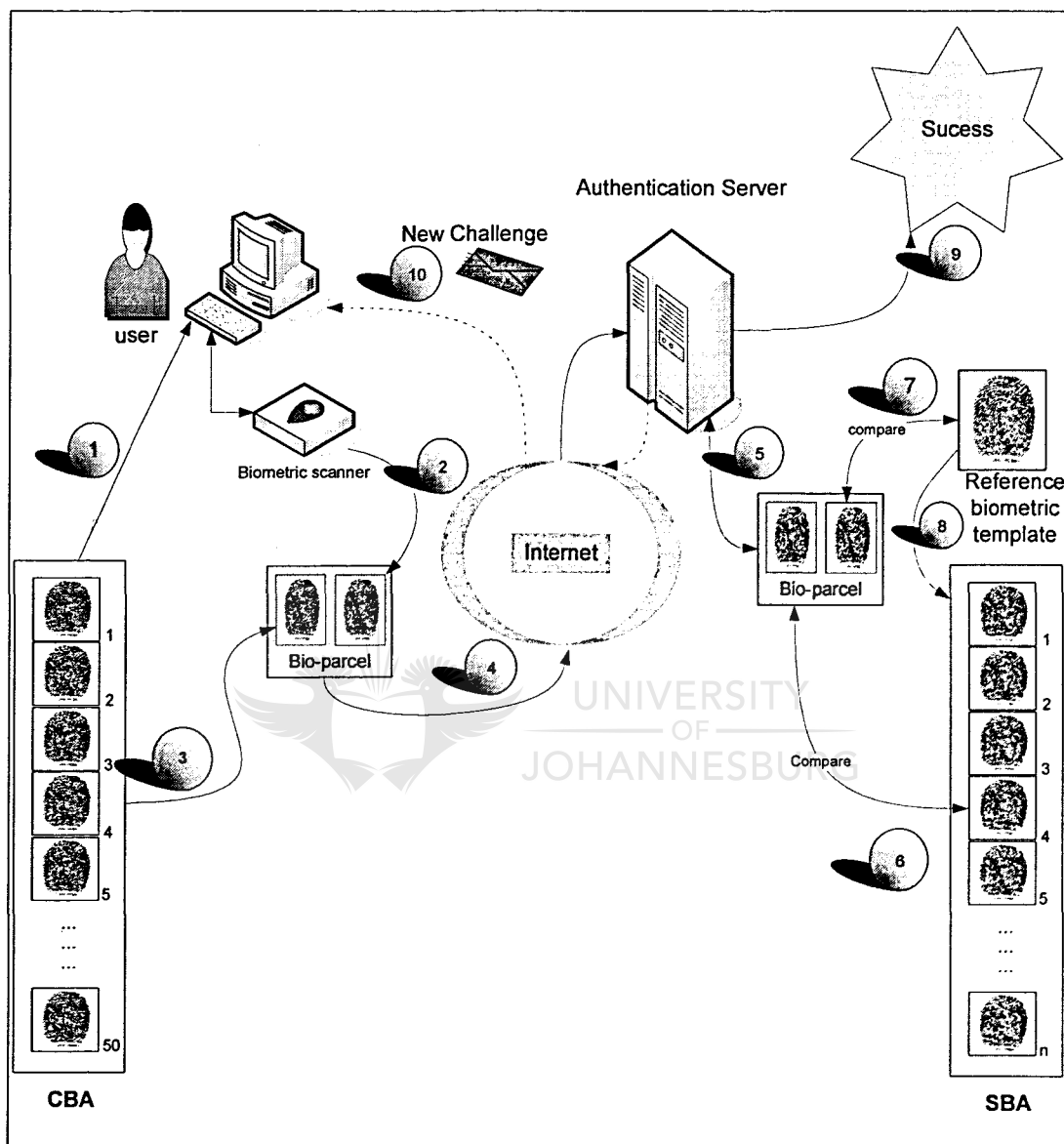


Figure 9.3: BioVault version 2.0

As illustrated in figure 9.3, a client side bio-archive (CBA) has been introduced to the system. As an example as illustrated in figure 9.3, this CBA would contain 50 randomly picked biometric data from the server's BA (SBA) of this particular client. The usage of 50 randomly picked biometric data is only a token value, and

only used in the thesis as an example. The SBA on the server still includes all biometric data ever offered by the client since his or her introduction to the system. The SBA provides the biometric data used in BioVault version 2.0 to populate the CBA. This population is done totally random. As will soon be discussed, these randomly selected biometric data of the user, will serve as a special key, and can be compared to the mechanism of a onetime pad.

Step 1 (As in figure 9.3)

When a user needs to be authenticated the user attaches the appliance containing the CBA with the previously offered biometric data to the terminal (for example the user's computer or ATM machine), where he intends to do the transaction.

Step 2

The user will provide a fresh biometric characteristic as shown, directly to the biometric scanner. The scanner will digitize the biometric characteristic and forward the biometric data to the driver software of the biometric device.

Step 3

The Client hardware offers a bio-parcel containing the biometric data from:

- 1) The freshly provided biometric data received from the biometric scanner
- 2) A biometric from the CBA that was challenged by the authentication server during the previous authentication encounter.

In this example the authentication server requested the 4th biometric data in the CBA to be supplied. BioVault version 2.0 will thus automatically include the 4th biometric data from the user's personal BA into a bio-parcel as shown in step 3.

The bio-parcel, that now includes 2 separate biometric data, (freshly digitized biometric data and an old biometric data from the user's CBA), will be submitted.

Step 4

The biometric bio-parcel is submitted via the internet or any networked environment to the authentication server.

Step 5

Once the server receives the bio-parcel, the server separates the freshly offered biometric data from the requested biometric data.

Step 6

During this step BioVault version 2.0 must first ensure that the expected old biometric data requested during the previous communication is supplied by the user. In this step a symmetric match will be performed, thus the server will need a 100% match as shown in step 5, between the requested biometric data and the biometric data in the SBA. If the old biometric data supplied from the user's CBA does not match 100% with the requested biometric data in the SBA, authentication fails immediately at this point.

Step 7

Once the server successfully symmetrically matched the forwarded anticipated challenge, the server asymmetrically matches the freshly offered biometric data from the user with the reference biometric template in the database. If the offered biometric data falls within the tolerances defined in the matching algorithm, the system will accept the biometric data provisionally as authentic, and proceed to step 8.

Step 8

The server checks the SBA to ensure that the freshly supplied biometric token is not any biometric data that is replayed, as discussed in chapter 8. The authentication server will compare the offered biometric data to all previously offered biometric data stored in the SBA. If an exact match is found, the authentication server will reject the authenticity of the biometric data, as a 100% exact match of biometric data at this stage is unlikely.

Step 9

If the bio-parcel passed all the requirements, authentication is successful. The freshly received biometric data is added to the existing biometric data in the SBA.

Step 10

The server will subsequently generate a new challenge. This challenge is randomly selected from the possible biometric data currently in the CBA of the user, and must thus fall between 1 and the number of biometric data that is stored in the CBA of the user. In the illustrated example the number would need to be between 1 and 50. This means that the server might, for example, generate 37. This challenge generated is submitted back to the user.

This challenge is then kept for the next time that the user communicates with the authentication server, so that the user's hardware can supply the 37th biometric data from the CBA to the authentication server on request.

9.3.3. Discussion of the BioVault version 2.0 approach

A number of tests have been done on the protocol. The protocol ensures that a person using a latex finger print will not be successfully authenticated. In order to generate the anticipated biometric data, to be sent to the authentication

server, a hacker would need the following to generate the bio-parcel expected by the authentication server:

- A latex finger print,
- The correct challenge generated by the authentication server during previous communication in order to determine,
- The correct old biometric data requested by the authentication server.

One can make the following observations without fear of contradiction:

1. This approach doubles the size of the authentication parcel submitted via the network. For certain biometric characteristics, this will not really be a problem. For example, hand geometry biometric is approximately 72 bits in total [117]. However, for other biometric technologies, this may result in a very large bio-parcel. For example, a biometric voice sample is approximately 100kb per second [36].
2. The fresh biometric data and the old biometric data are sent un-encrypted. In the event that a hacker sniffs and intercepts the bio-parcel, the contents can be extracted. There is not too much that the hacker can do with the bio-parcel, as this parcel is only valid for one transaction.
3. A dedicated hacker can theoretically build a database of a particular user by intercepting the biometric data that the user forwards during various transactions. This will be addressed in chapter 10.
4. Outside the BioVault version 2.0 approach, the hacker can generate new biometric data; all biometric characteristics are translated into electronic presentation, as noted in chapter 4. A hacker can alter the biometric data slightly. The mechanisms of BioVault version 1.0 will accept this altered biometric data as it does not constitute a symmetric match to any tokens in the SBA.

5. The BioVault version 2.0 approach would require a hacker to obtain the challenged biometric data, in order to generate the correct bio-parcel.
6. The longer a user uses the BioVault protocol, the more old biometric data will be available for use. The old biometric data will in effect become a large pool of special keys, similar to one time pad technology.

9.4. CONCLUSION

In this chapter the first step was taken towards solving the issues related to biometric characteristic duplication. As people interact with their environment latent biometric images are left behind.

If a fake biometric characteristic is generated from a latent biometric image, by whatever means, a hacker could use this fake biometric characteristic to be authenticated as the authentic user.

By providing the user with a CBA, containing a large number of old biometric data of the particular user, the user can generate a bio-parcel consisting of old biometric data, as challenged by the authentication server, and fresh biometric data.

A hacker can generate a fake biometric characteristic, but without the CBA, or more specific, the exact challenged biometric data, a hacker will not have the ability to masquerade as the actual user.

In chapter 10, the protocol will be secured and improved using XOR operators to securely lock the bio-parcel. This will ensure that a hacker cannot gain any access into the contents of the bio-parcel.

Biometric issues			BioVault solutions		
Chapter #	Chapter Name	Identified Issue	Chapter #	BioVault version	Completed
4	Replay	Biometric data replay	8	Version 1.0	<input checked="" type="checkbox"/>
5	Authenticator Duplication	Manufacturing of fake biometric characteristics	9	Version 2.0	<input checked="" type="checkbox"/>
5	Authenticator Duplication	Slight altering of biometric data	10	Version 3.0	<input type="checkbox"/>

BioVault Problem-Solution matrix, version 2.0



Chapter 10: BioVault Version 3.0

10.1. INTRODUCTION

Chapter 8 introduced the BioVault version 1.0, and illustrated how electronic replay of biometric data can be solved. Chapter 8 concluded with two flaws remaining once electronic replay is solved.

The first flaw as identified in Chapter 8, related to biometric characteristic duplication. A biometric characteristic is duplicated from a latent biometric image.

Chapter 9 focused on a solution to the problems related to the duplication of biometric characteristics. As concluded in Chapter 9, electronic duplication is a major issue if biometrics is to be utilized as the de facto method to authenticate a person.

As a consequence of the testing of BioVault version 1.0 the second flaw emerged. A hacker can alter intercepted biometric data slightly, resulting in the failure of BioVault version 1.0. The mechanism of BioVault version 1.0 accepts the illicit biometric data as authentic as no 100% match between the offered illicit biometric data and the biometric data in the SBA was detected. This chapter focuses on the solution of this problem.

Chapter 9 demonstrated how a fake biometric characteristic, created from latent biometric images, could be manufactured and subsequently used for illicit authentication.

Chapter 9 introduced an additional component to the BioVault model known as the client-side bio-archive (CBA). This bio-archive includes the most recent submitted biometric data and also a number of previously used biometric data.

The next section will briefly illustrate the mechanism of BioVault version 2.0, to outline the mechanism of BioVault version 2.0. BioVault version 3.0 is based on version 2.0, and extends the functionality and security of BioVault version 2.0.

Biometric issues			BioVault solutions	
Chapter #	Chapter Name	Identified Issue	Chapter #	BioVault version
4	Replay	Biometric data replay	8	Version 1.0
5	Authenticator Duplication	Manufacturing of fake biometric characteristics	9	Version 2.0
5	Authenticator Duplication	Slight altering of biometric data	10	Version 3.0

Table 9.1: BioVault Problem-Solution matrix

10.2. BACKGROUND

UNIVERSITY
OF
JOHANNESBURG

BioVault version 2.0 is a completely functioning model of the BioVault system. Version 1.0 solved the problems related to biometric data replay, and the problems of biometric characteristic duplication were solved in version 2.0. Version 2.0 is briefly illustrated in the following diagram.

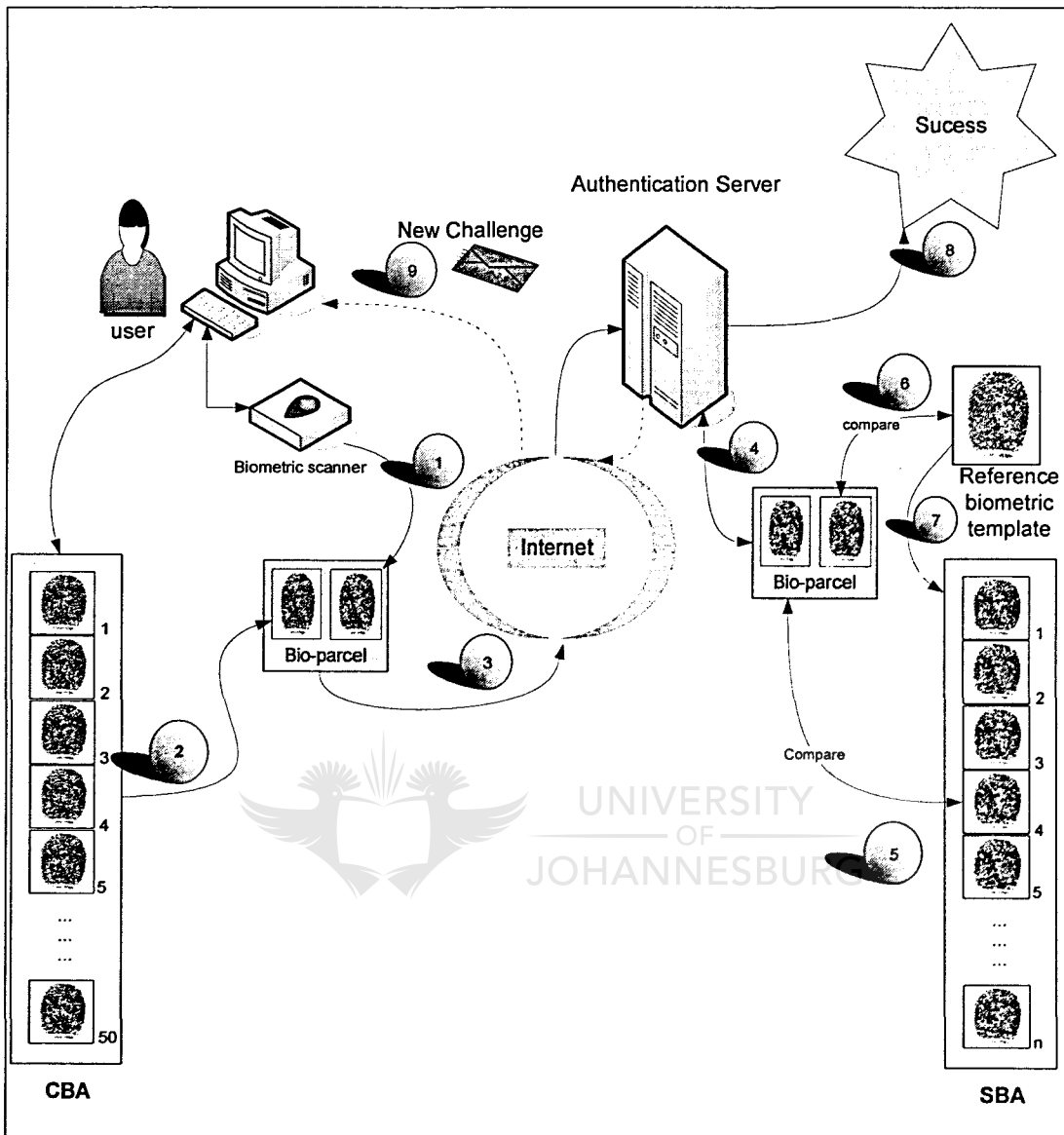


Figure 10.1: BioVault version 2.0

The mechanism of BioVault version 2.0 is illustrated in figure 10.1. The complete stepwise discussion of the internal mechanism of BioVault version 2.0 can be found in Chapter 9, section 9.3.2.

As illustrated in figure 10.1, the bio-parcel, containing fresh biometric data and old biometric data from the CBA, is submitted un-encrypted via a public network.

One can assume that this bio-parcel can be sniffed by a hacker during network transmission.

The sniffing of a bio-parcel is illustrated in the next section.

10.3. EXPLOITING BIOVAULT VERSION 2.0

The following illustration, demonstrates how the bio-parcel can be sniffed while in transit via an unprotected public network.

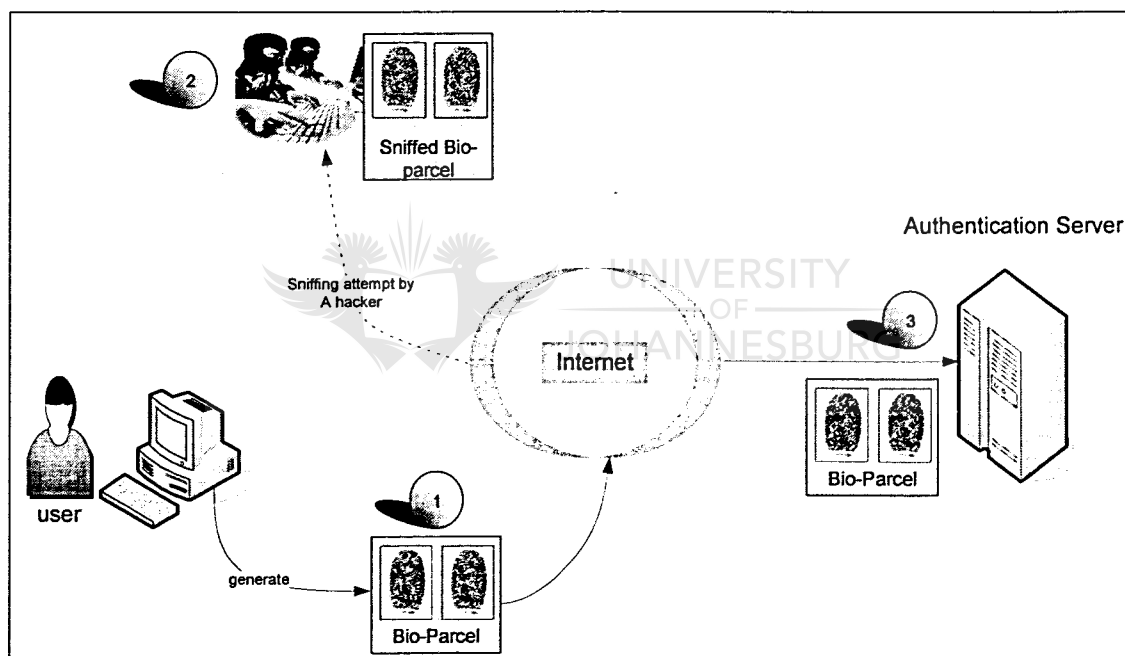


Figure 10.2: BioVault version 2.0 exploitation

In an attack on the mechanism of BioVault version 2.0, a hacker is able to sniff the bio-parcel during its transmission via the network, as demonstrated in figure 10.2.

Step 1

The user generates the bio-parcel as determined by the methodologies prescribed by BioVault version 2, and submits the new bio-parcel to the authentication server.

Step 2

During transmission the bio-parcel is sniffed by a hacker, who stores it for later usage.

Step 3

The bio-parcel arrives at the authentication server, and is considered for validity. If it conforms to the rules governing BioVault version 2.0, it succeeds authentication. The server responds with a challenge back to the user. This challenge consists of an instruction from the authentication server, to the user's hardware to submit particular biometric data from the CBA, into a bio-parcel for next request for authentication.

This challenge can be intercepted, and is illustrated in figure 10.3.

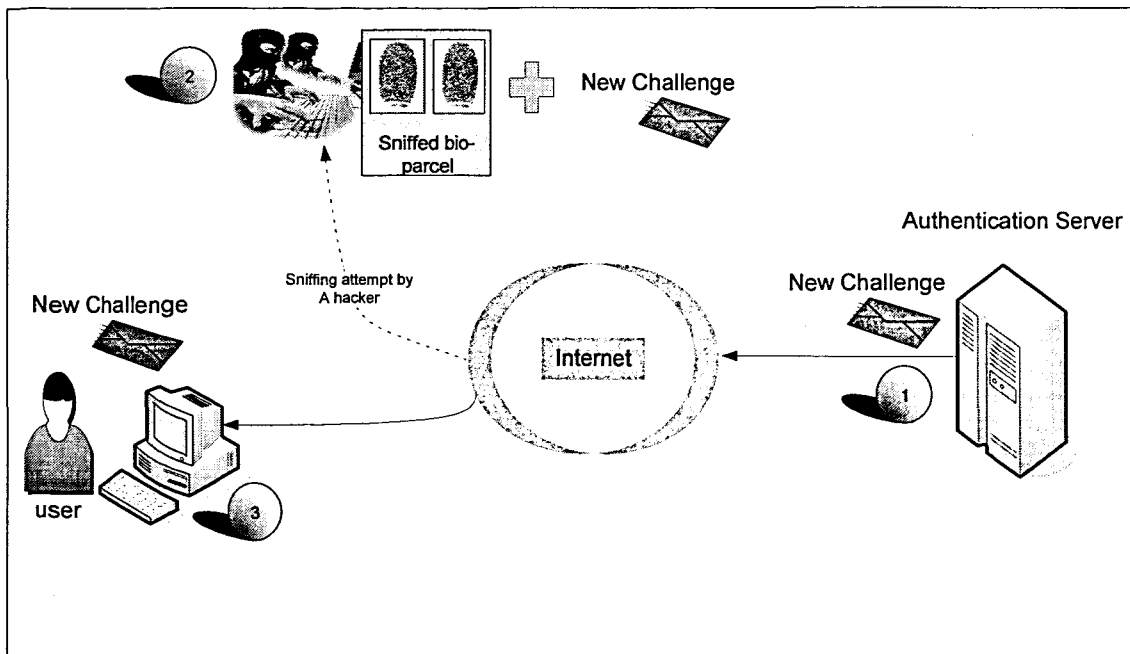


Figure 10.3: Interception of challenge

Figure 10.3 illustrates this process, however, during the return communication the challenge is intercepted by the hacker.

Step 1

The authentication server sends the challenge to the user, selecting a particular number that points to specific biometric data in the user's CBA. This biometric data must be presented by the user during a subsequent request for authentication.

Step 2

The challenge is intercepted by a hacker during the network transmission. At this stage the hacker is in possession of the bio-parcel as submitted by the user, as well as the challenge requesting the next biometric data to be submitted from the CBA.

Step 3

The user receives the challenge, and stores it for the next instance authentication is required.

10.4. USAGE OF SNIFFED INFORMATION

If a hacker manages to successfully sniff the bio-parcel and challenge from the authentication server as illustrated in figure 10.2 and figure 10.3, the hacker is in possession of the following:

- 10.4.1) Fresh biometric data in electronic format.
- 10.4.1) Old biometric data from the CBA.
- 10.4.2) The challenge from the authentication server.

The bio-parcel and challenge from the authentication server, as described in BioVault version 2.0 are not encrypted, as encryption significantly increases the size of the bio-parcel.

Should encryption be introduced to protect the bio-parcel, the BioVault environment is burdened with shared symmetric key management. This would mean that the authentication server would need to track all keys shared with the various users of the system, or at least keep track of all the public keys of every user (if a public key infrastructure is used).

10.4.1. Fresh biometric data from the bio-parcel

It was demonstrated during the research of BioVault that a hacker can intercept the biometric data, and use this biometric data for an electronic replay attack. However this problem was successfully addressed in BioVault version 1.0.

Further investigation and testing of BioVault version 1.0, indicated that BioVault version 1.0 could be subverted, by slightly altering biometric data found in electronic format, so that the altered biometric data does not yield a 100% match with any previously offered biometric data from a particular user. The altered biometric data would still be accepted during the asymmetric comparison of the matching algorithm.

Considering that the hacker intercepted the bio-parcel (at this stage the bio-parcel is in clear text), and obtained the biometric data of a given user, the hacker could alter this fresh biometric data, to insure that a 100% match will not be detected by BioVault.

10.4.2. Old Biometric data from the bio-parcel

As illustrated in figure 10.2, the hacker intercepted the clear text bio-parcel containing the fresh biometric data as discussed in section 10.4.1, and the old biometric data. This biometric data was demanded from the user's CBA as a challenge from the authentication server during previous communication, and is now submitted for a symmetric match to the biometric data in the SBA.

The hacker has succeeded in obtaining a biometric data furnished from the CBA. If the hacker monitors the user diligently, he can assemble an illicit CBA sniffed from the user.

The hacker is however unfamiliar with the number positions of the biometric data in the CBA.

10.4.3. Challenge from the authentication server

The hacker monitoring the traffic between user and authentication server, will also intercept the server's challenge to the user and this challenge is not encrypted either.

Patient monitoring of communication between the user and authentication server, will eventually enable the hacker to assemble the complete CBA of the monitored user.

In order to determine the position of biometric data in the CBA, the hacker needs to intercept the challenge from the server; this will yield the particular number of the biometric data that the user will send during the next communication with the authentication server. The moment the user sends the next bio-parcel for authentication the hacker will be in possession of both the position of the biometric data and the biometric data itself.

10.4.4. Conclusion

BioVault version 2.0 does not secure the sending of the bio-parcel or the challenge from the authentication server.

Therefore a hacker monitoring traffic is able to assemble his own illicit CBA for a particular user. Theoretically he can provide the correct biometric data demanded by the authentication server from the illicit CBA. By utilizing a fake biometric characteristic or altering any of the intercepted biometric data, he is also able to complete the bio-parcel with "fresh" biometric data.

The next section will introduce BioVault version 3.0, demonstrating how the flaws of BioVault version 2.0 as discussed in sections 10.4.1 – 10.4.3 are solved,

without the introduction of symmetric encryption, or the usage of a PKI infrastructure.

10.5. BIOVAULT VERSION 3.0

In order for a hacker to masquerade as the authentic user, the hacker will need

- A fake biometric characteristic,
- Access to the authentic user's CBA,
- and also need to know the exact challenge from the authentication server for the specific biometric data in the CBA.

This is possible if BioVault version 2.0 is used as discussed in section 10.4. In order to prevent the problems as described in section 10.4, BioVault version 3.0 has been developed.

BioVault version 3.0 is an adapted version of BioVault version 2.0. No additional components are introduced into the BioVault version 3.0 model. The aim of the BioVault version 3.0 is to secure the bio-parcel while transmitted via a public network, without using encryption systems with elaborate encryption key management issues.

The authentication mechanism of BioVault version 3.0 as illustrated in figure 10.4 is discussed in eight steps. The challenge phase of BioVault version 3.0 is illustrated in figure 10.5 and discussed thereafter.

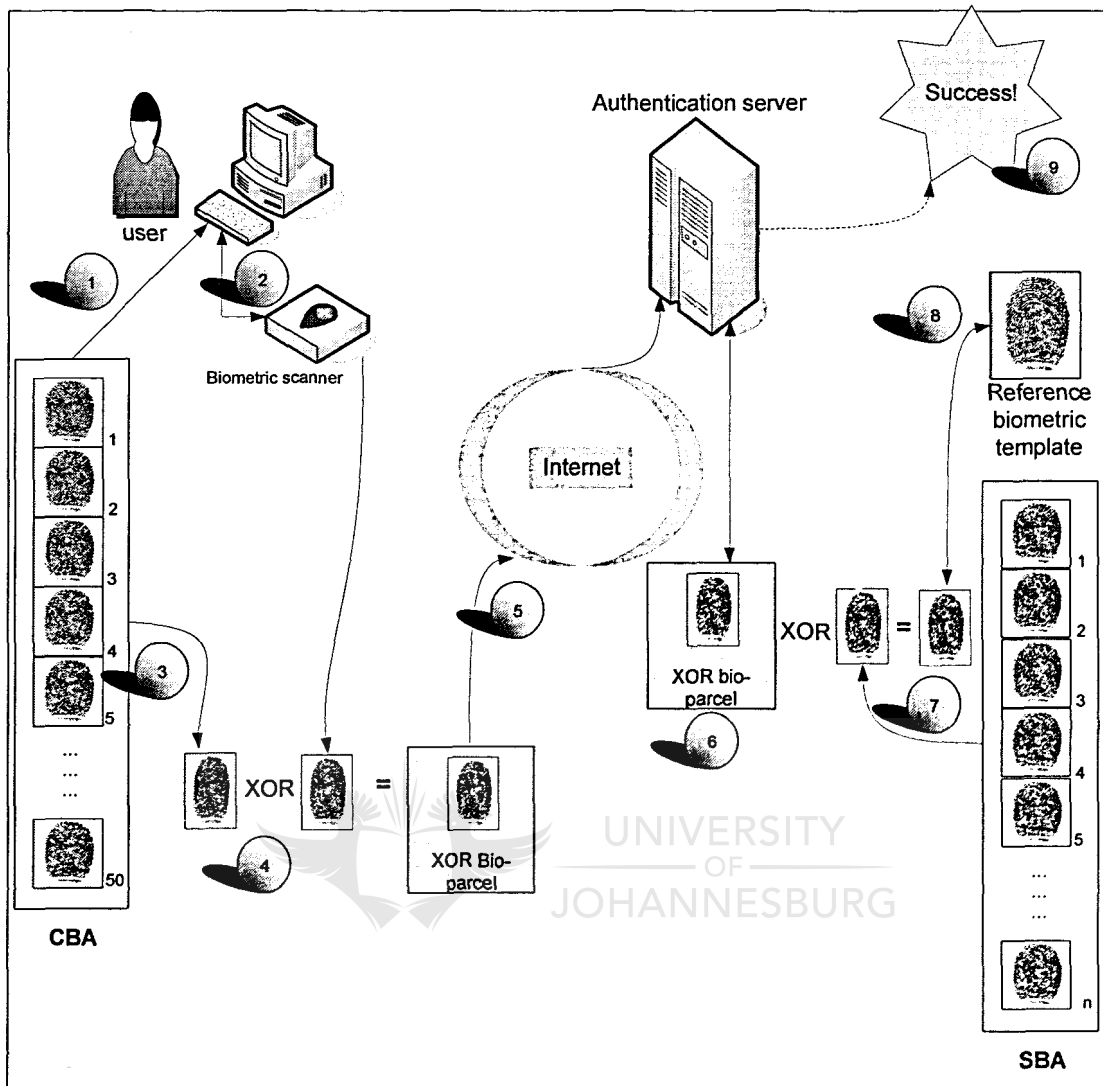


Figure 10.4: BioVault version 3.0

Step 1

When a user needs to be authenticated the user attaches the appliance containing the CBA with the previously offered biometric data to the terminal (for example the user's computer or ATM machine), where he intends to do the transaction.

Step 2

The user provides a fresh biometric characteristic as shown, directly to the biometric scanner. The scanner will digitize the biometric characteristic and forward the biometric data to the driver software of the biometric device.

Step 3

During the previous encounter with the authentication server, the server sent a challenge to the user (as will be discussed shortly in figure 10.5). This challenge demanded specific biometric data from the CBA that had to be included at the time of the next contact with the authentication server. In figure 10.4, the server requested the 4th biometric data in the CBA. The system will thus automatically obtain the 4th biometric data from the user's CBA.

Step 4

The BioVault client side software will take the electronic representation of the freshly offered biometric data and XOR it with the electronic representation of the 4th biometric data obtained in step 3 from the CBA. For example:

Electronic representation of fresh biometric data from scanner:

10101110111011010

Electronic representation of challenged (4th) data from CBA:

10110101111011110

New bio-archive after XOR process:

00011011000000100

This results in a smaller bio-parcel than proposed in BioVault version 2.0, as only the result of the XOR process will be submitted to the authentication server as the XOR bio-parcel.

Step 5

The XOR bio-parcel is submitted via the internet or any networked environment to the authentication server.

Step 6

The server receives the XOR bio-parcel as shown in step 6, and prepares to run the XOR operator on the bio-parcel.

Step 7

The server requested previously that the client must XOR the fresh biometric data with the fourth biometric data in the CBA. The server obtains the biometric data in the SBA that corresponds with the expected biometric data received from the user in the XOR bio-parcel.

The server must then XOR the received XOR bio-archive with the 4th biometric data from the SBA, corresponding with the 4th biometric data in the CBA, in order to get the fresh biometric data of the user. For example:

XOR bio-archive received from user:

00011011000000100

Expected 4th biometric data from SBA:

10110101111011110

Result of XOR process yields the fresh biometric data:

10101110111011010

Step 8

The fresh biometric data extracted from the XOR bio-archive during step 7, is now asymmetrically matched to the reference biometric template found in the database. The authentication server compares the freshly offered biometric data

with the reference biometric template. If the offered biometric data falls within the tolerances defined in the matching algorithm, the system declares the biometric data as authentic and adds this biometric data to the SBA, after checking the SBA for an exact match to exclude replay attempts.

Step 9

As the bio-parcel passed all the requirements, authentication is pronounced successful.

The server proceeds to the generation of a new challenge destined for the user. This process is outlined in figure 10.5.

