Innovative Location Based Scheme for Internet Security Protocol

A proposed Location Based Scheme N-Kerberos Security Protocol Using Intelligent Logic of Believes, Particularly by Modified BAN Logic

By

Nabih T. Abdelmajid
05007973

A Thesis Submitted for the Degree of Doctor of Philosophy

Department of Computing
University of Bradford

2010

UNIVERSITY OF BRADFORD
MAKING KNOWLEDGE WORK

Abstract

The importance of the data authentication has resulted in the science of the data protection. Interest in this knowledge has been growing due to the increase in privacy of the user's identity, especially after the widespread use of online transactions. Many security techniques are available to maintain the privacy of the user's identity. These include password, smart card or token and face recognition or finger print. But unfortunately, the possibility to duplicate the identity of a user is still possible. Recently, specialists used the user's physical location as a new factor in order to increase the strength of the verification of the user's identity.

This thesis focused on the authentication-based user's location. It is based on the idea of using the Global Position System in order to verify the user identity. Improving Kerberos protocol using GPS signal is proposed in order to eliminate the effect of replay attack. This proposal does not expect a high performance from the user during the implementation of the security system. Moreover, to give users more confidence to use security protocol, it has to be evaluated before accepting it. Thus, a measurement tool used to validate protocols called BAN logic was described. In this thesis, a new form of BAN logic which aims to raise the efficiency checking process of the protocol protection strength using the GPS signal is proposed.

The proposed form of Kerberos protocol has been analysed using the new form of BAN logic. The new scheme has been tested and compared with the existing techniques to demonstrate its merits and capabilities.

Acknowledgements

First of all, I would like to thank God. This work has been supervised by Dr. Alamgir Hossain and Prof. Simon Shepherd from the University of Bradford and Dr. Khalid Walied from Alzaerqa'a University. I would link to thank Dr. Hossian for support encouraging me to complete the work. I believe that I have been fortunate to have the experience of Prof. Shepherd. Many thanks to Dr. Khalid Waleed's support.

Thanks to Dr. Mumtaz Kamala for his help and support.

Thanks for my father and mother. I hope that I have introduced a big delight to your heart. and for my dear mother for she's concern and sincere prayer on a daily basis.

I would like to thank every one in my family who supported me.

Great Thanks for my dear wife Ruba, she have had the greatest impact on this achievement.

Table of Contents

List of Figures

List of Tables

List of Publications

Some of the finding were published these are:

1. Nabih A, Hossain M A, Shepherd S and Khaled M, "Where you are Based Authentication: An Improved Security Protocol Using BAN Logic", Proceedings of the 7th European Conference on Information Warfare and Security, 30 June to 1 July, 2008, Plymouth, UK, ACI.

2. Nabih A, Hossain M A, Shepherd S and Khaled M, “Improved Kerberos Security Protocol Evaluation using Modified BAN Logic”, the 10th IEEE international Conference on Computer and Information Technology (CIT 2010), 29 June – 01 July, 2010 in University of Bradford, UK, pp. 1610-1615.

3. Abdelmajid N. T., Hossain M. A., Shepherd S., Mahmoud K, “Location-Based Kerberos Authentication Protocol”, Proceedings of The Second IEEE International Conference on Information Privacy, Security, Risk and Trust (PASSAT2010), Aug 20, 2010 - Aug 20, 2010, Minneapolis/USA, pp. 1099-1104.

4. Abdelmajid N. T., Hossain M. A., Shepherd S., Mahmoud K, “ Location-Based Kerberos Authentication Protocol Evaluation using Modified BAN Logic”, Computer & security, Elsevier Sc Journal. (Submitted)

Chapter 1:

Introduction

1.1 Introduction

Information security has been crucial since medieval times. Users have been perturbed from this challenge. At all times, the interference by undesirable elements of personal information and property is a source of major concern. Recently, the world turned to use online in all walks of life, especially after the communications revolution. This rapid development in communications soon accelerated the work and increased efficiency and productivity, but unfortunately it also increased opportunities for hackers to practice their undesirable act. This placed a huge responsibility on researchers to develop security protocols in order to provide secure communication lines. Many security strategies using very powerful encryption codes, such as Rivest, Shamir and Adelman (RSA) [14, 67], Data Encryption Standard (DES) [18, 25] or Message Digest version 5 (MD5) [109], have been proposed to eliminate the ability of hackers to interfere within the information and communication domain. One of these strategies called Kerberos protocol [8, 57, 84, 121]; although, it is relatively secure online key exchange protocol, even then many international reports assert the growing incidents of hacking. This resulted in professionals to derive mechanisms to check the protocol before use. Therefore, Burrows, Abadi and Needham [10] produced a formal testing structure for security protocol called BAN logic. This logic won the admiration of many specialists, especially when it discovered flaws in many of the protocols that were thought by all to be robust. Despite some strategies of full certification by BAN logic, it also still remained under attack.

This thesis illustrates the problems and presents new approach followed by Kerberos protocol. It uses the user's physical location as a new factor in order to increase the strength of the verification of the user's identity. In addition, it presents a new form of BAN logic which also aims to raise the efficiency checking process of the protocol protection strength.

1.2 Research Scope

This thesis includes four main areas; Authentication, Security protocols, Global Position System and BAN logic. Each of the main areas is discussed below:

1.2.1 Authentication

Authentication is a process which aims to check whether the user identity is genuine and bona fide or forgery. There are three main factors that have been used to authenticate the user identity. The first factor called "something you know" such as, user name and password. The second factor is called "something you have" such as, token or smart card. The third factor is "something you are" such as, finger print, iris or facial scan.

Recently, user's address has been added as a new authentication factor. This address can be captured by using a sensor device.

This thesis describes the authentication factors in detail and explores many strategies that apply to these factors. The advantages and disadvantages of each are presented in the literature review section.

1.2.2 Security Protocol

A security protocol is a set of steps that are made during the process of communication between two parties, so as to ensure that communication has taken place without there being breakthrough. In this thesis, Kerberos was chosen because of its fame and power, and is thus studied in detail. As Kerberos needs more research and development, a new form of Kerberos is suggested by adding the user's physical location address using the facility of Global Position System (GPS).

1.2.3 Global Position System (GPS)

"Global Position System is a radio navigation system that allows land, sea, and airborne users to determine their exact location, velocity, and time 24 hours a day, in all weather conditions, anywhere in the world"[1]. GPS is accurate and robust. Therefore, it is proposed that by using the strength of GPS's signal there is a strong likelihood to increase the authentication level of the user's identity.

1.2.4 BAN Logic

BAN logic is a group of rules used to analyse the exchange messages between two parties. It helps to determine whether the message is secure against hackers or not. Full details about BAN logic are presented, and the need for its improvement. Then, a new

[1] GPS resources "http://www.gis2gps.com/GPS/gps.html"

measurement tool followed on BAN which is more robust and more effective than BAN logic.

1.3 Motivations

Although the world is using modern and sophisticated techniques to prevent hackers from penetrating the user’s identity, the world still suffers from many cases of intrusion and theft. This is what stimulated this study; but suffices to highlight the following problems:

Motivation 1:

Most users do not follow the correct instructions in the definition of the protocol before using it, which may cause a hack. The reason for this behaviour is due to several factors, such as:

1. Indifference by users of the consequences of inaccurate definitions.

2. Some users believe that they are beyond the scope of hackers.

Motivation 2:

Some of the definitions are changeable from case to case. This makes the accuracy of the identification extremely difficult. For example, in some cases, the user has to define the required time for every single service. This time varies depending on the type of service, size of the network and the amount of demand for the service. These factors make it difficult to accurately define.

Motivation 3:

One of the main disadvantages of the security protocols is that they rely on the user's performance. Therefore, there is a direct relationship between the proficiently of the user and the strength of the security protocols. So, in case of the use of weak password, users are likely to be more easily prone to attack. Or, if the user has installed some of the wrong setting, the system will be vulnerable.

Motivation 4:

The measurement tools, which most of the people are using to check the protection quality of the security protocol, do not adequately take care of the performance of the user. It is a group of logical or mathematical operations that are taking place to make sure that the sending and receiving messages have been done in a correct way without paying attention to many important details, which may cause the message for a breakthrough, although the accuracy of these operations. For example, measurement tool request a password to encrypt the message, but it does not check the strength of this password. This may lead to give a positive result about the quality of the messages, where in fact, the message is vulnerable because of using a weak password.

1.4 Aims and Objectives

This study is concerned on the issue of the authentication. Further details are presented with the following points:

1. One of the most important aims for this study is to develop a new protocol that can ensure adequate protection to the user, irrespective of the user not following instructions to protect them. This technique does not need administrative

solution and it should not depend on the education of the users on how to use the system to protect themselves. The aim is to protect them technically without getting them to carry out any task prior.

2. This study is also aim to produce another layer of the protection in addition to the encryption level. This new layer characterize by a fixed definition that can be used to access different services. The importance of this goal is the elimination of much verification that have been used to implement security systems that often lead to errors being exploited by hackers to penetrate systems.

3. To complete the process of ensuring that the user is protected, a new mechanism to examine the protection level of the Protocol must be developed in which it takes into account the inadequate performance of the user. In other words, the aim is to make sure that the user is protected in spite of the relatively poor showings in the definitions of the system.

Raising the effective level of the existing encryption code, or building a new encryption systems will not necessarily solve the problem. This is because the reason of the existence of the problem is not weak in the existing encryption software. Searching for technology that is different from the predecessors is a must. This thesis has considered the following steps to achieve the aims mentioned above:

1. Literature survey to explore the existing strategies, their strength and weakness.

2. The possible use of the user's physical location address through the GPS signal is used in this thesis due complexity of calculating the physical address.

3. And then, to ensure the protection of the user, the GPS signal was considered as a prerequisite to accept the messages without involving the user in the drafting of this signal.

4. It was necessary then, to add the user's physical address as a key condition to the available measurement checking tools of the protocol quality in order to confirm that the message is secure.

5. Finally, the ease of use the system has been confirmed by detail examination and comparing them with currently available systems.

1.5 Contributions

In this thesis, it is shown that the reason for the continued success of hackers, despite the presence of advanced security technologies due to poor performance of the user. Therefore, the user is going to be compelled in a technical context to protect themselves. This is achieved by the following:

Contribution 1:

A new form of security protocol is proposed followed on Kerberos protocol which is shortly called N-Kerberos. N-Kerberos has a new level of protection which relies on the user's physical location captured by the military GPS signal (P(Y) code). The quality of added protection level is not based on the user's performance. Moreover, the user is compelled to send his location's signature, otherwise the message will not be accepted.

Contribution 2:

The second contribution aims to verify whether the user is transmitting the messages using his official location or not. A new feature to BAN logic is incorporated, which said that the message must contain the right location signature, otherwise the message will not be accepted.

Contribution 3:

The third contribution aims to implement the new approach of Kerberos protocol and subject it using the form of BAN logic.

1.6 Outline of the Thesis

The rest of the thesis is set out as follows:

Chapter 2 gives details of the authentication. It demonstrates the different authentication factors and Keys, how it works and shows its advantages and disadvantages. In addition, classify in details the using of user's address in order to authenticate the user identity. Considerable challenges were encountered pertaining to data protection, especially when using sensors. It is suggested that authentication needs more investigation in order to be stronger and more effective.

Chapter 3 explains the relevant security protocols and gives examples such as Needham Schroeder and Kerberos protocols [10]. The short coming of Kerberos protocol are highlighted and proposed a new form of Kerberos. This new form contains the physical location signature as a new authentication factor.

Chapter 4 discusses a well known measurement tool called BAN logic. It is to check the quality of protection of the security protocols. It is shown that it needs to be modified and a new measurement tool followed by BAN logic that is called N-BAN Logic is proposed. Finally, the proposed protocol in chapter three is scrutinised with the aid of N-BAN logic.

Chapter 5 explains an implementation of the proposed security protocol (N-Kerberos). It gives details of where it can be applied.

Chapter 6 gives a summary of the research work presented in this thesis and suggests future work.

Chapter 2:

Literature Review

2.1 Introduction

The authentication of the users' identity has caught the attention of many researchers; considering its great importance in the field of data security. Authentication presents a real challenge, especially with the surge in using of online transactions. The user's identity can be verified by many factors called authentication factors. These factors have different ways of implementation; the first factor is the password and/or the personal information. The second factor is by using devices such as token or smart card. The third factor is the reliance on features such as sound waves, iris, facial and fingerprint. After the wide use of the online transactions, developing more appropriate ways becomes necessary, as will be explained in details.

This chapter is described into two parts; in the first part, the importance of using the authentication for user identity and the different aspects of authentication process are presented in details. The various strategies available to authenticate the user's identity using the authentication factors are presented and also the advantages and disadvantages of each of these strategies are discussed. Whereas in the second part of the chapter, location focused authentication is presented. This part explains why choosing the new factor is important, what are the challenges to demonstrate the efficiency of using it and then some studies on the use of this factor will be presented.

The remainder of this chapter is set out as follows; the value of the authentication and the methods of attacks against the authentication exchange process are given in section 2.2. Details of authentication factors are illustrated in section 2.3. Section 2.4 presents the way of achieving much superior authentication. In section 2.5, the well-known authentication keys is introduce, argue their advantages and disadvantages. Section 2.6 shows the different methods used to identify the user's physical location such as sensors and GPS receivers. Challenges faced by using sensors and full details of strategies used to overcome these challenges have been presented in the same section. This section also contains full detail of the GPS signal's and the reasons it is considered superior in determining the user's identity. The justification of the proposed research is presented in section 2.7. Finally, conclusion and future work are discussed in the last section.

2.2 The Value of Authentication

Authentication is an automated process of verifying the identity of entity, such as user, computer or application. It is information used to confirm the genuineness prior to accessing a service. This essential element of authentication becomes even more crucial with the surge in the use of the internet. The remarkable and significant growth on the use of on-line transactions has enabled internet identity thieves and computer hackers to carry out their undesirable acts. The reliable picture of online fraud has been shown on the Internet Crime Complaint Center's (IC3)[2] statistics as a baseline. IC3 reported that online banking fraud is increasing. In order to appreciate the importance of authentication, some selected methods for attacking authentication exchange process are listed below:

- **Eavesdropper attacks**, where an attacker steals the message which are sent between two participants and attempts to modify it. Then, the attacker authenticates himself as a legitimate user [71].

- **Man-in-the-middle attack (MITM)**, which the attacker control the entire conversation between the victim and the server, making them believe that they are talking directly to each other over a private connection. The attacker intercepts all messages going between the two parties and replaces them to different ones. This type of attack called bucket-brigade attack, or sometimes Janus attack [112].

- **Malicious code attacks**, an attacker send an executable application to the user in order to control the victim's computer. One of the most dangerous malicious codes is Access Violations [123]; the attacker accesses the personal computer and steals a confidential data such as list of login names and passwords, credit card numbers and many other information. Denial of Service (DoS) [135] is also another example of malicious code attack; an attacker stops the user from using the system by deleting files that are open at the time of the attack.

[2] The IC3 began operation on May 8, 2000, as the Internet Fraud Complaint Center and was established as a partnership between the National White Collar Crime Center (NW3C) and the Federal Bureau of Investigation (FBI) to serve as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime

- **Password discovery attacks**, an attacker aims to determine the password. There are many available applications in which to help attackers to ascertain the password relying on guessing the passwords or dictionary attacks [22].

- **Phishing attacks**, it is called a social engineering attacks. The attacker sends a counterfeit website, which is almost identical to the legitimate one, and asks the user to enter their details. This is to forge or compromise users' sensitive information [48, 65].

- **Replay attacks**, an attacker records the message sent from the legitimate user and replays it to the verifier to attempt to mislead the verifier [72].

These attacks highlight the need for a robust and enhanced authentication; it is of vital importance than ever in order to establish trust and confidence between two parties doing transactions over an open network. There are many factors that are available and used to verify the identity of the user. The next section shows these different factors of authentication.

2.3 Authentication Factors

The ways in which the users can verify their identity is called authentication factors. These methods or factors are then categorised into three groups; the first factor called "Something you know", the second factor is "Something you have" and "Something you are" is the third factor. Using username and password or some personal information is a well-known example of "something you know". The user needs to remember and insert group of string and characters to verify him/her self before accessing the resources [112, 117, 119]. The second factor is based on what the user has to verify him/herself such as token, smart card, secure ID card, USB keys, etc. The hackers will not be able to access the resources unless he/she has a device. It is relatively difficult to be hacked than using a password. Note that such objects have a complicated cryptographic key see chapter 9 in [112]. "Something you are" is based on unique human physical characteristics. This method of authentication is called biometrics. It can be used to differentiate between persons. Some organisations use this factor in such systems as Fingerprint and Iris recognition [50-52, 95]. Table 2.1 shows the three authentication factors. O'Gorman provides more details regarding authentication factors made comparisons on their features [92].

Table 2.1: Examples of authentication factors

Factor name	**Examples**
Something you know	Password, personal information
Something you have	Smart card, token
Something you are	Fingerprint, eyes scan

Nowadays, many systems use multi-factor authentication in conjunction in order to increase the authenticity quality. It has been noted that using many factors as opposed to one factor give a superior level of authentication assurance, which will be discussed in the next section.