10.6. SERVER CHALLENGE PARCEL FOR USER

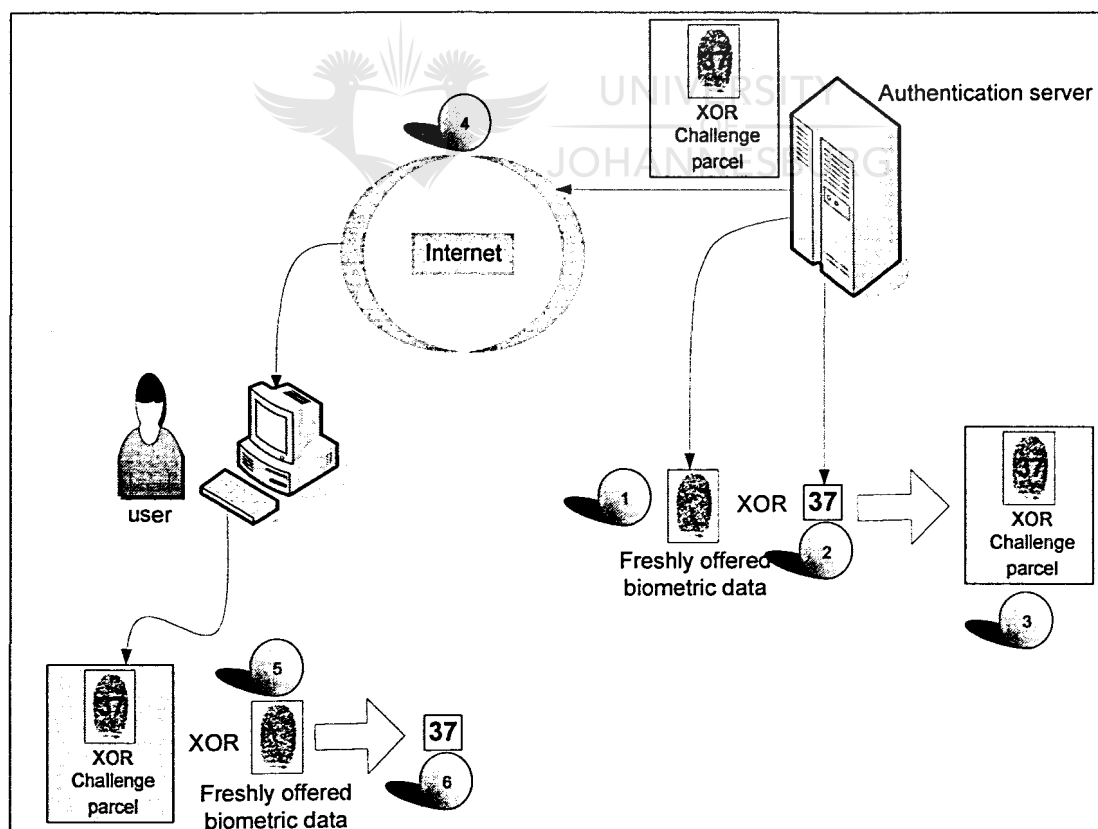


Figure 10.5: Challenge parcel from authentication server

In the event of a successful authentication process as discussed in section 10.5, the server proceeds to generate a challenge parcel to the user, for future authentication.

Step 1

The authentication server obtains the fresh biometric data extracted from the XOR bio-parcel during the authentication phase, discussed in section 10.5.

Step 2

The authentication server generates a challenge to the user. This challenge is in the form of a number, relating to specific biometric data in the CBA. This number must fall between 1 and the size of the CBA. In this example the server randomly selected the number 37. Once the number is selected the server stores a marker that points to the corresponding biometric data in the SBA

Step 3

The authentication server XOR's the binary value of the randomly selected number with the binary representation of the fresh biometric data. For example:

Electronic representation of the fresh biometric data:

10101110111011010

Binary representation of the number 37:

0000000000100101

Challenge parcel after XOR process:

10101110111000000

Step 4

The XOR challenge parcel is sent to the user via the internet or any networked environment.

Step 5

The client side software of the user obtains the fresh biometric data digitized during step 1 of the authentication phase, in section 10.5.

Step 6

The client side software will XOR the fresh biometric data, with the XOR challenge parcel received from the authentication server in step 4. For example:

XOR Challenge parcel from server:

10101110111000000

Electronic representation of fresh biometric data:

10101110111011010

Result after XOR operation:

00000000000100101

The client side software converts the binary value derived from the XOR operation to decimal, in order to find the challenged CBA token that must be used in the next communication with the authentication server. The decimal value of 00000000000100101 is subsequently translated to the decimal number 37, demonstrating that the 37th biometric data from the CBA will be used to generate the next XOR bio-parcel, for a subsequent request for authentication as described during the authentication phase in section 10.5.

10.7. CONCLUSION

In the event of a hacker intercepting the XOR bio-parcel, he obtains nothing usable. As the hacker does not possess the challenge biometric data, he cannot gain access to the fresh biometric data of the user. This bars him from slightly altering fresh biometric data to subvert the SBA check. The lack of access to the fresh biometric data renders the effort of sniffing the XOR bio-parcel senseless.

In an attempt to succeed in illicit authentication, the hacker needs to obtain, or be in possession of:

- 1) The fresh biometric data used in the previous user–server contact to extract the CBA biometric data number from the XOR-parcel as challenged by the server.
- 2) He needs the CBA of the given user, containing biometric data of the user – which could be well in excess of the 50 mentioned in the example.
- 3) Fresh biometric data to be XOR-ed with the correct biometric data from the CBA.

It is an almost unavailing process to gather all the components for a BioVault version 3.0 authentication if the hacker does not have access to all the components of the process. Even if the hacker manages to assemble the correct XOR bio-parcel, the success will be only a single opportunity.

Identity theft is virtually impossible in the BioVault version 3.0 environment.

Efforts from a hacker to obtain the CBA in its total (numerically correct) entirety for illicit application can be hurdled by frequently updating the CBA in a secure environment. The authentication server can, at given intervals, prompt the user

to present the CBA in a controlled environment for biometric data updating, augmenting, and reshuffling.

Biometric issues			BioVault solutions		
Chapter #:	Chapter Name	Identified Issue	Chapter #	BioVault version	Completed
4	Replay	Biometric data replay	8	Version 1.0	<input checked="" type="checkbox"/>
5	Authenticator Duplication	Manufacturing of fake biometric characteristics	9	Version 2.0	<input checked="" type="checkbox"/>
5	Authenticator Duplication	Slight altering of biometric data	10	Version 3.0	<input checked="" type="checkbox"/>

BioVault Problem-Solution matrix, version 3.0

The next chapter will discuss the way that BioVault can be used for biometric encryption followed by chapter 12 focusing on biometric signatures.



Chapter 11: BioVault, Biometric Encryption

11.1. INTRODUCTION

Chapter 10 concluded the final version of BioVault. This final version of BioVault solved the problems related to:

- 1) Latent biometric images lifted from a user's environment.
- 2) Biometric data acquired in electronic format and replayed at a later stage and
- 3) Biometric data altered in electronic format to subvert the detection mechanisms of BioVault version 1.0 and BioVault version 2.0.

The following diagram summarizes the development at this stage:

Biometric issues			BioVault solutions		
Chapter.#	Chapter.Name	Identified Issue	Chapter.#	BioVault version	Completed
4	Replay	Biometric data replay	8	Version 1.0	<input checked="" type="checkbox"/>
5	Authenticator Duplication	Manufacturing of fake biometric characteristics	9	Version 2.0	<input checked="" type="checkbox"/>
5	Authenticator Duplication	Slight altering of biometric data	10	Version 3.0	<input checked="" type="checkbox"/>

BioVault Problem-Solution matrix, version 3.0

BioVault focused on providing a mechanism that will allow biometric data to be used securely via a networked environment for identification and authentication.

Von Solms and Eloff [1] describe the five information security services as:

- 1) *Identification and authentication* – The mechanisms that typically enforce this service are passwords, tokens and biometrics.

- 2) *Confidentiality* – Enforced by encryption algorithms using a secret key (either a password or secret value stored on a token like a smartcard).
- 3) *Integrity* – Enforced by message authentication codes or hashing algorithms using a secret key. This secret key can either be a password or a secret value stored on a token.
- 4) *Authorization* – Enforced by e.g. access control lists, access control directories or an access control matrix, based on a supplied username and password or username and token.
- 5) *Non-Repudiation* – Enforced by the public and private key infrastructure. These systems rely on passwords to access a person's private key.

This chapter will demonstrate how the BioVault infrastructure can be used to enforce confidentiality. Chapter 12 will demonstrate how the BioVault system can be utilized to sign electronic documents using a person's biometric characteristic, thereby enforcing non-repudiation.

If the BioVault infrastructure is implemented in an environment, it will be possible for a person to use a biometric characteristic to digitally sign a document, or to encrypt a document destined for a specific person.

11.2. BACKGROUND

To date, it has not been possible to use a biometric characteristic directly as the secret key for an encryption algorithm, or for a message authentication code (MAC) algorithm. The reason for this is vested in the fact that a biometric data is almost without fail asymmetric. This was discussed in depth in Chapter 4. In order for an encryption algorithm to function, the secret key provided to encrypt a message must be exactly the same (symmetrical) as the secret key utilized to decrypt the message.

If a secret key is used to generate a MAC (Message Authentication Code), this exact same secret key must be provided to test the MAC.

The possibility that a person can provide biometric data matching previously provided biometric data completely is highly unlikely. This makes biometric characteristics useless as secret keys for a MAC or encryption.

Digital signatures use encryption and MAC as its underlying, primary technology.

The sections to follow will demonstrate how the BioVault infrastructure allows biometric characteristics to be used to ensure confidentiality.

11.3. ENCRYPTION USING A SECRET KEY OR BIOMETRIC CHARACTERISTIC

This section investigates the usage of a symmetric secret key for encryption and considers the feasibility of using a biometric characteristic as a secret key for an encryption algorithm.

11.3.1. Secret key encryption

If a user John intends to send a message to another user Sam via an unsecured network, the message needs to be encrypted. $C = E^k(M)$ where

C = Cipher message

M = Original message

k = secret key

E = Encryption algorithm

The encryption process using a secret key is illustrated in figure 11.1.

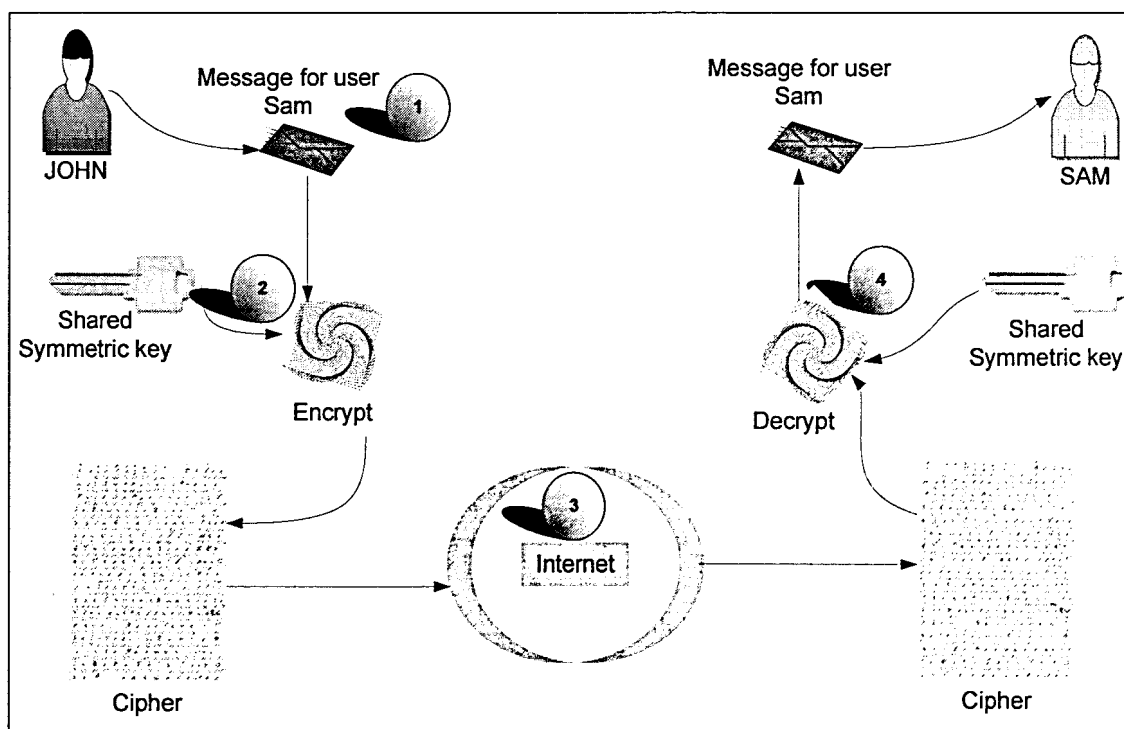


Figure 11.1: Symmetric secret key encryption

As illustrated in figure 11.1, John intends to send a secret message to Sam. In order to secure the message during the transmission, John encrypts the message using an encryption algorithm. In order for the encryption algorithm to provide cipher text that is totally random, a secret key is provided. This secret key is shared by Sam and John as illustrated in figure 11.1. The secret key provided by John to encrypt the message is exactly the same as the secret key that Sam needs to decrypt the message.

Step 1

John generates the message to send to Sam.

Step 2

John provides a secret key to the encryption algorithm, and the encryption algorithm uses this secret key to generate the cipher text.

Step 3

The message in cipher text is sent via the internet to Sam. If a hacker should intercept this message, the hacker needs to be in possession of the secret key shared by Sam and John, in order to decrypt the message.

Step 4

Sam receives the message sent by John and uses the same encryption algorithm and the secret key they share. Provided the key Sam applies to the encryption algorithm is the same as the one used by John, Sam retrieves the original un-encrypted text John created.

From this example it is obvious that biometric data cannot be employed for secure encrypted communication between people. If John used his biometric data as the secret key for encrypting a message intended for Sam, Sam would have needed the same biometric data John used. She would not be able to provide the same biometric data to decrypt the message, as this was John's biometric data that Sam does not possess. This is explained in more detail below.

11.3.2. Biometric data for encryption

Figure 11.2 illustrates an attempt by John to encrypt personal information using his biometric characteristic. This information will be used in the future by John, and must be decrypted using the same biometric characteristic that John supplied during the encryption process.

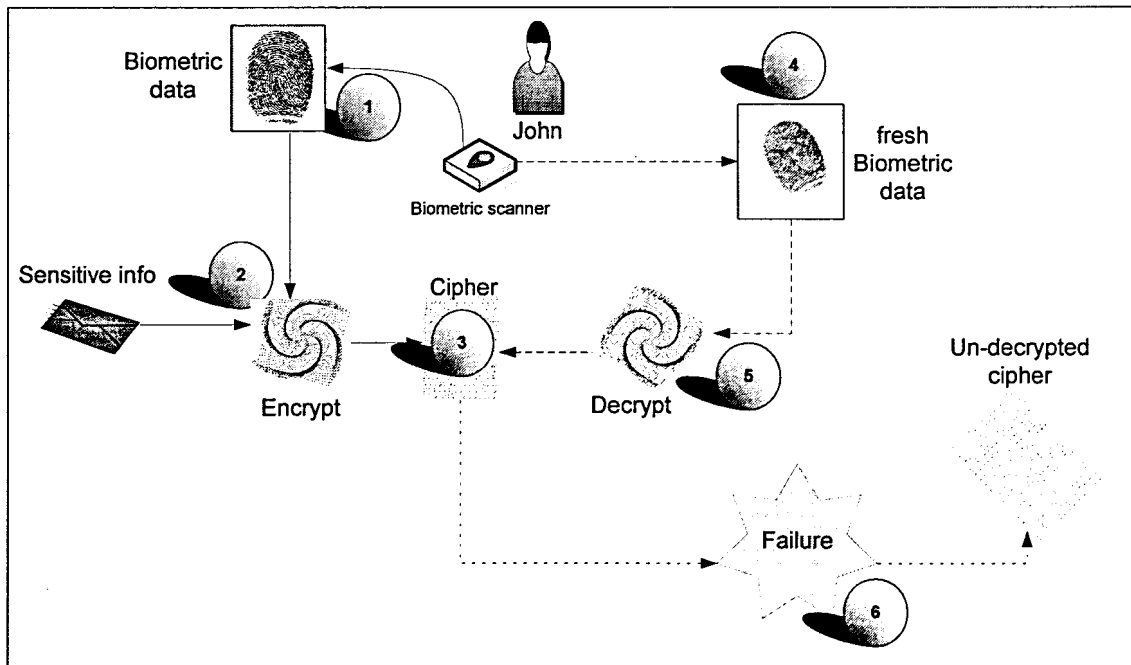


Figure 11.2: Biometric secret key encryption attempt

If John has sensitive information that he wishes to protect, John can use encryption to safeguard this information. If a password is used as the secret key, this same password would be required to decrypt the sensitive information at a later stage. However, as illustrated in figure 11.2, John used his biometric characteristic to encrypt the sensitive information.

Step 1

John supplies his biometric characteristic, in this instance his left thumb, to the biometric scanner. The biometric scanner will convert the biometric characteristic to an electronic representation, known as biometric data.

Step 2

This biometric data is then used as the secret key for the encryption algorithm, resulting in the sensitive information being transformed into cipher text.

Step 3

John saves the cipher text for future use.

Step 4

At a later stage John provides another biometric characteristic of his left thumb, which was used to encrypt the sensitive information a while ago, to the biometric scanner.

The biometric scanner converts the biometric image to an electronic representation.

Step 5

The new biometric data is used in an attempt to decrypt the cipher text that John created previously.



Step 6

Since John did not manage to position his finger exactly as he did during the encryption phase, the new biometric data is not identical to the biometric data used during the encryption process. This results in failure of the decryption of the cipher.

11.3.3. Conclusion

From the above discussion, it is evident that the usage of biometric data as the secret key for an encryption algorithm raises many issues.

Firstly, it is not possible to use biometric data between two parties such as Sam and John, who wish to communicate confidentially over a network, as they need to share a secret key. This secret key must be exactly the same for both parties. The fact that Sam and John do not share a biometric characteristic that will match completely, makes biometric data unfit for encryption between two parties.

Secondly, if a person uses a biometric characteristic as the secret key for personal encryption, the person must provide exactly the same biometric characteristic, in exactly the same way, in order to decrypt the cipher. However, as already discussed in chapter 6, biometric data is asymmetric by nature. The possibility that John would manage to provide the same biometric data matching the biometric data he presented during encryption is highly unlikely, resulting in the decryption of the cipher to fail.

The next section demonstrates how the BioVault infrastructure can be used to encrypt communication between two people using biometric characteristics.

11.4. BIOMETRIC ENCRYPTION

In this section, the BioVault infrastructure is used to allow John to send an encrypted message to Sam, by using a biometric characteristic. The method relies on the fact that John and Sam are both part of the BioVault environment –

very much as EBay [98] relies on the fact that buyers and sellers are both part of the PayPal [100] environment, as discussed in Chapter 7 (Electronic commerce).

The whole encryption method using the BioVault infrastructure is a 4-phased process.

11.4.1. Biometric encryption overview

In *phase 1*, John identifies himself to the authentication server, and indicates that he wants to send an encrypted message to Sam. In order to send an encrypted message to Sam, John requests a "biometric key" of Sam from the server.

In *phase 2*, the authentication server retrieves a biometric key from Sam's SBA, ensuring that the key being transmitted to John is found inside the CBA of Sam. This biometric key is then transmitted to John.

In *phase 3*, John uses the biometric key of Sam received from the server, as an encryption key to create the encrypted message, and sends this encrypted message to Sam via the network.

In *phase 4*, Sam receives the encrypted message sent by John, and decrypts the message by comparing all the biometric keys found in Sam's CBA, against the received cipher text. In essence, Sam will perform a 'brute force attack' on the cipher using all biometric data in her CBA as the possible key of the cipher.

The server ensures that John uses a biometric key that is found inside Sam's CBA. Finding the shared biometric key, and decrypting the message is thus done very fast. All the biometric keys inside Sam's CBA will be compared (brute forced) against the cipher.

11.4.2. Biometric encryption discussion

Diagram 11.3 illustrates the first phase of biometric encryption. John will need to acquire Sam's biometric data in order to encrypt the message destined for Sam. This biometric data will be supplied to John by the authentication server.

11.4.3. Phase 1 – Request of biometric data

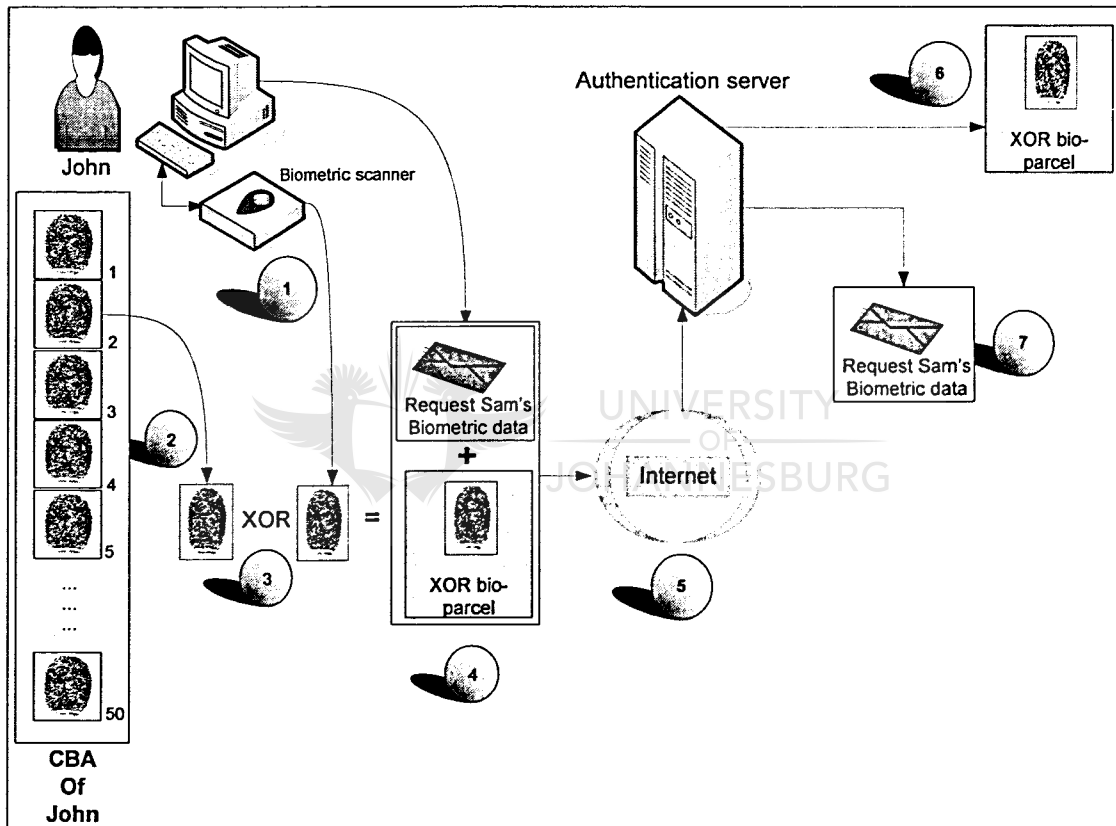


Figure 11.3: Request by John for Sam's biometric data

John intends to send a message to Sam. In figure 11.3 the request phase for Sam's biometric data is illustrated.

Step 1

John provides a fresh biometric characteristic (as shown in step 1) directly to the biometric scanner. The scanner digitizes the biometric characteristic and forwards the resulting biometric data to the driver software of the biometric device.

Step 2

During a previous encounter with the authentication server, the server sent a challenge to John (as per BioVault version 3.0). This challenge demanded specific biometric data from John's CBA that needs to be included during the next contact with the authentication server. In figure 11.3, this request demanded the 2nd biometric data in John's CBA. The system will thus automatically obtain the 2nd biometric data from John's CBA.

Step 3

The BioVault client side software XOR's the freshly offered biometric data with the electronic representation of the 2nd biometric data obtained in step 2, resulting in the XOR bio-parcel.

Step 4

John indicates that he wants to communicate with Sam confidentially, and generates an unencrypted text message requesting biometric data of Sam. This request is concatenated with the XOR bio-parcel, generated earlier by John's client side software.

Step 5

These two combined messages are then sent via a network to the authentication server. In the event that the message is sniffed during transmission, the hacker would be in possession of the XOR bio-parcel he cannot decrypt, as well as the

clear text request that John wants to communicate with Sam confidentially. Neither is of any value to a hacker.

Step 6

Once the server receives the message from John, the server will evaluate the XOR bio-parcel provided by John. The server will confirm that the correct anticipated biometric data is received, and that the fresh biometric data as supplied by John is authentic. This step applies the rules as discussed in Chapter 10, relating to the functioning of BioVault version 3.0. John is now formally identified and authenticated by the authentication server.

Step 7

The second part of the message received by the server is the request by John to communicate with Sam. The server will check if Sam is a registered user of the BioVault system. If Sam is a registered user, the second phase of the process is initiated.

At this stage John sent a request to the server, stating that he wished to communicate with Sam. The server authenticated John, based on the fact that the fresh biometric data supplied by John was accepted and the expected biometric data from John's CBA was correctly supplied.

Subsequently the server ensured that Sam is a user on the BioVault system, allowing the second phase to commence. Phase two is illustrated in figure 11.4.

11.4.4. Phase 2: Submission of biometric data of Sam to John

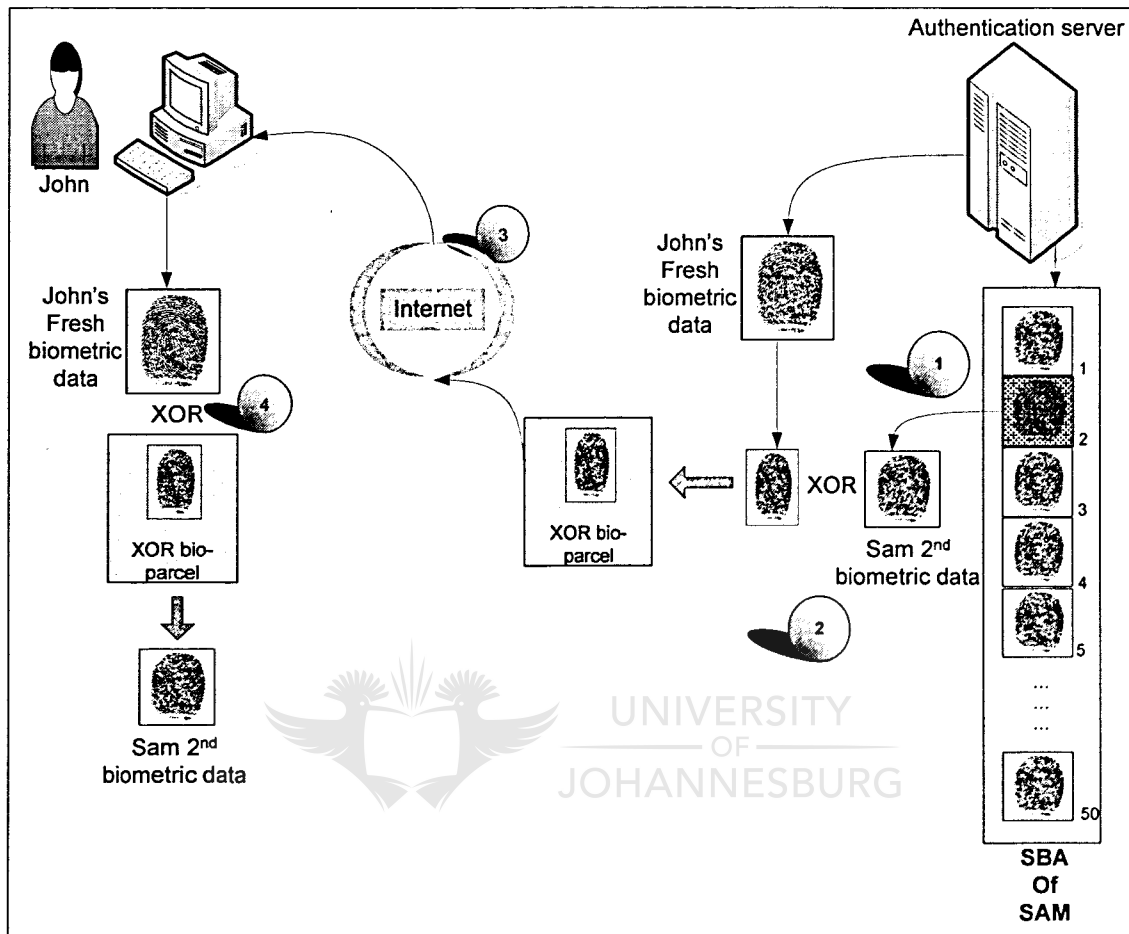


Figure 11.4: Sam's biometric data submitted to John

During the second phase the server will send stored biometric data from the SBA of Sam, back to John. The server is aware that this biometric data exists inside Sam's CBA. The steps below explain this process:

Step 1

The server obtains biometric data, in this particular illustration the second biometric data, from the SBA of the user Sam. The biometric data is selected

randomly from the subset of the SBA which corresponds to Sam's CBA, and is therefore present in the CBA of user Sam.

The server marks this biometric data as "used for encryption" to prevent this particular biometric data ever again rendered for encryption or authentication. This guarantees that Sam and John are the only people in possession of this biometric data.

Step 2

The server will XOR the biometric data from Sam's SBA, in this case the 2nd one, with the fresh biometric data received in phase 1 from John, creating a new XOR bio-parcel.

Step 3

The XOR bio-parcel is then transmitted via the network, back to John. If this parcel is sniffed during transmission, the hacker will not have much use for the received bio-parcel.

Step 4

John receives the XOR bio-parcel. John uses the fresh biometric data he supplied during the first phase, and XOR's this fresh biometric data with the bio-parcel received. This step yields the biometric data sent by the authentication server to John – i.e. biometric data number 2 in Sam's SBA.

Once John is in possession of this biometric data of Sam, John can proceed to the third phase, of sending an encrypted message to Sam.

11.4.5. Phase 3: Encrypted communication between John and Sam

At this stage John is in possession of a symmetric copy of the second biometric data in the SBA of Sam. As illustrated in figure 11.5, he can proceed to encrypt a message for Sam using the biometric data made available by the server of biometric data found in Sam's SBA. The server is aware that this biometric data is also found in Sam's CBA.

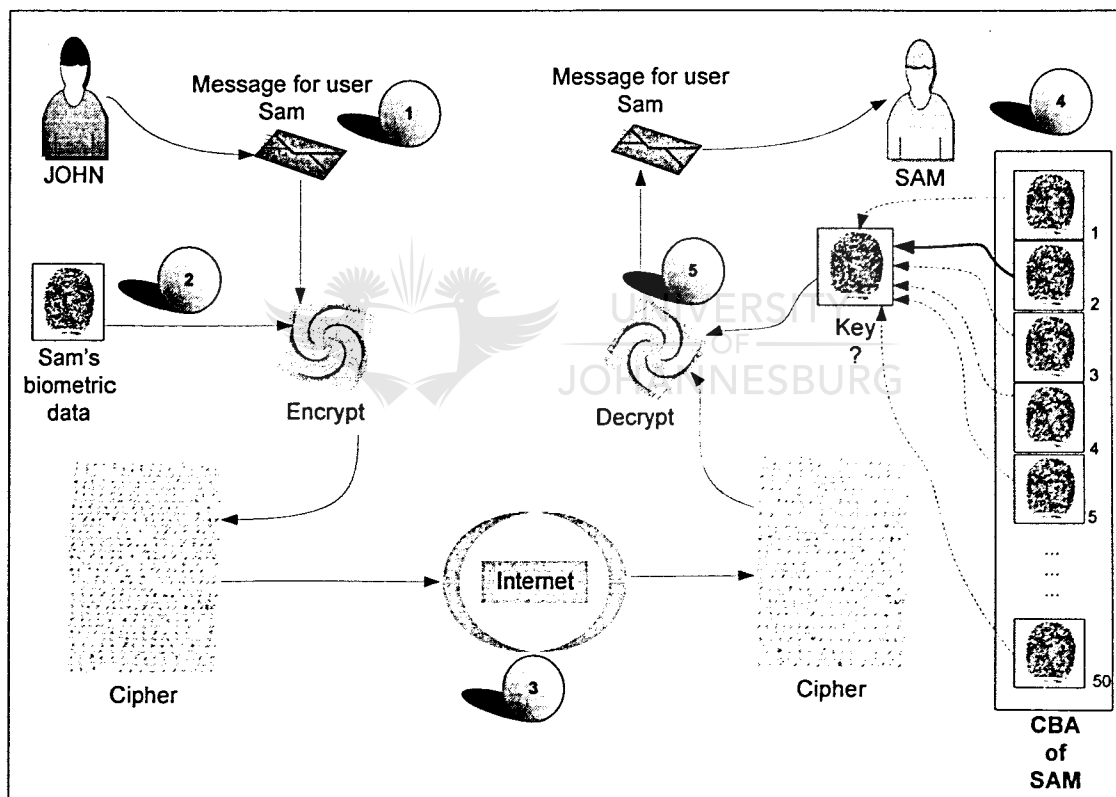


Figure 11.5: Cipher decryption

Figure 11.5 illustrates in 5 steps how John will send an encrypted message to Sam and how Sam will decrypt the message.

Step 1

John generates the message that he intends to send to Sam.

Step 2

John provides the received biometric data of Sam to the encryption algorithm, and the encryption algorithm uses this biometric data as a secret key to generate the cipher text.

Step 3

The message in cipher text is sent via the internet to Sam. If a hacker should intercept this message, the hacker must be in possession of the correct biometric data of Sam, in order to decrypt the message. Considering the working of BioVault version 3.0, this is highly unlikely.

In the final phase Sam will need to decrypt this message sent by John to her, using the biometric data inside her CBA. This process is illustrated in step 4 and step 5 of figure 11.5.

Step 4

Sam receives the message sent by John and accesses her own CBA. The client software on Sam's machine uses all the biometric data in her CBA to brute force the cipher. As there are only a limited number of biometric data in the CBA, this process will unlock the cipher rapidly.