2.4 Strong Authentication

Strong authentication is defined as the use of more than one factor of authentication in order to achieve secured communication channel. Systems can use particular form of authentication which use two or three independent factors of user identity being utilised together to have a strong authentication than the use of single factor [92]. Multi factors authentication can deliver higher level of authentication assurance because the amount of work for an attacker generally increases with using more than one factor; the attacker therefore needs to find out only the password in case of using one factor. While they need to find out the password and steal or copy the smart card when using two authentication factors [92]. Each authentication factor represents independent protection level. Protection systems that use two authentication factors such as token and password or biometrics, provide two protection levels. Therefore, the user needs to pass two levels to access the data. Therefore, by stealing the token alone, it does not allow them to reach the data. Furthermore, by using three authentication factors, token, password and biometrics need to be used to access the data. Figure 2.1 shows the multi factors authentication.

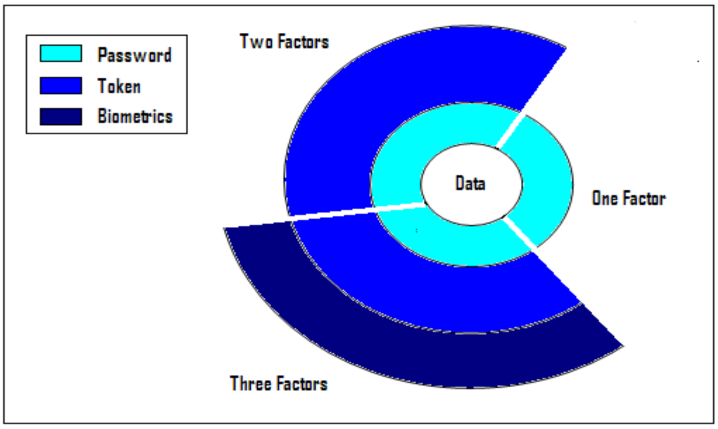


Figure 2.1 Multi factors authentication

Details of available keys to authenticate user’s identity, how it works and advantages and disadvantages are presented in the next section.

2.5 Authentication Keys

There are many keys, which can be used to ensure that data exchanged from one participant to another remains unchanged by any unauthorized third party. These keys called authentication keys and also called electronic or digital keys. It is relying, entirely on electronic encryption codes based on unique information. Applying more than one authentication key would thus create additional layer of security [92]. The following are the details of the well known authentication keys:

1. Passwords
2. Hardware tokens
3. One-Time Passwords
4. Biometrics.
5. Knowledge-base
6. Out-of-Band

There are however other available models and brands. The details and the way of using each of the authentication keys are considered together with the advantages and disadvantages of each.

2.5.1 Password

It is a secret string of characters used to provide or gain access to information on a network. It is a discrete word and supposed to be shared between the user and the server or the verifier. Using password is going to be a good method to authenticate the user identity if the user uses a combination of letters and numbers as it reduces the chances of piercing the password [118]. For example, the number of possible password can be calculated by:

(N^F)

N … Total number of characters

F … Password length

Table 2.2 shows the needed time to crack the different length of password by using 100.000 encryption operations per second. The first column shows the password length, second column is for the crack time and the number at the top total number of character [6].

Table 2.2: Time needed for password crack [6]

94		
3	8.3	Seconds
4	13.0	Minutes
5	20.4	Hours
6	2.63	Months
7	20.6	Years
8	1.93	Millennia
9	9.86	Millennia
10	670	Millennia
11	45,582	Millennia
12	3,099,562	Millennia

It is shown that more than 20 years is needed to crack the password of 7 digits. A hacker will therefore need an entire life time to crack a 12 digit password.

On the other hand, there are many precautions that must be taken into account when using the password. Most of the problems of using the password are as a result of the user choosing or using inappropriate password combination. The following are considered to be some of the draw backs:

1. It may not be easy for the users to memorize the password all the time. It is overhead management particularly for individuals with memory loss [30].

2. Users may write the passwords down in place that is accessible to others, or using the same password for long periods or, usually, choosing an easy to guess passwords. All of these will increase the capability to steal the password [9, 100].
3. Most users are not following a good instruction to choose a good password [63]. This may lead to easy penetration.
4. Most users write user name and password down or save then in a word file in the PC. This will invariably encourages poor security practices[30].
5. In online transactions, using password, as a unique authentication factor without using a fixed life for the message, will give the attacker a good chance to have a long time to steal the signal and attempt to decrypt it and reuse it as a legitimate user.
6. There are many types of attacks that could occur concerning password. The following are some of them:
    a. **Man-in-the-middle attack**, attacker will be able to catch the signal sent from one participant to another [112].
    b. **Insider attack**, system manager who has access to the password file can carry out these passwords [113].
    c. **Phishing attacks**, attacker can steal the password by sending a fake or dummy website, as described in section 2.1 [59, 120].

A survey of the password mechanism is proposed in [54]. Hardware token has been proposed instead of password in order to overcome the drawbacks mentioned above. Details of hardware token is presenting in the next section.

2.5.2 Hardware Token

Hardware tokens are special devices that can encrypt the identity information, such as password, before sending them to the verifier. This is a combination between password and device. In the likely event that the token is lost or stolen; it will be redundant and unable to be used. It is an implementation of using password “something you know” and token or smartcard “something you have” in the same time [33]. Using both password and token instead of using password to authenticate the user identity might decrease the ability of hackers. In addition, the user can easily notice if taken is stolen or not in their possession as it is a physical object. In an attempt to overcome the issue surrounding remembering passwords; systems are now relying on unique personal information such as biometrics to authenticate the smart card [19, 90, 110, 137].

There are, on the other hand, some drawbacks in using smart card or token. These are listed below:

1. The user has to carry an additional smart card or USB. This will irritate many users
2. Smart card can be stolen and all the data can be cracked by using power and time attack [97].
3. Clients or customers can not authenticate his/her identity if his/her token is lost. They will be out of the service until it is replaced.
4. User may not be relied upon to keep their private key secret [128].
5. Managers have to do many complex and critical tasks, such as keep issuing a different set of keys periodically and download software into the computer in order to use the hardware device. In addition, they have to manage the token and the cryptographic keys.

2.5.3 One Time Password

One time password (OTP) is an implementation of disposable password [7] as it can only be used once. There are two main controls for OTP to be high secure strategy; password's length and number of iteration time for hashing the password. Figure 2.2 shows the structure of generating the hashed OTP [118].

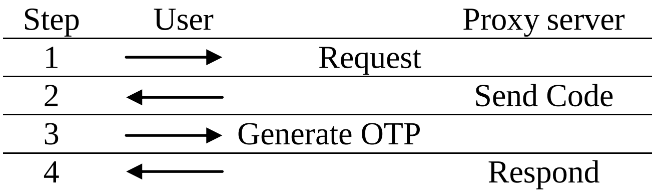


Figure 2.2: Generating Hashed OTP

The user asks the proxy server to login by sending the user-ID in step 1. In step 2, the proxy server checks the validity of the user-ID. If acceptable, the proxy server will send to the user a challenge message which includes the seed and sequence number (N), which is the iteration number of hashing. OTP will be generated by hashing the seed number with the stored password N times and save them in the server. In the next step, the user will pass the seed number and his/her password to the proxy server after hashing it N time. The Proxy server, in the forth step, will compare the received OTP with the one which is stored in the server to check the user validity. Finally, the value of N will be changed, so, the hacker would not be able to generate the next password.

For example, a user uses a list of password printed on a sheet or send it by a secured e-mail channel. Every user has a different password list and each password has a serial number, as shown in table 2.3. The user should insert the user name and requested password from the table, and this password would not be used again.

Table 2.3: List of password

ID	Password
0001	HGFARUI5
0002	THUAZP5B
0003	6FS4J9CM
0060	WGTECVB7
0064	RTHIO34C

For example, suppose you are debiting £1000 by ATM bank machine. The bank will ask you to insert on the password from the list you have. Figure 2.3 explain this example.

Confirmation Letter
You are attempting to debit £1000
from your account.
Please confirm by entering the
password password number 0064:---

You will not be asked to enter this
code later.

Figure 2.3: Confirmation letter

Figure 2.4 shows another example of using OTP. A USB Token that generates One Time Password (OTPs) [128]. The token connects to the USB port. It can then transmit and receive an encrypted data.

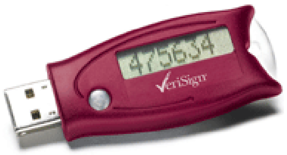


Figure 2.4: One Time Password token

OTP is more robust because of using different password for every different time. However, it has some disadvantages, as follows:

1. Using shared table of password is not secure because it has the same problems as written-down passwords. This table could be lost, stolen or copied and then being used by another user as a legitimate and autherised user.

2. One-time password needs more management time and also more cost. Managers will need to issue the list of password and monitor the using of these password list to update when the current password are used. In addition, special software has to be installed in the verifier's computer.
3. Users may share list of password with others.
4. In some cases, the token itself may be vulnerable to the replay attack [132].
5. The token may not be protected against phishing attack [93] . Details of phishing attack will be provided in chapter six.

User’s biometrics verification is another type of password. It is not easy to be pretended as will be illustrated in the next section.

2.5.4 Biometrics Verification

Biometrics is a unique human physiology characteristics being measured to authenticate the user identity. Usually, Biometrics refers to the technology of using the human body characteristics. It is divided into two main sets as follows:

- **Physiological**, which is related to the human body characteristics such as fingerprints, hand geometry and retina.

- **Behavioral**, which is related to the person's behavior such as hand written signature, gait, and voice waves.

To prove that the user is who he says that he is, the system needs to check its database of previously taken or registered samples to see if the live sample matches the reference sample. Its security is dependent on the hard to copy or forge the sample. Biometrics features is not possible to be forged. Moreover, users can not borrow or lend his biometrics. In addition, most of the biometric data is stable for a long time. Therefore, user does not need to memorize different password. For more information about how biometrics authentication works, refer to reference [77]. This method of authentication has its own unique disadvantages, some of which are presented below:

1. The Biometric feature is easy to attack by replicating it because it is based on not secrecy number [17, 104]. In addition, this replication is relatively not costly.
2. Biometrics is not identical every time. The possibility of false match for identification is greater than that for verification [31, 51, 94, 131].
3. Attacks against the biometrics features are very dangerous by contrast with any other authentication key, because a person's biometrics is unchangeable data and losing any part of his biometrics may cause a break of his identity privacy.
4. In some cases, biometrics is for public use. The Biometrics Institute in Australia has a draft Privacy Code [80] that is currently being reviewed by the (Australian) Office of the Privacy Commissioner prior to final publication. The draft has already been issued for public comment. The Department of Internal Affairs is developing a similar document for New Zealand government agencies. This document is intended for release by late 2006.
5. The biometric is a number that does not differ from the other key; the difficulty is the ability to counterfeit the original document, but the secrecy of the number does not make it a highly secured [17].

2.5.5 Knowledge Based

This is a well-known medium in identity authentication. It challenges the user to provide some special information, where the attacker does not know this information. It is unlikely for the attackers to know this particular information about the user. The user confirms this information at the beginning of the registration process for the server to be used in challenging the user. The users are usually presented with easy information to keep in mind such as favorite colour, favourite name, mother maiden name, etc to answer the questions when receiving the challenges from the server. Figure 2.5 illustrates an example of server's challenge questions[49]. If the user's answers are matched with the information stored when registered, then server will accept the user to use the resources or services.

Authentication Center
Answering these couple of questions are
requested to ensure your identity before
accessing the resources:
: ------------------**Date of Birth**
:------------------**Your Favourite Color**

Figure 2.5. Challenge Questions

To have a stronger methodology of asking, questions should not be fixed. The data should be changeable such as the data based on the history of previous "access signature". This is accomplished by collections of information about the user's website accessing such as IP address, browser settings and geographic location without the need of collecting the user's personal information. Another type of question is relying on the previous use of the resource or service. Figure 2.6 illustrates an example of intelligent questions.

Authentication Center

Answering these couple of questions are
requested to ensure your identity before
accessing the resources:
: ------------------**Date of Birth**
: ------------------**Your Favourite Color**
------------------**What is your last amount**

Figure 2.6: Intelligent Challenge Questions

This method of authentication is not being as it was before, however listed below are the disadvantages.

1. The server challenges the user by fixed number of questions. The answers of these questions can be known if hackers follow the user many times. For example, server might ask the user about his/her favourite colour, best day, date of birth or post code. This group of questions can be collected by hackers and use it later for replaying the server.
2. It is considered that although, intelligent questions are used to reduce the ability of hackers, the user may not prefer to use it because it is not easy to perform; the user needs to memorize a lot of information such as his/her bank account and/or last time using the resources and so on.
3. It is an overhead management. Managers have to manage all questions and answers every time.
4. It is an open time for attacker trying to discover this type of information because it is fixed information.

2.5.6 Out-of-Band Authentication

This way of authentication depends on communication with the users, by using channels registered with organisations, during the transactions. This challenge called on-line communication. It prevents threats to access the information. This is through immediate confirmation from the user through different devices which are easy-to-access by the user such as telephone calls, mobile phone messages, and emails. It is very fast and very familiar for the user to use. In addition, it does not need any special software to be downloaded neither in the personal computer nor in the server. Moreover, the managers do not have any over head management to manage this method of authentication.

Further details pertaining to band authentication can be found in [106]. Listed below are the disadvantages of using this method:

1. Out-of-Band authentication is not secure because an attacker can steal and re-use the personal information by harking the call.
2. Unscrupulous support staff in the organisation may steal the user's personal information.
3. This method is not base on an encrypted data; data is sent as a plain text. This will increase the ability of hackers.

All methods mentioned above suffer from many drawbacks. Thus, finding more practical solutions are an essential need. Figure 2.3 shows the summary of the advantages and disadvantages of authentication keys.

Table 2.4 Advantages and disadvantages of Authentication keys

Authentication Key	Details of authentication keys
Password	Advantages
	- High customer and verifier acceptance. - Well understood.
	Disadvantages
	- Customer needs to use different password for different verifier. - Customer may forget his password. - Generally, people do not follow good instructions to choose good password. - Attacks works by obtaining the password as only one factor.

Token	Advantages
	- Stronger security than using password only. - Using two authentication factors. - Customers can easy notice if token is stolen or losted.
	Disadvantages
	- It comes with an increase in cost. - Token can be stolen or copied. - If user forget or loose his token, he will be off service - until managing to have another one. - Overhead management.
One-Time-Password	Advantages
	- Simple to use. - Easy to implement.
	Disadvantages
	- Using shared table of password is not safe. - Overhead management.
Biometrics	Advantages
	- Customers do not need to carry any devices or memorize their passwords or personal information.
	Disadvantages
	- Should be used in conjunction with other protection. - Biometrics could be stolen or copied. - It is not identical every time. - Biometrics is static, where it is not recommended. - Biometrics is used, in some cases, for public.

Knowledge Base	Advantages
	- Some information is changeable.
	Disadvantages
	- It uses, in almost, fixed number of questions. - It not easy for users to memorize a large number of information. - Over head management. - Easy for hackers to follow up the user's information due to its fixed.
Out-of-Band	Advantages
	- Very easy, fast and familiar for user to use. - No need for any pre installed or implementations.
	Disadvantages
	- It is open to attack for many ways of attacks.

2.6 Authentication Mechanism & Evaluation

The wide using of online transactions provides a good chance for hackers to penetrate the system. Therefore, many authentication mechanisms have been proposed for key exchange. The most popular authentication mechanism protocol is Kerberos protocol. It is proposed to authenticate the end users to the server. Chapter three discussed Kerberos protocol and the problem with it in details. The authentication mechanisms have to be evaluated before using, in order to give users more confidence to use these mechanisms. Burrows, Abadi and Needham produced a formal logic called BAN logic to evaluate the authentication mechanisms protocols [10]. BAN Logic is presented in chapter four.

2.6.1 Encryption Algorithms

Encryption is the process of converting a plaintext message into cipher text which can be decoded back into the original message. An encryption algorithm along with a key is used in the encryption and decryption of data. There are several types of data encryptions which form the basis of network security. Encryption schemes are based on block or stream ciphers. The type and length of the keys utilized depend upon the encryption algorithm and the amount of security needed. Algorithms play a significant role in ensuring the integrity of data. They provide necessary security when communications occur over insecure platforms, such as communications that involve the internet or outside networks. Below is some of the most popular encryption algorithms and how they are used to protect sensitive information.

2.6.1.1 Symmetric Algorithms

Symmetric algorithms use a single key to encrypt and decrypt data. These encryption algorithms typically work fast and are well suited for encrypting blocks of messages at once. The most known example is the DEA (Data Encryption Algorithm) [27] which is specified within the DES (Data Encryption Standard) [18]. Triple DES is a more reliable version while AES (Advanced Encryption Standard) [15] has become new the government standard.