Step 5

As the biometric data Sam used to decrypt the message is the same as the biometric data used by John, Sam will retrieve the original, unencrypted message from the cipher created by John.

11.5. CONCLUSION

This chapter demonstrated how the BioVault infrastructure avails itself to encrypt a message using biometric characteristics.

Considering that a user generates a number of biometric data every day, each one unique, this method of encryption is closely related to one time pad technology.

The keys used, are very long and do not conform to any pattern. As biometric data is provided, the authentication server marks it as "used for encryption" between two users in the specific user's SBA. It will thus not be used ever again for digital signatures or as part of the challenge-response system of BioVault.

The major problem found with normal password-based encryption keys, is the transportation of such encryption keys between the two parties that intend to communicate securely. One of the major benefits of the approach as discussed in this chapter is that the two parties that intend to communicate securely, need no previous communication with each other. The method has certain similarities with the PGP root server approach [119] and with typical PKE environments [118].

Biometric keys exchanged between two users can always be used between the two users for secure communication. The biometric keys exchanged between two users are unique and asymmetric in nature. They do not share a symmetric key like a password. The biometric data thus used for encryption is linked to the user receiving the encrypted message, in much the same way as a public key has a relation to the private key.

The next chapter will demonstrate how the BioVault infrastructure can be used to sign documents using a person's biometric characteristic.



Chapter 12: BioVault, Biometric Signatures

12.1. INTRODUCTION

Chapter 11 introduced the first application of the BioVault infrastructure. It was demonstrated that biometrics can successfully be used to encrypt a message that is destined for a specific person provided both people are part of the BioVault version 3.0 environment.

This chapter will introduce biometric signing using the BioVault infrastructure.

It is possible for a person to use a fresh biometric characteristic to digitally sign a document, ensuring that the integrity of the document is above suspicion. Signing a document with a person's biometric characteristic will also attest that the authentic person signed the document, as there is a direct link between the person and his biometric characteristic. A biometric characteristic is part of the user signing the document. This makes biometrics, as the authenticator, a very desirable and usable aspect of the BioVault version 3.0 environment.

12.2. BACKGROUND

Biometric data could to date not be used as the secret key of a MAC algorithm as biometric data is almost without exception asymmetric - as discussed in chapter 4.

In order for a MAC algorithm to function, it is a prerequisite that the secret key provided to create a MAC for a particular message is identical to the secret key used to test the MAC for that particular message. This is clearly illustrated in figure 12.1.

A password or a pin is used in a MAC algorithm to constitute the MAC for a particular message. The password or pin cannot irrefutably be linked to the user. With the key (password or pin) the MAC will test authentic but does not authenticate the presenter of the key as the actual generator of the message.

As biometric data is physically part of the user, it addresses this thorny problem. Traditionally people used physical attributes to authenticate themselves on documents. A person will sign a document with a unique signature to authorize or affirm a transaction. In ancient times potters left their fingerprints on an article as proof of its authenticity [120].

A MAC algorithm contributes largely to ensure the integrity of a document, and provided a user keeps his secret key secure, the system will function satisfactory. However, the possibility exists that the secret key for the MAC algorithm can be compromised, resulting in failure of the system.

If a secret key is used to create a MAC, this identical secret key must be provided to test the MAC.

As it is highly improbable that a person would be able to provide biometric data identical to previously provided biometric data, therefore it renders biometrics unfit to use as the secret key for creating a MAC.

Digital signatures use encryption and hashing as its subjacent, primary technology.

The following section details the typical functioning of a mechanism used to enforce integrity, using a secret key only the user is familiar with.

12.3. CREATING A MAC USING A SECRET KEY OR BIOMETRIC CHARACTERISTIC

This section discusses the usage of a symmetric secret key to generate a MAC for a particular message and considers the feasibility of using a biometric characteristic as the secret key to generate a MAC.

12.3.1. Secret key Message Authentication Code (MAC)

If a user intends to send a message to another user via an unsecure network, the message may be altered during transmission due to transmission problems.

Secondly, a non-secret message often needs to be sent to a group of people. The integrity of this message and the authenticity of the sender often require verification. In order to test the integrity of a message, a Hash [121] or CRC check [122] is done. These technologies are keyless, and do not authenticate the originator of the message.

In order to affirm integrity of the message, and the authenticity of the sender, a MAC [118] algorithm is used. A message authentication code (MAC) is a key based hashing algorithm.

A MAC process is illustrated in figure 12.1.

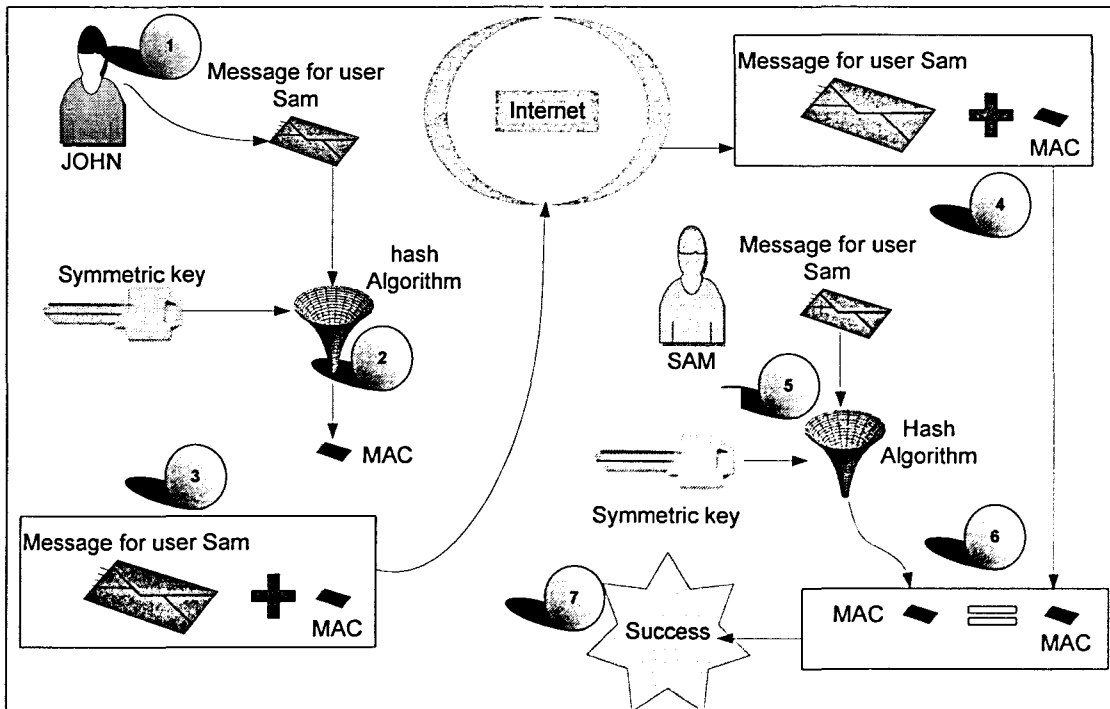


Figure 12.1: Mac process

As illustrated in figure 12.1, John wishes to send a secret message to Sam. In order to secure the integrity of the message during the transmission, John will sign the message using a MAC algorithm. In order for the MAC algorithm to provide a MAC that is unique for this specific message, and linked to John, a secret key must be provided. This secret key is shared between Sam and John as illustrated in figure 12.1. The secret key provided by John to generate a MAC for the message is exactly the same as the secret key that Sam will provide to test the MAC.

Step 1

John generates the message that he intends to send to Sam.

Step 2

John provides a secret key to the hash algorithm, and the hash algorithm uses this secret key to generate the MAC of the provided message.

Step 3

The message and the MAC are added together in the same message parcel to be sent via the network to Sam. If a hacker should intercept this message, the hacker will be able to read the message as it is not encrypted; however the hacker would not be able to alter the message in any way- as altering of the message will result in the MAC test to fail when tested. In order to generate a new MAC, the hacker must be in possession of the secret key used by John to generate the MAC.

Step 4

Sam receives the message sent by John. This message contains the original message sent by John and also the generated MAC of this message.

Step 5

Sam will read the message, and to ensure that the message is unaltered and sent by the authentic John, Sam will pass the message through the same hashing algorithm that John used, applying the same secret key, John applied. This will generate a new MAC of the message received from John.

Step 6

Sam will then compare the freshly generated MAC with the MAC received from John.

Step 7

As the message was not altered during transmission, and it was indeed the authentic John that generated and sent the MAC, the fresh MAC and the received MAC will match 100%, resulting in a successful MAC matching. The authenticity of John is proved by Sam using the mutual secret key shared only between the two of them.

Currently a number of MAC algorithms exist, and are widely available for usage to ensure the integrity of a message and the authenticity of the sender. All the algorithms rely on a secret key, which must be symmetrical to the original key. Even in a PKI environment, the key used to sign the message (private key) and the key used to test the signature are mathematically related to each other and the eventual key part used in the MAC process, is symmetrical.

12.3.2. Biometric MAC

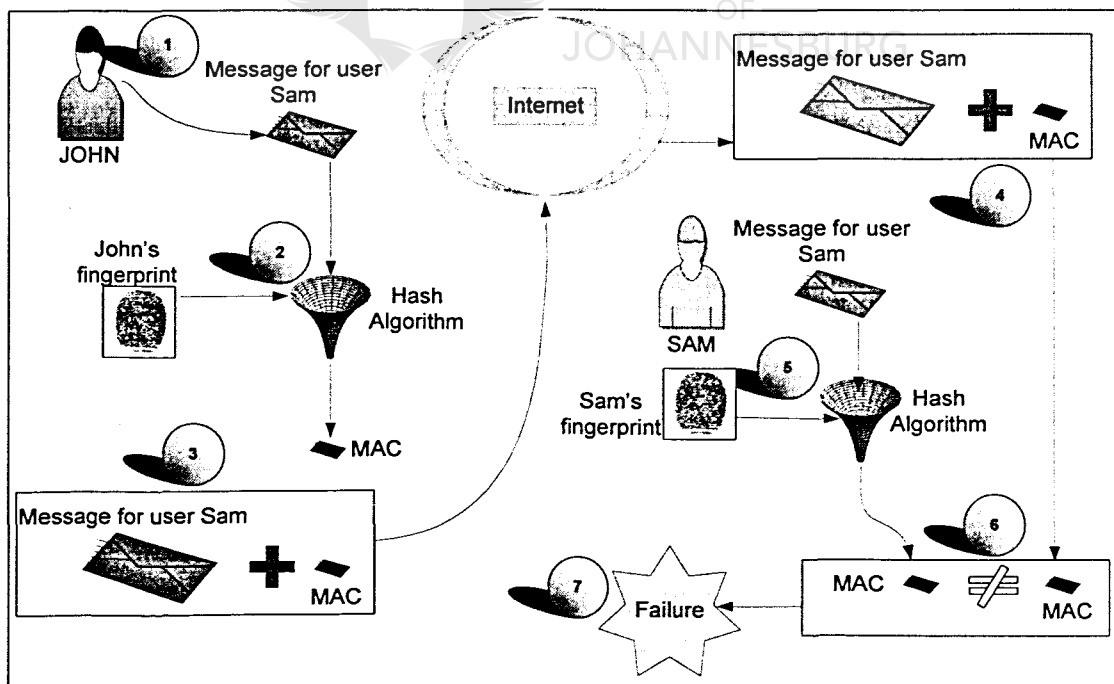


Figure 12.2: Using biometric data for MAC generation

If a biometric characteristic is used in stead of a secret key, the testing of the MAC results in failure, and is illustrated in figure 12.2.

Step 1

John generates the message that he intends to send to Sam.

Step 2

John provides his fingerprint to be used by the MAC algorithm as the secret key for the MAC process. The hash algorithm uses this biometric characteristic to generate the MAC for the provided message.

Step 3

The message and the MAC are added together in the same message parcel to be sent via the network to Sam. If a hacker should intercept this message, the hacker will be able to read the message as it is not encrypted, however the hacker would not be able to alter the message in any way, altering of the message will result in the MAC test to fail. In order to generate a new MAC, the hacker must be in possession of the biometric characteristic that was used to generate the MAC.

Step 4

Sam receives the message sent by John. This message contains the original message sent by John and also the generated MAC of this message.

Step 5

Sam reads the message, and to ensure that the message is unaltered and sent by the authentic John, Sam passes the message through the same MAC algorithm that John used, applying *her* biometric characteristic (as she does not

have John's biometric characteristic). This will generate a new MAC of the message received.

Step 6

Sam compares the freshly generated MAC, (generated using her biometric characteristic), with the MAC received from John (generated using his biometric characteristic).

Step 7

As the secret keys used (in this example two different biometric characteristics) to generate the two message authentication codes are not the same, the testing of the MAC fails.

12.3.3. Conclusion

Once again it is clear that the secret key used for generating the MAC and the secret key used for testing the MAC must be symmetrical. If John generated a MAC using his biometric characteristic, Sam would not be able to test the MAC, as her biometric characteristic will be significantly different, and for this reason would not be able to generate the same MAC.

Secondly, if John signed a document, and generated a MAC using one of his fingerprints, he would not be able to test the MAC at a later stage, as he will not have the ability to provide the same fingerprint again that was used to generate the MAC.

From the above mentioned example it becomes apparent that a biometric characteristic cannot simply be used as the secret key to generate a MAC. John used his biometric characteristic as the secret key for generating a MAC of the

message destined for Sam; Sam would not be able to provide the same biometric characteristic to test the MAC.

12.4. USING BIOMETRICS CHARACTERISTICS TO GENERATE A MAC.

In this section, the BioVault infrastructure is used to allow John to sign a message using his biometric characteristic. This method relies on the fact that both John and Sam are part of the BioVault environment – very much as EBay [98] relies that buyers and sellers are both part of the PayPal [100] environment, as discussed in Chapter 7 (Electronic commerce).

The BioVault-based process to generate a MAC using a biometric characteristic is a 6-phased process.

- *In the first phase* John creates a message and signs this message, using his biometric characteristic. Then John generates two message bundles:
 - A message bundle destined for the authentication server containing a BioVault bio-parcel, and the MAC generated during the signing process.
 - The message bundle destined for Sam, containing the message for Sam, and the MAC generated during the signing process by John.
- *In the second phase*, the authentication server receives the message bundle that contains the MAC and a bio-parcel. The server handles the bio-parcel according to the rules prescribed by BioVault version 3.0, and associates the fresh biometric data from John with the received MAC in John's SBA.
- *In the third phase*, Sam reads the message from John, and in order to test the MAC she generates a new message bundle. This message bundle includes:

- A BioVault bio-parcel.
- The MAC received in her message bundle.

She sends this new message bundle to the authentication server.

- *In phase 4*, the server will test Sam's authenticity using the received bio-parcel. If the server is content with Sam's authenticity, the server proceeds to phase 5.
- *In phase 5*, the server generates a new bio-parcel destined for Sam. The bio-parcel includes the biometric data John used to generate the MAC of Sam's message. The server sends the bio-parcel to Sam via the internet.
- *Phase 6*, Sam extracts John's biometric data from the received bio-parcel as sent by the server, and uses this biometric data to MAC the message she received from John in order to test the integrity of the message received.

Diagram 12.3 illustrates the first phase that John follows to sign a message. This message is sent to Sam, who needs to test the integrity of this message.

12.4.1. Phase 1 – Signed message destined for Sam

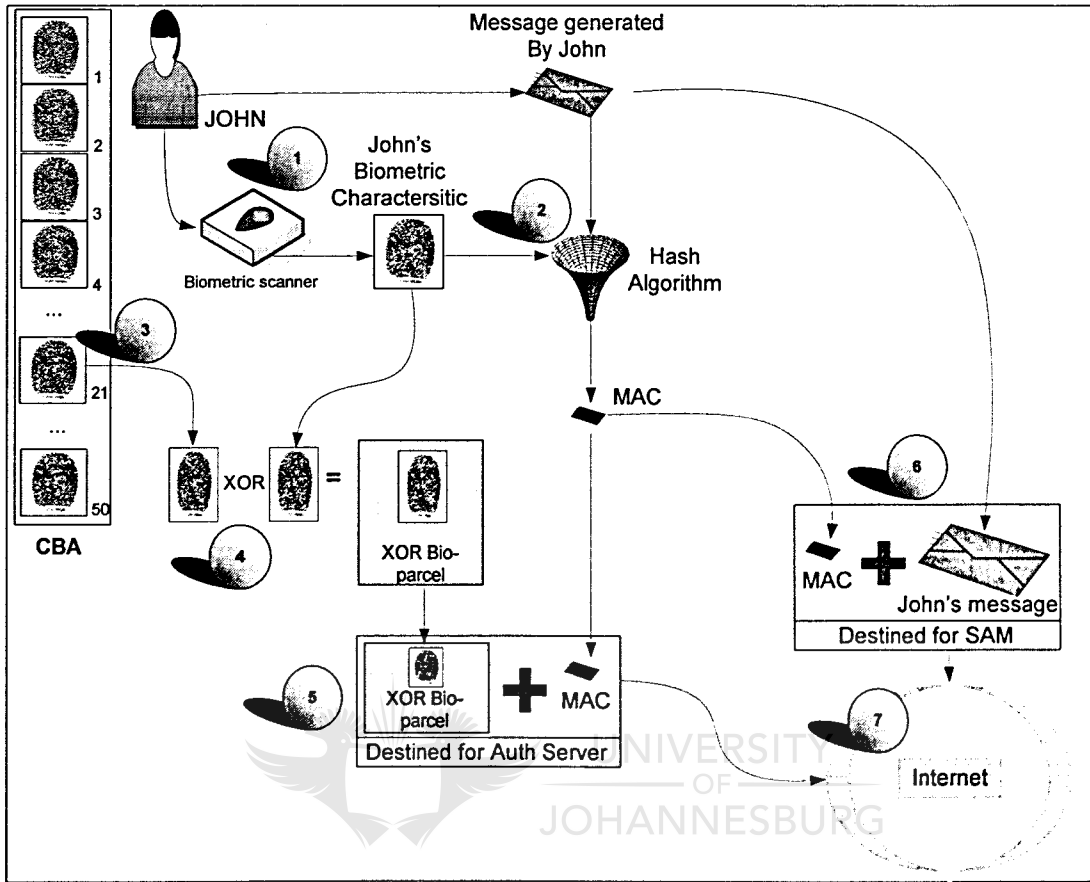


Figure 12.3: Signed message destined for Sam

John intends to send a message to Sam. This message does not necessarily contain any sensitive information. However, it is important that the authenticity of the message can be confirmed beyond any doubt, and that the integrity of the message can be tested. Therefore John signs the message using his biometric characteristic. Figure 12.3 illustrates the first phase in this process that relies on the BioVault version 3.0 infrastructure.

Step 1

John provides a fresh biometric characteristic to the biometric scanner. The scanner digitizes the biometric characteristic and forwards the digitized electronic version of the biometric characteristic to the driver software of the biometric device.

Step 2

The freshly digitized biometric characteristic is used as the secret key for a hashing algorithm to generate a unique MAC for the message from John.

Step 3

During a previous encounter with the authentication server, the server sent a challenge to John (as per BioVault version 3.0). This challenge demanded specific biometric data from John's CBA that had to be included during the next contact he makes with the authentication server. In the figure 12.3, this request required the 21st biometric data in John's CBA. The system will thus automatically obtain the 21st biometric data from John's CBA.

Step 4

The BioVault client-side software takes the biometric data of the fresh biometric characteristic (that was also used as the secret key in the hashing algorithm) and XOR's the fresh biometric data with the 21st biometric data obtained during step 3, resulting in the XOR bio-parcel.

Step 5

The MAC generated in step 2 is then concatenated with the bio-parcel, resulting in a message bundle. This bundle (consisting of the MAC and the bio- parcel) is addressed to the authentication server.

Step 6

A second message bundle is created. The message bundle consists of the MAC generated in step 2 and the message John generated. This message bundle is addressed to Sam.

Step 7

The two message bundles are then sent via the network to the authentication server and to Sam respectively. If these messages are sniffed during transmission, the hacker would be in possession of a XOR bio-parcel that he cannot use, a MAC, that he cannot re-create, and a clear text message that he can read. This is not necessarily a sensitive message, as mentioned earlier, but if the hacker alters the message, the subsequent testing of the MAC will fail when Sam tests the MAC.

The two messages are delivered to the authentication server, and to Sam. The second phase illustrates the actions that the authentication server follows.

12.4.2. Phase 2: Authentication Server

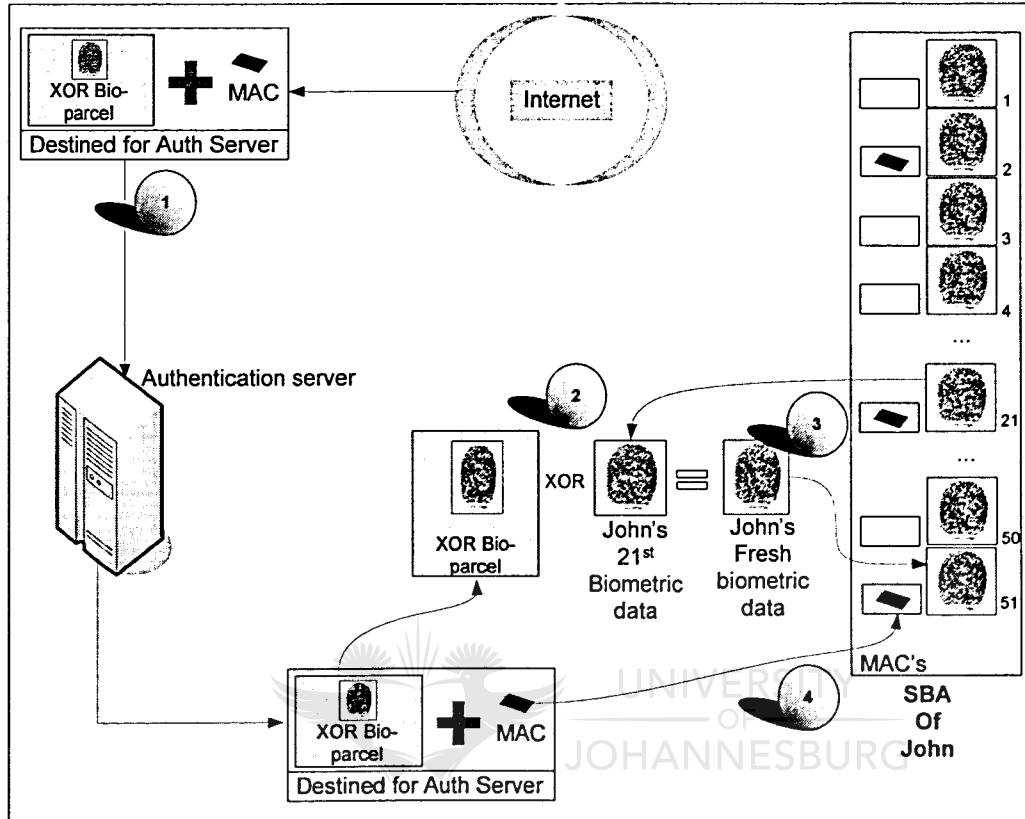


Figure 12.4: Authentication server process

During the second phase the server receives the message bundle John sent. The process the server follows is now discussed based on figure 12.4.

Step 1

The server receives the message bundle from John. The message bundle includes:

- A bio-parcel and,
- A MAC.

The server is aware that the bio-parcel must conform to the rules as stipulated in BioVault version 3.0.

Step 2

During previous communication with John, the server sent John a challenge to supply the 21st biometric data. For this reason the server will collect the corresponding biometric data from John's SBA (by using the marker that points to the requested biometric data as mentioned in section 10.6, step 2).

The server extracts the bio-parcel from the message bundle and XOR this bio-parcel with the corresponding biometric data from John's SBA. This step yields the fresh biometric data from John. The server tests the fresh biometric data from John for replay and authenticity as prescribed by the rules of BioVault version 3.0.

Step 3

If the server is content with the fresh biometric data, this biometric data is added to the SBA of John.

Step 4

The server obtains the MAC received in the message bundle from John and associates this MAC with the fresh biometric data received, in John's SBA. (Biometric data # 51 in figure 12.4)

The server now possesses the MAC and the secret key (biometric data) used to generate that MAC.

In the next phase it will be illustrated how Sam contacts the authentication server to ensure that the message sent by John is authentic.

12.4.3. Phase 3: Sam requests the biometric MAC key.

Sam received her own message bundle from John. This message bundle contained:

- The message, that Sam can read immediately, as well as a
- MAC to ensure the integrity of the message sent by John.

If Sam wishes to test the MAC, she will follow the method as illustrated in figure 12.5.

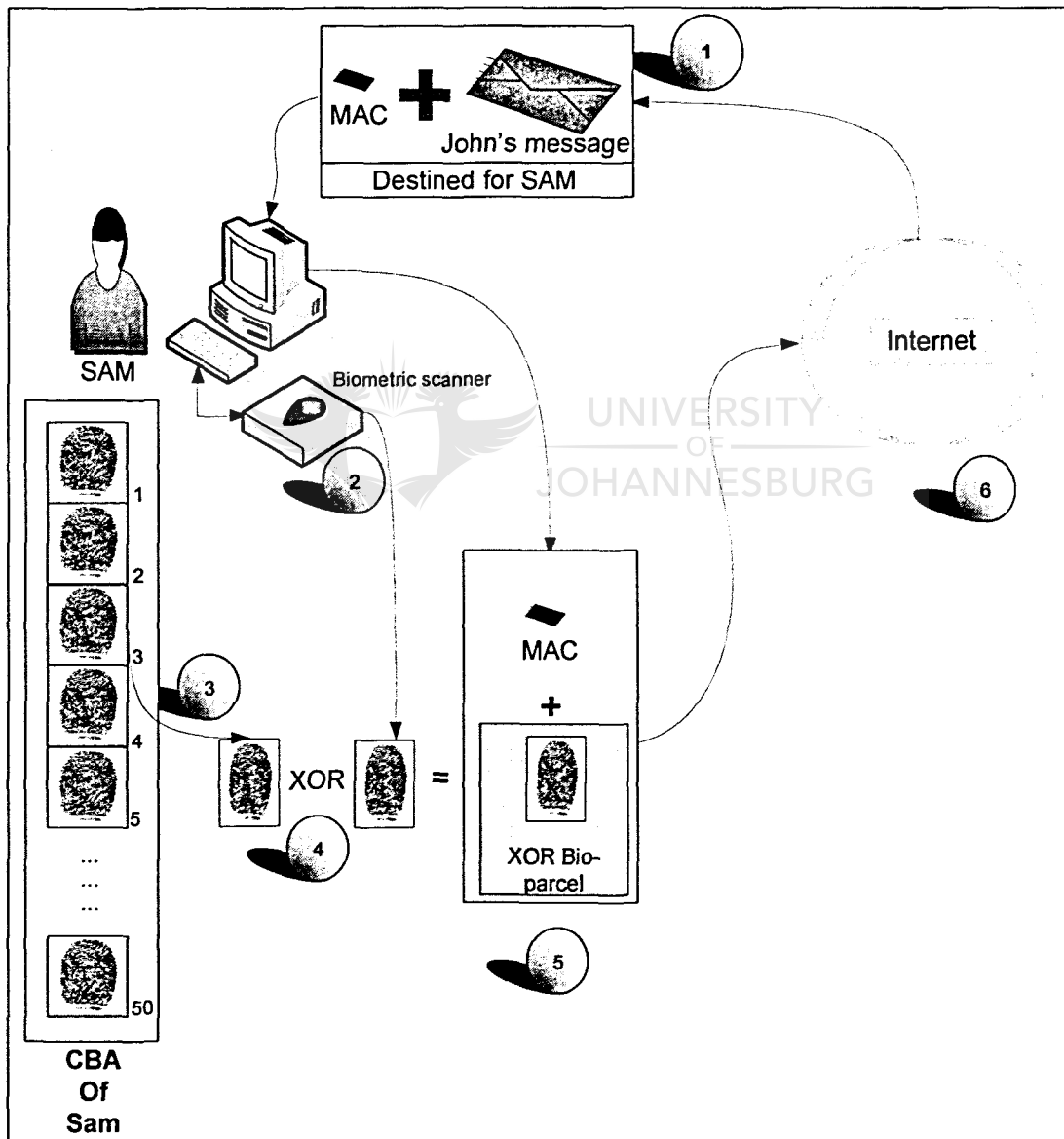


Figure 12.5: Request for biometric data

During this phase Sam receives the message bundle John sent her. She generates a message bundle destined for the authentication server to request the biometric data John used to generate the MAC for this message.

Step 1

Sam receives the message bundle from John, consisting of the clear text message and the MAC of this message. Sam can read the message, but to test the MAC she proceeds to the second step in this phase.

Step 2

Sam provides a fresh biometric characteristic as shown in step 2 to the biometric scanner. The scanner digitizes the biometric characteristic and forwards the digitized electronic version of the biometric characteristic to the driver software of the biometric device.



Step 3

During a previous encounter with the authentication server, the server sent a challenge to Sam (as per BioVault version 3.0). This challenge demanded a specific biometric data from Sam's CBA that had to be included during the next contact that she makes with the authentication server. In the current example, this request pointed to the 3rd biometric data in Sam's CBA. The system will thus automatically obtain the 3rd biometric data from Sam's CBA.

Step 4

The BioVault client-side software takes the electronic representation of the fresh biometric data, and XOR's this fresh biometric data with the electronic representation of the 3rd biometric data obtained during step 3, resulting in the XOR bio-parcel.

Step 5

The MAC received from John in step 1 is concatenated with this bio-parcel, resulting in a message bundle. This message bundle (consisting of the MAC and the bio-parcel) will be addressed to the authentication server.

Step 6

This message bundle destined for the authentication server, is sent by Sam via the internet to the authentication server.

The server receives the message bundle from Sam during the next phase, and supplies Sam with the biometric data that was used to generate the MAC of the message.

12.4.4. Phase 4: Confirm Sam's authenticity.

During this phase the server receives the message bundle from Sam, as well as the MAC John generated. The server tests Sam's authenticity according to the rules of BioVault version 3.0.

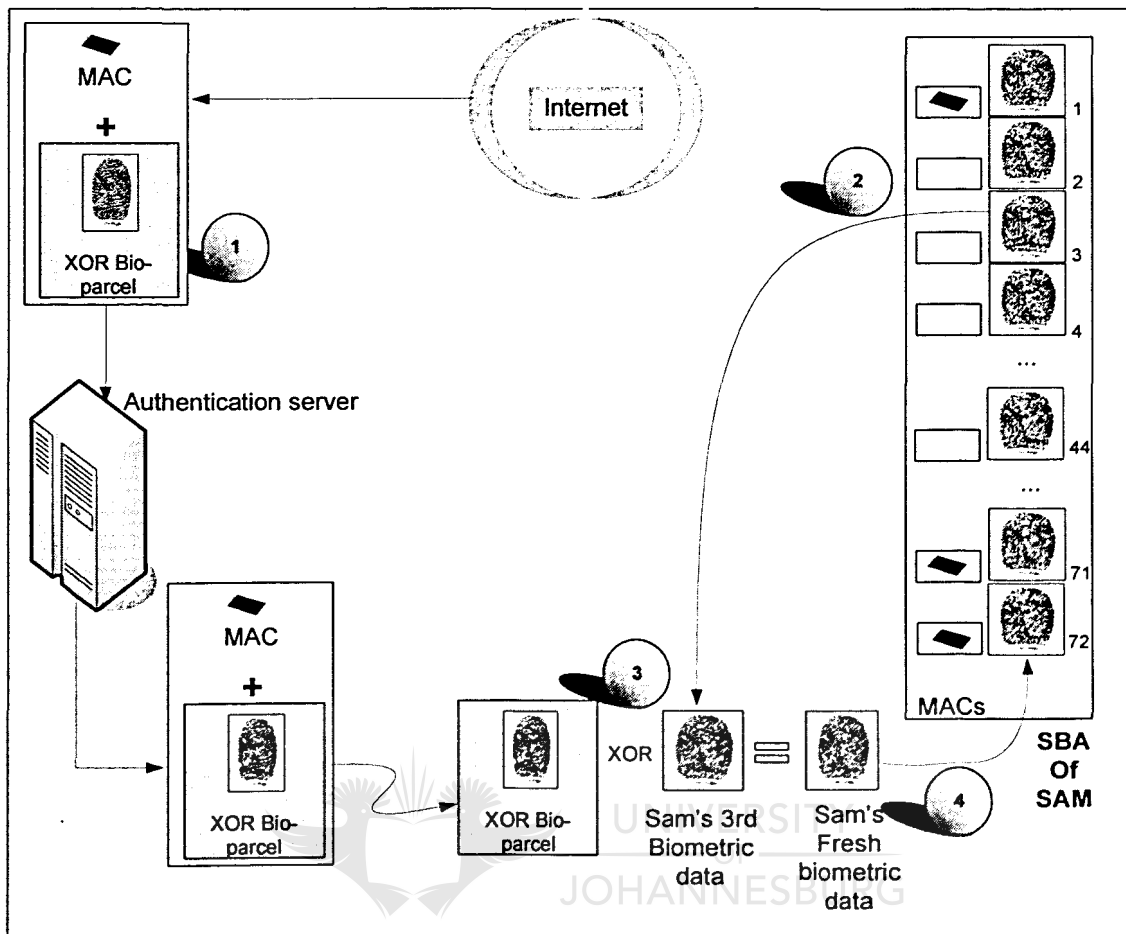


Figure 12.6: Sam's authenticity confirmation

Step 1

The server receives the message bundle from Sam. This message bundle includes a bio-parcel and a MAC. The server assumes that the bio-parcel must conform to the rules as stipulated in BioVault version 3.0.

Step 2

During previous communication with Sam, the server sent Sam a challenge to supply the 3rd biometric data in Sam's CBA. For this reason the server obtains the biometric data from Sam's SBA that corresponds with the 3rd biometric data in Sam's CBA.