2.6.1.2 Asymmetric Algorithms

These types of encryption algorithms involve a pair of relative keys that encode and decode messages. One key is used to encrypt data into ciphertext while the other key decrypts it back into plaintext. Asymmetric algorithms [96] are more commonly known as Public-key cryptography, first introduced in 1978 with RSA encryption [14, 67].

These schemes work by multiplying two large prime numbers to generate a larger number that is incredibly difficult to revert to the original form.

Asymmetric algorithms tend to be slower than their symmetric counterparts. Because of this, they aren't recommended for encrypting large amounts of data. The biggest advantage to such a scheme lies in the utilization of two keys. Hence the name, the public key can be made publicly available, enabling anyone to encrypt private messages. However, the message can only be decrypted by the party that owns the relative private key. This type of encryption algorithm also provides proof of origin to ensure to overall integrity of communications.

2.6.1.3 Hash Algorithms

Hash algorithms [74] function by transforming data of arbitrary length into a smaller fixed length, more commonly known as a message digest. These types of algorithms are considered one-way functions. The generated output varies, making them very efficient when it comes to detecting alterations that might have been made to a message. Hash algorithms are often generated by the DES algorithm to encrypt online banking transactions and other communications where messages can't afford to be corrupted.

2.7 Location-Based Authentication

A need to develop the security techniques is remaining as long as the wheel of scientific progress is in rapid rotation due to that the relationship between continuity and existence of modern scientific innovations and the need to find new technologies to protect its users is a direct correlation, specialists should not overlook this. Recently, the world has turned to use new methods to verify the user’s identity, especially after the huge increase in transfer of data used in wireless networks. Many international reports confirm the continued exposure to dangerous hack. “Trust wave’s Global Security Report 2010 summarizes findings from the Chicago-based firm’s investigations of 200-plus data breaches last year as well as 1,800 penetration tests of clients’ computer systems to find vulnerabilities. It is the third such annual report Trust wave has done, and the number of data breaches has gone up every year, according to Nicholas J. Percoco, senior vice president of SpiderLabs, Trustwave’s investigative and research division. Hackers went after payment card data in 98% of the cases Spider Labs investigated” [42]. As a result of the noticeable increase in online transaction token, biometrics and smart card are no longer widely used as before as they are cumbersome to manage and vulnerable to new attacks such as phishing attack [53] or a replay attack [61].

Location-Based Authentication is a new technique that uses the user’s physical location address as a key to authenticate identity [5]. There are different forms that can be used to verify the user’s physical location. A well known form is by using a sensor device. It is applied within a short scope, such as implementing the sensing wireless network in one building floor. This research includes the subject of sensor because there is a direct relation between them; sensors are using to verify the location of the user weather he is using a legitimate position or not. If the sensor node can receive the user’s signal, that is mean that the user is inside the legitimate region and so far he can use the services. This location-based authentication is the main scope of this research. Another method is by using GPS receiver that can receive the address of the user’s physical location from anywhere in the world. It is an intelligent sensor which is used to monitor user’s physical location and environmental conditions such as, temperature, sound, vibration and pressure. Both forms have the same policy, which is using the sensing facility to know the exact location of the user. In the next section, the method of the sensor operation, authentication of the user identity and what are the interfaced challenges are demonstrated. Note that you can skip this part and read a shortcut causes, available end of the section, which led to the search for the possible adoption of the GPS signal in order to verify the identity of the user.

2.7.1 Sensors

Wireless sensors network consists of many nodes. Each of node's hardware consist of microprocessor, storage area for data, sensors, Analog-To-Digital converters, a data transceiver, controllers that tie the pieces together and energy sources. Nodes can communicate to each other, sending and receiving the data, by using different protocols. The communications using sensors wireless network is different than those using the Internet; in Internet, the user named the server and send group of information, where sensor networks users are verified by many attributes such as sensor value range or physical location. User's request moves node by node from the production point to the server point. Root node can send a packet to its neighbor and this packet must identify the sender, the receiver and the distance between them. The node which receives the packet can resend it to another node. Therefore, packet can be received by more distance nodes

Professionals face many challenges to substantiate the source of the message. It is very easy for the administrator to find the rogue machine in case of using wired network, because signals can be physically traced from transmitter port to the receiver port. Whereas, in case of wireless network it cannot get information about the physical location of rogue machine. The administrator cannot know what hardware or software that rogue machine are using or what is the broadcasting power level of the rogue machine. Therefore, there is a good potential for the intruder to keep going in wireless network. A full detail pertaining to sensors can be found in [2]. There are two main ways which can be used to pretend the signal of wireless networking; misbehaviour nodes and decrypt the signal. The next two sections give details about each of them.

2.7.1.1 Misbehaviour Nodes

The failure to maintain the efficiency of the node may cause a lack of knowledge of the official position source of the message, and this is what helps attackers to keep going in their works. Thus, it is very important to find techniques which can help to follow up the efficiency of the nodes in order to suppress the basis of the intruder. Below are different ways that cause the misbehavior problem and a lot of techniques were proposed to defense against these ways.

1. Distortion

It is known that the signal may send in free space, especially in dealing with huge institute, making them vulnerable to distortion by several factors such as the weather or collision with other signals sent at the same time [107]. This type of hack is called Rushing Attack [47]. This type of hacking has been concerned to disrupt the arrival of the message to the target. The hacker sends a quick signal to all nodes adjacent to the target before the arrival of the official signal, and thus prevents the official letter from reaching the target, as shown in the following picture.

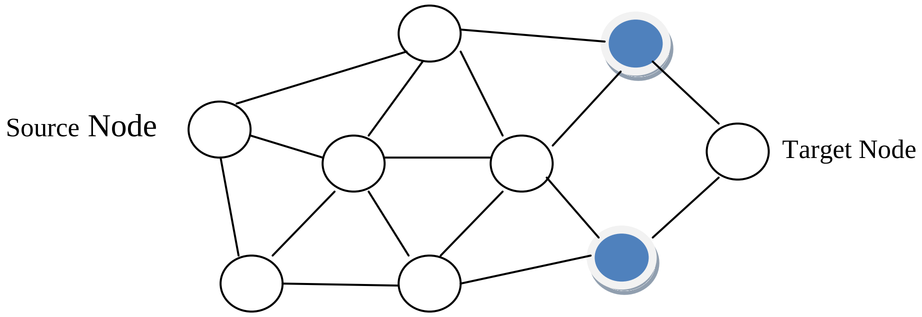


Figure 2.7 Rushing Attack

Another type of attack used to misleading the signal and disable the service is called Wormhole Attack [46]. In this type of hacking, the hacker changes the signal’s orientation to a different path.

This distortion would reduce the efficiency of the accuracy of the signal which would adversely affect the ability to calculate accurately the position, which will make the administrator rejection and has to stop the service or to accept it as a valid signal in spite of its vulnerability to penetration.

To overcome this problem, many techniques are built particular to ensure that the message reach the target. One of such is Rashing Attack Prevent (RAP) [47]. This study adds a mark for each signal to identify the maximum communication range, which examines the neighbouring node.

Dynamic Source Routing Protocol (DSR) [20, 44, 55, 56, 79] is another study used for the protection of the rushing attack. This protocol follows-up on the signal to ensure that the signal reaches its intended target. It consists of two main concepts; Route Discovery which is used to choose the best nodes to reach the target, and Route Maintenance to check whether the node has worked properly or not.

Yih-Chun Hu *et al* produce Packet leashes [45]. This technique is to defend against Wormhole Attack. It is determining the distance between two points, assumed by geographic leashes, and determines the time needed to send it by temporal leashes, which represents the time stamp.

Another technique on the upgrading of the accuracy of location calculation technique called follow-me application [39]. It rests on the continued follow-up to the user wherever he went using the equipment and network resources. It uses the theory of non-typical readings rejected and is called a statistical outlier rejection algorithm. These studies are based on the implementation of several main axes; group of monitors transfers the user-specific data that are obtained using a fine-grained location system. It is then converted to the form of executable applications and compares it with a list of the correct data previously stored.

There is another system to follow up the user's location, which is almost similar to the previous study significantly [38, 41, 129, 130]. This study is based on the portable badge carried by the staff for the duration of the time. This Badge send a signal containing a globally unique code through the ten parts of a second every 15 seconds to tell the location of the user and for this reason called “Active Badge”. The sensors distributed all over the place receive the signal, explore and translate it into a form that can be read and determine whether the user's exists or abroad.

Hightower *et al* had adopted another approach in order to reach a high degree of accuracy in the calculation of the user's location [40].

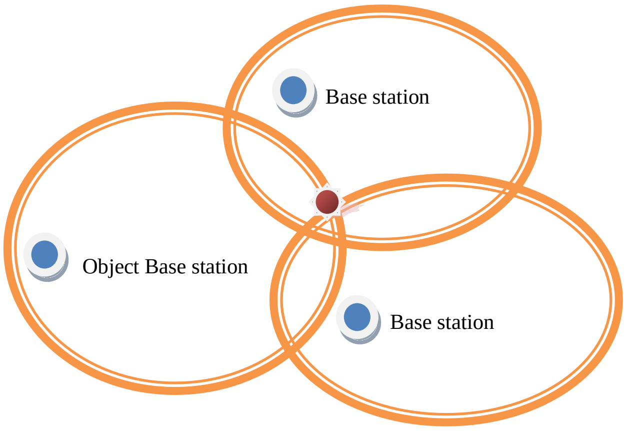


Figure 2.8. Signals of three base stations

In short, the idea is using several base stations for the provision of a strong signal to know the limits of allowable work area. Then, the server will adopt the intersect region by three different areas. Finally, the server will transfer the data to the site of application used by the users. Figure 2.8 shows the general concept of the idea.

Unfortunately, these studies did not address all problems adequately due to many disadvantages. One of the greatest disadvantages encountered in these studies is that it does not respect the privacy of the user, causing them discomfort and privacy concern. This may lead them to make a deliberate act of failure in the hardware to stop monitoring them. Moreover, Infrared (IR) signal cannot penetrate walls in comparison with the radio signal [66]. Furthermore, these techniques have been facing several challenges due to dependence on staff such as wearing the badges. The employee may forget to wear it deliberately in order to conceal their where about and hence put it away, which provides an opportunity for another user to get access to the services.

2. Redundancy and Delay:

The wireless network based on the distribution of a number of adjacent nodes which are used to transmit the signal from one node to another until the signal reaches the base station. There are many situations where the system has been enforced to use a greater number of nodes to cover a larger area of work, which would mean a large number of sending and receiving signals. This will lead to the emergence of the problem of delays. Clearly, the node will be obliged to receive many unwanted messages, which would cause delay and waste of the node’s energy. It should be taken into account that the reduction of the number of nodes is not an ideal solution due to the need of a large number of nodes in many cases.

Denial of Service attack (DoS) is one of the most common types of wireless signals attack that cause a delay problem. There are numerous forms which show this kind of hacking. One of the forms is when the penetrator jams the sent signals. It is also happens when a hacker sends a large number of messages which would drain the power of the node, point to mobilize memory, storage capacity, hence, blocking the nodes or at least the cause of inaccuracy in its work. In other words, this method depends on the hack of pumping several signals to fill the line between the node and the base station, it is called in some cases Path Denial of Service (PDoS) [134].

Jing Deng *et al* have produced a study made by identifying the transmitted signals every second to keep decreasing the number of sent signals and so far decreasing the possibility of the overload [23]. Although many other studies have been proposed to overcome this problem [36, 70, 78, 87], Unfortunately, the problem still exists. attacker can use Distributed Denial of Service attack (DDoS) [86]; attacker uses many computers to attack the network. In other words, multiple sources can be used from different locations to attack the network at the same time. “In DDOS attacks, attackers first explore the vulnerability in a particular system and thus he makes the first tools for the attack called master. Then the master uses other large amount of computer for the attack which is called agents. Now the attackers will instruct those machines by using a command. Therefore with the command of the attackers the master computer will follow its command and it transfer that instruction of command to different agents. Thus there will be a huge network created with large number of agents and master. Therefore when these all agents target the victim it will be almost impossible to handle that amount of request send by the agents and therefore the particular server or website will be immobilizes and it can't give service to the legitimate user"[3].

3. Weak Performance

The lack of attention to many things connected to node will lead of course, to attacks of the sent messages. There are many reasons that may lead to node misbehavior. They are as follows:

- **Weakness in battery**. One of the most important elements that control the misbehavior of the node is the power of the battery. The weaknesses in sensors' batteries may cause a clear difference in the degree of power of communication, which is making it difficult for the administrator to determine where the signal is coming from. This will give hackers a good chance of penetration[3]. In [3] a study is carried out in an attempt to obtain the required effectiveness from the node. This study divided the organization to multiple domains; each domain has specific signal strength and is not allowed to accept more or less of it. It has identified the minimum and maximum time to send the message. The most important objective of this study is to raise the accuracy of the signal by reducing the number of messages sent and received. Therefore, the batteries will be able to be working properly for a longer time**.** It is worth mentioning that there are many studies which have focused on this topic [122, 126, 136].

[3] http://freshtutorial.com/distributed-of-denial-service-attack/

- **Broken node**. If the node has fault software, this may lead to flood of sending the message. Some techniques have focused on the tracing the signal from the source to the destination to ensure the quality of the transmissions. One of these techniques is called Watchdog feature [64] that was added to the node to follow up and determine if the efficiency of the node work is effective or not. And then be avoided by using the Pathrater feature if bad efficiency. When node sends the signal, the node's watchdog will verify whether the next node sent the signal or not, by listening promiscuously to the next node. The Pathrater in the case of the misbehavior will choose another node to be sure that the signal is sent properly.

A Bayesian method is another strategy; the main trust of this method is taking subsequent observation of signal strengths and so far, acknowledge where the device might be [73]. However, data has to be trained in order to build the system. If error occurs in the training step, the robustness will be reduced and such errors can give the intruder good opportunity to disguise their location.

In another technique [125] which follows on Bayesian methods, and is called Server-side indoor location-sensing. This system does the test with the client before and records the different possibilities of transmission power of the client. The administrator can address all possible elusive tactics for rogue machine.

In the subsequent evolution of the Bayesian approach to localisation theory, a group of researchers identified its shortcomings as the lack of precision in the calculation of the user's location through the working on the sensing wireless network, and they have refer this to several causes [125]. One of these reasons is the complex links between the distributed nodes, which may affect the accuracy of the message. Another reason is the noisy electromagnetic interference which is caused by weatherproof such as sun spot and thunder storms that may weaken the power and accuracy of the received and sent message.

Another technique is to find the location of the node is to estimate for the unknown position of the node [26]. In case of using thousands of nodes, the possibilities of problems which can occur will be increased. In this study, the administrator does not need to know all the nodes in the wireless network. The network contains number of known nodes and others are unknown. If one node can contact another node, then the nodes are nearing to each other and they are within the permitted area. In this methodology, all nodes have to perform a centralized computation and communicate the information with a single computer in the network. The focus here has been on reducing the cost and the difficulty of management in diminishing interest in the degree of precision required. Because most institutions that use large number of sensors such as universities are available for all to visit. Therefore, it is easy for hackers to threaten the system.

2.7.1.2 Decoding the Signal

It has previously been stated that the signal is transferred over a cable or free space, which would make it vulnerable to be compromised and stolen. The possibility of decrypting the signal and change the contents gives the hackers a greater chance to penetrate the network and get the service. There are many studies that focus on the encryption of the signals before sending them. Most of these studies have adopted to encrypt the signal by a preset password using the method of one-way-hash chain [139]. Moreover, it uses a time stamp to prevent the replay attack [61]. It cannot be installed at a specific time to transmit the signal, therefore, the time identification has to be period of time such as from one second to three seconds. This certainly will give hackers good chance of a breakthrough, especially in the case of using a strong transmitter. Details of these techniques are as follows:

One of the suggested solutions to ensure that penetration is the construction of a secure channel by the parties, such as choosing a key in advance before starting to mutual the signal between them. This method is called priori trust relationship [81].

Hailun Tan produced a new security scheme using one way key chain [124]. This study divides the nodes into different groups according to the differences in the distance between the node and the base station. And each group has a different key, this key is one-way hash chain [61]; it is a symmetric cryptography key which is a known number, but it is difficult to return it back to find out its source. After collecting the group's information, the sensor node will examine the validity of the used key to accept or reject the packet. This study is very similar to the study of [115]. The difference between the two is that, this study is supporting multi-hop network, where the study in [115] support only one-hope network.

TESLA is another technique which is relying on encryption of the signal by using one-way chain key for key exchange in addition to time stamp to prevent replay attack [98]. This technique will increase the size of the packet to 24 bytes. Furthermore, one-way-chain key does not fit into the memory of the sensor node. Because of this, TESLA has been improved to πTESLA [99] and multi-level πTESLA [76] in an attempt to reduce the number of sent signals in order to overcome the overload problem. But this is not a viable solution, because the volume of sent messages is still considerably large.

Moreover, Tong Zhou and Krishnendu Chakrabarty in [127] concentrated on watchdog protocol with πTESLA [13]. They produced a Constrained Function Based Message

Authentication Scheme for Sensor Networks (CFA). Other similar studies are [28, 108, 114, 138].