Step 3

The server extracts the bio-parcel from the message bundle and XOR's this bio-parcel with the 3rd biometric data from Sam's SBA. This step yields the fresh biometric data from Sam. The server tests this fresh biometric data for replay and authenticity as prescribed by the rules of BioVault version 3.0.

Step 4

If the server is convinced of the authenticity of the fresh biometric data, this biometric data will be added to the SBA of Sam. The server obtains the MAC received in the message bundle from Sam and associates this MAC with the fresh biometric data added to Sam's SBA (Biometric data #72 in figure 12.6)

Once the server has confirmed that the current communication is with the authentic Sam, the server proceeds to the next phase to supply Sam with the biometric data that John used to generate the MAC.

12.4.5. Biometric data supplied to Sam.

In this phase the server sends Sam the biometric data that John used in the first phase to generate the MAC for the message she received.

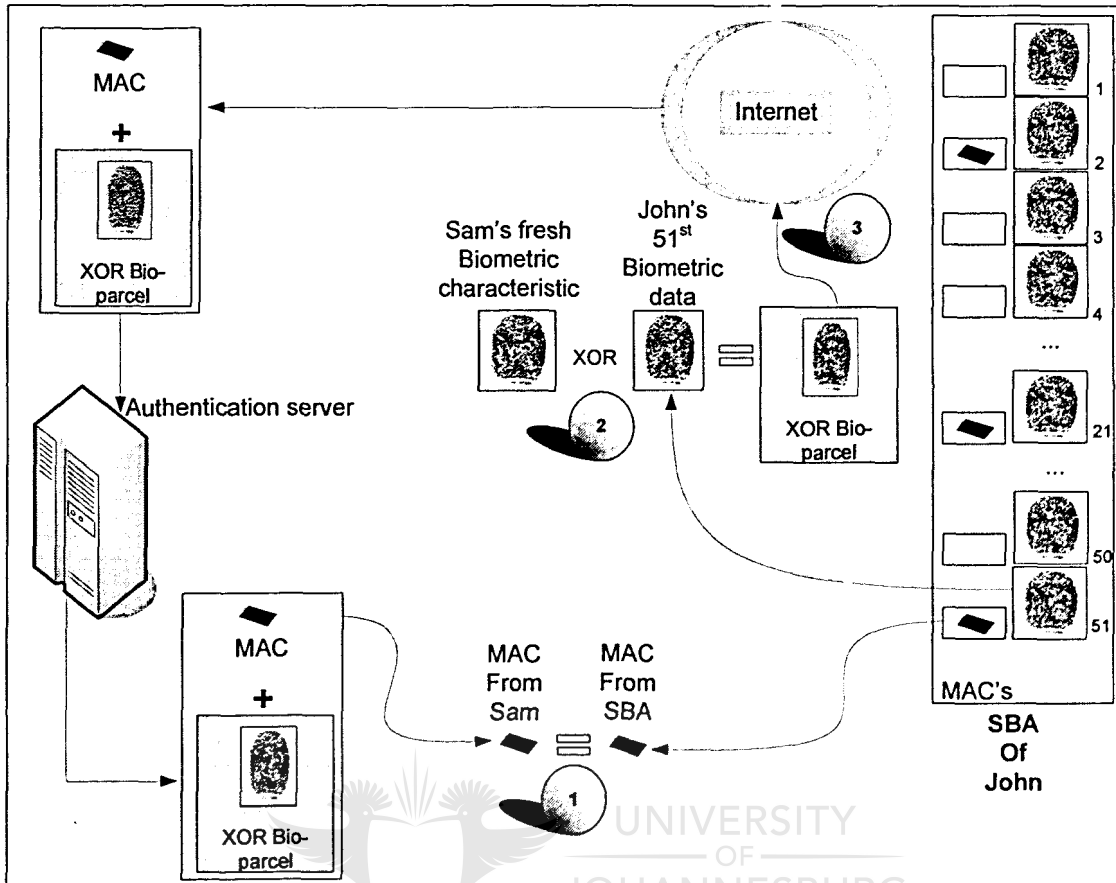


Figure 12.7: Supply of biometric data to Sam

During phase 4 the authentication server extracted Sam's fresh biometric data from the bio-parcel. The second part of the message bundle consisted of the MAC that John used to generate the message that was sent to Sam. In this phase the authentication server will check to see if this MAC exist in John's SBA, and if it does the authentication server will generate a new bio-parcel destined for Sam.

Step 1

The authentication server searches John's SBA for a match of the MAC that Sam sent in the message bundle. The server determines that the MAC received from

Sam in the message bundle, matches the MAC associated with the 51st biometric data in John's SBA.

Step 2

The authentication server uses the fresh biometric data Sam supplied in the message bundle and XOR's this fresh biometric data with the 51st biometric data found in John's SBA. This step will thus result in a new bio-parcel, destined for Sam.

Step 3

During the last step, the authentication server submits the new bio-parcel back to Sam.

In the final phase Sam extracts the biometric data that John used to generate the MAC of the message she received earlier. She finally uses this biometric data to test the MAC that she received with the message earlier to ensure the integrity of the message.

12.4.6. Phase 6: Test message's integrity.

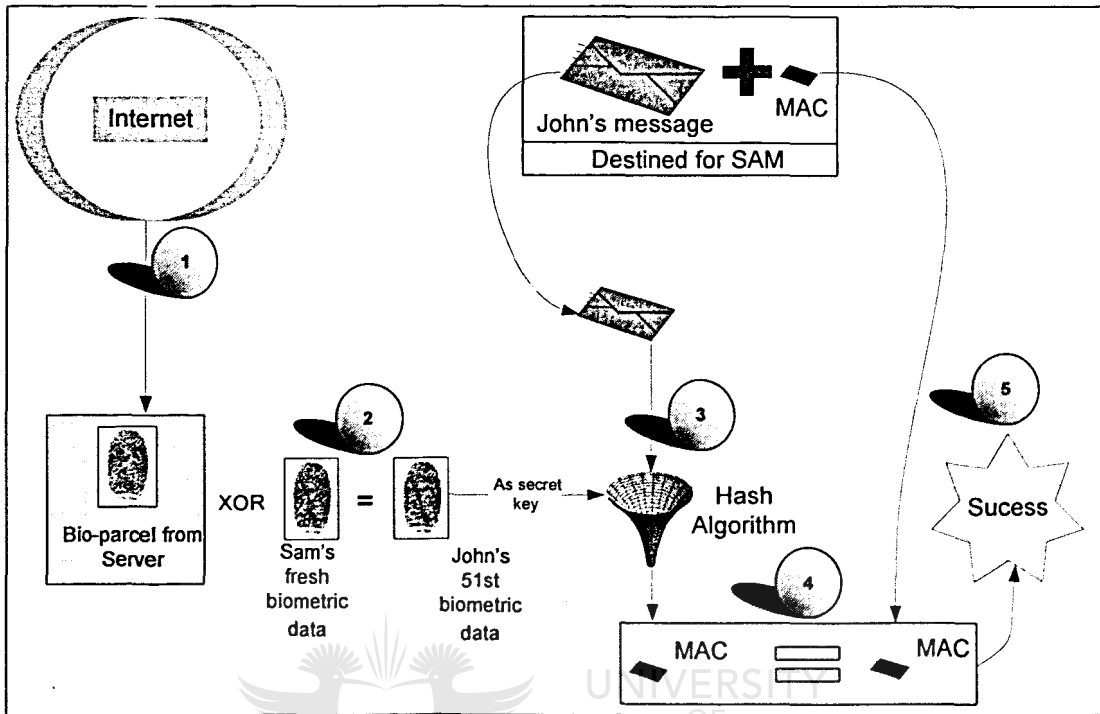


Figure 12.8: Test MAC using biometric data

Step 1

Sam receives the bio-parcel sent by the server during phase 5.

Step 2

Sam XORs her fresh biometric data that she generated in the 3rd phase, with the bio-parcel received from the server. This will yield the 51st biometric data that John used to generate the MAC of the message sent to Sam in phase 1.

Step 3

Sam uses the biometric data extracted from the bio-parcel, received from the authentication server, as the secret key for the hashing algorithm. This biometric

data as secret key is used to generate a MAC of the message that she received from John. This step will result in a fresh MAC being generated for the message from John.

Step 4

Sam compares the MAC that she received in the message bundle from John, with the MAC that she generated in step 3.

Step 5

As the message was indeed generated with the 51st biometric data in John's SBA, and the message was not tampered with, the testing of the MAC is a success, proving that the message from John is authentic and has not been altered at all since John sent the message.

At this stage Sam can be satisfied that the message is indeed from the authentic John, as his biometric data, which is directly related to him, generated the same MAC for the message. This also proved that the message was un-tampered with, and that the integrity of the message is above suspicion.

12.5. CONCLUSION

This chapter demonstrated successfully that the BioVault version 3.0 infrastructure can be used to facilitate the signing of documents in order to insure the integrity and authenticity of the document. This is extremely beneficial as the biometric data is directly linked to the signing party and for this reason allows non-repudiation to be enforced successfully.

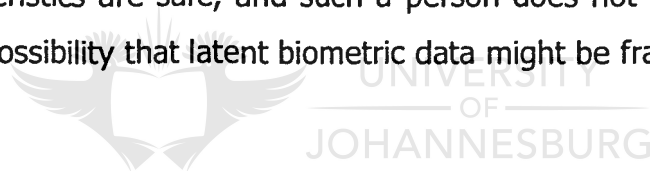
It is clear that there are once again certain similarities to the PKE environment, however, in the BioVault version 3.0 environment, a user does not need to

protect his “private key” as the private key is actually his biometric characteristic, and can subsequently be linked to the biometric key used to sign the document.

A user can, in the BioVault version 3.0 environment, become the signing party on behalf of a company, without this role interfering with his or her private status.

If a user at any stage feels that his or her identity is compromised in one or other way, this user can remove all existing biometric data inside the BioVault version 3.0 environment, cleaning all CBA and SBA data, removing the reference biometric template. A user can start with a clean slate, re-creating the SBA and CBA, with a fresh reference biometric template. The old “identity” is archived.

As long as a person is part of the BioVault version 3.0 environment, the person’s biometric characteristics are safe, and such a person does not need to concern himself with the possibility that latent biometric data might be fraudulently used.



Chapter 13: Conclusion

13.1. OVERVIEW

This chapter is the conclusion of the research of this thesis. In this chapter the aim and problem statement of this research will be considered. It will be shown in this final chapter that the BioVault model developed during this research, successfully solves the problems associated with biometric characteristics used for identification and authentication.

13.1. PROBLEM STATEMENT OF THIS THESIS:

If biometric technology is to be considered as the standard to identify and authenticate persons, the risk of the biometric being stolen is high. A biometric characteristic cannot be simply replaced as one would replace a stolen token or password.



The original statement as formulated in Chapter 1, page 6 was:

Firstly, biometric data in electronic format can be stolen in various ways and be replayed at a later stage for false identification and authentication. The electronic data of a biometric can be acquired from various sources. For instance, during the capturing phase of the biometric data, during the transmission phase from the biometric device to the terminal, or even when the biometric data is sent over a network – to name only a few.

Secondly, a fake biometric characteristic can be manufactured for a given biometric in order to deceive the biometric matching algorithm into authenticating the manufactured fake biometric characteristic; e.g. a fake latex biometric characteristic can be manufactured from a latent finger print left by a person on a glass.

The problem statement mentions two specific problems to be solved

- 1) Biometric data replay
- 2) Manufacturing of a fake biometric characteristic.

Due to the two mentioned problems, the wider application of biometrics for identification and authentication – specifically if used for digital signatures – is still hazardous.

13.2. MENTIONED DELIVERABLES OF THE THESIS:

The following deliverables were mentioned in Chapter 1 of this thesis:

1. A complete system for detecting biometric misuse attempts.
2. A system that will ensure the safe keeping of biometric tokens during network transmission.
3. A system that will allow users of this model to encrypt sensitive information using biometrics.
4. A system that will allow users of this model to digitally sign electronic documents using biometrics.

13.3. EVALUATION OF THESIS SUCCESS.

If the thesis is considered, it is concisely clear that the problem statement was successfully solved, and that all the deliverables of this thesis were delivered.

However, let us have a brief look at the various aspects as listed in section 13.1 and section 13.2.

13.3.1. Solutions to problem statement

Biometric data in electronic format can be stolen in various ways and be replayed at a later stage for false identification and authentication. The electronic data of a biometric can be acquired from various sources. For instance, during the capturing phase of the biometric data, during the transmission phase from the biometric device to the terminal, or even when the biometric data is sent over a network – to name only a few.

Chapter 8 introduced BioVault version 1.0. This version of BioVault included a Server-side bio-Archive. This archive gave the server the ability to store (ordered) each and every biometric token ever received from the user. If a biometric token is submitted over the network, and intercepted, the resulting replay attempt will fail, as the server will find that the illicit biometric data from the hacker, matches the previously offered biometric data from the user exactly.

Chapter 8 managed to solve the first of the two major problems as stated in the problem statement successfully. However chapter 8 only solved the problem of biometric data that was presented and accepted by the authentication server. If a hacker managed to obtain biometric data that was never presented to the server, BioVault version 1.0 would fail. Biometric data generated from a fake biometric characteristic, or acquired from the biometric device directly (but never submitted to the server) would not be detected by BioVault version 1.0.

A fake biometric characteristic can be manufactured for a given biometric in order to deceive the biometric matching algorithm into authenticating the manufactured fake biometric characteristic; e.g. a fake latex biometric characteristic can be manufactured from a latent finger print left by a person on a glass.

If a fake biometric characteristic is manufactured and used for identification and authentication, the hacker will have an unlimited supply of biometrics to offer to the authentication server. In order to solve this problem BioVault version 2.0, chapter 9, and the secure BioVault version 3.0, chapter 10, were developed.

These versions of BioVault introduced a client side bio-archive, ensuring that even if a hacker manages to generate a fake biometric characteristic, the biometric data resulting from that fake biometric characteristic, will not be usable at all. For this reason, BioVault version 2.0 and version 3.0 solve the second part of the problem statement.

13.3.2. Deliverables, delivered

This section will briefly indicate how this research solved the 4 deliverables as proposed in chapter 1

A complete system for detecting biometric misuse attempts.

BioVault version 1.0 as discussed in chapter 8 has the ability to detect any attempt to use previously used biometrics. The same mechanism is also included in BioVault version 2.0 and version 3.0.

A system that will ensure the safe keeping of biometric data during network transmission.

The incorporation of the XOR bio-parcel, ensures that all biometric data traversing a network are protected, without adding a complex solution such as an elaborate encryption method. Encryption has a number of issues that needs to be considered, for instance the key sizes to be used, protection of these keys,

and key management. XOR is a fast and reliable approach to protect the contents of the bio-parcel.

A system that will allow users of this model to encrypt sensitive information using biometrics.

In chapter 11, it is illustrated how biometrics can be used to encrypt a document. This solution relies on BioVault version 3.0 infrastructure. As stated in chapter 11, if biometrics are used to encrypt a document (using the BioVault infrastructure) there is a direct link between the person that encrypted the document and the key used for encryption.

A system that will allow users of this model to digitally sign electronic documents using biometrics.

The last, and probably most important deliverable of this thesis, is the fact that electronic documents can successfully be signed by using biometric characteristics. This is a significant feature of this research. The purpose of a signature of any document is to link the signer directly to the signed document. If the PKI environment is used, the signer is only linked to his private key (which is not actually part of him, and is only protected by a password or pass-phrase). The ability to use biometric characteristics links a signed document irrefutably to the signer.

13.4. CONCLUSION

The result of this thesis is a complete biometric protocol, allowing a user to use biometric characteristics for secure web communication, web identification & authentication, and to digitally sign electronic documents by using his biometric characteristic.

Four full international papers based on this research were published; the published papers are included in Chapter 15.

This research also spawned a number of other research projects, relating to technologies that might be used for the CBA, and optimization of the SBA.

Once this protocol is implemented, the problems usually associated with biometric data will finally be laid to rest.

15 May 2009.

Chapter 14: Research Results

14.1. OVERVIEW

This chapter includes all published articles that were internationally accepted. The chapter concludes with a patent that was discovered during the research of this thesis, and is referenced in this thesis.

14.2. INTERNATIONALLY ACCEPTED ARTICLES

IE3'2005 – Poznan, Poland (Attached)

- Authors:** Tait B.L., Von Solms SH
- Article title:** "BioVault: Solving the problem of replay in biometrics – an electronic commerce example"
- Book Details:** Challenges of expanding internet: E-commerce, E-business and E-government ISBN 0-387-28753-1
- Conference details:** 5th IFIP conference I3E'2005, Poznan, Poland, October 28-30, 2005.

ICGeS 2008 – UK Docklands (Attached)

- Authors:** Tait B.L., Von Solms SH
- Article title:** "Secure biometrically based authentication Protocol for a public network environment"
- Book Details:** Global e-security Springer Volume 12, ISBN 1865-0929
- Conference details:** 4th International Conference, ICGeS 2008, London, UK, June 23-25, 2008.

ICGS3'09 2009 – East London University, UK (Attached)

- Authors:** Tait B.L., Von Solms SH
- Article title:** "Biometrically based electronic signatures for a public networked environment"
- Book Details:** Published in Springer-Verlag regarding LNCS
- Conference details:** 5th International Conference on Global Security, Safety & Sustainability, ICGS3'09, London, UK.

IFIP I3E 2009– Nancy, France (Attached)

- Authors:** Tait B.L., Von Solms SH
- Article title:** "BioVault: Biometric based encryption."
- Book Details:** Published in Springer within the IFIP book series
- Conference details:** 9th IFIP Conference on e-Business, e-Services, and e-Society, I3E 2009, Nancy, France.



14.3. PATENT PROPOSAL

The attached patent was discovered during the research of this thesis. However as already mentioned in Chapter 8, this patent proposal corresponds partially to the working of BioVault version 1.0. As the reader is firmly aware at this stage, BioVault version 1.0 still includes various shortcomings, thus rendering this patent proposal of little use.

INTERNATIONALLY ACCEPTED ARTICLES

IE3'2005 – Poznan, Poland (Attached)

- Authors:** Tait B.L., Von Solms SH
- Article title:** "BioVault: Solving the problem of replay in biometrics
– an electronic commerce example"
- Book Details:** Challenges of expanding internet: E-commerce,
E-business and E-government ISBN 0-387-28753-1
- Conference details:** 5th IFIP conference I3E'2005, Poznan, Poland,
October 28-30, 2005.

BIOVAULT: SOLVING THE PROBLEM OF REPLAY IN BIOMETRICS

An electronic commerce example

Prof Basie von Solms & Bobby Tait
Johannesburg University

Basie@adam.rau.ac.za, bobby@csrau.rau.ac.za

Abstract:

One of the major risks involved in using biometrics for identification and authentication over open public networks, is the danger that the electronic biometric token (for e.g. a fingerprint or iris) can be intercepted and replayed by an unauthorized party.

Furthermore, it is possible to make an unauthorized copy of a biometric token, without the permission and knowledge of the real owner, and use that for unauthorized transactions. This can for e.g. happen when a fingerprint is 'lifted' from an object the owner has used, and a latex copy is made from this token [5].

This paper reports on a system in development, called Biovault, which addresses precisely the problems mentioned above, and which may help to make biometric tokens much safer to use over open public networks, for specific application in electronic commerce.

Key words:

Electronic Commerce, Biometrics, Biometric Tokens, Identification, Authentication, Replay, Identity theft

1. INTRODUCTION

Identification and authentication over insecure networks had always been a problem that caused serious information security risks. Several reasons for this can be identified, but the two discussed below are amongst the most serious ones.

Firstly, a password, even in encrypted form, can be intercepted by a third party, and reused or replayed at a later stage without the knowledge of the owner of the password.

The system which performs the authentication will never know whether the password is the original version originating from the real owner, or whether it is a replayed version of the password [4].

Supporting technologies like time stamps may help, but do not solve the problem completely.

Digital Identities, allowing the use of digital signatures, do offer some help, but do also not solve the problem, as there is no real relationship between the user and his digital identity.

Secondly, with both passwords and digital signatures, the real owner is not authenticated – rather the person who is in possession of the password or private key needed to create the digital signature, is authenticated [1]. If the password or private key had been compromised in any way, unauthorized people may masquerade as the real owner, and the computer system will not be able to identify this masquerading. The bottom line is that the system doing the authentication cannot determine whether the real owner, or a masquerader, is offering the password, token or digital signature.

Biometrics, of course, goes a long way in solving the second problem discussed above [2]. In most cases, the real owner of the biometric token must be present when the token is 'taken', for e.g. when a fingerprint is scanned on a digital fingerprint reader. Therefore the token is directly linked to the owner, and cannot be used by someone else [4].

Again, this is however not always true. A biometric token can be 'lifted' from an object handled by some person, and techniques do exist to make a copy of that lifted token and use it in a replay situation [5].

Furthermore, even when using biometric tokens, the same risks as for passwords exist. A biometric token send over an insecure network can be

intercepted, and replayed at a later stage, without the knowledge and authorization of the real owner.

As in the case of the password, the computer system will not know whether the token is supplied by the real owner, or by a masquerading person.

The problems discussed above are some of the major reasons why biometrics had not yet moved into the mainstream for identification and authentication over insecure networks.

The system described in this paper, Biovault, goes a long way in addressing the problems identified above.

In the following paragraphs, we will describe how Biovault does address these problems, and what future research and development are envisaged to use Biovault as a secure biometrically based identification and authentication mechanism for e-commerce over insecure networks.

2. THE BASIS OF BIOVAULT

The basic design pillar, on which Biovault is based, has to do with what we call the symmetry and asymmetry differences between password and biometric tokens.

2.1 Symmetry

When an offered password is matched by a computer system to a stored version of the specific password, a 100% match is required, i.e. the offered version must exactly match the stored version – we call this symmetric matching because the error acceptance ratio between the 2 versions must be zero to accept the offered version as valid.

2.2 Asymmetry

When an offered biometric token is matched by a computer system to a stored version of the specific biometric token, a 100% match is not required – actually the chances of a 100% match is anyway very slim. This is inherent in the mathematical algorithms used to create and match biometric tokens. The algorithms must make provision for the fact that, for e.g. a fingerprint, can be positioned a little differently on the reader as when the stored master copy was read. The error acceptance ratio between the offered and stored



versions is therefore greater than zero – the precise ratio can be set, and any offered token differing from the stored version within the error acceptance ratio, will be accepted as a match, and therefore lead to valid authentication. For this reason we call this asymmetric matching

2.3 The Token Archive (TA)

Biovault makes use of the fact that if an offered biometric token and any stored biometric token matches 100%, the chances that the offered biometric token is a replay of a previously used biometric token, is very high, and the offered biometric token is not accepted.

For this model to function a Token Archive (TA) is introduced on the Authentication Server. This TA will store all biometric tokens that the user ever used in his life time. It is quite clear that this TA might become very big, hence take long to search and match the offered token with the whole TA.

In order to speed up the searching of possible 100% matches in the TA, all biometric tokens will be sorted ascending in the TA, making it possible to do binary searching inside the TA. Using Binary Searching will allow the server to detect a possible 100% match at incredible speeds. The matching speed is described by the function $O(\text{Log}N)$ [6]. This function demonstrates that as data becomes larger, there is no significant rise in search time

The following paragraph describes the first (initial) version of Biovault.

3. BIOVAULT VERSION 1

This initial version made provision for a Biovault master copy of the owner's biometric token stored during the registration phase, as well as a Biovault Token Archive (TA) stored on the computer system.

Whenever a token is offered to the computer system, the offered token is first compared with the Biovault master copy of the token stored during registration of the user. If a non-identical match within the acceptance ratio is determined, the offered token is then compared with all versions stored in the TA. If an identical match is found with any version stored in the TA, the offered version is rejected, and the user is requested to offer another copy. The process is then repeated with the new offered copy received.

If no identical match is found between the offered copy and any version stored in the TA, the offered version is stored in the TA, and the offered version is accepted as a valid token, and the user is authenticated.

Figure 1 illustrates this operation

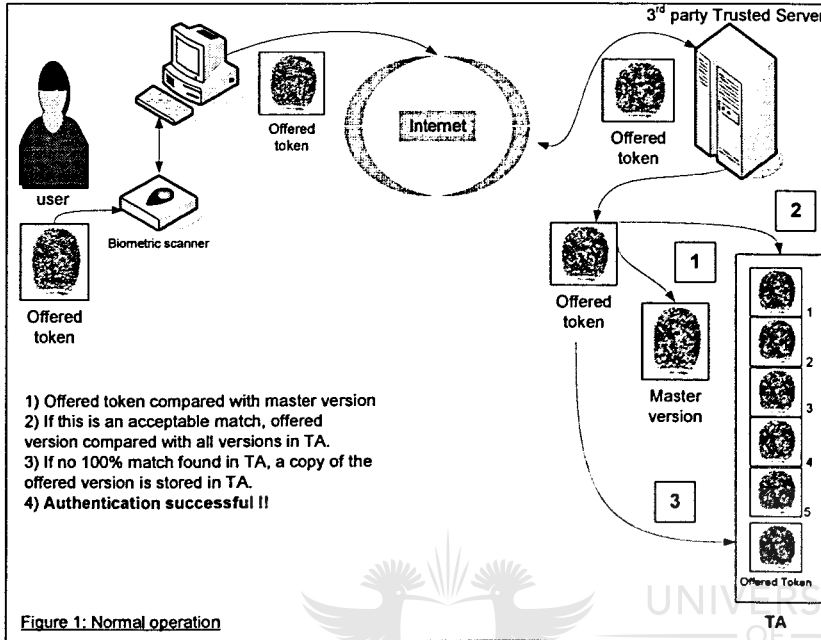


Figure 1. Normal Operation

If the offered token was intercepted while being sent to the computer system, this intercepted version could be replayed at a later stage to try to masquerade as the real owner.

Biovault Version 1 however, recognizes this replay attempt. When the replayed version was received by the computer system, it was first compared to the stored master version. If an acceptable match was found, it was compared to all versions stored in the TA. In this case a 100% would be found, because the original offered version, of which a copy was intercepted, had been stored in the TA. The replayed version would then be rejected.

This is illustrated in Figure 2.

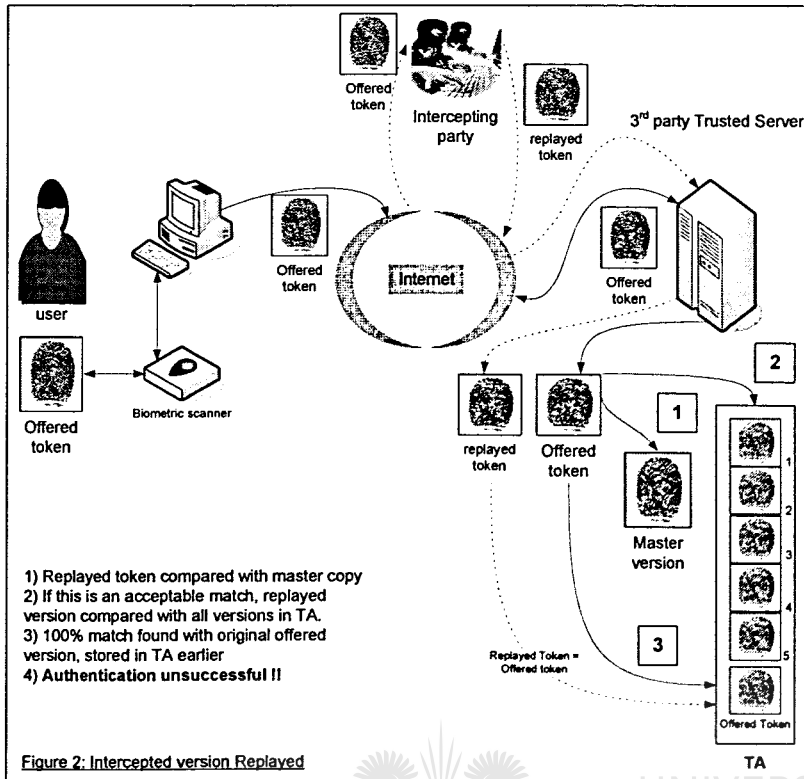


Figure 2. Intercepted version Replayed

The developed system works perfectly. It was proved easily that if an offered token is intercepted during a transaction, and the interception does not cause the aborting or termination of the transaction – ie the offered token does reach the computer system, replay of the intercepted token at a later stage, results in the replayed token being recognized as such and rejected.

The concept of the TA therefore seemed to solve some of the major problems.

However, some other problems still could not be solved.

Firstly, if a unauthorized token, ‘lifted’ from some object is replayed into the system, Biovault Version 1 accepted the lifted version, because it did not have an identical copy of the lifted version in its TA, and therefore assumed this version to be ‘unblemished’. Biovault Version 1 could not determine whether this version really came from the real owner – all it could determine

is that it had not received this version of the token before. This is illustrated in Figure 3.

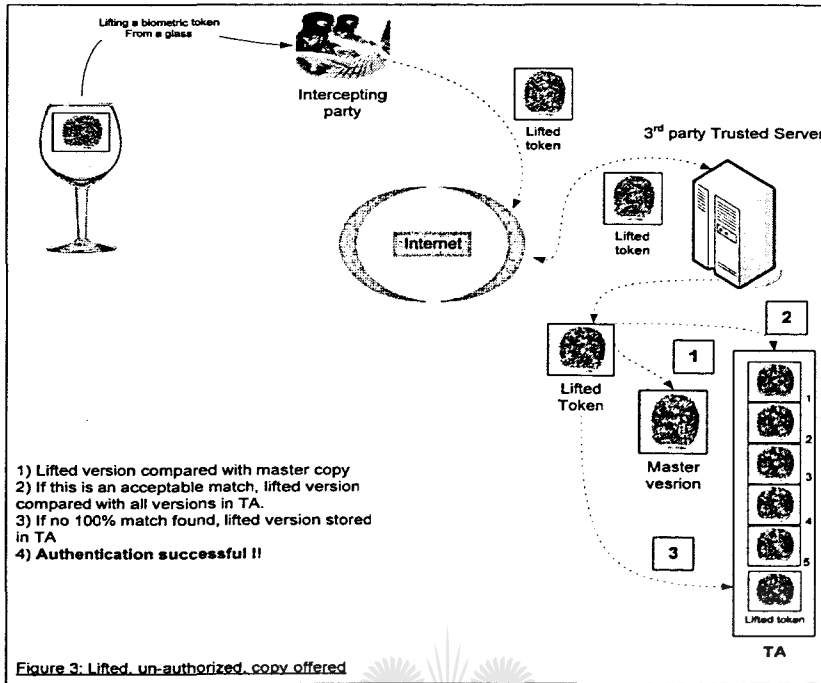


Figure 3. Lifted, un-authorized, copy offered

Secondly, it was determined that if a (clear text) token is intercepted, it is possible to ‘tweak’ the electronic version of the intercepted token in such a way that it differs from the original version just enough to be accepted by the computer system. The tweaking resulted in another version of the original token, differing just enough to still fall within the error acceptance ratio.

Biovault Version 2 addressed both problems by using encryption.

4. BIOVAULT VERSION 2

This version ensured that the offered version, ie the one acquired directly from the owner, was first ‘digitally signed’ by the owner, by encrypting it with the private key of the owner. The computer system then first decrypted

the offered version with the public key of the owner. (The reader is assumed to be up to date on the theory of Public Key encryption).

This approach solved both problems identified in Version 1.

Firstly, any 'lifted' version was not digitally signed by the owner, and when decrypted by the computer system using the public key of the owner, always resulted in an electronic string which fell outside the error acceptance ratio, and was therefore always rejected.

Secondly, trying to 'tweak' the digitally signed version of the offered token always resulted in a string which was rejected. Tweaking an encrypted version of the offered token was exceedingly more difficult than tweaking the clear text version.

Note that if a digitally signed version of the offered token was intercepted and replayed, it would immediately be recognized as a reply, because the offered version itself would by that time, be stored in the TA. This is just a more advanced case of the situation described in paragraph 3 above.

Biovault Version 2 worked perfectly, and solved many of the problems inherent in Biovault Version 1.

However, some more problems and difficulties were identified.

Firstly, requiring all participants to have a Public/Private key pair in order to digitally sign biometric tokens, placed a significant burden on potential rollout of Biovault. Furthermore this did not really improve on systems that uses biometrics to gain access to one's private key [7]. All that Biovault 2 accomplished was merely to use ones private key to gain access to your biometric token.

Secondly, we were still worried that a token, digitally signed by the owner, could be intercepted, and the transaction in some way aborted or terminated before the offered token reached the computer system. If this happened, the offered token would not become part of the TA (because the computer system never received it), and the intercepted version could then successfully be replayed at a later stage. This is illustrated in Figure 4.

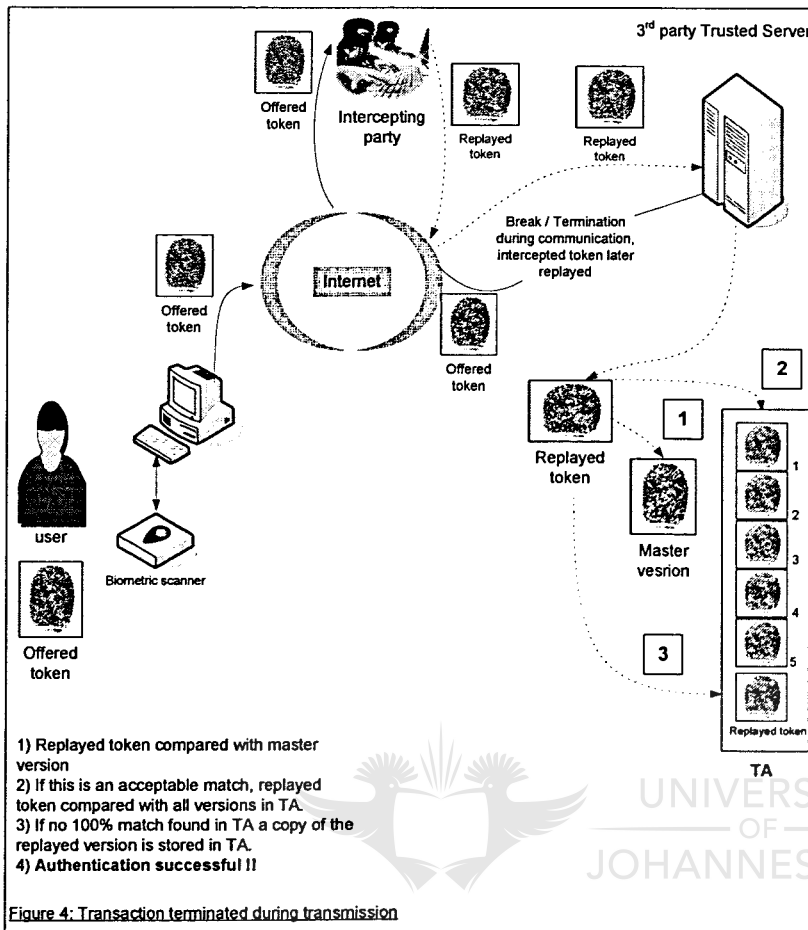


Figure 4. Transaction terminated during transmission

This resulted in Biovault Version 3

5. BIOVAULT VERSION 3

The inherent problem with Biovault Version 2 was that if a biometric token is created with the involvement of the real owner, ie a token that the owner really wants to offer to the computer system for identification and authentication purposes, the moment this token leaves the workstation of the owner, the owner has no copy or record of that token. If the token

successfully reached the computer system, a copy will be stored in the TA. However, if the offered token is intercepted during transit, and does not reach the computer system, as mentioned at the end of the previous paragraph, neither the owner nor the computer system has a copy. This means there is a 'hot' copy of the offered token, the intercepted version, out in the open. This hot copy can then be used in a replay effort at a later stage. Such an effort will most probably be successful, because the computer system does not have a copy in Biovault master TA.

As an initial option (version 3A) in solving this problem of a hot copy, a personal TA will be created on the workstation of the user, in which a copy of every token sent to the computer system was first stored locally before it was sent to the computer system and offered for identification and authentication.

This meant that no unrecorded 'hot' copies of offered tokens could exist.

By synchronizing the personal and master TA from time to time, it is possible to identify any offered tokens which was sent to the computer system, and never received by the computer system. This synchronizing effort updates the system TA, and caused any offered copy which was intercepted and never reached the computer system, to be included in the master TA. Replaying such an intercepted copy at a later stage, would the result in rejection. The reader should be able to see that this solution solves the problem illustrated in Figure 4. This is illustrated in Figure 5

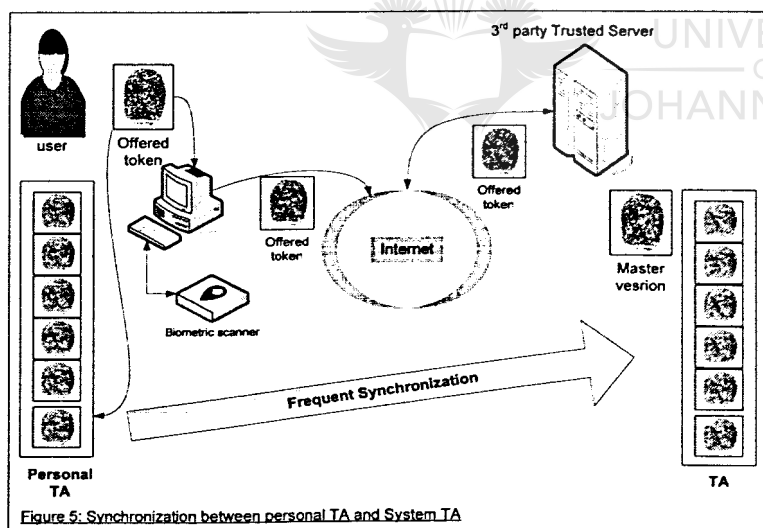


Figure 5. Synchronization between personal TA and System TA

6. A PRACTICAL E-COMMERCE APPLICATION OF BIOVAULT.

One of the primary objectives during the development and research of Biovault was that the developed system must be usable for electronic commerce. Electronic commerce can benefit from an environment where the client can be sure that his money will only be paid from his account on his request. The money vendor like Visa card [8], wants to be sure that the request to pay money, came from a authentic account holder, and a seller like Amazon [9] want to be ensured that they will get their money, and preferably not be informed that the transaction was fraudulent, after goods have been dispatched.

With the development of Biovault, the possibility of biometric replay is not of much concern. In order to demonstrate the usage of Biovault during an online purchase, the process will be discussed in two phases. Figure 6 illustrates the first phase of purchasing a book from Amazon [9]

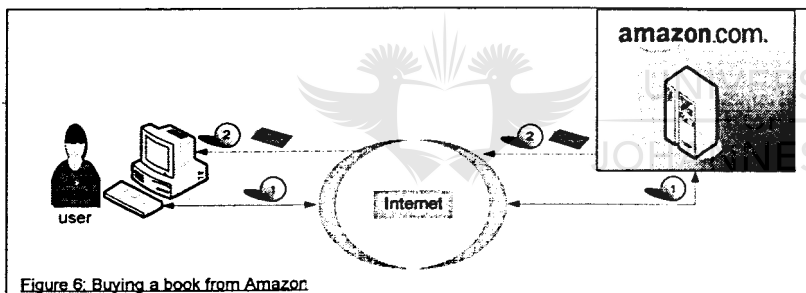


Figure 6. Buying a book from Amazon

During this phase the user will visit the website of Amazon as shown in step 1. The user will then find the book that he wishes to buy, place it in his shopping cart, and proceed to the checkout section on Amazon's website.

Amazon will then inform the user the total amount payable, including shipping and handling, this is illustrated by the little envelope in step 2. This is a familiar process to everybody that buys a book from Amazon. The next phase will demonstrate how the user will use the Biovault model to pay for the book. Currently, when a user uses a token like a credit card to pay for a

transaction, the Visa Card server is contacted by the seller to ensure that the credit card is authentic and that the card is not reported as stolen. Once the authenticity is verified, Visa will inform the seller that the money will be paid, and an authorization code is supplied [8] to the seller. With the Biovault environment the same basic model will be used, and is illustrated in figure 7

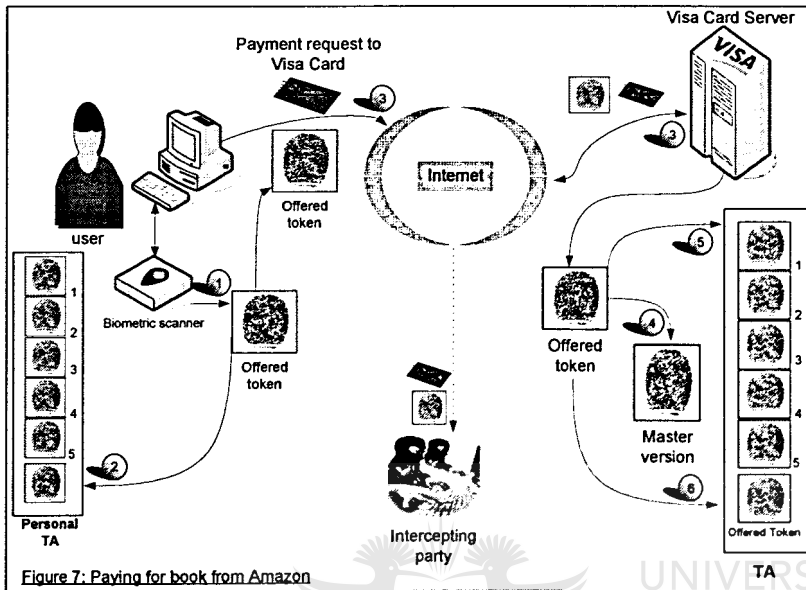


Figure 7. Paying for a book from Amazon

During the first step the user provides a fresh biometric token, this fresh biometric token will be placed in the personal TA during step 2. This will ensure that one keeps track of all biometric tokens destined for payment. The user will then submit the payment request and fresh biometric token to his money vendor, in this example Visa, during step 3.

Take note that the offered biometric token and payment request to Visa is sniffed by an intercepting party during transmission. Step 4 illustrates how the Biovault mechanism authenticates the user against the master version of the biometric token. If the matching algorithm is satisfied with the offered biometric token, the system will proceed to step 5 to confirm whether this offered token is unique and not a replayed old token already in the TA.

If the system did not discover an identical copy in the TA, the new offered token will be added in to the TA in the last step.

At this stage the Visa server is satisfied that it is the authentic user that is requesting money to be paid to Amazon. The Visa server will typically now confirm that the user has the necessary funds available to pay for the Amazon transaction.

If the funds are available, the Visa server will provide Amazon with an authentication code (step 2), for the amount payable. The user will receive a transaction result directly from the Visa Server in step 3. This is illustrated in Figure 8.

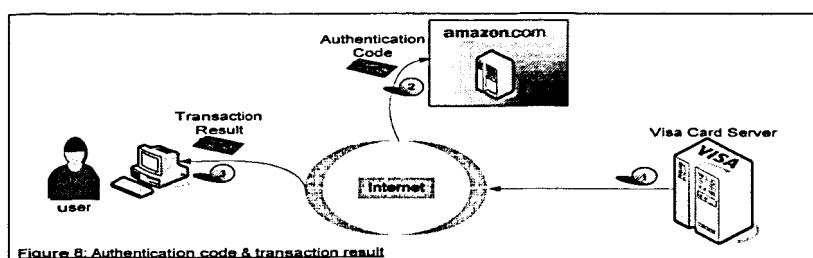


Figure 8. Authentication code & transaction result

7. REPLAY OF INTERCEPTED BIOMETRIC TOKEN.

In order to complete the electronic commerce example, figure 9 illustrates the scenario of a hacker replaying the sniffed biometric token procured earlier in figure 7.

The intercepting party would typically alter the payment request for Visa in such a way that the money must be paid to a Swiss bank account, this results in an updated payment request. The intercepting party will then submit the replayed biometric token and updated payment request to the Visa server indicated by step 1, figure 9.

The Visa server will receive the payment request and biometric token (step 2 in figure 9) and match the replayed token to the master version (step 3 in figure 9). If the matching algorithm is satisfied with the matching ratio, the replayed version will be compared to all the old biometric tokens in the TA (step 4 in figure 9). Step 5 in figure 9 indicates that the token supplied is a token that has been used at an earlier stage, because a 100% is found with a biometric token in the TA.

For this reason the Authenticity of the user is rejected and the transaction is unsuccessful.

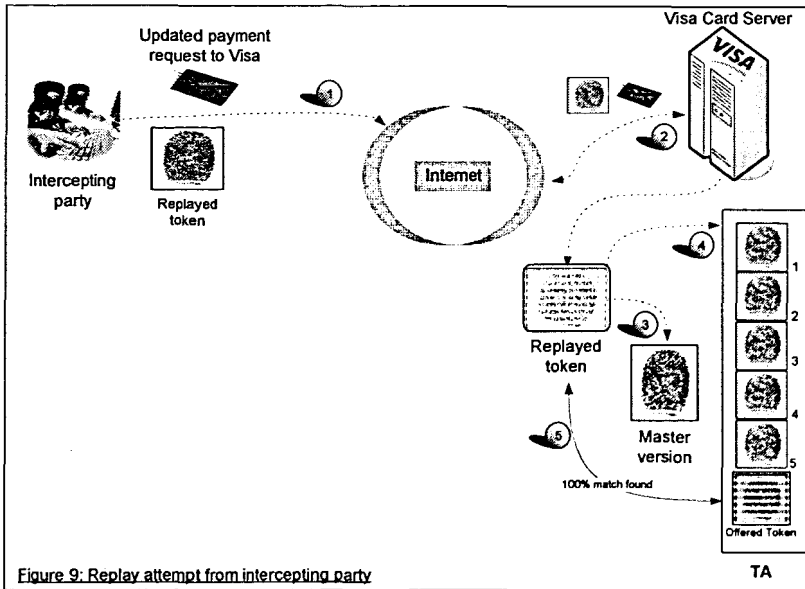


Figure 9. Replay attempt from intercepting party

The reader may reason that in figure 7, if the interception takes place successfully, but the offered token does not reach the Visa card server, a replay of the intercepted token (hot copy), may be successful, because the offered token did not reach the server's TA.

This issue is addressed by the synchronization step illustrated in figure 5, and also extensively addressed in Biovault version 4.

We will not expand on this issue at this point.

8. BIOVAULT VERSION 4

Biovault Version 3 is fully operational. Biovault Version 4 is being designed at present. This version will use Biovault to implement the concept of 'biometric digital signatures'.

Furthermore in version 4 the user will not need to frequently synchronize the personal TA with the server. This version of Biovault will be much easier to roll out, and will not need much additional hardware to function. Version 4 we also address a number of problems still inherent in version 3.

Using this version 4, it is investigated that unique digital signatures can be created using biometric tokens.

9. SUMMARY

We are convinced that Biovault is addressing many, if not all, of the problems which had prevented the very powerful technology of Biometrics to be used properly for identification and authentication over insecure public networks. Biovault allows for applications in many domains, including electronic commerce (as demonstrated), Point of sales transactions, and even Automated teller machine transactions. During the presentation of Biovault, a demonstration of Biovault version 3 will be given as proof of concept.

10. REFERENCES

- [1] Secrets and Lies – Digital security in a Networked World. Bruce Schneier.
- [2] Namitech – <http://www.namitech.co.za>
- [3] Biometrics – A look inside. John D. Woodward Jr. ISBN 0-07-222227-1
- [4] Biometrics: Advanced Identify Verification: The Complete Guide - Julian D. M. Ashbourn
- [5] T. Matsumoto, H. Matsumoto, K Yamada, S. Hoshino, 2002, “Impact of artificial gummy fingers of fingerprint systems” Proceedings of SPIE Vol #4677, Optical security and counterfeit deterrence techniques IV.
- [6] <http://www.ics.uci.edu/~eppstein/261/f03-outline/11.fraccasc>
- [7] <http://www.activcard.com>
- [8] <http://www.Visacard.com>
- [9] <http://www.amazon.com>

INTERNATIONALLY ACCEPTED ARTICLES

ICGeS 2008 – UK Docklands (Attached)

Authors:

Tait B.L., Von Solms SH

Article title:

“Secure biometrically based authentication Protocol
for a public network environment”

Book Details:

Global e-security Springer Volume 12,
ISBN 1865-0929

Conference details:

4th International Conference, ICGeS 2008, London,
UK, June 23-25, 2008.

Secure biometrically based authentication protocol for a public network environment

Bobby Tait and Basie von Solms

University of Johannesburg
Kingsway, Aucklandpark 2006
btait@uj.ac.za
basievs@uj.ac.za

Abstract. Biometric technology allows a computer system to identify and authenticate a person directly based on physical or behavioral traits [1]. However passwords and tokens that are currently widely used for authentication purposes do not directly authenticate a person; whenever a person offers a password or token the system only authenticates the presented password or token as authentic, but not the actual person presenting it [2], [8]. For this reason a lot of research went into developing a protocol that will allow a person to securely use a biometric token for personal authentication. Biometric technology is an attractive option for authenticating a person as there is a direct link between the person and a person's biometric token. This paper discusses a protocol, named BioVault. BioVault ensures safe transport of biometric tokens over un-secure networked environment without using any encryption technologies. The BioVault protocol also lays the foundation for biometrically based encryption, and biometrically based digital signatures.

Keywords: Biometrics, Authentication, Network Protocol, Electronic commerce, Internet communication.

1. Introduction

Biometrics is not a new technology at all; the notion of using a physical trait for authentication dates back over a thousand years, when potters in the east would make an imprint of their fingerprints in the clay as an early form of brand identity and to ensure the authenticity of the article [3].

Humans rely mainly on a person's physical traits for identification and authentication, as we would authenticate a person based on the person's voice, face, smell or even behavior, to name only a few [2].

Biometrics in the IT world is the science of equipping a computer system with the necessary "senses" to allow the computer system to authenticate a person based on something the person is. In other words, using something that is inherently part of a person (for e.g. DNA), to ensure the authenticity of the person. A number of factors influence the adoption of biometrics as a mainstream authentication technology, including aspects such as cost, complexity and reliability [6], to name only a few.

2 Bobby Tait and Basie von Solms

However two major concerns investigated in this article are related to the possibility that the biometric token can be:

- Intercepted and replayed at a later stage,
- A fake biometric token can be manufactured [6] and then used at a later stage. The BioVault protocol addresses these two concerns.

The next section will briefly elaborate on these two problems.

2. Compromise of a biometric token

If a password or token is compromised, the person using that token or password can simply replace the compromised password or token with a new one. For example, if a person's bank card is stolen, the bank will void the stolen card and issue a new card.

All biometric tokens are converted to an electronic representation of the biometric token [7]. It was successfully demonstrated that once the biometric token is in electronic format, this electronic format can be intercepted during the various transport phases, and later used in a replay attempt [9].

Thus, the first problem that had to be addressed by this protocol related to the distinct possibility that a biometric token can be compromised in electronic format and then reused at a later stage to allow a hacker to masquerade as the owner of the biometric token.

Secondly, as a person interacts with his physical environment, the person leaves biometric information behind. For example, articles that the person touch will often have a latent print of the person's fingerprint, or drinking from a glass will leave saliva on the glass with DNA information inside the saliva.

During our research, the suggestions of Prof Matsumotho [6] were tested, and it was successfully demonstrated that a fingerprint can be lifted from a glass that a subject touched. This lifted fingerprint could then subsequently be used to fabricate a latex mould of the person's fingerprint, which in turn, could be used to spoof the biometric fingerprint scanner.

Unfortunately a person can not merely change a stolen DNA or a stolen fingerprint token as one would change a compromised token or password.

In order to address the problems identified, the BioVault protocol was developed and will be discussed in the remainder of this article. BioVault version 1.0 addresses the first problem identified, and BioVault version 2.0, which is an extension of BioVault version 1.0, addresses the second problem.

3. Introduction to the BioVault version 1.0 protocol

BioVault [7] does not rely on any specific biometric technology to function; however certain technologies are inherently stronger technologies and would obviously be preferred by industry.

During the development of the BioVault protocol the following important goals were set:

- 1) Safe transport of a biometric token over an un-safe network like the internet.
 - 2) Detection of replay attempts of biometric tokens in electronic format.
 - 3) Protection against manufactured tokens from latent prints.
 - 4) Enabling a user to use a biometric token to encrypt a document
 - 5) Enabling a user to use a biometric token to digitally sign a document.
- (4) And (5) will not be discussed in this paper.

3.1. Symmetry and Asymmetry

One of the fundamental concepts of the BioVault protocol relies on the fact that biometric tokens are an asymmetric authentication mechanism, and makes virtually every presented biometric token unique. A 100% match between the reference biometric token stored in the biometric store, and the biometric token presented by the user, are very unlikely. Thus each accepted biometric token can be linked to a given transaction performed by the user.

Passwords and tokens, on the other hand, are symmetric authentication mechanisms. Whenever symmetric mechanisms are to be used, the fact remains that a symmetric match must be truly symmetric, thus a 100% correlation is expected between the stored password in the password database, and the presented password. Figure 1 illustrates a very basic approach to the BioVault version 1.0 protocol

3.2. The Token Archive (TA)

As illustrated in figure 1, a token archive (TA) is created for the user on an authentication server. This TA will store every biometric token used by the user that was successfully authenticated by the biometric matching algorithm. To ensure that a specific token inside the TA can be found very fast, the TA will be sorted, thus a binary search algorithm can be used to find a biometric token in the TA very efficiently.

3.3. The basic BioVault process

Step 1: In the first step as illustrated in figure 1 the user must offer his fingerprint to the biometric scanner. The scanner will digitize the fingerprint and hand the digitized electronic version of the fingerprint to the driver software of the biometric device.

Step 2: During the second step, the offered biometric token is submitted via the internet or any networked environment to the authentication server.

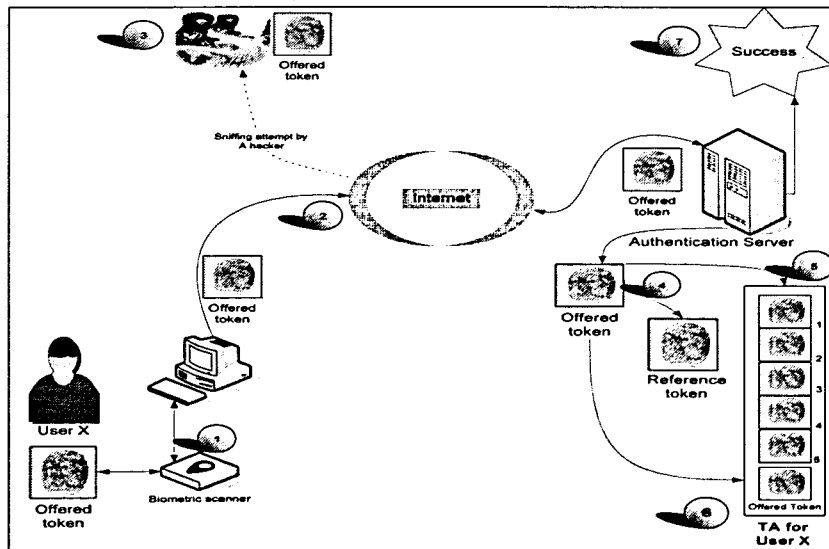


Fig. 1. Compromise of biometric token during network transmission

Step 3: During this step a hacker sniffs all the packets that the users submits over the network, and re-assembles these packets to get the electronic representation of the offered biometric token. However, the hacker does not interfere with the authentication process of the user, and the process continues with step 4

Step 4: Once the offered biometric token from the user arrives at the authentication server, the server will fetch the reference biometric token in the biometric token database. The reference biometric token is the template that was stored during the enrolment process.

The authentication server will then compare the offered biometric token with the reference biometric token. If the offered biometric token falls within the tolerances defined in the matching algorithm, the system will accept the biometric token provisionally as authentic, and proceed to step 5

Step 5: During step 5 the authentication server will compare the offered biometric token to all biometric tokens stored in the TA. If an exact match is found, the authentication server will reject the authenticity of the biometric token, as a 100% exact match of a biometric token is highly unlikely.

Step 6: However, if an exact match is not found in the TA, the authentication server will add the newly received biometric token to the user's TA for future usage, as illustrated in step 6.

Step 7: Once BioVault version 1.0 is satisfied with the authenticity of the offered biometric token, and now convinced that the offered token is not an electronically replayed biometric token, the server will send back a "successful" result to the user.

At this stage, the user has been successfully authenticated. Without the knowledge of the user or the authentication server, a hacker managed to acquire the electronic representation of the biometric token. This electronic biometric token is then stored

by the hacker hoping that he can use this token to be falsely authenticated in the future, by replaying this biometric token.

Fortunately, BioVault version 1.0 has the ability to detect this type of replay attempt, and is illustrated in figure 2.

3.4. Detection of replay

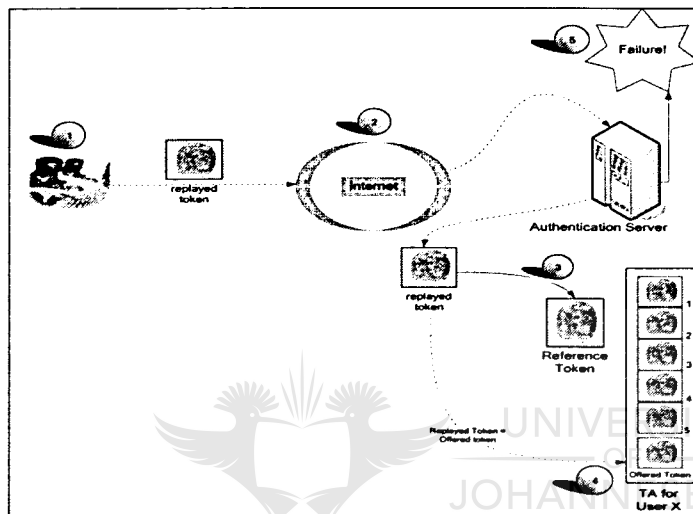


Fig. 2. Detection of replay.

Step 1: The hacker fetches the previously sniffed electronic biometric token and contacts the authentication server

Step 2: The hacker then replays the electronic biometric token via the internet or networked environment to the authentication server.

Step 3: Once the replayed token from the hacker arrives at the authentication server, the authentication server will compare the replayed biometric token with the reference biometric token. Considering that the token was previously accepted as authentic the authentication server will once again accept the biometric token provisionally as authentic, and proceed to step 4.

Step 4: The authentication server will compare the replayed biometric token to all biometric tokens stored in the TA. At this stage an exact match will indeed be found in the TA, this will cause the authentication sever to suspect replay, and reject the replayed biometric token.

Step 5: Considering that an exact match was found it the TA, the authentication server will immediately force a rejection of the replayed token, resulting in an authentication failure.

Considering that there is a very small possibility that a 100% might be possible, the server will request a fresh biometric token from the user.

6 Bobby Tait and Basie von Solms

If this basic approach of BioVault version 1.0 is considered it is clear that this system will only detect tokens that was sniffed during transmission and the replayed at a later stage. If a hacker managed to generate a latex biometric token from a glass, the system will accept the biometric token as authentic. It was also discovered that the electronic representation of a biometric token can be altered slightly, in order to prevent a 100% match being made, but still being accepted by the biometric matching algorithm

BioVault version 1.0 was expanded to address these issues. This resulted in BioVault version 2.0

4. BioVault 2.0

This section introduces a few new concepts that will form part of the progression from BioVault 1.0 to BioVault 2.0.

4.1 The client-side token archive (CTA).

The first concept to be introduced is the Client side Token Archive (CTA). This token archive will consist of a limited number of previously used biometric tokens of the specific user. The larger this token archive the stronger the system will be.

The biometric tokens inside this CTA are totally random and provided to the user by the authentication server. The authentication server will populate the CTA from time to time with different previously offered biometric tokens of the given user.

The Token Archive (TA) introduced in BioVault 1.0 will now be referred to as the Server Side Token Archive (STA), for clarity.

4.2 The Token Parcel

The token parcel is the second concept to be introduced. The token parcel will always include a freshly offered biometric token and an old biometric token that is fetched from the CTA as requested by the authentication server. The contents of the token parcel will be joined using a XOR operator. This is illustrated in figure 3. The aim of the XOR operator is to secure the token parcel while transmitted over a public network, without using encryption systems. Encryption systems introduce a lot of system overhead like key management and may increase the amount of data being sent. For the example as illustrated in figure 3 this CTA would include 50 randomly picked biometric tokens from the STA of this specific user.

Step 1: Whenever a user needs to be authenticated, the user will provide a fresh biometric token as shown in step 1 directly to the biometric scanner. The scanner will

digitize the fingerprint and hand the digitized electronic version of the fingerprint to the driver software of the biometric device.

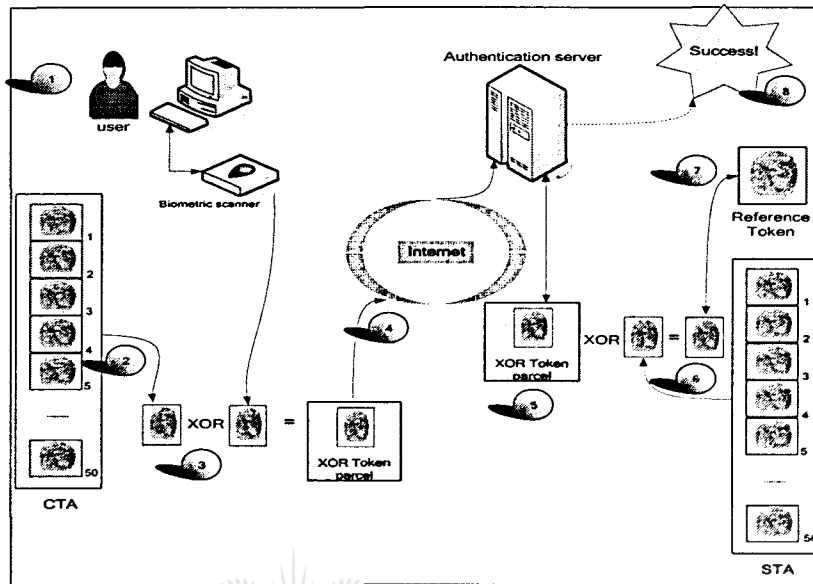


Fig. 3. BioVault version 3.0

Step 2: During a previous encounter with the authentication server, the server sent a request to the user (as will be discussed). This request demanded a very specific biometric token from the CTA that must be included during the next contact that the user makes with the authentication server. In the figure 3, this request pointed to the 4th biometric token in the CTA. The system will thus automatically fetch the 4th biometric token from the user's CTA.

Step 3: The BioVault client side software will take the electronic representation of the fresh biometric token and XOR it with the electronic representation of the 4th biometric token fetched during step 2. This result will be submitted to the authentication server as the XOR token parcel.

Step 4: The XOR biometric token parcel is submitted via the internet or any networked environment to the authentication server.

Step 5: The server receives the XOR token parcel and prepares to run the XOR operator on the token parcel

Step 6: The server requested that the client must XOR the fresh biometric token with the fourth token in the CTA. Therefore the server will fetch the 4th biometric token in the STA.

The server XOR's the received token parcel with the 4th biometric token from the STA in order to get the fresh biometric token of the user.

Step 7: The fresh biometric token extracted from the XOR token parcel during step 6, is then asymmetrically matched with the reference biometric token in the database in step 7. If the offered biometric token falls within the tolerances defined in the

matching algorithm, and the offered biometric token does not appear in the STA, the system will accept the biometric token as authentic. The offered biometric token will then be added to the STA.

Step 8: If the token parcel passed all these conditions, authentication is a success.

If the authentication process resulted in a success the server will proceed to generate a challenge parcel for the user, to be used during the next communication between the user and the authentication server.

5. Conclusion

If a hacker intercepts the XOR token parcel, the hacker does not gain anything usable. The hacker does not have the challenge token, thus he can not gain access to the fresh token. If he can not get access to the fresh token, there is no sense in sniffing the XOR token parcel.

If a hacker lifts a token from a glass as discussed in section 3, and then tries to use this lifted token, it will be rejected. To successfully use this lifted token, the hacker must also be in possession of the correct number for the requested biometric token in the user's CTA, which he does not have. Even if the XOR challenge parcel is sniffed step 4 above, he will not be able to retrieve this requested number, as he does not have the freshly offered biometric token that was used in the XOR parcel.

6. Bibliography

1. Julian Ashbourn, Biometrics: Advanced Identity Verification: The Complete Guide, ISBN: 978-1852332433
2. Von Solms SH, Tait BL. "Solving the problem of replay in Biometrics- An electronic commerce Example". Proceedings of 5th IFIP Conference on Challenges of expanding internet: E-commerce, E-business, and E-government. (I3E'2005) p468-479. Springer – ISBN 0-387-28753-1. Poznan, Poland 28-30 October 2005.
3. Thalheim, Krissler and Ziegler. "Body Check." C't Magazine 11 (2002): 114.
4. John D. Woodward Jr, Nicolas M. Orleans. Identity assurance in the information Age – Biometrics, ISBN 0-07-22227-1
5. Peter T. Higgins, Principal investigator for MITRE experimentation in Biometrics 1990.
6. T. Matsumoto, H. Matsumoto, K Yamada, S Hoshino, 2002, Impact of artificial gummy fingers on fingerprint systems" proceedings of SPIE Vol 4677, Optical security and counterfeit deterrence techniques IV.
7. Tait B.L. , von Solms SH, BioVault: a Secure Networked Biometric Protocol, D.Com Dissertation, University Of Johannesburg 2008
8. Digital Persona – U are U technologies : <http://www.digitalpersona.com>
9. Willis, David and Mike Lee, "Biometrics under your thumb." Network computing. June 1, 1998

INTERNATIONALLY ACCEPTED ARTICLES

ICGS3'09 2009 – East London University, UK (Attached)

Authors: Tait B.L., Von Solms SH

Article title: "Biometrically based electronic signatures for a public networked environment"

Book Details: Published in Springer-Verlag regarding LNCS

Conference details: 5th International Conference on Global Security, Safety & Sustainability, ICGS3'09.

Biometrically based electronic signatures for a public networked environment

Bobby Tait and Basie von Solms

University of Johannesburg
Kingsway, Aucklandpark 2006
btait@uj.ac.za
basievs@uj.ac.za

Abstract. Signatures are internationally used as a method to sign documents. This ensures that a person signing a document agrees to the terms as stipulated in the document. A signature is biometric in nature, and is usually directly related to the signing party. This paper explains in what way biometric data¹ can be used to digitally sign a document. Currently, the electronic signing of a document relies on the PKI environment, which is in essence based on passwords [7]. Passwords, unlike biometrics, are not physically part of the user, and hence, only authenticates the presented password as authentic, and not the user presenting the password. This paper defines a digital signature of a message M , as a key-based hash H [5], [6] of message M , where the key used is absolutely unique to the creator (owner) of the specific signature. To verify the digital signature, this absolutely unique key, belonging to the creator, must be available and be used. The whole process is based on the BioVault protocol [1], [2]. This protocol utilizes any form of biometric technology as the fundamental authenticator of a user.

Keywords: Security, Digital signature, MAC, Biometrics, Authentication, Integrity, Identity management, trust management, BioVault.

1. Introduction

In this paper, key-based hashing, for example the data authentication algorithm is used to create a digital signature. For this reason the key used to create a digital signature must be:

- Uniquely linked to the creator of the signature (the signer)
- Always in the possession of only the signer (the key must also always be readily available to the signer)

Considering the above mentioned points, ordinary password-like keys, cannot be used because:

- Such keys are not uniquely linked to the signer.
- Such keys are not in possession of the signer only, because the person verifying the signature must have the same key.