Kyusuk Han and Kwangjo Kim produced a model called Light Weight Security Model [37]. This model discussed the problem of protecting the user identity taking into account the importance of maintaining user privacy. This study elaborates in detail because of many similarities with the Kerberos protocol which is a key component of this thesis as will be explained in the next chapter. However, this study does not depend on the sensing location in the definition of the user's position, but considered it as an initial stage prior to the authentication phase. Light Weight Security Model includes three main components; "*C*" is a client, "*SP*" is a service provider and "*OP*" as a trusted operator. Assume *C* and *OP* share key K_C and *OP* and *SP* share key K_{SP}. *C* tries to prove his location to the *SP*, while *SP* shall examine the validity of location data transmitted from *C* in collaboration with the trusted party *OP* as a certified as follows:

C asked the *SP* to get access to the service. Then, the *SP* requests client's physical location information (LocInfo). *C* requests the proof of his location information from *OP* to be sent to *SP*. Then, *OP* sends to *C*:

Enc{MACK_{SP} (IDC, LocInfo), MACK_{C} (LocInfo, MACK_{SP}(IDC, LocInfo)))

This message includes two parts; the first one is encrypted by Kc, MACK_{C} (LocInfo, MACK_{SP}(IDC, LocInfo)), which is only known by C and OP, so far, C can decrypt this part of the message. The second part is encrypted by Ksp, MACK_{SP} (IDC, LocInfo), this part of the message is a ticket for C to be sent to prove his location information to the SP. C should be sure to match MACK_{SP}(IDC, LocInfo) from the message with MACK_{SP}(IDC, LocInfo) from the ticket. If it matches, then C is assured that MACKC (LocInfo, MACKSP(IDC, LocInfo)) is not forged, Then, C continues operation. There after, C sends IDC, Enc(LocInfo, MACKSP (IDC, LocInfo)) to SP. Then, SP decrypt the received message and match the LocInfo in the ticket with LocInfo which is out of the ticket. Figure 2.9 shows the steps of Light Weight Security Model.

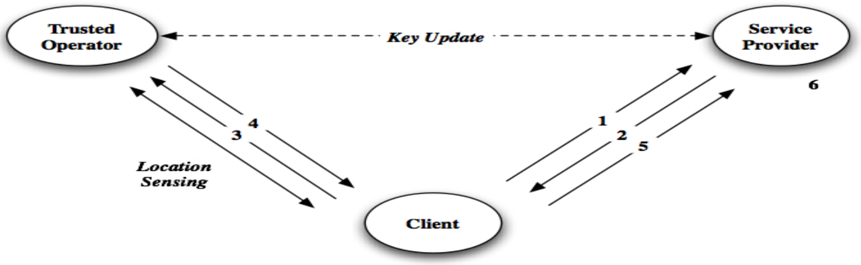


Figure 2.9: steps of Light Weight Security Model.

The last step of this model is updating the key. OP and SP will create a new key K’SP, so, next time K’SP is used to generate MACK'SP (IDC, LocInfo'). In addition, the message has a time stamp to avoid reuse it again. As mentioned before, this technique is similar to Kerberos. In the next chapter, Kerberos will be discussed in detail and clarify the weaknesses associated with it.

The next table is to show in brief the list of these challenges, suggestion solutions and classify the risks expected to occur in the absence of finding suitable solutions to these problems.

Tabel 2.5 Over view the challenges of using sensors

Challenges	needs to be done	The effects of no solutions
Distortion	The use of techniques to reduce the distortion and ensure that the message reached the target clearly	The arrival of the message is unclear or not true, which may lead to be rejected
Redundancy and Delay	Reduce the number of sent messages and making sure that there is no effect on the quality of the work.	Reject the message because of its use more time than the allotted
Weak performance	The use of techniques to ensure effective tools of nodes	Ineffective Work, and therefore provides weak points enable hackers to penetrate the network and access to the service.
Authentication	Signals have to be encrypted before sending signals to avoid penetration	Easily penetrable, and the representation of penetrating the same as if the official user

The following list summarises the problems that are still plaguing the sensing wireless network regarding stopping hackers accessing users' privacy:

1. Although there are of studies undertaken to tackle the problem of overload, the problem still exists. The main reason for this is the need to use cryptographic techniques and indicate that it needs to occupy a large volume of the signal. For

the ease this problem, specialist must find techniques of strong protection using a small size or should develop the sensor devices to accommodate large volume data.

2. The method used in the protection of the wireless is still relatively expensive. This is because of the need to use multiple passwords depending on the locations.

3. The used protection techniques depend on the user to determine their passwords. Thus, the degree of protection will depend on how the user follows the correct methods in the selection of passwords.

4. The dependence on time in the systems of protection does not lead to feel more confident. The attacker may use a quick devices to accomplish the task during the period allowed. In addition, the administrator can not reduce the period to the stop the hacker because it could lead to the inability of the legitimate user to access the services.

5. A lot of definitions that have been proposed by both the user and the administrator. Sometimes this will require specialist kills and knowledge.

6. In some systems, the follow-up movements of the users are not acceptable to many of them. This may lead the user to abort the work in multiple ways.

Using a sensor to find an accurate user’s physical location in order to verify his identity has been faced by many problems as mentioned above. Although many strategies have been proposed to defend against these challenges, it is still suffering from many problems. This thesis proposed another way which is more accurate and robust than using sensors. It is using the facilities of GPS signal. GPS has been used to track addresses and courier services, but it is not used in the science of the Authentication. In the next section, a detail of the GPS signal and why it can be used to authenticate the user's identity are presented.

2.7.2 Global Position System (GPS)

The Global Positioning System (GPS) was designed to provide global weather, navigation and timing information to military users in all weather conditions regardless of day and night, anywhere on the Earth which has an unobstructed view of the four or more GPS satellites. Every physical location has a unique location signature created by a Location Signature Sensor (LSS). It is read by microwave signals transmitted by the thirty satellite constellation of the GPS. It consists of three main factors as presented in the next section.

2.7.2.1 Factors of GPS.

The GPS consist of three main factors, as listed below:

1. **The space factor** consists of a 32 operating satellites. They distributed over the sky and constantly moving a complete orbits in every 11 hours, as shown in figure 2.10. Every satellite transmits one-way signals indicating its current position and time.

Figure 2.10 distributed satellite around the earth.

The first satellite was launched in 1978 and they were completed them in 2008. Figure 2.11 shows the availability of these satellites.

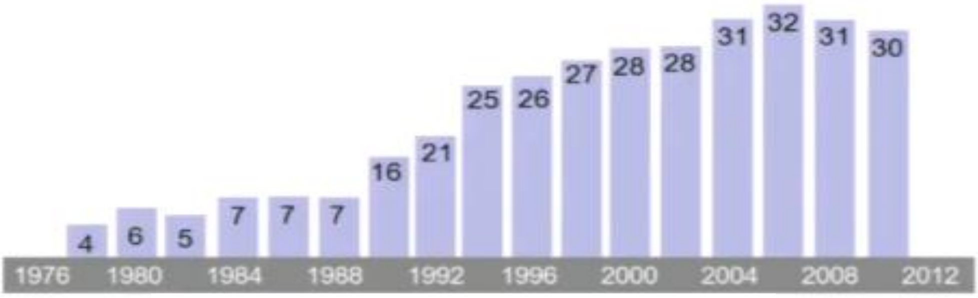


Figure 2.11 Availability of the satellites [103]

1. **The user** is the second factor. This factor contains the GPS receiver, which receives the signals from the GPS satellites and uses these signals in order to calculate the user's position co-ordinates.

2. **The Ground factor** are control stations. There are several ground stations in different places all over the world. The master station is in Colorado. The others are in Hawaii, Kwajalein, Diego Garcia, Ascension Island, Cape Canaveral and Florida. These stations are constructed to monitor the efficiency of the satellites signal through the occasional command manoeuvres and administer the satellite clocks. It monitors the movement of GPS satellites and updates the date of satellite. Monitoring the signal using this factor is a very important in order to reach a public confidence in using it safely.

In recent years, GPS has been used in many places such as, cars, planes, construction equipment and boats. The GPS may become a worldwide utility and can be described as a consumer item.

2.7.2.2 Determine the Precise User's Location.

In order to determine the user's location, user's GPS receiver has to be viewed by 3 or more satellites. This is based on calculating the distances between the receiver and the position of each one of the three satellites, and then performing some mathematics operations to calculate the position using time of transition and the speed of light [58]. To illustrate this, suppose an object is 2 miles away from a main selected reference point. One could not know where it is exactly because it could be 2 miles in any direction from the main selected reference point. With only this information, the number of possibilities of the location could be huge number. But, if one is told you that are also in 2 miles from another closer reference point, now one eliminate the possibilities numbers of the exact location. It would be known that it is somewhere perimeters of these two spheres intersect, as shown in figure 2.12, but still the number of possibilities of my location is high.

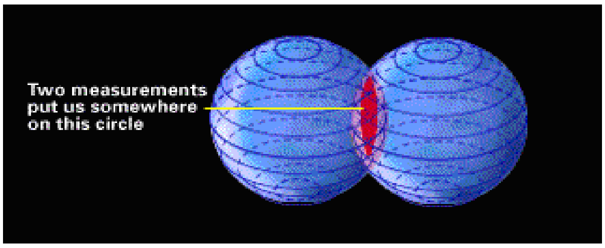


Figure 2.12 Intersection of two spheres

Using another sphere it will help to come closer to the exact location. If one is in 1 mile closer, this will further reduce the number of possibilities of the preferred location. In fact, the more spheres you add, the more accurate position you achieve. Figure 2.13 shows how the intersection of three satellites. Details of determining the user's location can be found in [141]

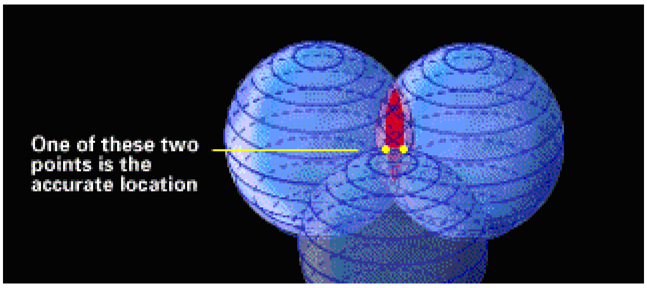


Figure 2.13 Intersection of three spheres

Thus, there are two main things must be known in order to calculate the user's physical address; the location of three or more GPS satellites and the distance between the GPS receiver and three satellites. GPS receiver calculates the distance between the GPS receiver and the satellite by measuring the time it takes the signal to travel from the satellite to the GPS receiver. This signal is a radio signal and it uses the speed of light to travel. So, GPS receiver will calculate the distance by multiply the speed by the time. To do this, the clock used by both the satellite and the receiver are synchronized and very accurate. "A clock error of 1/100 second, which is difficult to imagine but quite common from car races or skiing races, would in GPS navigation lead to a mistake in the position of about 3000 km" [43]. Therefore, It is not easy for any entity in cyberspace to pretend to be in any place other than where its Location Signature Sensor (LSS) actually is [24, 133]. Moreover, the GPS signal is designed to be protected against the jam [35]. Examining the possibility of jamming the GPS signal code will be presented in chapter 5. These are other reasons that give high confidence for the GPS to be used to authenticate the user's identity safely. Below is detail about position determination with GPS:

"In a considerably simplified approach, each satellite is sending out signals with the following content: I am satellite X, my position is Y and this information was sent at time Z. In addition to its own position, each satellite sends data about the position of other satellites. These orbit data (ephemeris und almanac data) are stored by the GPS receiver for later calculations. For the determination of its position on earth, the GPS receiver compares the time when the signal was sent by the satellite with the time the signal was received. From this time difference the distance between receiver and satellite can be calculated. If data from other satellites are taken into account, the present position can be calculated by trilateration (meaning the determination of a distance from three points). This means that at least three satellites are required to determine the position of the GPS receiver on the earth surface. The calculation of a position from 3 satellite signals is called 2D-position fix (two-dimensional position determination). It is only two dimensional because the receiver has to assume that it is located on the earth surface (on a plane two-dimensional surface). By means of four or more satellites, an absolute position in a three dimensional space can be determined. A 3D-position fix also gives the height above the earth surface as a result.

Simplified, the position determination by means of a GPS works on the sample principle as the distance of thunderstorms can be judged: the time is measured between lightning and the following thunder. The speed of light is so high that the delay between the time where the flash hits the ground and the time the observer sees the flash can be neglected. The speed of sound in the earth’s atmosphere is approximately 340 m/s. This means that for example a difference of 3 seconds between lightning and thunder corresponds to approximately 1 km distance to the thunderstorm. However, this procedure is not yet a determination of a position, but only a determination of a distance. If different people on fixed positions would determine the time span between lightning and thunder, this would allow the determination of the position where the flash hit the ground!

In the following an explanation is given, how the position determination by GPS works. For simplification, in the first step we assume that the earth is a two-dimensional disk. This allows us to do some understandable sketches for illustration. The principle can then be transferred to the model of a three-dimensional globe.

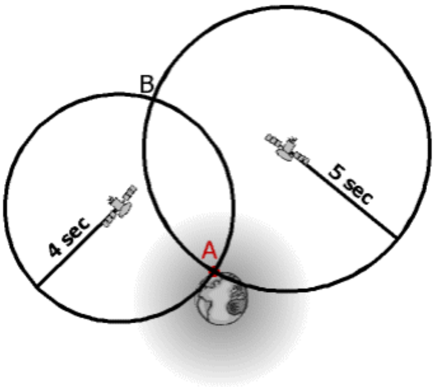


Figure 2.14 Position determination with two satellites

In Figure 2.14 on the left, the time needed by a signal to travel from the first of two satellites to the receiver was determined to be 4 s. (In reality this value is far too high. As the signals travel with the speed of light (299 792 458,0 m/s), the actual time span for signals from the satellite to the receiver lies in the range of 0.07 s.) Based on this information, we can at state that the receiver is positioned somewhere on a circle with a radius of 4 s around the first satellite (left circle). If we perform the same procedure with a second satellite (right circle), we get two points of intersection. On one of the two points the receiver must be situated. Now we have used two satellites. But the process is called trilateration, not dilateration so don't we need a third satellite? We may use a third satellite but we could also assume that the receiver is located somewhere close to the earth's surface and not deep in space, so we can neglect point B and know that the receiver must be found on point A. The area in the picture above which shaded grey is the region in which GPS signals are supposed to be “realistic”. Positions outside this area are discarded, so is point B. This assumption replaces the third satellite which would in theory be required for the process of trilateration. In this example an unequivocal position is obtained from only two satellites. So we just need a third satellite for a third dimension and that's it? Well, in principle yes. But the problem lies in the determination of the exact runtime of signals. As explained above, satellites impose a sort of time stamp on each transmitted data package. We know that all clocks of satellites are absolutely precise (they are atomic clocks after all) but the problem is the clock in our GPS receiver. Atomic clocks being too expensive, our GPS receivers are based on conventional quartz clocks which are comparatively inaccurate. What does this mean in practice?

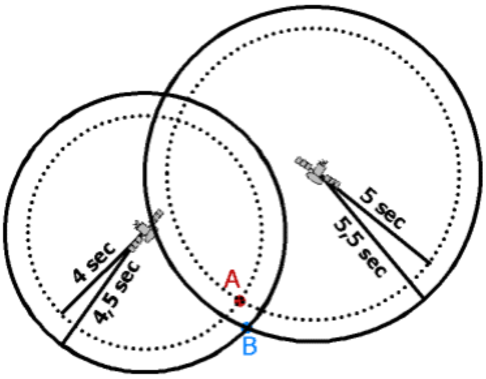


Figure 2.15 2D position determination with 2 satellites and clock error

Let's stick to our example and suppose the clock in our receiver is 0.5 seconds early compared to the clock in the satellite. The runtime of the signal seems to be 0.5 s longer than it actually is as shown in Figure 2.15. This leads to the assumption that we are on point B instead of point A. The circles that intersect in point B are called pseudoranges. They are called “pseudo” as long as no correction of the synchronisation errors (bias) of the clocks has been performed. Depending on the accuracy of the clock in the GPS receiver, the determined position will be more or less wrong. For the practice of GPS based navigation this would mean that no determined position can ever be of any use, as the runtimes of the signals are so short, that any clock error has an overwhelming influence on the result. To achieve an accuracy of 10 m of the position, the runtime of the signal must be precise to 0.00000003 seconds.

As atomic clocks are no option in GPS receivers, the problem is solved in another and quite elegant way; If a third satellite is taken into account for the calculation of the position as shown in Figure 2.16 , another intersection point is obtained: in case that all clocks are absolutely precise.

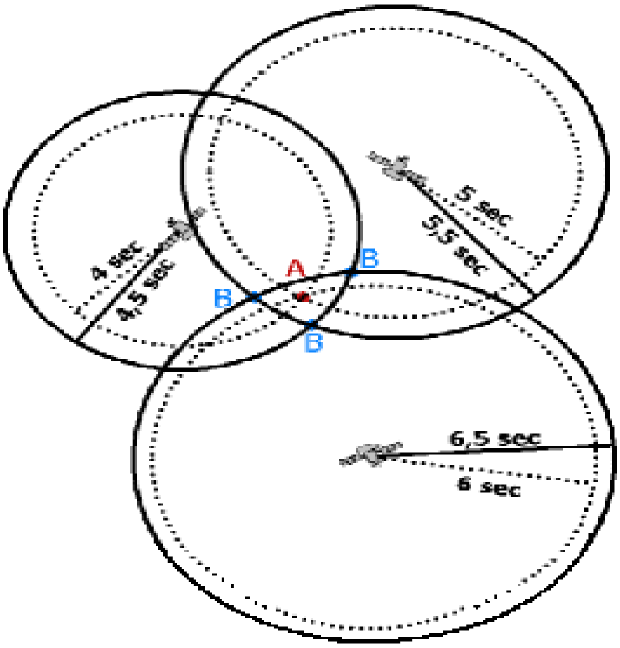


Figure 2.16 2D position determination with 3 satellites and corrected clock error

point A would be obtained, corresponding to the actual position of the receiver. In case of the receiver clock being 0.5 s early, the three intersection points B are obtained. In this case the clock error stands out immediately. If now the time of the receiver clock is shifted until the three intersection points B merge to A, the clock error is corrected and the receiver clock is synchronized with the atomic clocks in the satellites. The GPS receiver can now be regarded as an atomic clock itself. The distances to the satellites, formerly regarded as pseudoranges, now correspond to the actual distances and the determined position is accurate" [43].

2.7.2.3 GPS Signal: C/A and P-Code.

Each GPS satellite transmits two signals; a secure encrypted signal exclusively for military users called P-code signal and a non secure civilian signal called coarse acquisition or the civilian code (C/A). The length of P-code is 6.1871×10^{12} bits long (6,187,100,000,000 bits) and repeat only once a week. They are broadcast for two different frequencies and the military signal provides better security than civilian signals. The military signal is also designed to resist electronic attack. P-code has been encrypted by modulation with the W-code to generate the Y-code in order to prevent any attacks by unauthorized users. Moreover, P(Y) code has good property, which is if you have a snapshot of received P(Y) code of your position, you can identify the location. On the other hand, it is difficult to ascertain what P(Y) code should have done if you know where you are [116]. Again, using the facilities of P(Y) code increases the confidence of using it to authenticate the user's identity safely. For the ranging codes and navigation message to travel from the satellite to the receiver, they must be modulated onto a carrier frequency. In the case of the original GPS design, two frequencies are utilized; one at 1575.42 MHz (10.23 MHz × 154) called L1; and a second at 1227.60 MHz (10.23 MHz × 120), called L2. Besides redundancy and increased resistance to jamming, a critical benefit of having two frequencies transmitted from one satellite is the ability to measure directly, and therefore remove, the ionospheric delay error for that satellite.

2.7.2.4 Accuracy of the GPS.

There are a number of factors that affect the GPS accuracy, such as noise sources from the radio signals, weather conditions, physical obstructions and the natural objects such as a mountains or tall buildings between the satellite and the GPS. The best environment to achieve the best accurate determination of the position can happened only when the satellite and receiver have a clear view of each, in order to increase the accuracy. Differential GPS (DGPS) has been proposed. DGPS uses a known position of one receiver and obtain the different between the real range and the pseudo range to correct the error and have a better result. Figure 2.17 shows the idea of DGPS. Thus, It has been noted that the GPS gives an accurate location output [82]. The increased security of the GPS have been discussed by many researchers, some of these are [24, 75, 82, 111].

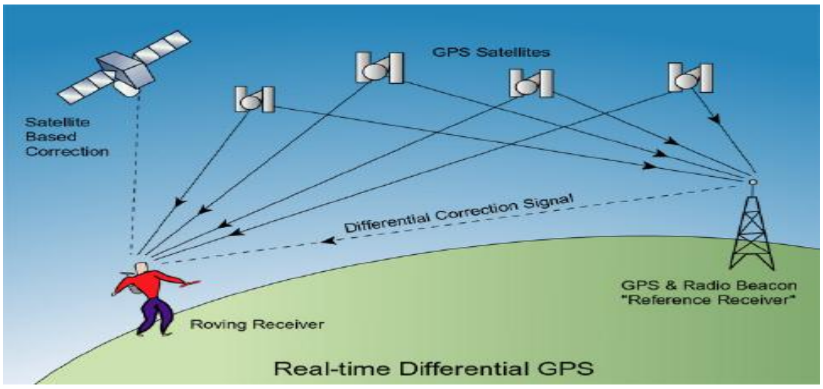

GPS Satellites
Satellite Based Correction
Differential Correction Signal
GPS & Radio Beacon "Reference Receiver"
Roving Receiver
Real-time Differential GPS

Figure 2.17 Differential GPS

2.7.2.5 Authentication in GPS

Since the military signal is not easy to spoof or jam and has a high level of accuracy, it has attracted the attention of using this signal to authenticate the user identity. It is contributed that user can capture the P(Y) code and there is no presumption or assumption her to get the P(Y) code from the military institution.

User can store the P(Y) code to verify his physical address signature to the server. Therefore, if the administrator determines where users are allowed to work through in advance, the military P(Y) signal could serve to publicize the location of the user profile and thus his identity. We do not say that the user will send his captured P(Y) code to the server as it is received, because it may be stolen by hackers, and re-use it later on the basis that they are a legitimate use. But, what may make sense is that the server may ask number of questions to the user that the answers are related to his location signature (P(Y) code). Table 2.5 shows the reasons that can lead to the use of GPS to authenticate the user identity.

Table 2.6 Reasons to use the GPS to authenticate the user identity.

No.	Reasons leads to use P(Y) code to authenticate the user's identity
1.	Gives an accurate location output.
2.	Cannot be spoofed.
3.	Cannot be jammed.
3.	Not easy to be decrypted.
4.	Available in all weather, conditions, day and night, anywhere on the Earth.
5.	Relatively not expensive.
6.	Commonly accepted.

GPS however is used only outdoors in the sense that the receiver should have a direct "view" to at least four GPS satellites. In the next section, details of N-Kerberos protocol using the facility of the GPS are given.

As there are no strategies that used the GPS signal in wireless network for the purpose of the authentication. One study used the GPS to increase the accuracy of the sensors. The detail of this study is as follows:

In July 2002, a group proposed a study to enhance the wireless network security using Global Position System (GPS). The signal may be beyond the limits of the building and so far, the attacker can capture the signal if their position is close to the building. This study is aiming to disable the signal out of the limit of the building; Authors used a wireless piconet network device in addition to GPS receiver; GPS to determine and provide earth coordinates to gatekeeper of wireless network [11].

Figure 2.18 shows wireless network devices, the first one inside the authorised building permitted it to have authorised access to the wireless network. The attacker building is not permitted to have authorized access to the wireless network. GPS signal has been added in addition to the sensor's signal because GPS signal can help the administrator to define the exact limit of the building, where this can not be done by the signal of the sensors. Although attacker can be within the limit of the sensor's signal, his signal will be rejected because his GPS signal is out of the definition of the autherised building. Figure 2.19 shows the process flow of authorization of a piconet wireless network device within defined absolute earth coordinates.

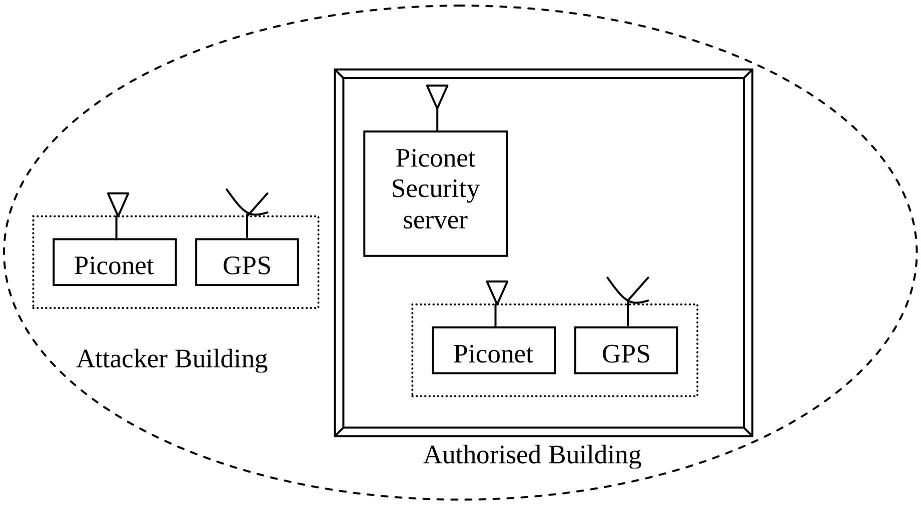


Figure 2.18: Wireless network devices

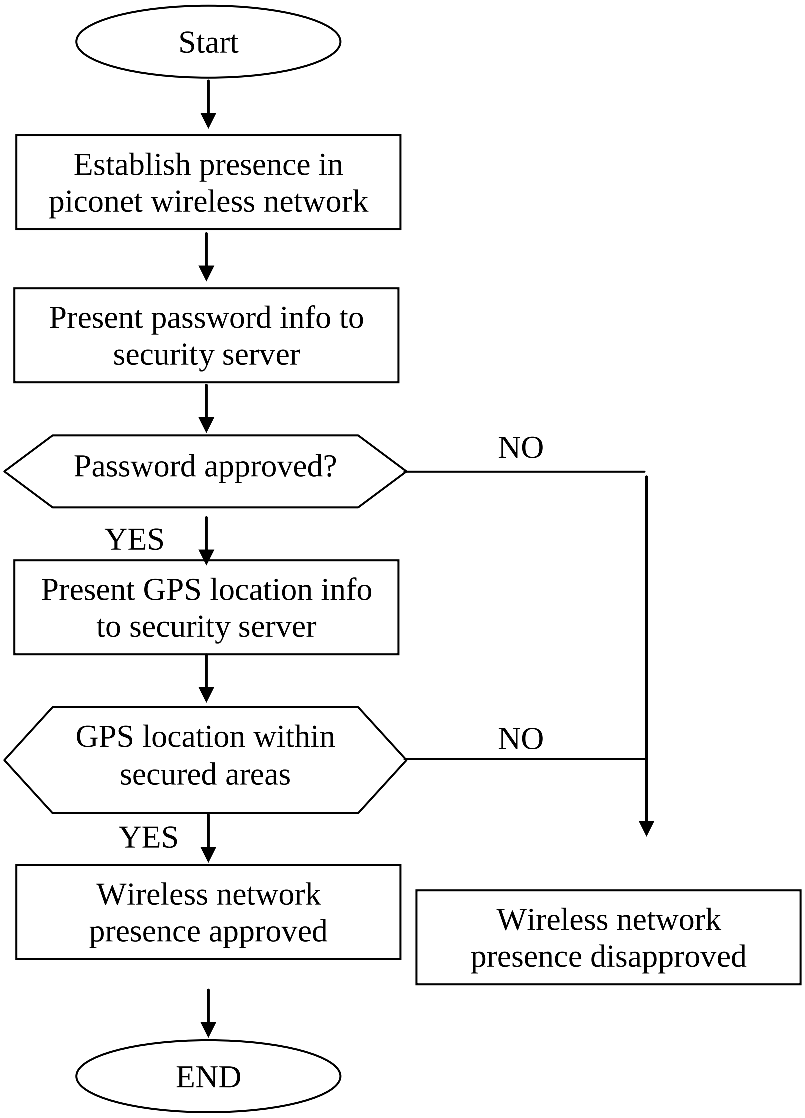

Start
Establish presence in piconet wireless network
Present password info to security server
Password approved?
NO
YES
Present GPS location info to security server
GPS location within secured areas
NO
YES
Wireless network presence approved
Wireless network presence disapproved
END

Figure 2.19 process flow of authorization of a piconet wireless network

In fact, this study did not take into account many questions such as:

It does not provide the type of the GPS signal that are going to be used. In addition, it did not study the quality of the civilian or military signal.

The civilian signal is not secure, as explained before. In addition, all areas of the building must be covered. This may requires the implementation of many GPS receivers in different places in the building.

2.8 Justification of the Proposed Research

The world still suffers from the penetration of the user's privacy, despite the availability of several protection techniques. These techniques rely on raising the level of encryption code and training the users to use the protection system efficiently in order to develop its performance. Unfortunately, the problem still exists in two specific objectives:

1. The degree of the strength of the encryption code depends on the skill of the developer. Note that in many cases, the level of the used encryption is not enough. In many cases, users do not have good skills, which lead to provide an opportunity for hackers to penetrate.

2. Training the users to use the system is not enough to make sure that the use of the system was properly. In another word, nothing to force the users technically to pursue what is required.

This study uses the geographic location address as a new authentication factor. This address achieved from the GPS system and has been encrypted using a very efficient technique that making it difficult to penetrate. Moreover, user has been enforced to follow the right steps, otherwise, the system will not work. The details will be explained in the following chapters.

2.9 Summary

This chapter clarified why it is essential to have authentication in order to reduce the likely hood of the theft user’s identity. The authentication factors were specified in details and showed the methods of using more than one factor at a time. Several authentication keys, were discussed and presented how they functioned, advantages and disadvantages associated with each key. Since the ability and audacity of hackers has been increase in recent years, the computer world also needs to enhance the level of user identity authentication. It is felt that the authentication strategies available so far are not sufficiently secure. The next part of the chapter highlighted inadequacies of other methods of authentication and the issues pertaining to concerns of data protection, especially with the emergence of the wireless network. This main factor is the user's physical location. The challenges encountered by professionals regarding data protection in using sensors, such as the overload of signals, misbehavior nodes, redundancy and the authentication of the signals. In addition, several studies that aimed to protect the data sending and receiving signals against hackers have been reviewed. It is felt, there are still concerns with regards to privacy of the end user.

The application of Global Position System (GPS) technology is considered in order to address the issue surrounding privacy of the user. Details of the facilities of the GPS signal have been presented in order to conclude that it would use in the authentication of the user’s identity.

In this regard, a new protocol is proposed using the services of GPS to verify and authenticate the identity of the user in the next chapter.

Chapter 3:

Kerberos and N-Kerberos Protocols

3.1 Introduction

Most organizations use online communication rather than more traditional forms. Online communication procedures are faster and relatively more cost effective compared to traditional physical communication. However, online systems provide opportunity for hackers and intruders to carry out malicious acts. With these challenges in mind, security specialists have adopted using of data encryption programs to protect and secure sent and received messages during the process of communications. For this purpose, many encryption codes, such as MD5 [109], DES [18, 25] or RSA [14, 67] have been devised. Unfortunately, despite the adoption of encryption of messages and strong encryption programs, users are still prone to persistent penetrations. This can be attributed to many reasons; in some instances, hackers are able to crack the encryption program. For example, although RSA is one of the most powerful encryption codes, certain security protocols that use RSA remain susceptible to attack [6, 7, 16, 68, 105].

Another reason is that users do not necessarily follow protection instructions [63]. So far, most people do not feel that online communication is a secure environment. In this regard, a different approach is adopted compared to the conventional method of software encryption where the user may not necessarily follow the precautions expected of them.

In this chapter, the meaning of the protocol and its key features are demonstrated. Kerberos protocol, which is the most popular protocols of key exchange, is presented. Details of its beginning and causes of its evolution are presented, then the problems associated with it are analysed. Furthermore, in order to enhance the features of Kerberos, GPS technologies are incorporated.

The remainder of this chapter is set out as follows: what is the protocol and details of how it works are clarified in section 3.2. Section 3.3 gives the details of Needham Schroder and Kerberos protocols, Needham Schroeder protocol are also analysed and its problem and limitations are presented. Then, Kerberos is considered to solve Needham’s problem. Needham problem will be clarified in section 3.3.1. Attack in Kerberos is described in section 3.4. A new form of Kerberos called N-Kerberos is introduced in Section 3.5. The summary is discussed in section 3.6.

3.2 What is The Protocol?

The protocol is a set of ordered messages to describe the communication between two participants. Participants can be clients or services. Establishing a secure communications through insecure open network is the main concern for any security communication protocol; the aim of such protocols is to ensure that the exchange route is secure and it can be used for key exchanging process. These protocols rely on two main points, which are:

1. Encryption code.
2. Using a nonce.

The first point is that the message has to be encrypted using an encryption key. This key must be shared between the two participants only. The sender must encrypt the message using the key which is agreed upon with the receiver before sending the message. Otherwise, the receiver will not recognize the message. Where the second point is a message must includes a nonce, such as a random number or time stamp. Nonce stands for number used once. It is a random number issued in an authentication protocol or time stamp to ensure that old communications cannot be used in the future [10].