¹ Biometric data – Biometric characteristic - for instance a fingerprint- in digital format

2 Bobby Tait and Basie von Solms

This paper suggests a way to use biometric data as this key. Such a key is, by definition, uniquely linked to the signer, and always in possession of only the signer.

The paper is based on the BioVault protocol [2]. This biometric based protocol ensures that the following goals are met for biometric data:

- 1) Safe transport of biometric data over an un-safe network like the internet.
- 2) Detection of replay attempts of biometric data in electronic format.
- 3) Protection against manufactured biometric characteristics² from latent prints³.

The biometric digital signature process relies on the fact that both the receiver and the sender of the message is part of the BioVault infrastructure, in the same way that eBay [3] expects buyers and sellers to be part of the PayPal [4] system.

2. Biometric based digital signature.

Signing a document using the BioVault protocol is a 6-phased process.

In order to digitally sign a message using the BioVault protocol entails hashing the message using the biometric data of the signing party as the key to the hashing algorithm – in essence generating a MAC.

Suppose John wants to send a clear text message to Sam, but also want to add his digital signature to the message so that Sam can verify that the message did indeed really originate from John.

Figure 2 illustrates the first phase that John would follow in order to sign a message. This message will be sent to Sam, and Sam will need to test the integrity of this message.

2.1 Phase 1 – Sign message destined for Sam

John wants to send a message to Sam. This message does not necessary contain any sensitive information. However, it is important the authenticity of the message can be confirmed, and that the integrity of the message can be tested. For this reason John will sign the message using his biometric data. Figure 2 illustrates the first phase in this process that relies on the BioVault infrastructure.

Step 1: John will provide fresh biometric data as shown in step 1 directly to the biometric scanner. The scanner will digitize the fingerprint and hand the digitized electronic version of the fingerprint to the driver software of the biometric device.

Step 2: This freshly digitized biometric data is then be used as the secret key for a hashing algorithm to generate a unique Mac for this message from John.

² Manufactured biometric characteristic – generating a false biometric characteristic using for e.g. latex.

³ Latent print – A physical residue left by a user that touched for e.g. a glass.

Step 3: During a previous encounter with the authentication server, the server sent a challenge to John (as per BioVault protocol). This challenge demanded very specific biometric data from John's Client Bio-Archive (CBA) that must be included during the next contact that he makes with the authentication server. In the figure 2, this request pointed to the 21st biometric data in John's CBA. The system will thus automatically fetch the 21st biometric data from John's CBA.

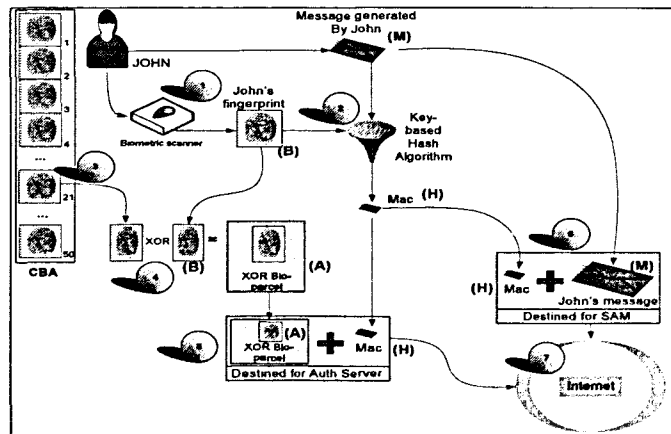


Figure 2

Step 4: The BioVault Client side software takes the electronic representation of the fresh biometric data (that was also used as the secret key in the hashing algorithm) and XOR this fresh biometric data with the electronic representation of the 21st biometric data fetched during step 3, resulting in a XOR bio-parcel.

Step 5: The Mac generated in step 2 will then be concatenated with the bio-parcel, resulting in a message bundle. This bundle (consisting of the BioVault parcel & the Mac) will be sent to the authentication server.

Step 6: John creates a second message bundle. This message bundle consists of the Mac generated in step 2 and the message John generated for Sam. This message bundle is then address to Sam.

Step 7: These two message bundles are then sent over a network to the authentication server, and to Sam. If these messages are sniffed during transmission, the hacker would be in possession of a XOR token parcel that he cannot decrypt, a hash, that he cannot re-create, and a clear text message that he can read. This is not necessary a sensitive message, as mentioned earlier, but if the hacker alters the message, the testing of the Mac will fail later on.

The two messages are delivered to the authentication server, and to Sam. The second phase will illustrate the actions that the authentication server follows.

2.2 Phase 2: Authentication Server

During the second phase the server receives the message bundle that John sent. The process that the server follows is illustrated in figure 3.

Step 1: The server receives the message bundle from John. This message bundle includes a bio-parcel, and a Mac. The server is aware that the bio-parcel must conform to the rules as stipulated in the BioVault protocol

Step 2: During previous communication with John, the server sent John a challenge to supply the 21st bio-data. For this reason the server will fetch the matching biometric data from John's SBA. The server extracts the bio-parcel from the message bundle and XORs the bio-parcel with the matching biometric data from John's SBA. This yields the fresh biometric data from John. The server tests this fresh biometric data for replay and authenticity as prescribed by the rules of the BioVault protocol.

Step 3: If the server is satisfied with the fresh biometric data, this biometric data will be added to the SBA of John (as per BioVault protocol).

Step 4: The server fetches the Mac received in the message bundle from John and associate this Mac with the fresh biometric data received, in John's SBA.

The server is now in possession of the Mac and the key (biometric data) used to generate the Mac. The server marks the new (51st) biometric data in John's SBA as used, and will not allow usage of it in future again.

In the next phase it will be illustrated in what way Sam will contact the authentication server to ensure that the message as sent by John is authentic.

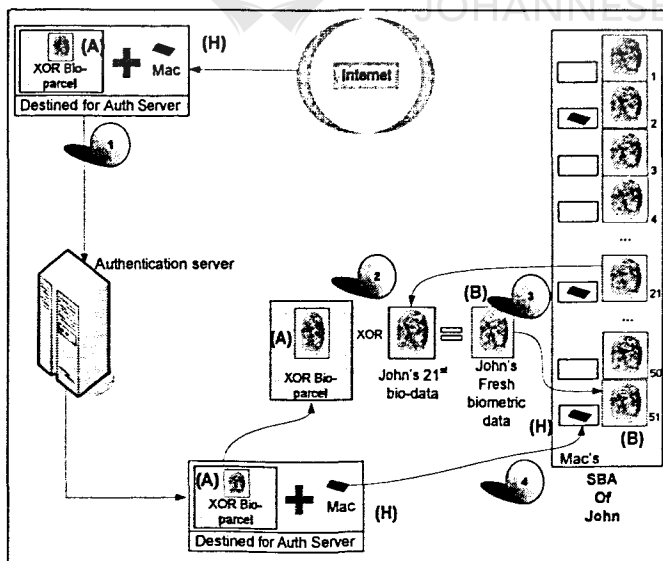


Figure 3

2.3 Phase 3: Sam requesting the hash key

Sam received her own message bundle directly from John. This message bundle included the message (that Sam can read immediately), as well as a Mac (to ensure the integrity of the message as sent by John). If Sam wishes to test the Mac, she must follow the method as illustrated in figure 4.

Step 1: Sam receives the message bundle from John, consisting of the clear text message and the Mac of this message.

Sam can read the message, but to test the Mac she will proceed to the second step in this phase.

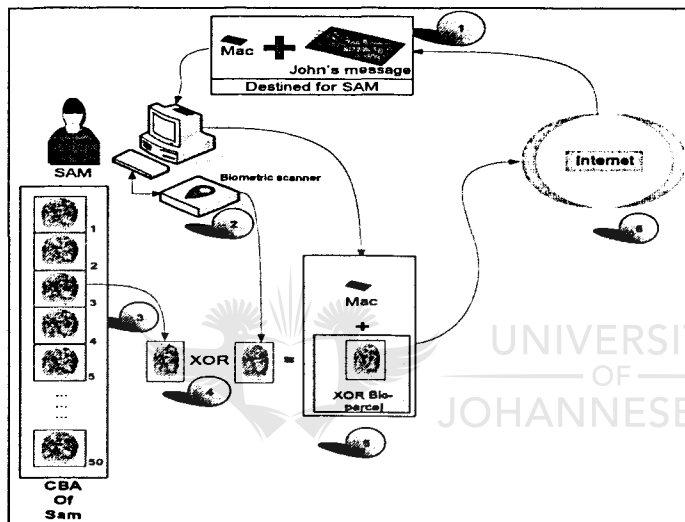


Figure 4 Mac key request

Step 2: Sam will provide fresh biometric data directly to the biometric scanner. The scanner will digitize her fingerprint and hand the digitized electronic version of the fingerprint to the driver software of the biometric device.

Step 3: During a previous encounter with the authentication server, the server sent a challenge to Sam (as per BioVault protocol). This challenge demanded specific biometric data from Sam's CBA that must be included during the next contact that she makes with the authentication server. In figure 4, this request pointed to the 3rd biometric data in Sam's CBA. The system will thus automatically fetch the 3rd biometric data from Sam's CBA.

Step 4: The BioVault client side software will take the electronic representation of her fresh biometric data, and XOR this fresh biometric data with the electronic representation of the 3rd biometric data fetched in step 3, resulting in the XOR bio-parcel.

Step 5: The Mac received from John in step 1 will then be concatenated with the bio-parcel, resulting in a message bundle. This bundle (consisting of the Mac and the bio-parcel) is addressed to the authentication server.

Step 6: This message bundle destined for the authentication server, is sent via the internet to the authentication server, by Sam.

2.4 Phase 4: Confirm Sam's authenticity

During this phase the server receives the message bundle from Sam. The server verifies Sam's authenticity according to the rules of the BioVault protocol. This is illustrated in figure 5.

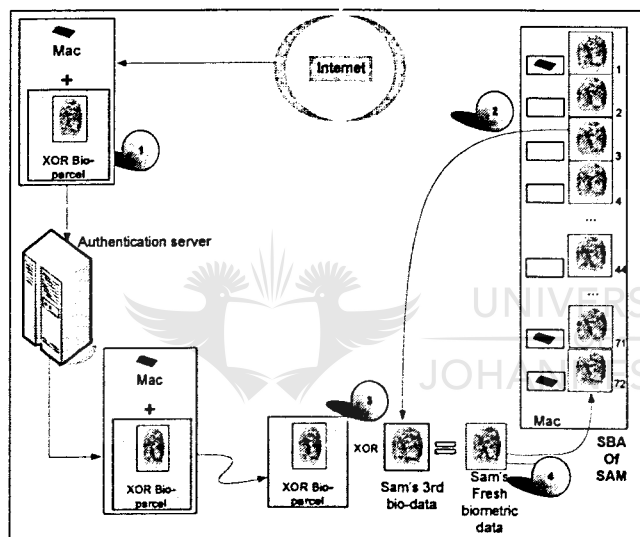


Figure 5 Confirm Sam's authenticity

Step 1: The server receives the message bundle from Sam. This message bundle includes a bio- parcel, and a Mac. The server is aware that the bio- parcel must conform to the rules as stipulated in BioVault protocol.

Step 2: During previous communication with Sam, the server sent Sam a challenge to supply the 3rd biometric data in Sam's CBA. For this reason the server will fetch the matching biometric data from Sam's SBA.

Step 3: The server extracts the bio- parcel from the message bundle and XORs this bio- parcel with the matching biometric data from Sam's SBA, this step will yield the fresh biometric data from Sam. The server will then test this fresh data for replay and authenticity as prescribed by the rules of BioVault protocol.

Step 4: If the server is satisfied with the fresh biometric token, this token will be added to the SBA of Sam.

2.5 Phase 5: Biometric key supplied to Sam

The authentication server checks to see if this Mac that the server has just received from Sam exists in John's SBA, and if it does, the authentication server will generate a new bio- parcel for Sam.

Step 1: The authentication server searches John's SBA for a match of the Mac that Sam sent in the message bundle. The server determines that the Mac received from Sam in the message bundle, matches the Mac associated with the 51st biometric data in John's SBA.

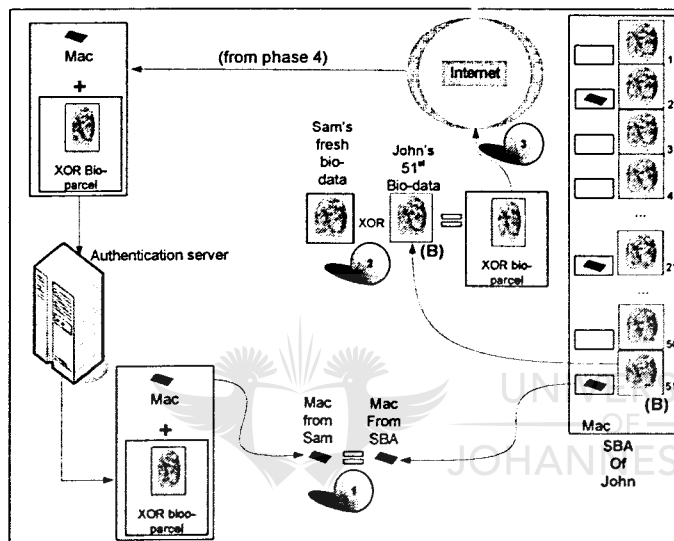


Figure 6 Biometric data supplied to Sam

Step 2: The authentication server uses the fresh biometric data that Sam supplied in the message bundle and XORs this fresh biometric data with the 51st biometric data found in John's SBA - this was the biometric data John used to sign the original message. This step results in a new bio-parcel, destined for Sam.

Step 3: During the last step, the authentication server sends this bio-parcel to Sam.

In the final phase Sam will extract the biometric data that John used to generate the Mac, and finally use this biometric data to test the Mac.

2.6 Phase 6: Test message's integrity

Step 1: Sam receives the bio-parcel sent by the server

Step 2: Sam XORs her fresh biometric data that she generated in the 3rd phase, with the bio- parcel received from the server. This will yield the 51st biometric data that John used to generate the Mac.

Step 3: Sam uses the biometric data that she received from the authentication server as the secret key for the hashing algorithm, and generates a fresh Mac for the message that she received from John.

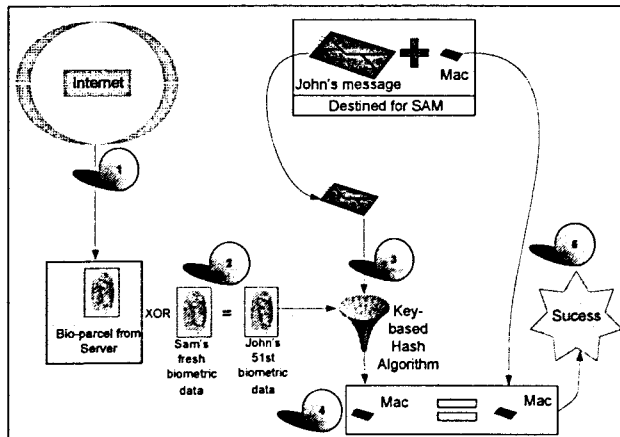


Figure 7 Message integrity test

Step 4: Sam then compares the Mac that she received in the message bundle from John with the one now freshly generated, to see if the generated Mac = the received Mac.

Step 5: If the message was indeed signed with the 51st biometric data in John's SBA, and if the message was not tampered with, the testing of the Macs will be a success, proving that the message from John is authentic and has not been altered at all since John sent the message. Sam can now discard John's biometric data because it can never be used again for anything, as the server has marked this biometric data as 'used'

3. Conclusion

Let us evaluate the process in section 2 with the requirements listed in section 1 where we specified that the key used in the signing process must be:

- Uniquely linked to the creator of the signature (the signer).
- Always in the possession of only the signer (the key must always be readily available to the signer).

The process in section 2 conforms to both because:

- The biometric data is uniquely linked to the signer of the message, John
- This biometric data can never be used again, so a new signature will demand new, fresh biometric data which can only come from John.

The suggested process means that every document signed by John will require new, fresh, biometric data (key). In the same way this fresh biometric data (key) can

be seen in Public key encryption terminology as John's private key, except that for every signature, a new private key is required.

This paper demonstrated successfully that the BioVault protocol infrastructure can be used to implement the signing of documents in order to insure the integrity of a document. This is very beneficial as the biometric data is directly linked to the signing party and for this reason allows non-repudiation to be enforced successfully.

4. Bibliography

1. Tait B.L., Von Solms SH, BioVault: a Secure Networked Biometric Protocol, D.Com dissertation, University of Johannesburg 2008.
2. Tait B.L., Von Solms SH "Secure biometrically based authentication Protocol for a public network environment" Global e-security Volume 12, ISBN 1865-0929 4th International Conference, ICGeS 2008, London, UK, June 23-25, 2008. Proceedings
3. Ebay online Auction: <http://www.ebay.com> / <http://www.ebay.co.uk>
4. PayPal online payment environment: <http://www.paypal.com>
5. Message authentication codes:
<http://www.rsa.com/rsalabs/node.asp?id=2177>
6. Charles P. Pfleeger, Shari Lawrence Pfleeger, "Security in Computing" third edition, Prentice Hall, ISBN 0-13-035548-8
7. Blake Ives, Kenneth R. Walsh, Helmut Schneider "The domino effect of password reuse" "Communications of the ACM" Volume 47, Number 4 (2004), Pages 75-78

INTERNATIONALLY ACCEPTED ARTICLES

IFIP I3E 2009– Nancy, France (Attached)

Authors: Tait B.L., Von Solms SH

Article title: "BioVault: Biometric based encryption."

Book Details: Published in Springer within the IFIP book series

Conference details: 9th IFIP Conference on e-Business, e-Services, and e-Society, I3E 2009.

BIOVAULT: BIOMETRICALLY BASED ENCRYPTION

Mr.B.L. Tait¹, Prof S.H. von Solms²

¹ University of Johannesburg, Kingsway Avenue, Auckland Park, Gauteng, South Africa,
Btait@uj.ac.za

² University of Johannesburg, Kingsway Avenue, Auckland Park, Gauteng, South Africa,
basie@uj.ac.za

Abstract. Biometric based characteristic authentication is an asymmetric [1] authentication technology. This means that the reference biometric data generated during the enrolment process and stored in the biometric database, will never match any freshly offered biometric data exactly (100%). This is commonly accepted due to the nature of the biometric algorithm [2] central to the biometric environment.

A password or pin on the other hand, is a symmetric authentication mechanism. This means that an exact match is expected, and if the offered password deviates ever so slightly from the password stored in the password database file, authenticity is rejected.

Encryption technologies rely on symmetric authentication to function, as the password or pin is often used as the seed for a random number that will assist in the generation of the cipher. If the password used to encrypt the cipher is not 100% the same as the password supplied to decrypt, the cipher will not unlock.

The asymmetric nature of biometrics traditionally renders biometric data unfit to be used as the secret key for an encryption algorithm.

This paper introduces a system that allows biometric data to be used as the secret key in an encryption algorithm. This method relies on the BioVault infrastructure. For this reason BioVault will briefly be discussed, followed by a discussion of biometrically based encryption.

Keywords: Encryption, Biometrics, BioVault, security, secure transaction, data protection, key management, privacy-enhancing technology, data security.

1 Introduction.

To date, it was not possible to use a biometric data directly as the secret key for an encryption algorithm or for a MAC algorithm. The reason for this resides in the fact that a biometric authentication process is always asymmetric. In order for an encryption algorithm to function, the secret key provided to encrypt a message must be exactly the same (symmetrical) as the secret key used to decrypt the message.

If a secret key is used to generate a MAC, this exact same secret key must be provided to test the MAC.

The possibility that a person would repeatedly be able to provide biometric data that would be 100% the same as earlier provided biometric data is highly unlikely. This makes biometric data useless as the secret keys for hashing or encryption.

Digital signatures use encryption and hashing as its underlying, primary technology.

The paper is based on the BioVault protocol. Because of the length restriction on this paper, the BioVault protocol cannot be discussed in detail. However a short discussion of the protocol will be given, followed by a detailed discussion of how the protocol can be used to create biometrically based digital signatures.

For a detailed discussion of the BioVault protocol see [6], [7].

In the sections to follow it will be demonstrated how the BioVault infrastructure allows biometric data to be used for encryption.

2 Encryption using a secret key or biometric data.

2.1 Secret key encryption.

If a user wishes to send a message to another user over an unsecured network, the message must be encrypted in one or other way. $C = E_k(M)$ [3] where:

C = Cipher message

M = Original message

k = secret key

E = Encryption algorithm

The typical encryption process using a secret key is illustrated in figure 1

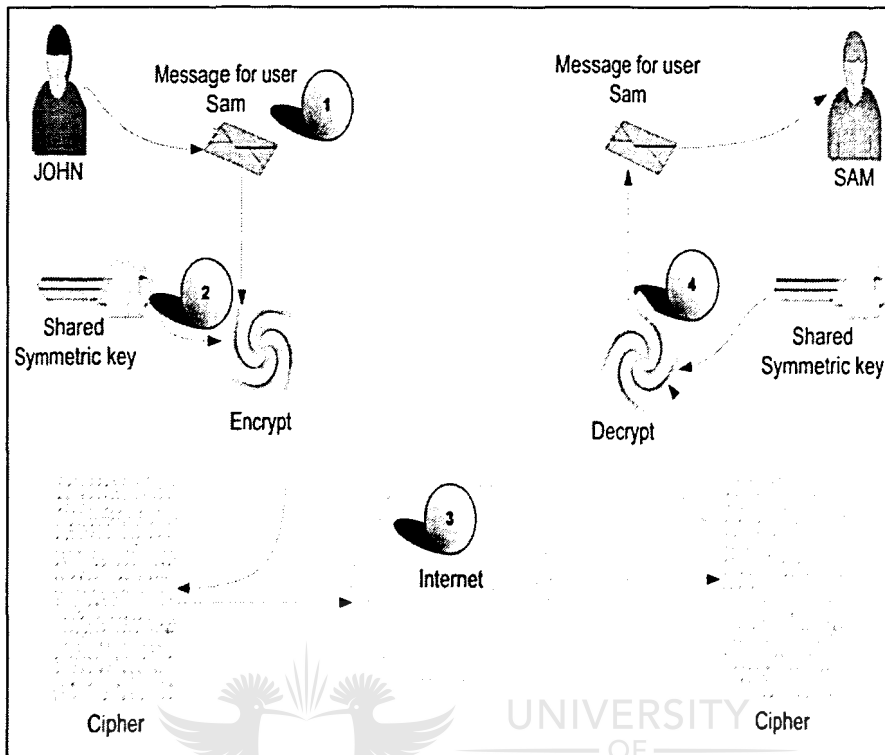


Figure 1: Typical encryption process.

As illustrated in figure 1, John wishes to send a secret message to Sam. In order to secure the message during the transmission, John encrypts the message using an encryption algorithm. In order for the encryption algorithm to yield cipher text that is absolutely random, a secret key must be provided. This secret key is shared between Sam and John as illustrated in figure 1. The secret key provided by John to encrypt the message is exactly the same as the secret key that Sam will provide to decrypt the message.

Step 1

John generates the message that he wishes to send to Sam.

Step 2

John provides a secret key to the encryption algorithm, and the encryption algorithm uses this secret key to generate the cipher text.

Step 3

The message in cipher text is sent over the internet to Sam. If a hacker should intercept this message, the hacker must be in possession of the secret key shared between Sam and John, in order to decrypt the message.

Step 4

Sam receives the message sent by John and uses the same encryption algorithm and the secret key that is shared between the two of them. If the secret key that Sam supplied to the encryption algorithm is exactly the same as the secret key used by John, Sam will retrieve the original, unencrypted message that John created.

From the above mentioned example it becomes clear that biometric data can not be used for secure encrypted communication between two people.

If John used his biometric characteristic as the secret key for encrypting a message destined for Sam, Sam would not be able to provide the same biometric characteristic to decrypt the message (as this was John's biometric characteristic that Sam does not possess).

In this paper it is illustrated in what way the BioVault infrastructure is a solution in allowing John to send an encrypted message to Sam, by using his biometric characteristic. This method relies on the fact that both John and Sam are part of the BioVault infrastructure – very much as EBay [4] relies on the fact that buyers and sellers are both part of the PayPal [5] environment. The BioVault infrastructure is a new development, and subsequently not commonly known. For this reason the following section will give a brief outline of the BioVault infrastructure, followed by an explanation of biometrically based encryption. For a detailed discussion of the BioVault infrastructure see [6], [7].

3 Brief introduction to BioVault version 3.0

BioVault does not rely on any specific biometric technology to function, however certain technologies are inherently stronger technologies and would obviously be preferred by industry.

During the development of the BioVault protocol the following important goals were set:

1. Safe transport of biometric data over an un-safe network like the internet.
2. Detection of replay attempts of biometric data in electronic format.
3. Protection against manufactured biometric characteristics from latent prints.
4. Enabling a user to use biometric data to encrypt a document
5. Enabling a user to use a biometric data to digitally sign a document.

Enabling a user to use biometric data to digitally sign a document (5), will not be discussed in this paper.

3.1 Symmetry and Asymmetry.

One of the fundamental concepts of the BioVault protocol relies on the fact that the biometric authentication process is inherently asymmetric. This makes virtually every presented biometric characteristic unique. This feature that is inherent to biometric technology can be used to detect any form of electronic replay of earlier presented biometric data. A 100% match between the reference biometric data stored in the biometric store, and the biometric data presented by the user, is unlikely. Furthermore it is possible to record biometric data, and check if any biometric data was ever received before.

Password and token based authentication mechanisms, on the other hand, are symmetric. Whenever symmetric mechanisms are to be used, the fact remains that a symmetric match must be absolutely symmetric, thus a 100% correlation is expected between the stored password in the password database, and the presented password.

3.2 BioVault components.

The following components are part of the BioVault infrastructure:

3.2.1 The Bio-Archives (BA).

Two Bio-archives (BA) are created; one bio-archive on the authentication server known as the Server bio-Archive (SBA) and one Client side bio-Archive known as the CBA. The SBA will store all biometric data used by the user that was successfully authenticated by the biometric matching algorithm. The SBA will assist in the identification of possible replay attacks. For this reason access to the biometric data stored in the SBA must be very fast. To ensure that specific biometric data inside the SBA can be found very fast, the SBA will be sorted. Considering that SBA is sorted, a binary search algorithm can be used to find biometric data in the SBA efficiently.

The CBA will assist in biometric data protection during transmission.

Initially the CBA will consist of a limited number of previously used biometric data of the specific user (to be discussed in more detail later). The larger this bio-archive the stronger the system will be.

The biometric data inside this CBA are totally random and provided to the user by the authentication server. The authentication server will populate the CBA from time to time with different previously offered biometric data of the given user.

Whenever a secure connection is established between the user and the authentication server, the server can update the CBA. However it is recommended that the CBA is updated under strictly controlled environments. This means that CBA can be updated by the authentication server, whenever a user visits a bank or ATM machine, as an example.

CBA storage.

The Bio-Archive that the user will use, will store previously offered biometric data. The following are possible options that can be used to store the CBA.

1. A USB flash memory – These tiny appliances like the Micro SD memory, presently offer surprisingly large storage space with storage sizes reaching 64Gb [114], furthermore, no additional equipment will be needed to integrate this technology into the environment.
2. A Smart card –These devices however need additional equipment and storage capacity on smartcards is limited.
3. A subcutaneous microchip – This technology ensures that a person cannot forget or misplace his CBA, but workable and acceptable solutions are still in development. Storage capacity is limited and technology is controversial. [8], [9].

3.2.2 The Bio- Parcel used during the authentication process.

The Bio- parcel will always include freshly offered biometric data and old biometric data that is obtained from the CBA as requested by the Authentication server. The contents of the bio-parcel will be joined using a XOR operator. This is illustrated in figure 2. The aim of the XOR operator is to secure the bio-parcel while transmitted over a public network, without using encryption systems. Encryption systems using for example shared symmetric keys, introduces a lot of system overhead.

For the example as illustrated in figure 2 the CBA would include 50 randomly picked biometric tokens from the SBA of this specific user. The SBA on the server will still include each and every biometric data ever used by the user in his lifetime. As will soon be discussed, these randomly selected biometric data of the user, will serve as a special key, and can be compared to the working of a one time pad

3.3 BioVault Mechanism

Step 1 (As in figure 2)

When a user needs to be authenticated the user attaches the appliance containing the CBA with the previously offered biometric data to the terminal (for example the user's computer or ATM machine), where he intends to do the transaction.

Step 2

The user provides a fresh biometric characteristic as shown, directly to the biometric scanner. The scanner will digitize the biometric characteristic and forward the biometric data to the driver software of the biometric device.

Step 3

During the previous encounter with the authentication server, the server sent a challenge to the. This challenge demanded specific biometric data from the CBA that

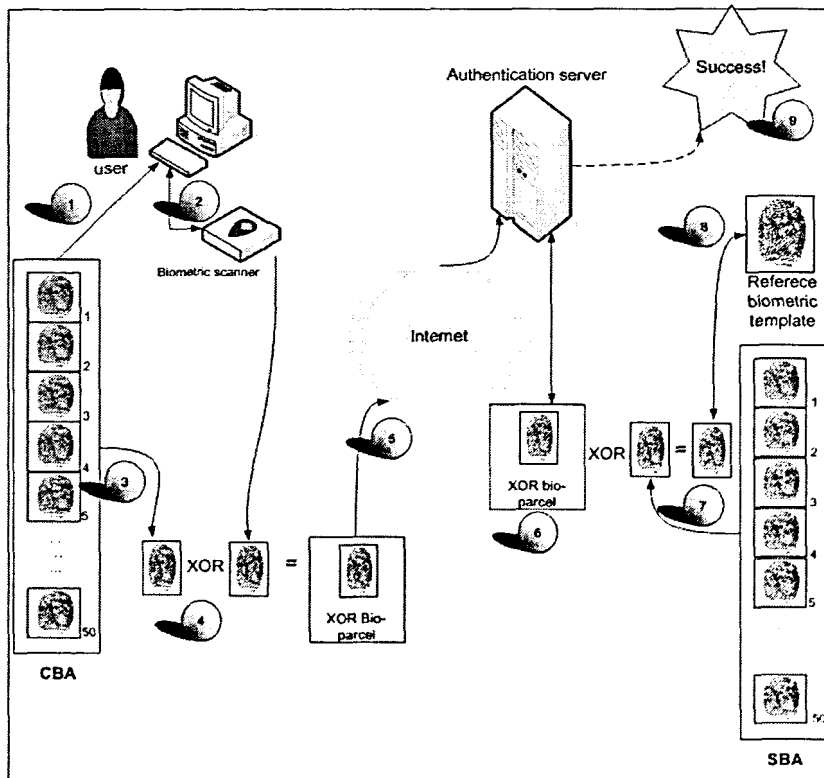


Figure 2: BioVault version 3.0.

had to be included at the time of the next contact with the authentication server. In figure 2, the server requested the 4th biometric data in the CBA. The system will thus automatically obtain the 4th biometric data from the user's CBA.

Step 4

The BioVault client side software will take the electronic representation of the freshly offered biometric data and XOR it with the electronic representation of the 4th biometric data obtained in step 3 from the CBA. For example:

Electronic representation of fresh biometric data from scanner: 10101110111011010
 Electronic representation of challenged (4th) data from CBA: 10110101111011110
 New bio-archive after XOR process: 00011011000000100

This result in a smaller bio-parcel than proposed in BioVault version 2.0, as only the result of the XOR process will be submitted to the authentication server as the XOR bio-parcel.

Step 5

The XOR bio-parcel is submitted via the internet or any networked environment to the authentication server.

Step 6

The server receives the XOR bio-parcel as shown in step 6, and prepares to run the XOR operator on the bio-parcel.

Step 7

The server requested previously that the client XOR the fresh biometric data with the fourth biometric data in the CBA. The server obtains the biometric data in the SBA that corresponds with the expected biometric data received from the user in the XOR bio-parcel.

The server must then XOR the received XOR bio-archive with the 4th biometric data from the SBA, corresponding with the 4th biometric data in the CBA, in order to get the fresh biometric data of the user. For example:

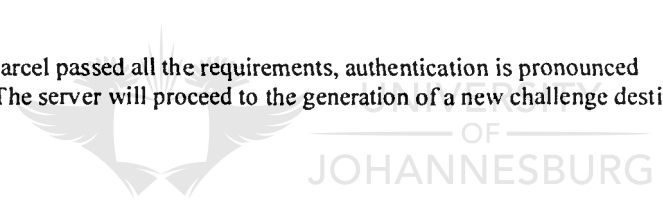
XOR bio-archive received from user:	00011011000000100
Expected 4th biometric data from SBA:	<u>10110101111011110</u>
Result of XOR process = the fresh biometric data:	10101110111011010

Step 8

The fresh biometric data extracted from the XOR bio-archive during step 7, is now asymmetrically matched to the reference biometric template found in the database. The authentication server compares the freshly offered biometric data with the reference biometric template. If the offered biometric data falls within the tolerances defined in the matching algorithm, the system declares the biometric data as authentic and adds this biometric data to the SBA, after checking the SBA for an exact match.

Step 9

As the bio-parcel passed all the requirements, authentication is pronounced successful. The server will proceed to the generation of a new challenge destined for the user.



4 Biometric Encryption using BioVault.

The whole encryption method using the BioVault infrastructure is a 4-phased process.

4.1 Biometric encryption overview.

In phase 1, John identifies himself to the authentication server, and indicates that he wants to send an encrypted message to Sam. In order to send an encrypted message to Sam, John requests a “biometric key” of Sam from the server.