Wide Mouth Frog protocol [1] is selected as an example to understand what is the protocol and how does it works. It contains two messages; the first one is from the client asking the server to communicate with the other participant as shown in figure 3.1.

$$\boxed{\begin{array}{l} 1: A \rightarrow S : A, \{N_a, K_{ab}, B\}_{K_{as}} \\ 2: S \rightarrow B : \{N_s, K_{ab}, A\}_{K_{sb}} \end{array}}$$

Figure 3.1: Wide Mouth Frog Protocol

Figure 3.2 shows the description of each character used in Wide Mouth protocol. S is the server, *A* and *B* are the participants or the machines, N_a, N_s are nonces. If the nonce is time stamp, the user will be sure that the message has been recently sent. *K* is a key generated by two participants. *A* and *B* need to communicate together using the K_{ab}

through the recommendation of server. *A* and *B* trust server *S*. *S* produces the key during the execution of the protocol. Communications between the server (*S*) and participants (*A* and *B*) will be by K_{as} and K_{bs} respectively; these keys have to be known by only both participants.

S	:	Server
A, B	:	Participants or Machines
N_m	:	Time nonce for m
K	:	Key
X	:	Message

Figure 3.2: Characters' meaning

The description of the protocol is as follows:

A reads the clock, obtaining the current time *N*, create his request and send it to the server with message 1.

Message1: $$A \rightarrow S : A, \{N_a, K_{ab}, B\}_{K_{as}}$$

A sends its chosen session key (K_{ab}) and the time stamp (N_a) to *S*, encrypted with its private authentication server key (K_{as}). Every message should have two conditions in order to be secure; encrypted and has a nonce verification [10]. The following list shows the analysis of the protocol.

- K_{as} is the shared key between *A* and *S*. Since S believes K_{as} as a key known only by *A* and *S*, and *A* sees message1 encrypted by key K_{as}, then *S* concludes that *A* actually sent message1. (In particular, S believes that the message was not generated by some attacker).
- Since the clocks synchronize, it is assumed that, *S* believes that the message is fresh or recently sent.

It is clear now that the two conditions are available in message 1. This would conclude that *S* believes that message 1 is coming from a legitimate participant (*A*). Message 2 is as follows:

Message 2: $$2 : S \rightarrow B : \{N_s, K_{ab}, A\}_{K_{bs}}$$

The two conditions are available in message two; it is encrypted by the shared key between S and B (K_{bs}) and it includes a nonce (N_s). Therefore, *B* would believes that the sender is *S* as explained in message 1. So far, B will start communicate with *A* using K_{ab} .

Unfortunately, there is a big problem in this protocol; the shared key is completely determined by A. This may give good chance for hacker to determine a key and hack the system. Moreover, A is not guaranteed that B exist, this may requires more functionality and capability from the server.

In the next section, Needham Schroeder protocol [10] will be presented and show why it is essential to enhance it.

3.3 Authentication Protocol

Needham Schroeder and Kerberos are very well known Security protocols which aim to establish secure channel for client to communicate. Needham-Schroeder (section 3.3.1) and Kerberos (section 3.3.2) protocols are introduced.

3.3.1 Needham Schroeder protocol

In 1978, Needham and Schroeder built a distributed authentication protocol [10, 91]. It is an exchange key between two participants through the recommendation of a third party. Needham and Schroeder protocol consists of five messages as shown in figure 3.3.

$$\boxed{\begin{array}{l}
1: A \to S : A, B, N_a \\
2: S \to A : \{N_a, B, K_{ab}, \{K_{ab}, A\}_{K_{bs}}\}_{K_{as}} \\
3: A \to B : \{K_{ab}, A\}_{K_{bs}} \\
4: B \to A : \{N_b\}_{K_{ab}} \\
5: A \to B : \{N_b - 1\}_{K_{ab}}
\end{array}}$$

Figure 3.3 Needham Schroeder protocol

Message 1 is the first participant (*A*) creates and send his request to the server (*S*). His request is a ticket to communicate with the second participant (*B*). When *S* receives *A*'s request, *S* will send message 2 including a session key (K_{ab}) and the ticket ($\{K_{ab}, A\}_{K_{bs}}$). This ticket is to be sent from *A* to *B* by Message 3. Then, A and B can start their conversation securely by message 4 and 5. Needham Schroeder protocol will now be analysed and some of its limitations are assessed critically.

As explained in section 3.2, the message must be encrypted and include a nonce in order to conclude that the message is secure. In Needham Schroeder protocol, Participants *A* and *S* predefined a shared key which is only known by *A* and *S*. In addition both clocks for *A* and *S* are synchronized. *A* reads the clock, obtaining the current time N_a, and sends message 1 to *S*. Then, *S* sends *A* the following message:

Message 2: $$S \to A : \{N_a, B, K_{ab}, \{K_{ab}, A\}_{K_{bs}}\}_{K_{as}}$$

Since K_{as} is only known by A and S, and A sees message 2 encrypted by K_{as}, then A concludes that S actually sent message 2. In addition, since the clocks are synchronized, we can assume that A believes that message 2 is fresh or recently sent.

According to the key conditions of the key exchange protocols, it can be assumed that the message 2 is secure. Then, A forwards the received ticket to B by message 3 as follows:

Message 3: $$A \rightarrow B : \{K_{ab}, A\}_{K_{bs}}$$

The aim of message 3 is that B needs to trust K_{ab} in order to be used to communicate with A securely. This message has been encrypted using K_{bs}. Since B believes K_{bs} as a key known only by B and S, and B sees message 3 encrypted by K_{bs}, then B concludes that S actually created this message. In addition, since B believes what the server believes, B would believe K_{ab}. But unfortunately, there is no time stamp in this message. Therefore, B is unable to confirm that message 3 is not replayed by another user. As mentioned before, two compulsory conditions have to exist in the message to be secure. Message3 is encrypted by private key, which achieves the first condition. However, the second condition cannot be achieved, because there is nothing to prove that the message is fresh such as a nonce or time stamp. The main limitation in this protocol is that message 3 is not protected by nonce. This will possibly give hackers opportunity to replay the message at any time. This protocol was very famous until 1987 and found a dormant bug which hung around which is message 3 does not have a nonce, undiscovered for a long time. This bug founded by Burrows, Abadi and Needham when they produced a measurement tool to check the strongest of the protocol, as will described in next chapter. Although, messages 4 and 5 used nuances and encryption key to ensure that they are both corresponded, these conversations are not secure because of the bug found in message 3. Improve Needham Schroder or create new key exchange protocol has been desirable. As a result, a new form of Needham Schroder called Kerberos protocol was developed. In the next section, Kerberos protocol is presented in details.

3.3.2 Kerberos Protocol

Kerberos is an authentication mechanism protocol designed for TCP/IP networks [8, 57, 84, 121]. It is a part of MIT's Project Athena following-on from the Needham Schroeder protocol. The environment of Kerberos contains many anonymous workstations and servers. All operations such as file storage, mailboxes, print and some others are implemented in the server, whereas workstations are mostly used for interactions and computing process. As workstations need to access servers to complete the processes, they are required to be authenticated. Kerberos is designed to authenticate the end-user to the server. To understand how Kerberos works, it will be divided into four different steps:

A. Authentication Exchange:

- The client requests a ticket from authentication server (*AS*) to the ticket-granting server (*TGS*) as shown in figure 3.4 (*KRB_AS_REQ*).
- AS then checks up the availability of client in its database and generates a session key (*SK1*) to use between the client and the *TGS* ($SK1_{C\text{-}TGS}$).
- Kerberos encrypts the *SK1* using the client's secret key. The *AS* also uses the *TGS*'s secret key ($K_{AS\text{-}TGS}$) to create and send the user a ticket-granting ticket (*TGT*). It is shown as (*KRB_AS_REP*) in figure 3.4.

B. Ticket-Granting Service Exchange:

- The client decrypts the message and recovers the session key, then uses it to create an authenticator containing his name and a time stamp.
- The client then sends this authenticator, along with the *TGT*, to the *TGS*, requesting access to the target server (*KRB_TGS_REQ*).
- The *TGS* decrypts the *TGT*, and then uses the *SK1* inside the *TGT* to decrypt the authenticator. It verifies information in the authenticator; the ticket and the time stamp. If all of these matchs then it allows the request to proceed.
- Then the *TGS* creates a new session key (*SK2*) for the client and application server (*AP*) to use, then encrypts it using *SK1* and sends it to the client.
- The *TGS* also sends a new ticket containing the client's name, a time stamp and an expiration time for the ticket (*KRB_TGS_REP*), all encrypted with the *AP*'s secret key ($K_{TGS\text{-}AP}$).

C. Client/server exchange:

- The client decrypts the message and gets the *SK2*.
- Finally ready to approach the *AP*, the client creates a new authenticator encrypted with *SK2*.
- The client sends the session ticket (already encrypted with the *AP*'s secret key) and the encrypted authenticator. Since the authenticator contains plain text encrypted with *SK2*, this proves how the client knows the key (*KRB_AP_REQ*).
- The *AP* decrypts and checks the ticket, the authenticator and the time stamp.
- For applications that require two-way authentication, the *AP* returns a message consisting of the time stamp plus 1, encrypted with *SK2*. This proves to the client that the server actually knew its own secret key and thus could decrypt the ticket and the authenticator.

D. Secure communications:

- The target server knows that the client is actually who he claims to be, and the two now share an encryption key for secure communications. Because only the client and AP share this key, they can assume that a recent message encrypted in that key originated from the other party.

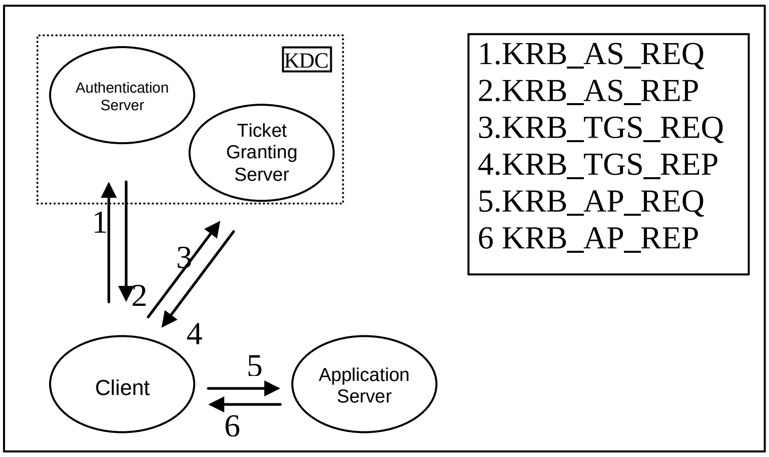


Figure 3.4 Kerberos authentication messages.

Figure 3.5 shows the contents of Kerberos messages. We refer to *AS* and *TGS* as Key Distribution Center (*KDC*). Message 1 is sent from client *A* to *KDC* (given the symbol *S*) requesting a ticket to use a service from *AP* (given the symbol *B*). Then, *S* sends *A* the following message:

$$\text{Message 2:} \quad \{N_a \ , \ B \ , \ K_{ab}, \ \{N_s \ , \ K_{ab}, A\}_{K_{bs}}\}_{K_{as}}$$

Message 2 includes the ticket ($\{N_s, K_{ab}, A\}k_{bs}$). The difference between this message and message2 in Needham Schroeder protocol is adding N_s. This will assist *B* to verify the freshness of message3. The purpose of N_s is to overcome the weakness of Needham Schroeder protocol. Detailed analysis of Kerberos is available in [8, 57, 84, 121].

$$
\begin{aligned}
&1: A \rightarrow S : A, B \\
&2: S \rightarrow A : \left\{N_a, B, K_{ab}, \{N_s, K_{ab}, A\}_{K_{bs}}\right\}_{K_{as}} \\
&3: A \rightarrow B : \{N_s, A, K_{ab}\}_{K_{bs}}, \{N_a, A\}_{K_{ab}} \\
&4: B \rightarrow A : \{N_b + 1\}_{K_{ab}}
\end{aligned}
$$

Figure 3.5 Kerberos protocol

The analysis below is a comparison of Kerberos protocol with Needham Schroder protocol:

Message 1 sent as a plain text. It does not need to have either nonce or encryption key; it is out of the attacker target range because it does not have the key. The other messages includes the key, therefore, it has to be secured. The analysis of message 2 in Kerberos is exactly as it was in message 2 of Needham Schroder; both messages have been encrypted by a shared key and each of them have a nonce. It will not be repeated again. It has to be said that the difference is in the ticket included in both messages; Ticket in Needham Schroder protocol does not have a nonce $\{K_{ab}, A\}_{K_{bs}}$, where the ticket in Kerberos includes the nonce $\{N_s, K_{ab}, A\}_{K_{bs}}$. Next is the analysing of message 3:

Message **3:** $\{N_s \ , \ A \ , \ K_{ab}\}_{K_{bs}} \ , \ \{N_a \ , \ A\}_{K_{ab}}$

As mentioned before, message 3 has the ticket ($\{N_s \ , \ A \ , \ K_{ab}\}_{K_{bs}}$) and the authenticator ($\{N_a \ , \ A\}_{K_{ab}}$).

Since *B* believes K_{bs} as a key known only by *B* and *S*, and *B* sees the ticket encrypted by K_{bs}, then *B* concludes that *S*, is the right ticket. In addition, since the clocks are synchronized, it can be assumed that *B* believes that the ticket is fresh or recently sent. Since *B* trust what *S* believes, *B* would trust K_{ab} which is in the message, and then *B* would decrypt the authenticator using key K_{ab}. Finally, both participants *A* and *B* can start their secure conversation through message 4.

A number of weaknesses have been found in Kerberos's messages by Bellovin *et al* [4]. This shows that Kerberos needs further investigation. In the next section, the limitations and weaknesses of Kerberos are presented.

3.4 Problem Definition (Attack on Kerberos)

Although Kerberos protocol is a sufficient mechanism, the possibilities of attacks still exist. Davis and Swick [21] illustrated some of Kerberos's deficiencies. [21] explored the vulnerability of the Kerberos protocol from the replay attacks. In this section, a replay attack problem is demonstrated and how it could affect Kerberos protocol.

A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. Kerberos has many mechanisms that aims to make replay attacks difficult. These are listed as follows:

1. The first mechanism is that authenticators rely on machines' clocks being roughly synchronized. In more details, the message must include a time stamp in order to prove that it is fresh or has been recently used. Given the following reasons, it is reasonable to challenge these points:
   - **a.** In some cases, time varies depending on different factors such as, the type of service, size of the network and the amount of demand for the

service. These factors make it difficult to accurately define. Therefore, a synchronization protocols may be unauthenticated [85, 103].

b. In addition, when a server is misled about the correct time, attackers can easily replay the authenticator.

c. Moreover, the attacker might be able to mount the attack within the configured time.

d. Furthermore, if the time is configured to be too short, the client will face problems in time synchronization.

2. Using a cache memory to store used authenticators is another mechanism to guard against re-use. This cache should ok all authenticators used within the allowable time skew. If the server uses a cache for the used authenticators, a passive attack becomes impossible. A server will reject all authenticators it has already seen [101]. Authenticator caching makes replay attacks slightly more difficult, but it is not a sufficient protective mechanism. This is because of the following reasons:

a. Keys have to be saved in particular storage area. Kerberos modification was made to store keys in the memory. However, this area could be attacked.

b. On the other hand, performing cache mechanisms is not considered a suitable for some other systems. For example, it is very difficult for TCP-based servers to store authenticators in UNIX system [102].

c. Moreover, it is easy to store the authenticator in UDP-based servers. However, the problem lies when a client re-transmit a request in the case that the server's response was lost [88].

3. The third Kerberos mechanism to stop replay attack is that, the ticket inside *KRB_AP_REQ* should include the network address of the client. It should verify that the source address of the message matches the address in the ticket. Again, there is a problem in this mechanism; it is noted that the network address is under full control of the attacker [69].

During this research, other possible reasons that may cause replay attacks are considered; these are as follows:

1. The administrators, in some cases, do not follow the required instructions to implement Kerberos in a designated manner. This is because of:
   a. Sense of irresponsibility, and lack of knowledge of the consequences of events that may occur because of the weaknesses in the definition of the system.
   b. Some users consider themselves beyond the range of the hackers.

2. The effectiveness of Kerberos relies on the server configurations and implementations. In other words, it relies on the performance of the user. In a situation where the user used a weak password, the system is likely going to be easily attacked [4].
3. The relatively large size of the verifications that are used in Kerberos protocol should be noted. The proliferation of these definitions and complexity increase the likelihood of errors [4].

Many protocols in Microsoft Windows domain use Kerberos v5 as the primary authentication mechanism. SMB (Server Message Block) and LDAPv3 (Lightweight Directory Access Protocol) are examples of such protocols. SMB and LDAPv3 protocols may be attacked by replay attack, password attack against TGT or pre-authentication data, and attack against message delivery time. Through a replay attack, the attacker will be able to access the shared files and modify directory entries with the victim's credentials. A Replay Attack on Kerberos v5 exploits the final message, *KRB_AP_REQ*. If an attacker is able to access the network traffic from the victim, he will be able to extract the *KRB_AP_REQ* sent by the victim, and then simply attempts to re-use this message to authenticate himself to a server. In some cases, the server will accept the replayed message sent by the attacker allowing him full access to the service with the victim's profile [60].

There is no suggestion that Kerberos is ineffective. But, it needs to follow up the performance of the users. One of the aims of this thesis is to protect the user, even in the likely event of failing to implement Kerberos protocol. To achieve this, a new form of Kerberos is proposed that will be called N-Kerberos. It works by adding client's physical position address. This Address can be determined by a Global-Position-System (GPS) receiver. Table 3.1 shows a summary of the Susceptibilities that may cause exposure Kerberos protocol to the problem of replay attack.

Table 3.1 Kerberos protocol against replay attacks

Techniques to prevent a replay attacks	Problems possibilities
Time stamp	1. Difficult to accurately define due to the instability of the required time for the implementation of the various services. 2. Server may be misled about the correct time. 3. Attacks can be carried out within the configured time. 4. In case of short time, legitimate client will face problems.
Cache memory	1. Cache memory could be attacked. 2. It is not suitable for other systems.
Network address	1. Network address is under full control of the attacker
Pre definitions	1. Administrators do not follow the required instructions. 2. The definitions are proliferation and complexity.

3.5 New Form of Kerberos (N-Kerberos)

Although Kerberos is one of the most secure protection key exchange mechanisms, it is considered not robust enough. The main concern is to eliminate the possibility of replay attacks. We propose a modification on Kerberos that will be called N-Kerberos. It works by adding client’s physical position address. This Address can be determined by a Global-Position-System (GPS) receiver, as described in chapter 2. The great development that has been achieved on the GPS over the past few years gave an indication of a potential for integration with different techniques to raise the level of data protection. It is proposed that Kerberos should include the physical address of the user in all messages given out, in addition to the previous two conditions; encrypting the messages using a strong password and having a time stamp. This thesis also requires the server to have a database of a list of legitimate and authorised users' positions addresses. Having these addresses will enable the server to test out the availability of a user's position address before allowing the users to utilize the services. These variables have been studies in three different phases:

Phase1: in this phase, the task of confirming the authenticity of the location falls within the responsibility of the server. Figure 3.6 shows the messages of phase1 of N-Kerberos protocol.

In the first message, user *A* sends a request from server S to obtain the key, which can be used to communicate with the user *B*. Then, the server sends his response to the user *A*. This response contains a special ticket ($\{N_s, GPS_a, K_{ab}, A\}_{K_{bs}}$) to be sent by *A* to *B* through message 3. Note that it will be preceded by the implementation of several Kerberos tasks.

$$\begin{array}{l} 1.A \rightarrow S : A, N_a, B \\ 2.S \rightarrow A : \left\{N_s, GPS_{b,} B, K_{ab}, \{N_s, GPS_a, K_{ab}, A\}_{K_{bs}}\right\}_{K_{as}} \\ 3.A \rightarrow B : \{N_s, GPS_a, K_{ab}, A\}_{K_{bs}}, \{A, GPS_a, N_a\}_{K_{ab}} \\ 4.B \rightarrow A : \{GPS_b, N_a + 1\}_{K_{ab}} \end{array}$$

Figure 3.6 Phase 1 of N-Kerberos

New tasks were added for the use of the GPS, which are as follows:

1. The server uses the list of legitimate users' physical location addresses to add *A*'s physical address to the ticket ($\{N_s, GPS_a, K_{ab}, A\}_{K_{bs}}$)
2. The physical location address of *B* must be added to the message ($N_s, GPS_{b,} B, K_{ab}$).

Message 3 has both a ticket and authenticator. The ticket ($\{N_s, GPS_a, K_{ab}, A\}_{K_{bs}}$) is encrypted by K_{bs} and the session key K_{ab} encrypts the authenticator ($\{A, GPS_a, N_a\}_{K_{ab}}$). The following are modifications to the previous Kerberos protocol:

1. *A* adds his physical location address derived from the GPS receiver to a part of the authenticator.
2. *B* will not believe the message unless the GPS_b located in part of the ticket, sent by server, matches the GPS_b located in part of the authenticator, sent by *A*.

In order for *A* to believe *B*, both the second message and the fourth message will be used to validate *B*'s physical location. To accomplish this, the second message will serve as the ticket, and the fourth message will serve as the authenticator. The GPS_b located in the fourth message, derived from the GPS receiver of *B*, must match the GPS_b located in the second message, sent by the server.

This method is preferred to compel the users to use their pre-defined physical location addresses, stored in the server, in order to acquire the private key which can be used to communicate with each other.

Unfortunately, a problem was identified during the examination of this phase. The problem is in the second message; it does not contain the physical address of user *A*, where there is no evidence that the recipient of the message 2 is the user *A*. Consequently, the hacker can compromise both the second and fourth messages and perform the required comparison of the (GPS_b) in message 2 with the (GPS_b)in message 4 without having to confirm his physical location. This means that the addition of the GPS feature in the second message did not add to the security of the message. To overcome this, phase 2 is proposed and are as follows.

Phase 2: In this phase, the responsibility of confirming the authenticity of the location falls to the user instead of the server, as it was in phase 1. Figure 3.7 shows phase 2 of N-Kerberos protocol. The method used in this phase is significantly different from the previous model. These differences are shown as follows:

1. The second message contains the physical address of user *A* (GPS$_a$) instead of the physical address of the user *B* (GPS$_b$). User *A* has to prove to server that he is using the legitimate position. This can be achieved by comparing the physical address in the message, sent by the server ($N_s, GPS_{a,} B, K_{ab}$), with that acquired from the GPS receiver, which is installed in *A*'s location. Thus, *A* will not be able to obtain the key K_{ab} in the absence of matching addresses.

$$
\boxed{
\begin{array}{l}
1. A \rightarrow S : A, N_a, B \\
2. S \rightarrow A : \left\{ N_s, GPS_{a,} B, K_{ab}, \{N_s, GPS_b, K_{ab}, A\}_{K_{bs}} \right\}_{K_{as}} \\
3. A \rightarrow B : \{N_s, GPS_b, K_{ab}, A\}_{K_{bs}}, \{A, N_a\}_{K_{ab}} \\
4. B \rightarrow A : \{N_a + 1\}_{K_{ab}}
\end{array}
}
$$

Figure 3.7 Phase 2 of N-Kerberos

2. The ticket included in the second message ($\{N_s, GPS_b, K_{ab}, A\}_{K_{bs}}$), sent from the server, contains the physical address of user B (GPS$_b$) instead of the physical address of user *A* (GPS$_a$). *B* has to prove that he is using his legitimate position. This can be achieved by comparing the physical address in the ticket, sent by server ($\{N_s, GPS_b, K_{ab}, A\}_{K_{bs}}$), with that received from his own GPS receiver which is installed in his location. Again, *B* will not be able to get the key K_{ab} in the absence of matching addresses.

3. There is no need to add the GPS$_a$ in both the authenticator and message parts of message 3, and no need to include GPS$_b$ in message four, as in this phase, there is no longer a need to compare the GPS$_a$'s in message three, and the GPS$_b$'s in messages 2 and 4.

Subsequently, the key can be used from any other place. Clearly, this causes a limitation, however this modification provides more protection against replay attacks. Unfortunately, another problem was found in this phase; there is nothing compelling the user to make a comparison between the two physical addresses. In other words, there is nothing preventing a hacker from stopping the comparison process, or to make it appear as if the comparison result is positive. As a result, Phase 3 was introduced to require users to make the comparison.

Phase 3: Note that the P(Y) code needs special hardware, available only to the U.S. government, to be decrypted, and it is designed to resist electronic attacks. Users can capture their P(Y) code and store it to verify their physical address signature to the server. Figure 3.8 show phase 3 of N-Kerberos protocol.

The signature P(Y) code has been used to encrypt the key *K*$_{ab}$. This will enforce the user to decrypt the signature using his P(Y). User B has to do the same to read the key from the ticket when received through message 3. The modifications to phase 3 are as follows:

$$
\begin{aligned}
&1.A \rightarrow S : A, N_a, B \\
&2.S \rightarrow A : \left\{N_s, \{K_{ab}\}_{sig_a}, B, \left\{N_s, \{K_{ab}\}_{Sig_b}, A\right\}_{K_{bs}}\right\}_{K_{as}} \\
&3.A \rightarrow B : \left\{N_s, \{K_{ab}\}_{Sig_b}, A\right\}_{K_{bs}}, \{A, N_a\}_{K_{ab}} \\
&4.B \rightarrow A : \{N_a + 1\}_{K_{ab}}
\end{aligned}
$$

Figure 3.8 Phase 3 of N-Kerberos

1. The server needs to capture the P(Y) of all users.
2. The server needs to encrypt the Key (K_{ab}) using the value of the P(Y) code of *A*.
3. User *A* needs to decrypt the message by the key K_{as}, and decrypt the key k_{ab} using the value of his P(Y) code.
4. The ticket, which is sent through message 3 has *B*'s signature. *B* needs to decrypt the ticket using K_{bs} , and then to uses the value of his P(Y) code to decrypt the K_{ab}.

Using this technique, the users are required to use their physical location addresses signature in order to read the key. The attacker will be constrained to use a maximum amount of time trying to decrypt Sig_a, which will cause problem with time synchronization. Therefore, N-Kerberos will eliminate the possibility of the replay attacks.

3.6 Summary

In this chapter, the method of using the key exchange protocols was presented. The aim of these protocols is providing a secure channel for key exchange between different parties. The well known key exchange protocols such as Needham Schroder and Kerberos protocols were selected. Needham Schroeder protocol has been used for a long time until a bug was found. Kerberos protocol was produced following on Needham Schroeder protocol. Kerberos protocol was also shown to overcome the problem of Needham Schroeder protocol. However, it was shown that there is a possibility to attack Kerberos. It is considered that Kerberos protocol needs more investigations and research to decrease the possibility of replay attack against it. For this reason, several phases were analysed. As a result, a new form of Kerberos protocol that is called N-Kerberos is derived. Every single physical location has a secret and well encrypted signature called P(Y) code that can be captured using the receiver of the Global Position System (GPS). This signature is used as a new factor, in determining enhanced authentication level of the user's identity. This new technique will significantly reduce the ability of the hackers, the likelihood of replay attacks. To verify this technique, in the next chapter, a new verification tool is presented in order to analyse N-Kerberos protocol.

Chapter 4:

BAN Logic and its Modification

4.1 Introduction

There are many security protocols available and users may not necessarily be aware of the efficiency of their security protocol. For this reason, there may be evidence of vulnerability of a hack without any evident reason. For example, Needham Protocol had been reliable and effective over a long period without alerting its deficiencies. Therefore, it is essential to evaluate security protocols before adopting it. This may give users more confidence to use these protocols. Burrows, Abadi and Needham produced a formal logic called BAN logic in 1989 to evaluate security protocols [10], which offers a formal testing structure for security protocol. Upon being subjected to BAN logic, many flaws have been found in different protocols such as Needham-Schroeder and CCITT X.509 [34]. Many recent protocols have been subjected to BAN [12, 29, 140].

In this chapter, a clear content of BAN logic is going to be given and also Needham protocol subjected to BAN logic. In addition, the need for modification of BAN will be proposed and there after a new form of BAN logic will be introduced. Furthermore N-Kerberos introduced previously will be subjected to the modified and enhanced BAN logic.

The reminder of this chapter is set out as follows: Description of BAN logic has been shown in section 4.2. Both Needham Schroeder and Kerberos will be subjected to BAN logic in section 4.3. The main outcome of this chapter is producing N-BAN logic which is followed on from BAN logic, will be described in section 4.4. N-Kerberos protocol is tested by N-BAN logic in section 4.5. Summary of the chapter is produced in the last section.

4.2 Description of BAN Logic

Analysing a protocol is a hard mental process as shown during the analyzing of Wide Mouth protocol in section 3.2. Therefore, developing a mechanism to analyse a protocol is valuable. Thus, a formal logic model called BAN Logic was developed by M. Burrows, M. Abadi and R. Needham[32]. BAN Logic helps the user to verify what is reasonable to be believed. It is a group of rules used to analyse data exchange protocol. It provides a formal method to determine whether transfer or exchange of information is safe and secure against any eavesdropper. BAN consists of three main steps to analyse any protocol [6] as described below:

1. **The first step** is to explore the initial assumptions from the protocol statements, and translate them to symbolic notations. For this purpose, BAN uses different logical constructs. Figure 4.1 shows some of these constructs.

2. **The second step** is to verify the goal. That is, verifying a secured communication channel between participants.
3. **The third step** is a group of rules and postulates that are performed to acquire the goal.

Assumptions derived from messages of protocol are subjected to BAN rules to obtain new assumptions until the goals are achieved. For example, if *A* believes that only *A* itself and *B* know key *K*, and participant *A* receives a message encrypted by key *K*, *A* may assume that the message is originated from participant *B*. Here a new result can be further used as a new assumption is achieved from previous assumptions.

$A \mid\equiv S$: A believes S (i.e. may act as if S is true)

$A \triangleleft X$: A has received a message X.

$A \sim X$: A once said X, A sent a message X.

$S \Rightarrow A$: S has jurisdiction over A (S has authority on A)

$\#(X)$: X is fresh

$A \xleftrightarrow{K} B$: K is a shared key between A and B

$\{X\}_k$: Message X is encrypted by the key K

Figure 4.1: BAN logical constructs

Constructs are used to build series of logical postulates that consist of two parts; the numerator part is the condition and the denominator part is the result. BAN logic has many rules used to analyse the protocol's messages. There are four main postulates and are illustrated bellow:

Postulate 1:

$$\frac{A \mid\equiv B \xleftrightarrow{K} A\ ,\ \ A \triangleleft X_K}{A \mid\equiv B \sim X}$$

This is called **message-meaning rule**. It means that if *A* treats *K* as a shared key which is only known by *A* and *B*, and *A* receives *X* encrypted by this key, then *A* would be certain that this message has been sent by *B*.

Postulate 2:

$$\frac{A \mid\equiv \#(X)}{A \mid\equiv \#(X,Y)}$$

This is known as **Part of the message rule**. This formula proves that if *A* believes that any part of the message was recently sent then *A* would believe that all parts of the message are recently sent. It avoids being confused by replays; if an intruder in the middle attempt to intercept the message and replay it again, the life time of the message will be longer than what it is suppose to be, then the receiver will decline this message.

Postulate 3:

$$\frac{A \mid\equiv \#(X)\ ,\ \ A \mid\equiv B \sim X}{A \mid\equiv B \mid\equiv X}$$

This is called **nonce-verification rule**. This verification postulate proves that *A* believes what *B* believes; if *A* believes that *X* was recently sent and believes that *B* is the sender of *X*, then *A* would believe that *B* believes *X*. The numerator part is the result of postulate one and postulate 2.

Postulate 4:

$$\frac{A \mid\equiv B \mid\equiv (X,Y)\ ,\ \ A \mid\equiv B \Rightarrow (X)}{A \mid\equiv X}$$

This postulate is called **jurisdiction rule**. It means that if *A* believes that *B* believes the message (*X*,*Y*), and *A* also believes that *B* has a jurisdiction over any part of the message *X*, then A is willing to believe *X*. In this rule, the first part of the numerator is the result of postulate 3. We can see that the postulates are a continuum series; postulate 3 depends on postulates 1 and 2 and postulate 4 rely on postulate 3. In other word, the analyser has to subject the message into postulate 1 and 2 before subjecting it into postulate 3, and so on postulate 3 before postulate 4.

BAN has many steps to go through in order to achieve that *A* believes *B*. These are called steps upgrades and shown bellow:

Upgrade 1: it is to upgrade from *A* sees *X* to *A* believes that *B* said *X*. Postulate1 mentioned above would perform this [10].

Upgrade 2: it is from *A* believes that *B* said *X* to *A* believes that *B* believes *X*. To reach this, we need to concatenate postulate2 with performing upgrade1 which called postulate3 mentioned above [10].

Upgrade 3: this upgrade is the final step; it is to upgrade from *A* believes that *B* believes *X* to *A* believe *X*. This means that *A* and *B* has a secure channel to communicate. To achieve this, postulate 4 mentioned above has to be performed.

As a case study, Wide Mouth Frog protocol is analysed by BAN logic:

The first step is exploring the initial assumptions from the protocol statements. Table 4.1 shows the derived assumptions and how it came up.

Table 4.1: Derived assumption from Wide Mouth protocol

Assumption	Meaning
Assumptions derived from message 1	
$S \mid\equiv \#(N_a)$	The live time of the message has been modified in the server before starting the communication.
$S \mid\equiv A \overset{K_{as}}{\longleftrightarrow} S$	The key has been created and modified for *A* and *S* before starting their communication and only known by *A* and *S*. Therefore, both of them believe K_{as}
$A \mid\equiv A \overset{K_{as}}{\longleftrightarrow} S$	
$A \mid\equiv S \Rightarrow K_{ab}$	*A* knows that key K_{ab} is in the keys list available in the server. Therefore, server has a control over K_{ab}.
$S \mid\equiv A \Rightarrow K_{ab}$	
Assumptions derived from message 2	
$B \mid\equiv \#(N_s)$	The live time of the message has been modified in all parts before starting the communication.
$S \mid\equiv B \overset{K_{bs}}{\longleftrightarrow} S$	The key has been created and modified for *B* and *S* before starting their communication and only known by *B* and *S*. therefore, both of them believe K_{bs}
$B \mid\equiv B \overset{K_{bs}}{\longleftrightarrow} S$	
$B \mid\equiv S \Rightarrow K_{ab}$	*B* knows that key K_{ab} is in the keys list available in the server. Therefore, server has a control over K_{ab}.