In phase 2, the authentication server retrieves a biometric key from Sam’s STA also found in Sam’s CTA, and sends it to John

In phase 3, John uses this biometric key of Sam, as an encryption key to create the encrypted message, and sends this encrypted message to Sam over the network.

In phase 4, Sam receives the message sent by John, and decrypts the message by testing all the biometric keys in her CTA, against the received cipher text. In essence, Sam will the ‘brute force’ the decryption of the cipher.

4.2 Biometric encryption discussion.

Figure 3 illustrates the first phase that John would follow in order to send an encrypted message to Sam.

4.2.1 Request of biometric data

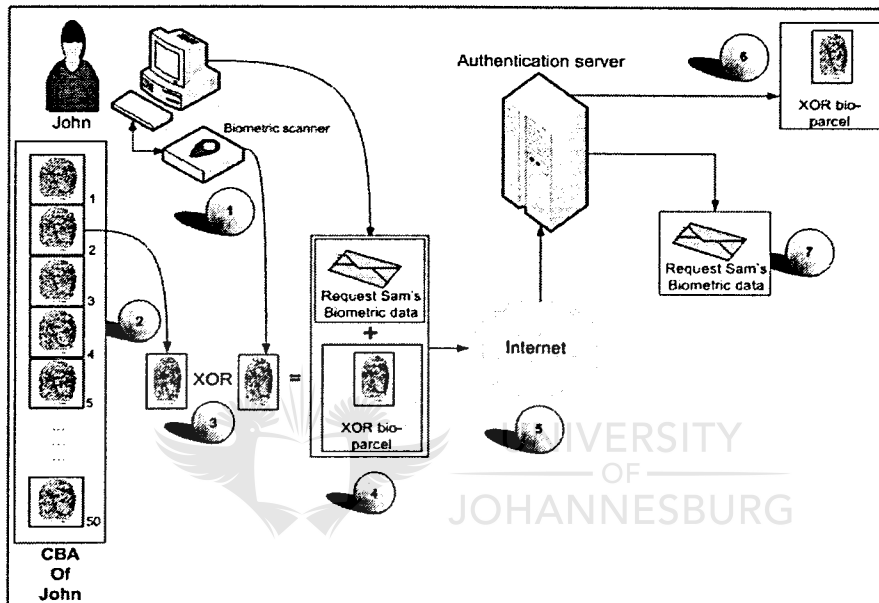


Figure 3: Request biometric data.

At this stage John sent a request to the server, stating that he wished to communicate with Sam. The server authenticated John, based on the fact that the fresh biometric data supplied by John was accepted and the expected biometric data from John’s CBA was correctly supplied.

Subsequently the server ensured that Sam is a user on the BioVault system, allowing the second phase to commence. Phase two is illustrated in figure 4.

4.2.2 Phase 2: Submission of biometric data of Sam to John

During the second phase the server sends stored biometric data from the SBA of Sam, back to John. The server is aware that this biometric data exists inside Sam’s CBA. The steps below explain this process:

Step 1

The server obtains biometric data, in this particular illustration the second biometric data, from the SBA of the user Sam. This biometric data is also present in the CBA of user Sam.

The server marks this biometric data as “used for encryption” to prevent this particular biometric data ever again rendered for encryption or authentication. This guarantees that Sam and John are the only people in possession of this biometric data.

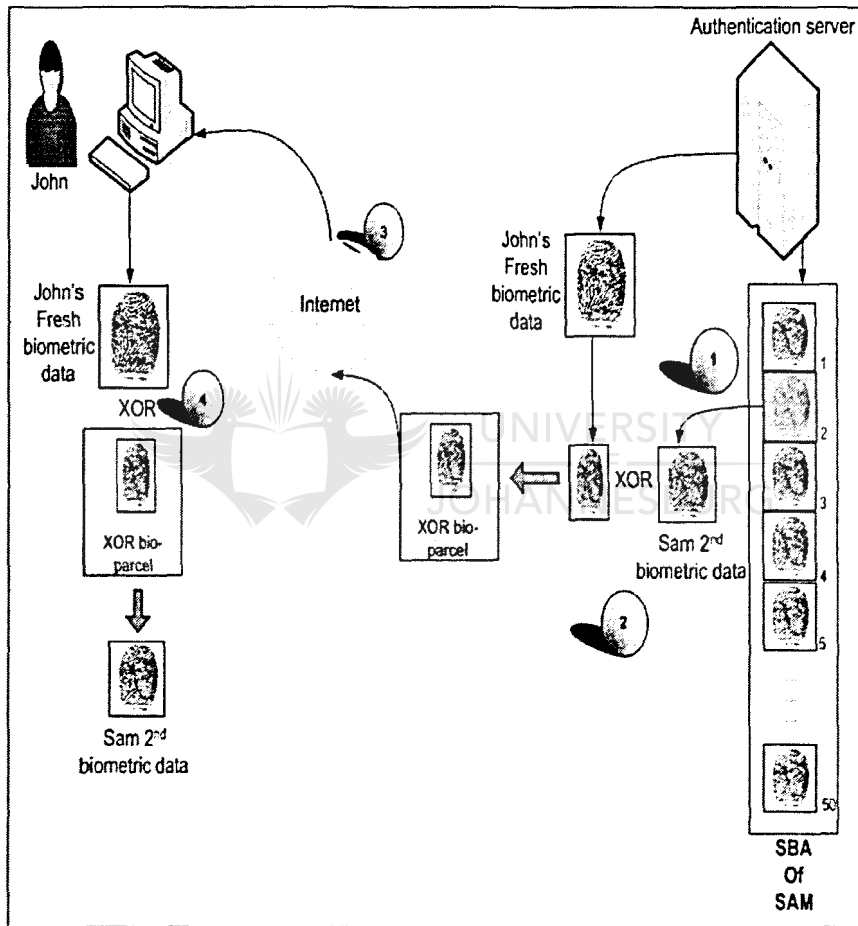


Figure 4 Submission of Sam's biometric data to John:

Step 2

The server will XOR the biometric data from Sam's SBA, in this case the 2nd one, with the fresh biometric data received in phase 1 from John, creating a new XOR bio-parcel.

Step 3

The XOR bio-parcel is then transmitted via the network, back to John. If this parcel is sniffed during transmission, the hacker will not have much use for the received bio-parcel.

Step 4

John receives the XOR bio-parcel. John uses the fresh biometric data he supplied during the first phase, and XOR this fresh biometric data with the bio-parcel received. This step yields the biometric data sent by the authentication server to John – i.e. biometric data number 2 in Sam’s CBA.

Once John is in possession of this biometric data of Sam, John can proceed to the third phase, of sending an encrypted message to Sam.

4.2.3 Phase 3: Encrypted communication between John and Sam.

At this stage John is in possession of a symmetric copy of the second biometric data in the CBA of Sam. He can proceed to encrypt a message for Sam using the biometric data made available by the server of biometric data found in Sam’s CBA, as illustrated in figure 5.

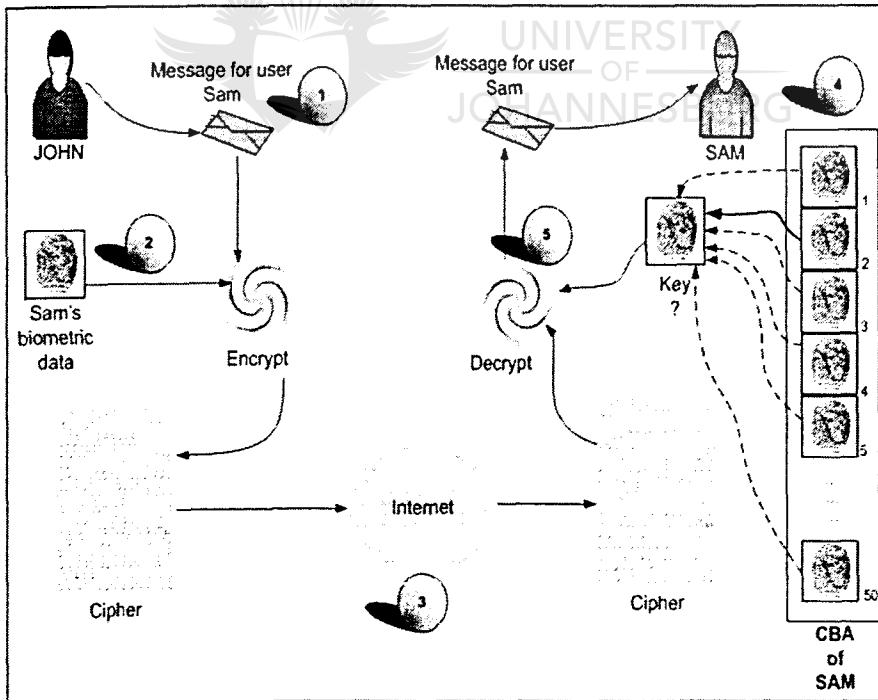


Figure 5: Encrypted communication between John and Sam.

It is illustrated in figure 5 the following steps indicates how John will send an encrypted message to Sam.

Step 1

John generates the message that he intends to send to Sam.

Step 2

John provides the received biometric data of Sam to the encryption algorithm, and the encryption algorithm uses this biometric data as a secret key to generate the cipher text.

Step 3

The message in cipher text is sent via the internet to Sam. If a hacker should intercept this message, the hacker must be in possession of the correct biometric data of Sam, in order to decrypt the message. Considering the working of BioVault version 3.0, this is highly unlikely.

In the final phase Sam will need to decrypt this message sent by John to her, using the biometric data inside her CBA. This process is illustrated in step 4 and step 5 of figure 5.

Step 4

Sam receives the message sent by John and accesses her own CBA. The client software on Sam's machine uses all the biometric data in her CBA to brute force the cipher. As there are only a limited number of biometric data in the CBA, this process will unlock the cipher rapidly.

Step 5

As the biometric data Sam used to decrypt the message is the same as the biometric data used by John, Sam will retrieve the original, unencrypted message created from the cipher created by John.

5 Conclusion.

This paper demonstrated that the BioVault infrastructure makes it absolutely possible to encrypt a message using biometric data.

Biometric data relates directly to the users. If a user used a person's biometric characteristic to encrypt a message (similar to using a person's public key in the PKI system) only the receiving party with the correct biometric data will be able to decrypt the message- however unlike the PKI system, biometric data is directly related to the user. If tokens and passwords are used, only the token or password are authenticated, the user offering the token or password are not necessary authentic. Biometrics authenticates the user directly.

If it is considered that a user generates a number of biometric tokens every day, each one unique, this method of encryption is closely related to one time pad technology – the keys used, are very long and do not form any pattern. As each key are used, this biometric key is marked as used for encryption by the server in the SBA, and will not be used ever again.

6 References

- [1] Tait, B.L., von Solms, S.H. “Solving the problem of replay in Biometrics- An electronic commerce Example”. Proceedings of 5th IFIP Conference on Challenges of expanding internet: E-commerce, E-business, and E-government. (I3E'2005) p468-479. Springer – ISBN 0-387-28753-1. Poznan, Poland 28-30 October 2005.
- [2] James Wayman, Anil Jain, Davide Maltoni, Dario Maio, Biometric Systems: Technology, Design and Performance Evaluation, Springer; 1 edition (December 16, 2004), ISBN 978-852335960.
- [3] Charles P. Pfleeger, Shari Lawrence Pfleeger, “Security in Computing” Third edition, Prentice Hall, ISBN 0-13-035548-8.
- [4] Ebay online Auction: <http://www.ebay.com> / <http://www.ebay.co.uk>.
- [5] PayPal online payment environment: <http://www.paypal.com>.
- [6] Tait, B.L., von Solms, S.H., BioVault: a Secure Networked Biometric protocol, D.Com Dissertation, University of Johannesburg, 2008.
- [7] Tait, B.L., von Solms, S.H. , Secure Biometrically Based Authentication Protocol for a Public Network Environment, Proceedings for the 4th International Conference on Global E-Security 23 – 25 June 2008, University of East-London, Docklands, United Kingdom, p238 – p246.
- [8] Howard Wolinsky “Tagging products and people. Despite much controversy, radiofrequency identification chips have great potential” EGE (2005b) Ethical Aspects of ICT Implants in the Human Body MEMO/05/97, 17 March. Brussels, Belgium.
- [9] EGE (2005b) Ethical Aspects of ICT Implants in the Human Body: Opinion Presented to the Commission by the European Group on Ethics. MEMO/05/97, 17 March. Brussels, Belgium: European Group on Ethics in Science and New Technologies.

PATENT PROPOSAL

The attached patent was discovered during the research of this thesis. However as already mentioned in Chapter 8, this patent proposal corresponds partially to the working of BioVault version 1.0. As the reader is firmly aware at this stage, BioVault version 1.0 still includes various shortcomings, thus rendering this patent proposal of little use.





US006636620B1

(12) **United States Patent**
Hoshino

(10) **Patent No.:** **US 6,636,620 B1**
(45) **Date of Patent:** **Oct. 21, 2003**

(54) **PERSONAL IDENTIFICATION
AUTHENTICATING WITH FINGERPRINT
IDENTIFICATION**

JP	63-288365	11/1988
JP	1-154295	6/1989
JP	6-325158	11/1994
JP	8-180173	7/1996
JP	9-116128	5/1997
WO	WO 94/10659	5/1994

(75) Inventor: **Satoshi Hoshino, Tokyo (JP)**

(73) Assignee: **NEC Corporation, Tokyo (JP)**

* cited by examiner

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

Primary Examiner—Samir Ahmed
(74) *Attorney, Agent, or Firm*—Foley & Lardner

(57) **ABSTRACT**

(21) Appl. No.: **09/200,981**

(22) Filed: **Nov. 30, 1998**

(30) **Foreign Application Priority Data**

Nov. 28, 1997 (JP) 9-328546

(51) **Int. Cl.⁷** **G06K 9/00**

(52) **U.S. Cl.** **382/124; 340/5.53**

(58) **Field of Search** **382/115, 124,**
382/125; 235/380, 492; 704/246, 273; 902/3,
4, 25; 340/825.3, 825.34; 283/68; 356/71;
705/1, 26, 42

A personal identification authenticating system for a client terminal in communication with a server. The server includes a computer and a database. The server performs a service whose uses are limited. The client terminal plays a role of an IC card authorizing device, while the server plays a role of an approval center. The database stores personal information of the service users. The stored personal information on the database includes information related to fingerprints and ID numbers of the service users. A client terminal user impresses one's fingerprint on a fingerprint sensor and puts one's IC card into a card reader. The IC card stores personal information of a card owner. The stored personal information on the IC card includes information related to a fingerprint and an ID number of the card owner. The client terminal includes an authenticator, which provides an authenticating signal if the sensed fingerprint information of the client terminal user matches stored fingerprint information of the card owner. The client terminal transmits the stored personal information of the card owner to the server upon occurrence of the authenticating signal which transmits an authorizing signal to the client terminal if the transmitted personal information of the card owner matches the stored personal information on the database. Upon receiving the authorizing signal, the client terminal user is authorized to access into the computer of the server.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,944,021 A	7/1990	Hoshino et al.	382/5
4,993,068 A	2/1991	Piosenka et al.	713/186
5,128,523 A	7/1992	Diehl et al.	235/441
5,446,290 A	8/1995	Fujieda et al.	250/556
5,623,552 A *	4/1997	Lane	382/124
5,635,723 A	6/1997	Fujieda et al.	250/556
5,708,497 A	1/1998	Fujieda	356/71
6,016,476 A *	1/2000	Maes et al.	705/1

FOREIGN PATENT DOCUMENTS

CN	2201059	6/1995
EP	0 379 333	7/1990

8 Claims, 5 Drawing Sheets

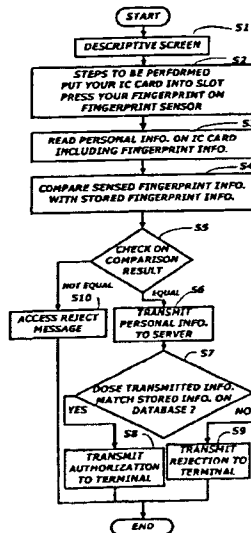


FIG. 1

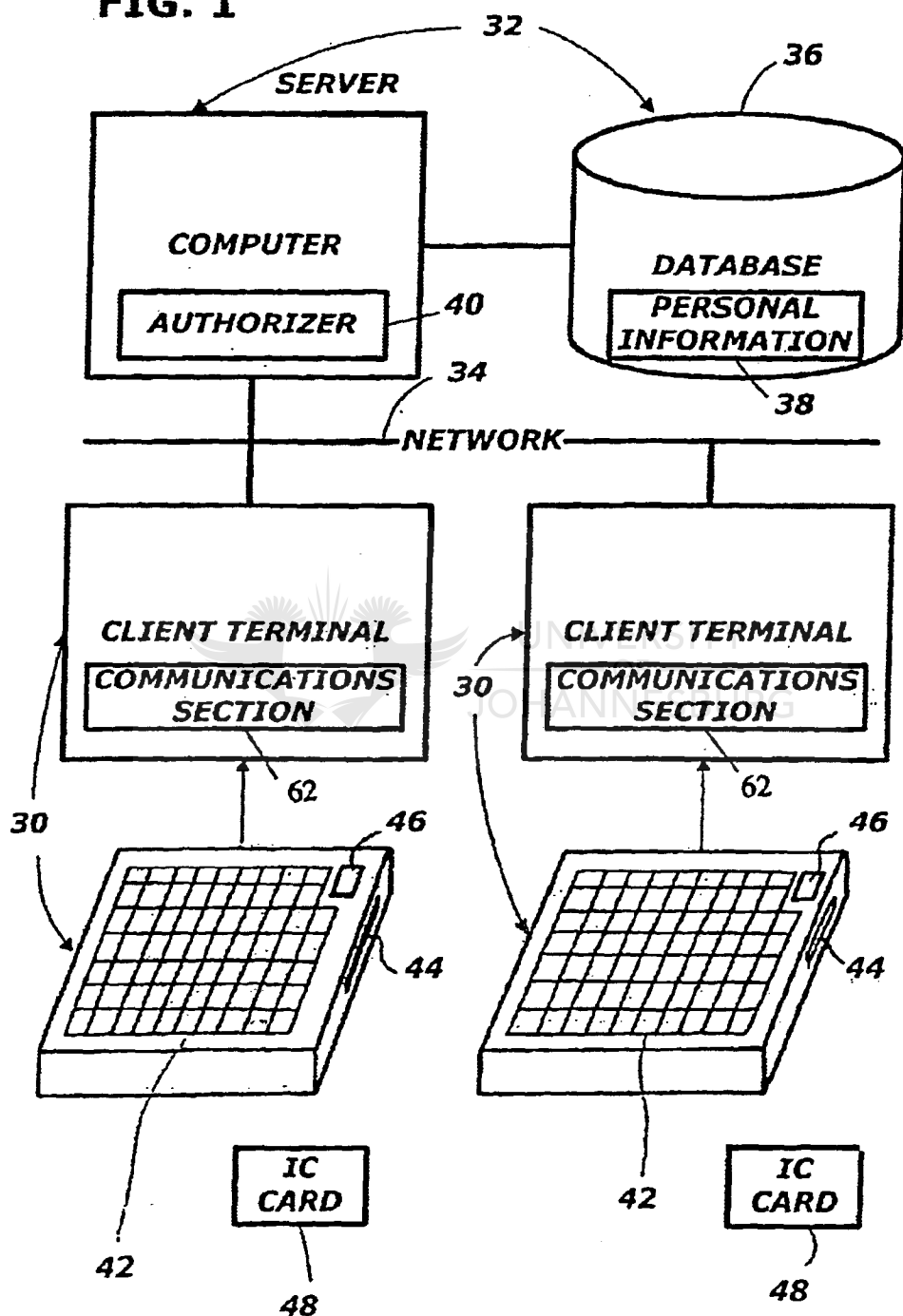


FIG. 2

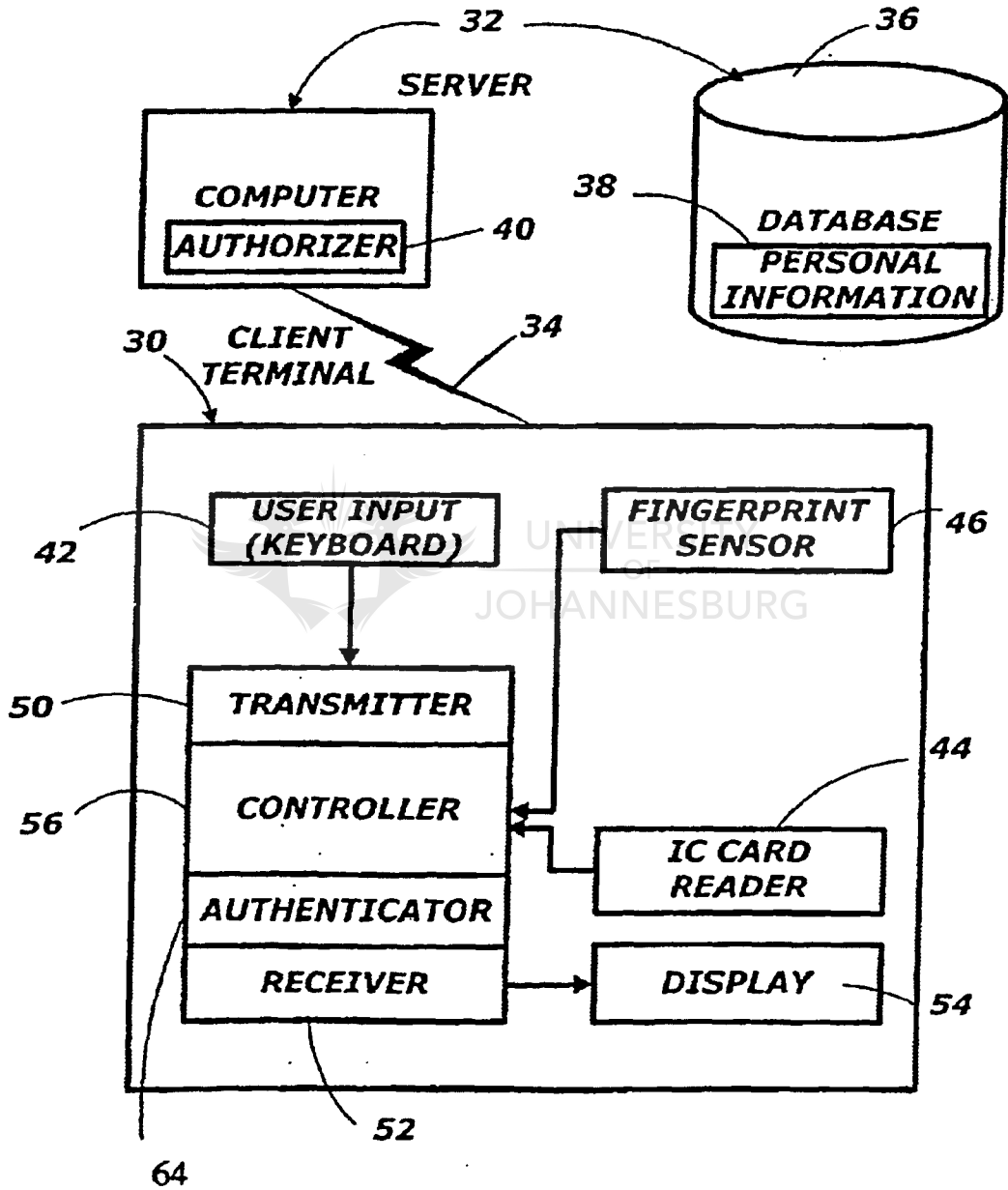


FIG. 3

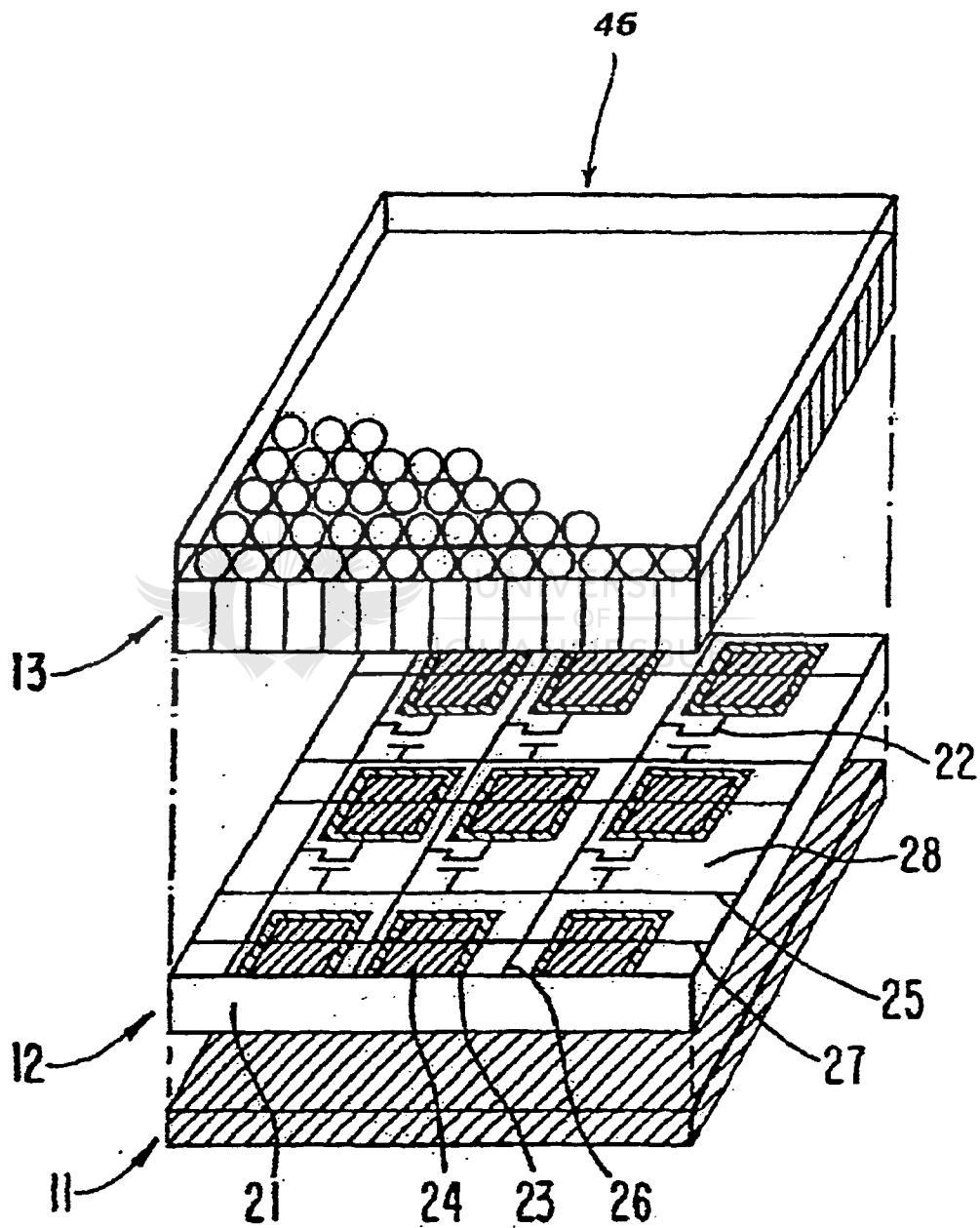


FIG. 4

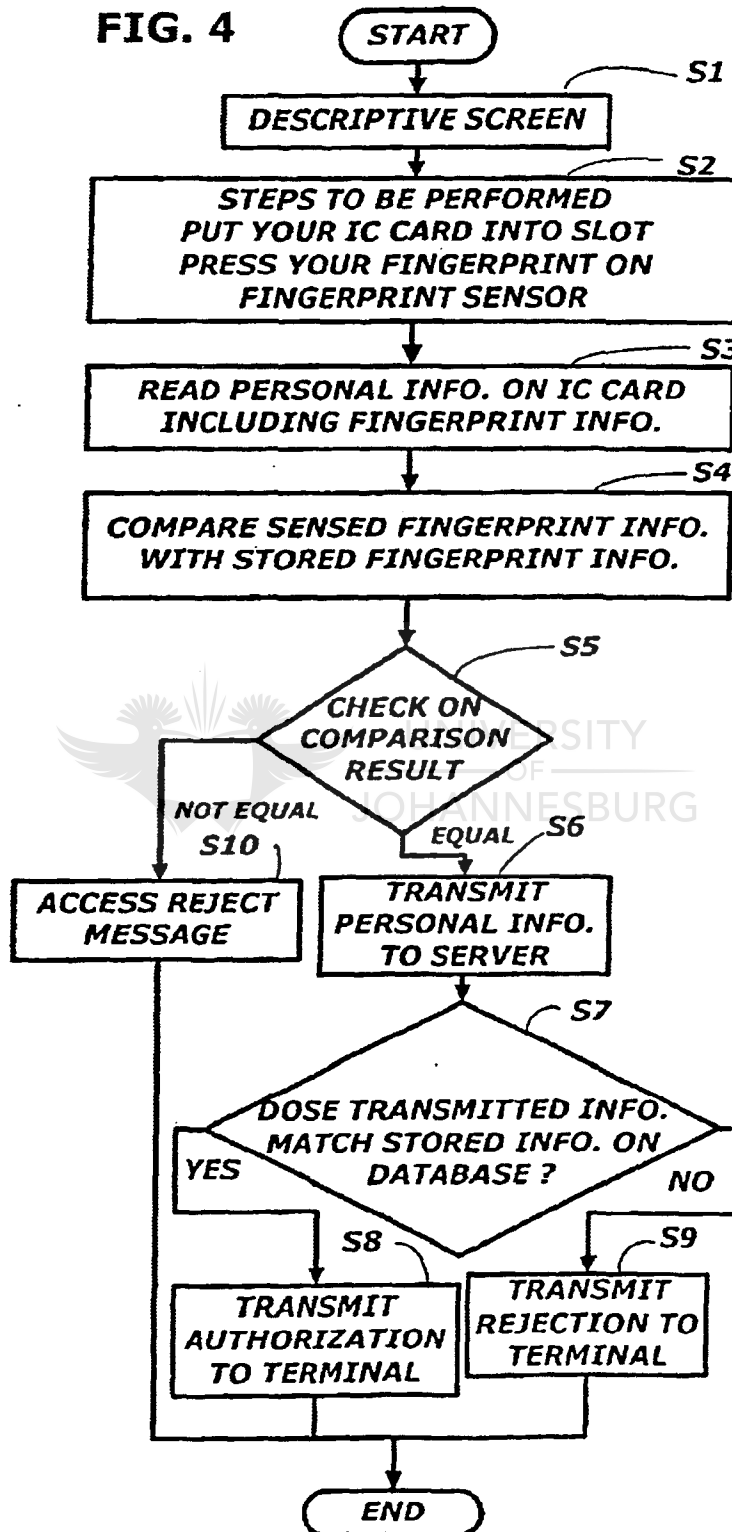
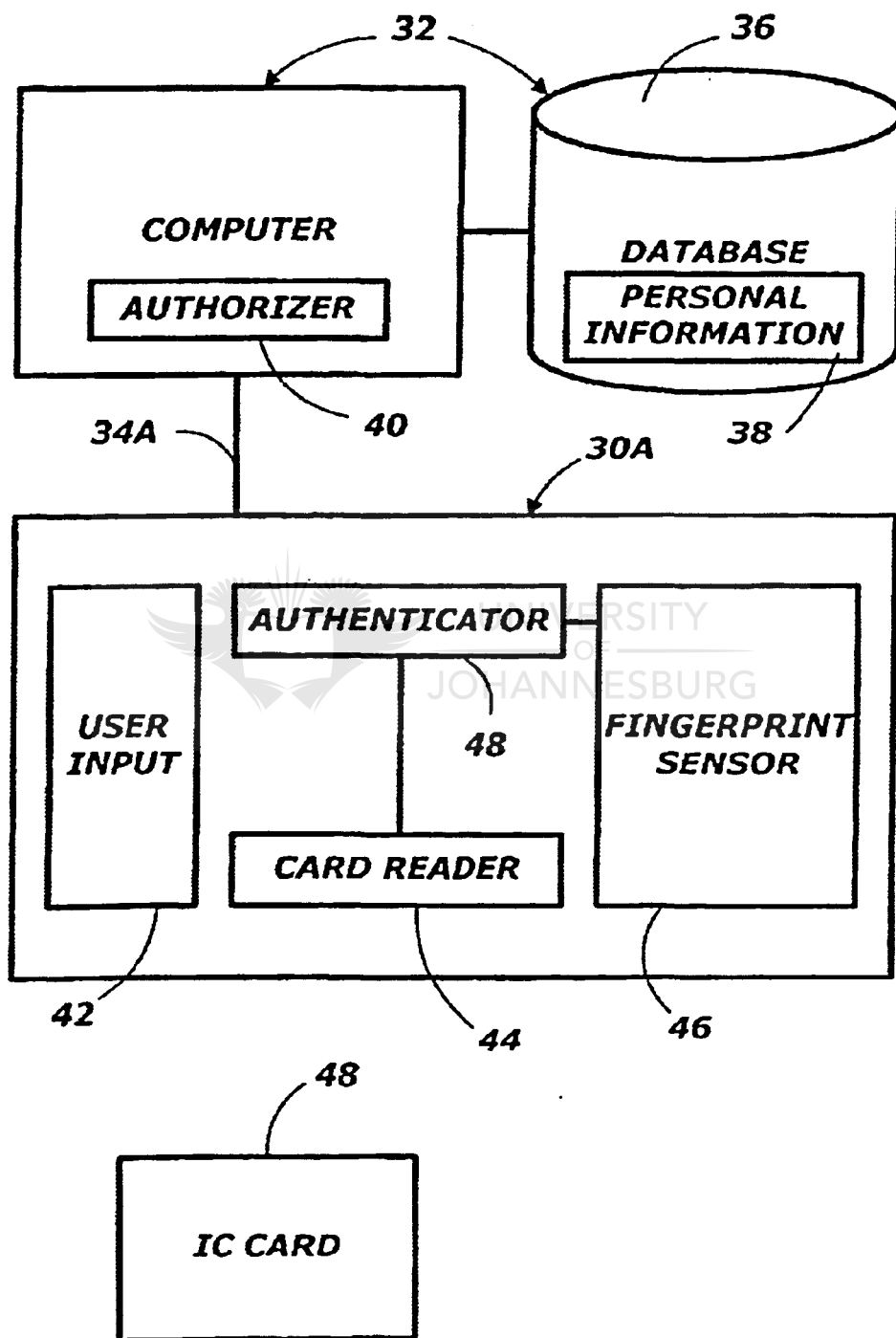


FIG. 5



**PERSONAL IDENTIFICATION
AUTHENTICATING WITH FINGERPRINT
IDENTIFICATION**

FIELD OF THE INVENTION

The present invention relates to a system for authenticating personal identification and more particularly to a personal identification authenticating system for a client terminal in communication with a server.

BACKGROUND OF THE INVENTION

Proving one's identify is necessary when accessing a computer whose users are limited. In order to prevent individuals other than the registered users from accessing the computer, a password or a personal identification number is issued with each ID card. Access to the computer is enabled only when both a password and an ID number corresponding to the user's number read from the ID card is entered through the keyboard.

Transaction execution systems which enable the performance of transactions, such as cash issuance at terminals remote from and in communication with a host data processing system having a central database in which account and other information is stored, are well known.

Such systems, which are frequently used by banks to extend their services, permit the issuance of cash or the receipt of deposits through a terminal, for example, an automatic teller machine (ATM). Such a terminal typically includes a mechanism for receiving and reading information from a card, a user input such as a keyboard, a display and document entry and exit apertures. Issuing a personal ID number with each credit card attains increased security for the issuance of cash or other banking transactions without intervention of a bank employee. A credit card transaction is then enabled only when an ID number corresponding to the account number read from the credit card is entered through the keyboard. This required correspondence prevents a thief or mere finder of a credit card from receiving cash, for example, from a terminal. Upon entry by a terminal user or a customer of a credit card and personal identification number, the terminal is instructed to communicate the credit card data and the personal identification number to the host for authorization of the transaction. At the host, a database of identification numbers is accessed by the card data. The identification number obtained from the database is compared with the personal identification number received from the terminal to perform a host PIN check.

When ID cards, credit cards or other cards are stolen, passwords and/or ID numbers read from cards are decrypted. Thus, presenting a password or a personal identification number with a card is woefully inadequate in preventing individuals other than the registered users from accessing the computer.

It is known to use fingerprints in conjunction with an identification card to verify ownership of the card. JP-A 63-288365 discloses an ATM wherein a selector button to be pressed by a customer for transaction is transparent. A fingerprint of the customer impressed on this transparent button is recorded using an optical system including a video camera. The recorded fingerprint information is compared with stored fingerprint information.

JP-A 1-154296 discloses an ATM wherein a selector button, such as a yen key, is provided with a fingerprint pickup head of an optical fingerprint recording system.

Various compact fingerprint sensors are disclosed by U.S. Pat. No. 5,446,290 (issued on Aug. 29, 1995) that is considered to correspond to JP-A 6-325158, U.S. Pat. No. 5,635,723 (issued on Jun. 3, 1997) that is considered to correspond to JP-A 8-380173, and U.S. Pat. No. 5,708,497 (issued on Jan. 13, 1998) that is considered to correspond to JP-A 9-136328.

In transaction execution systems, a transaction terminal is designed for maximum likelihood that the user of the terminal can perform the transaction in an error free manner even if the user has never operated the terminal before. Such a terminal typically includes a group of selector buttons which allow the customer to perform the transactions and a keypad which may be used by the customer to enter money amounts. Thus, the selector or key switches or buttons of the terminal do not exceed a certain number in the neighborhood of 40. The transaction terminal may include a supply of cash and a cash dispensing mechanism and may also include a depository for receiving customer deposits. These components would then be located within the security chest. In addition, the main control electronics for the terminal may also be located within the security chest so as to prevent any unauthorized access to the control electronics. In addition to the components of the terminal system located within the security chest, a number of components may be located outside the security chest. Thus, the terminal is not compact. In the transaction execution systems, a highly reliable communication means such as an exclusive line is used to establish communication between each terminal with the host data processing system.

In a local area network (LAN) or a wide area network (WAN), personal computers and workstations are used as terminals. Internet system with great number of servers and clients allows the use of desktop or hand-held terminals. A keyboard of such a terminal includes a great number of key or selector switches that amount in number to approximately 300. In the internet systems, each server may perform an exclusive service for a group of authorized users and also may perform an open service whose users are unlimited. Communication means used to connect each terminal to such a server is not highly reliable.

It would therefore be desirable to provide a personal identification authenticating system for use in a terminal that can request both an exclusive service and an open service to a server. The exclusive service requires authentication of personal identification of the terminal user before access to a computer of the server although the free service requires password only from the terminal user.

An object of the present invention is to provide a small-sized personal identification authenticating system for preventing unauthorized individuals from accessing a computer.

SUMMARY OF THE INVENTION

According to one aspect of the present invention, there is provided a system for authenticating personal identification, comprising:

- a server including a computer whose users are limited, said server having a database storing information related to ID numbers assigned to said users and information related to fingerprints of said users;
- an IC card storing personal information including information related to an ID number of the card owner and information related to a fingerprint of the card owner;
- a client terminal in communication with said server, said client terminal including a card reader for reading the

3

stored personal information on said IC card, and a fingerprint sensor for sensing a fingerprint of the client terminal user;

an authenticator that compares the sensed fingerprint information of the client terminal user with the stored fingerprint information of the card owner and produces an authentication signal if the sensed fingerprint information matches the stored fingerprint information;

a transmitter that transmits personal information including the sensed fingerprint information and the authentication signal to said server if the authentication signal is produced; and

an authorizer that compares the transmitted personal information of the card owner with the stored personal information on the database and produces an authorization signal if the transmitted personal information matches the stored information on the database, thereby to give the client terminal user an access to said computer of said server.

According to another aspect of the present invention, there is provided a method of authenticating personal identification for a client terminal in communication with a server that includes a computer and a database, the method comprising the steps of:

storing into the database information related to identification numbers and fingerprints of users who are allowed to access into the computer of the server;

storing into an IC card information related to an identification number and a fingerprint of each of the users; presenting descriptive screen to a client terminal user to give instructions to the client terminal user;

sensing a fingerprint of the client terminal user;

reading the stored information on the IC card;

comparing the sensed fingerprint information with the stored fingerprint information of the card owner;

transmitting the sensed fingerprint information of the client terminal user and the stored information of the card owner to the server from the client terminal if the sensed fingerprint information matches the stored fingerprint information of the card owner;

comparing the transmitted information with the stored information on the database; and

authorizing the client terminal use to access into the computer if the transmitted information matches the stored information on the database.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates client terminals in communication with a server incorporating a personal identification authenticating system according to the present invention.

FIG. 2 is a block diagram of the terminal.

FIG. 3 is a perspective view partially broken away of a fingerprint sensor.

FIG. 4 is a flow chart illustrating a method of authenticating personal identification.

FIG. 5 illustrates a terminal and a server, in the form of a single computer incorporating the personal identification authenticating system according to the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention will now be described more fully hereinafter with reference to the accompanying drawings, in

4

which preferred embodiments of the invention are shown. The terms "server," "client terminal," and "integrated circuit (IC) card" are used throughout the specification. The term "server" is meant to include a data processing system that performs a service for clients. The term "client terminal" is meant to include a terminal that requests services of a server. The term "IC card" is used to mean cards that can store personal information including information related to a fingerprint of the card owner, and is meant to include cards whose purpose is purely identification, and diverse other cards used for additional purposes as well.

Referring to FIG. 1, the personal identification authenticating system is designed to authenticate identification of a user of each client terminal 30. The client terminals 30 are in communication with a server 32 through a network 34. The server 32 includes a computer. In this embodiment, the server 32 can perform both an exclusive service whose users are limited and an open service whose users are unlimited although it may perform an exclusive service only.

The server 32 includes a database 36 storing personal information 38. The personal information 38 includes information related to ID numbers and fingerprints of users authorized to access the computer of the server 32. The server 32 also includes an authorizer 40, which compares personal information transmitted from a client terminal 30 with the stored personal information 38 on the database 36. The authorizer 40 transmits an authorization signal to the client terminal 30 if the transmitted personal information matches the stored personal information 38 on the database 36.

Each client terminal 30 includes a user input device in the form of a keyboard 42, an IC card reader 44, and a fingerprint sensor, preferably in the form of a semiconductor fingerprint sensor 46 (see FIG. 3). It also includes a communications section 62 for transmitting and receiving information to and from the server 32. The fingerprint sensor may sense information related to a fingerprint using a multiple of small capacitors to detect the ridges and valleys of a fingerprint. A client terminal user puts an IC card 48 into a slot of the IC card reader 44. Each IC card 48 stores personal information of the card owner. The stored personal information includes information related to an ID number of the card owner and information related to a fingerprint of the card owner. It is preferred that the fingerprint information be encrypted.

The client terminal 30 as illustrated in FIG. 2 carries an authenticator 64 in addition to the IC card reader 44 and the fingerprint sensor 46. The authenticator 64 is electrically connected to the fingerprint sensor 46 and the IC card reader 44. It compares information related to a sensed fingerprint with the stored fingerprint information on the IC card 48 and produces an authentication signal if the sensed fingerprint information matches the stored fingerprint information. A transmitter 50 is electrically connected to the IC card reader 44 and the fingerprint sensor 46 for transmitting the sensed fingerprint information, the personal information read by the IC card reader 44 and the authenticating signal to the server 32 only if the authenticating signal has been produced. A receiver 52, for receiving an authorization signal from the server 32, and a display 54, for indicating that a client terminal user has been approved for accessing the computer of the server 32, are preferably included in the client terminal 30. The keyboard 42 is used by the terminal user for entering information. The transmitter 50 is rendered responsive to the keyboard 42 for transmitting information entered by the keyboard 42 to the computer of the server 32 upon or after receipt of the authorizing signal from the server 32. A controller 56 controls operations of the client terminal 30.

5

The server 32 includes an access approval mechanism for receiving the personal information including the sensed fingerprint information along with the authenticating signal to compare this personal information with the stored personal information 38 from the database 36 and for approving access to the computer of the server 32. Specifically, the authorizer 40 transmits an authorizing signal to the client terminal 30 if the personal information transmitted from the client terminal matches the stored personal information 38 on the database 36. The authorizer 40 may transmit its signals over the network 34.

Referring now to FIG. 3, the fingerprint sensor 46 of FIGS. 1 and 2 will be described. The fingerprint sensor 46 of the illustrated type is disclosed in U.S. Pat. No. 5,446,290 issued on Aug. 29, 1995 to Fujieda et al., the disclosure of which is incorporated in its entirety herein by reference. Briefly explaining, the fingerprint sensor 46 includes a planar light source 11, a two-dimensional image sensor 12, and optical element 13. The two-dimensional image sensor 12 includes a great number of photosensitive elements 24 arranged two-dimensionally on a transparent substrate 21. Each photosensitive element 24 is formed on a light shielding plate 23 and connected to a terminal of a signal reading switch 22 in the form of a polycrystalline silicon thin film transistor (IFT). The switch 22 is further connected to a signal reading line 26 and a switching line 25. The photosensitive elements 24 arranged along the switching line are connected to a bias applying line 27. An opening 28 is provided in an area unoccupied by the lines 25, 26 and 27 and the light shielding plates 23.

A preferred method of authenticating personal identification is illustrated by the flow chart of FIG. 4. After activation of a client terminal 30, a descriptive screen is presented or shown by step S1. This screen offers a client terminal user instructions to put an IC card 48 into a slot of an IC card reader 44 and place a fingerprint on a fingerprint sensor 46. In accordance with the instructions on the descriptive screen, the user puts an IC card 48 into the slot of the IC card reader 44 and places a fingerprint on the fingerprint sensor 46 by step S2. Information related to the fingerprint is sensed and the stored personal information is read by step S3. The sensed fingerprint information is compared with the stored fingerprint information by step S4 to determine if there is a match. The comparison result is checked by step S5. If there is a match, the sensed fingerprint information by the fingerprint sensor 46 and the stored personal information read by the IC card reader 44 are transmitted from the terminal 30 to a server 32 along with an authenticating signal by step S6. At the server 32, the transmitted personal information including the sensed fingerprint information is compared with the stored personal information 38 on a database 36 by step S7. If the transmitted information by the client terminal 30 matches the stored information on the database 36, an authorization signal is transmitted to the client terminal 30 by step S8. If there is no match, a rejection signal or no signal is transmitted to the client terminal 30 by step S9. If, at step S5, there is no match between the sensed fingerprint information and the stored fingerprint information, an access reject message is presented or shown by step S10. In this case, the information will not be transmitted from the client terminal 30 to the server 32. This reduces load carried by the server 32 and the network 34.

From the preceding description, it is noted that the sensed fingerprint information, which has been compared with the stored fingerprint information, is transmitted to the server 34 along with the authenticating signal for comparison with the stored information 38 on the database 36. This authenticates

6

personal identification of a client terminal user with a high degree of accuracy and security even if the network 34 is not highly trustworthy.

FIG. 5 illustrates a terminal 30A connected a server in the form of a single computer 32 by a highly reliable communication line 34A. The same reference numerals as used in FIGS. 1 and 2 are used in FIG. 5 to designate like or similar parts. The system illustrated FIG. 5 may incorporate the personal identification authenticating system thus far described without any substantial modification.

If communications between client terminals and each server are highly reliable and trustworthy like the one illustrated in FIG. 5, the sensed fingerprint information may be transmitted directly to the server for comparison with stored data on a database of the server.

If client terminal users are authenticated with a high degree of accuracy and security, a server is enabled to perform such exclusive services as application software logon, encryption of application data, decryption of data with encrypted key and electronic signature and its verification with a high degree of security.

Once one is authorized as a user of an exclusive service performed by a server that performs various other open services, this user may request such services to this server through any one of client terminals that have incorporated the personal identification authenticating system according to the present invention.

What is claimed is:

1. A system for authenticating personal identification, comprising:

a server including a computer whose users are limited, said server having a database storing information related to ID numbers assigned to said users and information related to fingerprints of said users;

an IC card storing personal information including information related to an ID number of the card owner and information related to a fingerprint of the card owner;

a client terminal in communication with said server, said client terminal including a card reader for reading the stored personal information on said IC card, and a fingerprint sensor for sensing a fingerprint of the client terminal user;

said client terminal comprising:

an authenticator that compares the sensed fingerprint information of the client terminal user with the stored fingerprint information of the card owner and produces an authentication signal if the sensed fingerprint information matches the stored fingerprint information; and

a transmitter that transmits personal information including the sensed fingerprint information and the authentication signal to said server only if the authentication signal is produced by the authenticator; and

said server comprising:

an authorizer that compares the transmitted personal information of the card owner with the stored personal information on the database and produces an authorization signal if the transmitted personal information matches the stored information on the database, thereby to give the client terminal user an access to said computer of said servers

wherein said server does not receive any information from the client terminal if the authenticator determines that the sensed fingerprint information of the client terminal

7

user does not match with the stored fingerprint information of the card owner.

2. The system as claimed in claim 1, wherein said server performs both an exclusive service whose users are limited and an open service whose users are unlimited.

3. The system as claimed in claim 1, wherein the stored fingerprint information on the IC card is encrypted.

4. The system as claimed in claim 1, wherein said fingerprint sensor is a semiconductor fingerprint sensor.

5. A method of authenticating personal identification for a client terminal in communication with a server that includes a computer and a database, the method comprising the steps of:

storing into the database information related to identification numbers and fingerprints of users who are allowed to access into the computer of the server;

storing into an IC card information related to an identification number and a fingerprint of each of the users;

presenting descriptive screen to a client terminal user to give instructions to the client terminal user;

sensing a fingerprint of the client terminal user;

reading the stored information on the IC card;

comparing the sensed fingerprint information with the stored fingerprint information of the card owner;

transmitting the sensed fingerprint information of the client terminal and the stored information of the card

8

owner to the server from the client terminal only if the sensed fingerprint information matches the stored fingerprint information of the card owner;

comparing the transmitted information with the stored information on the database; and

authorizing the client terminal user to access into the computer if the transmitted information matches the stored information on the database.

6. The method as claimed in claim 5, further comprising the step of:

presenting access reject message to the client terminal user if the sensed fingerprint information fails to match the stored fingerprint information of the card owner.

7. The method as claimed in claim 5, wherein the server performs both an exclusive service whose users are limited and an open service whose users are unlimited.

8. The system as claimed in claim 1, further comprising a network that communicatively connects the server and the client terminal,

wherein traffic over the network is minimized by data only being sent from the client terminal to the server if the authenticator produces the authentication signal.

* * * * *



UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 6,636,620 B1
DATED : October 21, 2003
INVENTOR(S) : Satoshi Hoshino

Page 1 of 1

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Title page.

Item [*] Notice, please correct to read as follows:

-- [*] Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154 (b) by 480 days. --



Signed and Sealed this

Ninth Day of December, 2003

A handwritten signature in black ink, which appears to read "James E. Rogan". The signature is written in a cursive style and is positioned above a solid horizontal line.

JAMES E. ROGAN
Director of the United States Patent and Trademark Office

Chapter 15: References

Note that there might be references in this list that is not explicitly referenced from the thesis. This is due to the fact that many sources were used in the research of this thesis, in order to get an in depth understanding of the research field

15.1. References

- [1] Information Security; Von Solms SH, Eloff JHP.
- [2] Special Publication 800-12 An Introduction to Computer Security: The NIST Handbook; <http://sbc.nist.gov/cyber-security-tips/800-12/chapter16.html>
- [3] Matsumoto, T., Matsumoto H, Yamada K.; "Impact of artificial gummy fingers of fingerprint systems" Proceedings of SPIE. Vol. #4677.
- [4] Computer Networks and Internets, Third edition, Comer Douglas E, ISBN 0-13-091449-5
- [5] Amazon Online Store; <http://www.amazon.com>
- [6] Authentication: From Passwords to Public Keys; Richard E. Smith ISBN 0-201-61599-1
- [7] MAC address; http://en.wikipedia.org/wiki/MAC_address
- [8] TCP/IP Network administration, 2nd edition, Hunt C, ISBN 1-56592-3227
- [9] Absolute PC Security and Privacy; Michael Miller ISBN 0782141277
- [10] Principles of Computer Hardware; Clements A, ISBN 0-19927-3138
- [11] <http://picturethis.pnl.gov/im2/RFTag1/RFTag.jpg>
- [12] Principles of Computer Security; Williams D, Cothren C, ISBN 0-07-225509-9
- [13] F. J. Corbat, M. Merwin-Daggett, and R. C. Daley, "An Experimental Time sharing System,"

- [14] Smith, Richard E; "The strong password dilemma." CSI computer security journal. Summer 2002.
- [15] Adams, A. and Sasse, M. A. (1999). "Users Are Not the Enemy: Why Users Compromise Security Mechanisms and How to Take Remedial Measures." Communications of the ACM.
- [16] Wilkes, Maurice. "Time-sharing Computer systems. London: Macdonald. 1968.
- [17] Lophtcrack Security Software version 2.5 www.securityfocus.com/tools/1993
- [18] Lophtcrack ; www.securityfocus.com
- [19] Smith, Richard E; "The strong password dilemma." CSI computer security journal. Summer 2002.
- [20] "Advisory CA-1994-01: Ongoing Network Monitoring Attacks" February 3, 1994 <http://www.cert.org/advisories/CA-1994.html>
- [21] E-Token, Implimenting Corporate and E-commerce Security using strong Authentication: White Paper, March 2000.
- [22] Security Management; Great debates: Passwords vs Pass phrases Part 1 October 2004
<http://www.microsoft.com/technet/community/columns/secmgmt/sm1004.msp>
- [23] <http://bcddata.com/mm2.jpg>
- [24] <http://xw2k.sdct.itl.nist.gov/smartcard/images/smartcard.jpg>
- [25] "The smart card handbook"; Wolfgang Rankl, Wolfgang Effing; ISBN 0470856688
- [26] "Java Card Technology for Smart Cards: Architecture and Programmer's Guide" ; Zhiqun Chen ; ISBN 0201703297
- [27] Kunitake Kaneko, Hiroyuki Morikawa, Tomonori Aoyama; "Secure Session Migration Using Key-Insulated Public-Key Cryptosystems"
- [28] Credit card skimming, easy to get skimming equipment. 13 July 2006
<http://www.merchantaccountblog.com/archives/149>

- [29] Junkel, Richard. "Biometrics: Personal identification in networked society" .
Jain, Bolle, and Pankanti , eds. Boston: Kluwer academic Publishers.
- [30] TA-48 Mini Card reader <http://www.bcdata.com/ta48.html>
- [31] Korba, Jonathan "Windows NT Attacks for the Evaluation of Intrusion
Detection Systems" Massachusetts Institute for technology, PhD thesis.
- [32] "Advisory CA-1994-01: Ongoing Network Monitoring Attacks" February 3,
1994. <http://www.cert.org/advisories/CA-1994.html>
- [33] The ISO 17799 Directory <http://www.iso-17799.com/index.htm>
- [34] Ben Miller Biometric consortium Listserv, dated 2 Aug 2002
- [35] Wikipedia, the free encyclopedia: <http://en.wikipedia.org/wiki/Biometrics>
- [36] The International Biometric Industry Association. <http://www.ibia.org>
- [37] Bible, book of Genesis Chapter 27, verses 11-28.
- [38] Biometric Systems : Technology, Design and Performance Evaluation;
James Wayman, Anil Jain, Davide Maltoni; ISBN: 1852335963; Springer; 1
edition
- [39] "Biometric product testing: Final report " March 21 2001.
<http://www.cesg.gov.uk/technology/biometrics/>
- [40] Kodiak Computer Services. <http://www.kodiakcomputer.com/facilities>
- [41] Biometrics: Personal Identification in Networked Society, By Anil K. Jain,
Ruud Bolle, Sharath Pankanti, Edition: illustrated, Published by
Springer, 1999, ISBN 0792383451, 9780792383451
- [42] Handbook of Biometrics By Patrick Flynn, Arun Abraham Ross
Edition: illustrated, Published by Springer, 2007
ISBN 038771040X, 9780387710402
- [43] http://www.cardwerk.com/smartcards/smartcard_technology.aspx
- [44] Digital Persona Biometric device manufacturers:
<http://www.digitalpersona.com>
- [45] Faulds, Henry. "Skin Furrows of the hand" Nature. Xxii, 1880

- [46] Galton, Fancis; "Fingerprints" Macmillan and Co. New York: De Capo Press
- [47] Biometric Classification FBI; [www.fbi.gov/hq/ cjisd/takingfps.html](http://www.fbi.gov/hq/cjisd/takingfps.html)
- [48] Sodhi, G.S, Jasjeet Kaur. "On Henry's Fingerprint Classification System."
Fingerprint World. 28, No. 110 (October 2002) : 200
- [49] NIST - NIST ITL American National Standards for Biometrics.
<http://fingerprint.nist.gov/standard/index.html>
- [50] Fingerprint, palm print and pores:
<http://perso.orange.fr/fingerchip/biometrics/types/fingerprint.htm>
- [51] Biometrics: Identity Verification in a Networked World By Samir Nanavati,
Michael Thieme. Edition: illustrated, Published by John Wiley and
Sons, 2002. ISBN 0471099457, 9780471099451
- [52] Software developed by Mr. C Crossingham, advised by B.L. Tait.
August 2007.
- [53] Image Analysis and Recognition: International Conference, ICIAR 2004,
Porto, Portugal, September 29-October 1, 2004 : Proceedings
Published by Springer, 2004 ISBN 3540232400, 9783540232407
- [54] En Zhu, Jianping Yin, and Goumin Zhang "Fingerprint enhancement using
circular Gabor Filter" ICIAR 2004 Proceedings page 750.
Published by Springer, 2004 ISBN 3540232400
- [55] Matsumoto, T., Matsumoto H, Yamada K.; "*Impact of artificial gummy
fingers
of fingerprint systems*" Proceedings of SPIE. Vol. #4677.
- [56] Fingerprint Biometric Device Spoofing
<http://www.washjeff.edu/users/ahollandminkley/Biometric/index.html>
- [57] Fun With Fingerprint readers <http://www.schneier.com/crypto-gram0205.html>
- [58] Matsumoto, T.: Availability of Artificial Fingers That Fool Fingerprint
Systems, *Proc. JCP2000*, Yokoh ma, Japan, October (2000).
- [59] Yamada, K., Matsumoto H. and Matsumoto, T.: Can We Make Artificial

Fingers That Fool Fingerprint Systems? *Technical Report of IEICE and IPSJ*, ISEC2000-45, pp. 159-166, and Vol. 2000 No.68, pp 159-166 respectively, July (2000).

- [60] O'Gorman, L.: Fingerprint Verification, in *Biometrics: Personal Identification in Networked Society*, The Kluwer Academic Publishers, International Series in Engineering and Computer Science, Jain, A. K., Belle R. and ankanti, S. eds., Vol. 479, Chapter 2, pp. 43-64 (1999).
- [61] Biometric Systems : Technology, Design and Performance Evaluation; James Wayman, Anil Jain, Davide Maltoni; ISBN: 1852335963; Springer; 1 edition
- [62] Online Encyclopedia Answers: <http://www.answers.com>
- [63] Computer analysis of images and patterns: 10th international conference, CAIP 2003, Groningen, The Netherlands, Aug 25-27, 2003 : proceedings Published by Springer, 2003 ISBN 3540407308, 9783540407300
- [64] J. Daugman, United States Patent No 5,291,560, March 1, 1994; Biometric Personal Identification System Based on Iris Analysis. Washington D.C
- [65] L. Flom and A. Safir, United States Patent No. 4,641,349, February 3 1987; Iris recognition system. Washington D.C
- [66] Simo Huopio; Department of Computer Science, Helsinki University of Technology; Seminar on Network Security: "*Biometric Identification*
- [67] J. Daugman, "John Daugman's Webpage, Cambridge University, Computer Laboratory" 1999-2002, <Http://www.cl.cam.ac.uk/~jgd1000>
- [68] Iridian Technologies <http://www.iridiantech.com>
- [69] J. Daugman "How Iris recognition works," Univeristy of Cambridge, <http://www.cl.cam.ac.uk/users/jgd1000/irisrecog.pdf>
- [70] Bill Spence, Recognition Systems, Inc - Nov 24, 2002, "*Biometrics in physical access control: issues, status, and trends*".
- [71] Eastern Herald, Post Elizabeth, South-Africa, "Pension Payout scam" November 23 1999.

- [72] Fleming, S. T. (2003). Biometrics: Past, Present & Future. In R. Azari (Ed.), Current Security Management & Ethical Issues of Information Technology (pp. 111-132). Hershey, PA: IDEA Group.
- [73] Osten, et al. United States Patent 5,719,950 (17 February 1998) "Biometric Personal Authentication System" Washington D.C
- [74] Uniqueness of a Fingerprint: <http://www.bromba.com/faq/fpfaq.htm>
- [75] Cole, Simon. 2001. "Suspect identities: a History of Fingerprint and Criminal investigation." Harvard University Press
- [76] Galton, Fancis; "Fingerprints" Macmillan and Co. New York: De Capo Press
- [77] Fingerprint Biometric Device Spoofing
<http://www.washjeff.edu/users/ahollandminkley/Biometric/index.html>
- [78] National Center for State Courts (NCSC)
<http://ctl.ncsc.dni.us/biometweb/BMHand.html>
- [79] Ingersoll-Rand Inc. <http://www.recogsys.com/transition/index.htm>
- [80] Hand Geometry-based verification system: <http://biometrics.cse.msu.edu/>
- [81] Gordon Levin; "Real world most demanding biometric system";
FINAL_4_Final Gordon Levin Brief.pdf
- [82] Fingerprint Identification, Pattern Recognition and Image Processing Lab,
Department of Computer Science And Engineering, Michigan State
University [referred 10.11.1998]
- [83] University of Albany Library, 1988, "Finding aid for the Carleton P.Simon
Papers, 1881-1952, 1956 (APAP-073)
- [84] Information security applications: 6th international workshop, WISA 2005,
Jeju Island, Korea, August 22-24, 2005 : Published by Springer, 2006
ISBN 3540310126, 9783540310129
- [85] Philippe Oechslin, "Making a Faster Cryptanalytic Time-Memory Trade-Off ".
Lecture Notes in Computer Science, Volume 2729/2003,
ISBN 978-3-540-40674-7, pages 617-630
- [86] Miyauchi, H., et al.: Fluorogenic Detection for Latent Fingerprints on the

Colored paper with NBD-C1 and NBD-F, *Reports of National Research Institute of Police Science*. Vol. 42, No.4, pp. 16-18 (1989).

- [87] Ratha. N. K. and Bolle, R.: SMARTCARD BASED AUTHENTICATION, in *Biometrics: Personal Identification in Networked Society*, The Kluwer Academic Publishers, International Series in Engineering and Computer Science, Jain, A. K., Bolle R. and Pankanti. S. eds., Vol. 479, Chapter 18, pp. 369-384 (1999).
- [88] Tej Paul Bhatla, Vikram Prabhu & Amit Dua. "Understanding Credit card Fraud", *Card Business Review*, June 2007, page 3 – 7.
- [89] Love to Know – Credit card Skimming attacks
http://creditcards.lovetoknow.com/Credit_Card_Skimming
- [90] Rob C. A. A. van Schie* and Mark E. Wilson "Saliva: a convenient source of DNA for analysis of bi-allelic polymorphisms of Fcγ receptor IIA (CD32) and Fcγ receptor IIIB (CD16)"
Journal of Immunological Methods Volume 208, Issue 1, 13 October 1997, Pages 91-101
- [91] G. LEONIDA, "Handbook for printed circuit design, manufacture & assembly" Chapter 4. ISBN 0 901150 09 6
- [92] ASCII / American Standard Code for Information Interchange
<http://ascii-table.com/>
- [93] International Standards Organization (OSI) , ISO 7810, ISO 7811, ISO 7812, ISO 7813, and ISO 4909
- [94] Mosaic for X history: <http://www.ncsa.uiuc.edu/Projects/mosaic.html>
- [95] Pizza hut online : <http://www.pizzahut.com>
- [96] History of the internet:
<http://www.davesite.com/webstation/nethistory4.shtml>
- [97] Amazon online : <http://www.amazon.com>
- [98] Ebay online auction: <http://www.ebay.com>

- [99] Bidpay online payment : <http://www.bidpay.com>
- [100] Paypal : <http://www.paypal.com>
- [102] Absa bank – confirmed 5 February 2009 <http://www.absadirect.co.za>
- [103] Visa Card: <http://www.visa.com>
- [104] Master card: <http://www.mastercard.com>
- [105] American Express: <http://www.americanexpress.com>
- [106] Secure socket layer:
http://www.windowsecurity.com/articles/Secure_Socket_Layer.html
- [107] Chou, W, . Inside SSL: the secure sockets layer protocol
IEEE Explorer. August 2002
http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1045644
- [108] Confinity : Short history of Confinity that evolved into Paypal :
<http://www.confinity.com>
- [109] Ina Steiner "eBay to Acquire PayPal" July 08, 2002
<http://www.auctionbytes.com/cab/abn/y02/m07/i08/s00>
(last accessed 7 March 2009)
- [110] "Read this informative article to find out how it all began, how it grows,
and where Paypal is today!" <http://www.happynews.com/living/-online/historypaypal.htm>
- [111] PayPal on Wikipedia: <http://en.wikipedia.org/wiki/PayPal>
- [112] Patent Application – See Chapter 14
- [113] Derma Doctor – Hair loss: http://www.dermadoctor.com/article_Hair-Loss_46.html
- [114] Sandisk 64Gb backup USB flash memory drive :
[http://www.sandisk.com/Products/Item\(2723\)-SDCZ40-064G-A11-SanDisk_Ultrareg_Backup_64GBnbspUSB_Flash_Drivedagger.aspx](http://www.sandisk.com/Products/Item(2723)-SDCZ40-064G-A11-SanDisk_Ultrareg_Backup_64GBnbspUSB_Flash_Drivedagger.aspx)
Last accessed on 24 August 2009
- [115] Howard Wolinsky "Tagging products and people. Despite much
controversy, radiofrequency identification chips have great potential" EGE

(2005b) Ethical Aspects of ICT Implants in the Human Body MEMO/05/97,
17 March. Brussels, Belgium

- [116] EGE (2005b) Ethical Aspects of ICT Implants in the Human Body: Opinion Presented to the Commission by the European Group on Ethics. MEMO/05/97, 17 March. Brussels, Belgium: European Group on Ethics in Science and New Technologies
- [117] Richard L. Zunkel "Biometrics, Personal Identification in Networked Society" – 4 Hand Geometry Based Verification. Springer US, ISBN 978-0-387-28539-9
- [118] Berouz A. Forouzan "Introduction to Cryptography and Network Security" Mcgraw – Hill ISBN 978-0-07-110223-0
- [119] Simson Garfinkel "PGP: pretty good privacy" Published by O'Reilly, 1995 ISBN 1565920988, 9781565920989
- [120] Time magazine : "Ancient Impressions" Monday, Jun. 07, 1971
<http://www.time.com/time/magazine/article/0,9171,905147,00.html>
- [121] Ivan Bjerre Damgård, "A Design Principle for Hash Functions" Publisher Springer Berlin / Heidelberg, Advances in Cryptology — CRYPTO' 89 Proceedings. ISBN 978-0-387-97317-3
- [122] D. V. Sarwate "Computation of cyclic redundancy checks via table look-up", Communications of the ACM archive Volume 31 , Issue 8 (August 1988). ISSN:0001-0782