The second step is verifying the goal, which is what *B* needs to be sure that the received message is originating from *A* and vice versa. The last step is subjecting the assumptions into BAN logic rules and these are as follows:

Upgrade 1: upgrade from *S* sees message 1 to *A* believes that *B* sent message 1.

$$\frac{S \mid\equiv A \xleftrightarrow{K_{as}} S \ , \ S \lhd \{N_a, K_{ab}, B\}_{K_{as}}}{S \mid\equiv A \sim \{N_a, K_{ab}, B\}_{K_{as}}}$$

Postulate 1 …4.1

Since *S* believes K_{as} as a key known only by *A* and *S*, assumption, and *A* sees message1 encrypted by key K_{as}, then *S* concludes that *A* actually said message1.

Upgrade 2: upgrade from *S* believes that *A* said message 1 to *S* believes that *A* believes message 1. This will be achieved by performing postulate 2 and postulate 3.

$$\frac{S \mid\equiv \#(N_a)}{S \mid\equiv \#\{N_a, K_{ab}, B\}_{K_{as}}}$$

Postulate 2 …4.2

Since the clock is synchronized and *S* believes that part of the message 1 is fresh, it is assumed that, *S* believes that the message 1 is fresh or recently sent. (In particular, *S* believes that, message was not replayed by some attacker intercepted prior).

$$\frac{S \mid\equiv A \sim \{N_a, K_{ab}, B\}_{K_{as}} \ , \ S \mid\equiv \#\{N_a, K_{ab}, B\}_{K_{as}}}{S \mid\equiv A \mid\equiv \{N_a, K_{ab}, B\}_{K_{as}}}$$

Postulate 3 …4.3

Since *S* believes that message 1 is fresh and *S* believes that *A* said message 1, then *S* believes that *A* actually believes key message 1; *A* is the sender of message 1.

Upgrade 3: upgrade from *S* believes that *A* believes message 1 to *S* believe the key K_{ab} in message 1.

$$\frac{S \mid\equiv A \mid\equiv \{N_a, K_{ab}, B\}_{K_{as}} \;\;,\;\; S \mid\equiv A \Rightarrow K_{ab}}{S \mid\equiv K_{ab}} \qquad \text{Postulate 4 …4.4}$$

Since *S* believes that *A* believes message 1 and *S* also believes that *A* has a control over K_{ab}, then S would believes K_{ab}. In other word, because *S* believes that *A* is the sender of the message 1, which includes key K_{ab} and S knows that *A* is the only one who knows this key, then S would believes the message. Then S will send the key K_{ab} to *B* by message two. The rules for analyzing message 2 are presented bellow:

$$\frac{B \mid\equiv B \xleftrightarrow{K_{bs}} S \;\;,\;\; B \lhd \{N_s, K_{ab}, A\}_{K_{bs}}}{S \mid\equiv A \sim \{N_s, K_{ab}, A\}_{K_{bs}}} \qquad \text{Postulate 1 …4.5}$$

$$\frac{B \mid\equiv \#(N_s)}{B \mid\equiv \#\{N_s, K_{ab}, A\}_{K_{bs}}} \qquad \text{Postulate 2 … 4.6}$$

$$\frac{(4.5) \;,\; (4.6)}{B \mid\equiv S \mid\equiv \{N_s, K_{ab}, A\}_{K_{bs}}} \qquad \text{Postulate 3 … 4.7}$$

$$\frac{(4.7) \;,\; B \mid\equiv S \Rightarrow K_{ab}}{B \mid\equiv K_{ab}} \qquad \text{Postulate 3 … 4.8}$$

Finally, *A* and *B* believes each other and they can start to communicate with each other. In the next section. The deficiencies of Needham Schroeder protocol when subjected to BAN logic will be identified, and see how it is solved by Kerberos protocol.

4.3 Needham Schroeder and Kerberos subjected to BAN Logic

The limitations of Needham Schroeder Protocol that was described in the previous chapter when subjected to BAN logic are presented below:

First: Derived the assumptions from the protocol's messages. Figure 4.2 shows Needham Schroeder protocol. And Table 4.2 shows the assumptions derived from Needham protocol.

$$
\begin{aligned}
&1: A \rightarrow S : A, B, N_a \\
&2: S \rightarrow A : \left\{N_a, B, K_{ab}, \{K_{ab}, A\}_{K_{bs}}\right\}_{K_{as}} \\
&3: A \rightarrow B : \{K_{ab}, A\}_{K_{bs}} \\
&4: B \rightarrow A : \{N_b\}_{K_{ab}} \\
&5: A \rightarrow B : \{N_b - 1\}_{K_{ab}}
\end{aligned}
$$

Figure 4.2 Needham Schroeder protocol

Table 4.2 Derived assumptions from Needham Schroeder protocol

Assumptions derived from Needham Schroeder protocol
$S \mid\equiv A \xleftrightarrow{K_{as}} S$
$A \mid\equiv A \xleftrightarrow{K_{as}} S$
$S \mid\equiv \#(N_a)$
$A \mid\equiv \#(N_s)$
$A \mid\equiv S \Rightarrow K_{ab}$
$B \mid\equiv S \Rightarrow K_{ab}$
$B \mid\equiv B \xleftrightarrow{K_{bs}} S$
$S \mid\equiv B \xleftrightarrow{K_{bS}} S$
$A \mid\equiv \#(N_b)$

Second: Analysing the protocol. We will start analyzing message 2. The goal of this message is that participant *A* needs to be sure that *K_{ab}* is originated by *S*; the analysis is as follows:

- **According to postulate 1:**

$$\frac{A \mid\equiv A \xleftrightarrow{K_{as}} S \ , A \triangleleft \left\{N_s, B, K_{ab}, \{K_{ab}, A\}_{k_{bs}}\right\}_{K_{as}}}{A \mid\equiv S \sim \left\{N_s, B, K_{ab}, \{K_{ab}, A\}_{k_{bs}}\right\}_{K_{as}}} \tag{4.9}$$

- **According to postulate 2**:

$$\frac{A \mid\equiv \ \#(N_s)}{A \mid\equiv \ \#\left\{N_s, B, K_{ab}, \{K_{ab}, A\}_{k_{bs}}\right\}_{K_{as}}} \tag{4.10}$$

- **According to postulate 3:**

$$\frac{(4.9) \ , \ (4.10)}{A \mid\equiv \ S \mid\equiv \ \left\{N_s, B, K_{ab}, \{K_{ab}, A\}_{k_{bs}}\right\}_{K_{as}}} \tag{4.11}$$

- **According to postulate 4:**

$$\frac{(4.11) \ , \ A \mid\equiv \ S \Rightarrow \ K_{ab}}{A \mid\equiv \ K_{ab}} \tag{4.12}$$

We conclude that message 2 is secure and so far participant *A* believes *K_{ab}*. In message 3, the main goal is participant *B* needs to trust *K_{ab}*. The analysis of message 3 is as follows:

- **According to postulate1**

$$\frac{B \mid\equiv B \xleftrightarrow{K_{bs}} S \;\; , B \triangleleft \{K_{ab}, A\}_{k_{bs}}}{B \mid\equiv B \sim \{K_{ab}, A\}_{k_{bs}}} \tag{4.13}$$

- **According to postulate2**, there is no time stamp in this message. So far, postulate 2 cannot be performed and so on postulate 3. We conclude that *B* can not be sure that message 3 has been sent by *S*.

This is how BAN logic discovers the problem of Needham Schroeder protocol. Kerberos protocol solved this problem by adding a nonce to the ticket in both the main build of message 3 and the authenticator part of the message, as discussed in the previous chapter. Messages 1 and 2 in Kerberos protocol will not be scrutinized due to its similarity to the analysing of messages 1 and 2 in Needham Schroeder protocol. Next is analyzing message 3 of Kerberos protocol, which contains the correction of Needham protocol problem.

Message 3: $$3 : A \rightarrow B : \{N_s, A, K_{ab}\}_{K_{bs}} , \; \{N_a, A\}_{K_{ab}}$$

If *B* concludes that the message ($\{N_s, A, K_{ab}\}_{K_{bs}}$) is secure, *B* would be able to read the key $\mathrm{K_{ab}}$ and use it in order to open the authenticator.

- **According to postulate1:**

$$\frac{B|\equiv B \xleftrightarrow{K_{bs}} S \ , B \triangleleft \{N_s, A, K_{ab}\}_{K_{bs}}}{B|\equiv S \sim \{N_s, A, K_{ab}\}_{K_{bs}}} \tag{4.14}$$

- **According to postulate2**:

$$\frac{B|\equiv \#(N_s)}{B|\equiv \#\{N_s, A, K_{ab}\}_{K_{bs}}} \tag{4.15}$$

- **According to postulate 3:**

$$\frac{(4.14) \ , \ (4.15)}{B|\equiv S|\equiv \{N_s, A, K_{ab}\}_{K_{bs}}} \tag{4.16}$$

- **According to postulate 4:**

$$\frac{(4.16) \ , \ B|\equiv S \Rightarrow K_{ab}}{B|\equiv K_{ab}} \tag{4.17}$$

Following the analysis, *B* can trust the key K_{ab}. As demonstrated, Kerberos protocol has a full BAN logic guarantee [89] and is trusted by many authors [62, 83]. It is one of the most common key distribution protocols. Unfortunately, despite all postulates have been performed in Kerberos protocol and it has a full guarantee from BAN, it is still susceptible to attacks as explained above, section 3.4. Thus, BAN logic needs to be improved in order to enhance its ability to stop the Replay Attack. In the next section, a modified BAN logic is proposed.

4.4 New Form of BAN Logic (N-BAN)

It has been proven that BAN is a very important and successful method to evaluate communication protocols [121]. Although the three upgrades mentioned in section 4.2 are performed successfully in the Kerberos protocol, and despite Kerberos having a full guarantee from BAN, Kerberos is still susceptible to attacks as explained above. Thus, BAN logic needs to be improved in order to enhance its ability to stop possible replay attacks. BAN logic is considered to rely on pure logical operations that should exist in order to conclude that the message is secure, such as a strong key or time stamp. It is regardless if the users are following the required logical predefinitions in prescribed manner. A new form of BAN logic is proposed is called N-BAN logic, it will have a new rule that indicates whether a message has been sent from a legitimate position or not using the user's P(Y) code. It has been noted in the previous chapter that, this new factor does not rely on the user's choice; encryption codes which has been used in P(Y) code has a very high level of security. To implement this new rule, the effect of the jurisdiction rule on message 3 need to be explained. As discussed earlier, AP receives a ticket and authenticator from the client (*KRB_AP_REQ*). We also knew that the ticket is encrypted by the key ($K_{TGS\text{-}AP}$). Since the *AP* knows that this key is controlled by *TGS*, the *AP* will believe this message and use the session key to decrypt the authenticator. This proposal gives another layer of protection; in addition to the decryption the ticket, the *AP* has to use his physical address signature to prove his official site in order to read the key. Figure 4.3 shows the modification on jurisdiction rule.

$$\boxed{\frac{B \mid\equiv S \mid\equiv (X),\ \ B \mid\equiv S \Rightarrow \{X\}_{SIG_b}\ ,\ \ S \mid\equiv B \Rightarrow Sig_b}{B \mid\equiv \ X}}$$

Figure 4.3 Jurisdiction Rule in N-BAN Logic

A new factor to the jurisdiction rule is proposed. This factor is the user's physical location; the user must use his signature (SIG_b) in order to believe X, where SIG_b his P(Y) code, which cannot be obtained unless the user is using his physical location. In other words, the user must be in his nominated location to capture his P(Y) code in order to be used to verify his location and read X. By this modification, BAN compels the user to use his official site in order to conclude that the message is secure. Message 3 of Kerberos is chosen and did a comparison between BAN and N-BAN logics as shown in table 4.3.

Table 4.3 Comparison between BAN and N-BAN Logics.

The logic	Rules that must be perform by B in order to read K_{ab}
BAN	1. B believes that S believes all the contents of the message. 2. B believes that S has a jurisdiction control over K_{ab}.
N-BAN	1. B believes that S believes all the contents of the message. 2. B believes that S has a jurisdiction control over K_{ab}. 3. B must verify his location using the P(Y) code of his legitimate location.

In the next section, the proposed N-Kerberos protocol is going to be analysed using N-BAN.

4.5 Analysing N-Kerberos Protocol Using N-BAN

As mentioned in section 4.2, there are three main steps to analyze any security protocol. Figure 4.4 shows N-Kerberos protocol and Table 4.4 shows the first step of the analysis. It is deriving the assumptions from the protocol's messages and translating them to a form of logic of belief.

$$1. A \to S : A, N_a, B$$

$$2. S \to A : \left\{ N_s, \{K_{ab}\}_{Sig_a}, B, \{N_s, \{K_{ab}\}_{Sig_b}, A\}_{K_{bs}} \right\}_{K_{as}}$$

$$3. A \to B : \{N_s, \{K_{ab}\}_{Sig_b}, A\}_{K_{bs}}, \{A, N_a\}_{K_{ab}}$$

$$4. B \to A : \{N_a + 1\}_{K_{ab}}$$

Figure 4.4 N-Kerberos Protocol

Table 4.4 Extracted assumptions from Kerberos

Extracted Assumptions and expressed by logic of believe
$S \mid\equiv A \xleftrightarrow{K_{as}} S$
$S \mid\equiv \#(N_a)$
$A \mid\equiv \#(N_s)$
$S \mid\equiv A \Rightarrow Sig_a$
$A \mid\equiv S \Rightarrow Sig_b$
$A \mid\equiv S \Rightarrow K_{ab}$
$B \mid\equiv \#(N_s)$
$S \mid\equiv B \Rightarrow Sig_b$
$B \mid\equiv S \Rightarrow Sig_a$

$B \mid\equiv S \Rightarrow K_{ab}$
$B \mid\equiv B \xleftrightarrow{K_{bs}} S$
$S \mid\equiv B \xleftrightarrow{K_{bS}} S$
$B \mid\equiv \#(N_a)$
$A \mid\equiv \#(N_b)$

The second step is drawing the goal, which the server needs to verify that the key K_{ab} has been received by *A* and *B*. in other words, *A* and *B* need to trust that the communication channel between them is secure. Finally, the third step is performing the N-BAN rules.

N-BAN requires three main key conditions as opposed to two in BAN in order to conclude that the message is secure. These key conditions are:

1. The message has to be encrypted.
2. The message should include nonce verification.
3. The message should have the verified user's physical position.

Details of proving the theory are as follows:

Client *A* sends his request to *S*, and then S sends *A* message 2. It is confirmed that, *A* believes K_{ab}; Since *A* believes K_{as} as a secrete key between *A* and *S*, and *A* received encrypted message 2 by K_{as}, then *A* now believes that *S* has sent message 2, Postulate 1.

$$\frac{A \left| \begin{array}{l} \equiv A \xleftrightarrow{K_{as}} S, \\ A \triangleleft \left\{N_s,\ \{K_{ab}\}_{Sig_a}, B, \{N_s, \{K_{ab}\}_{Sig_b}, A\}_{k_{bs}}\right\}_{K_{as}} \end{array} \right.}{A \mid\equiv S \sim \left\{N_s,\ \{K_{ab}\}_{Sig_a}, B, \{N_s, \{K_{ab}\}_{Sig_b}, A\}_{k_{bs}}\right\}_{K_{as}}} \tag{4.18}$$

Since the clocks are synchronized, *A* believes that, N_s is fresh and so, *A* believes that all the message is fresh (In particular, *A* believes that the message was not a replayed message captured sometime in the past by an attacker), postulate 2.

$$\frac{A \mid\equiv \#(N_s)}{A \mid\equiv \#\left\{N_s,\ \{K_{ab}\}_{Sig_a}, B, \{N_s, \{K_{ab}\}_{Sig_b}, A\}_{k_{bs}}\right\}_{K_{as}}} \qquad (4.19)$$

Since *A* believes that the entire message is fresh and *S* has sent the message, then *A* also believes that *S* believes the message, postulate 3.

$$\frac{(4.18)\ ,\ (4.19)}{A \mid\equiv\ S \mid\equiv \left\{N_s,\ \{K_{ab}\}_{Sig_a}, B, \{N_s, \{K_{ab}\}_{Sig_b}, A\}_{k_{bs}}\right\}_{K_{as}}} \qquad (4.20)$$

The next step is to apply the jurisdiction rule. For this to be applied, *A* is required to capture his P(Y) code. If A is using his P(Y) code, he would be able to decrypt Sig$_a$ and read the Key K_{ab} as shown in equation 4.21.

$$\frac{(4.20)\ ,\ A \mid\equiv\ S \Rightarrow K_{ab}\ ,\ where\ \{K_{ab}\}_{Sig_a},\ S \mid\equiv\ A \Rightarrow Sig_a}{A \mid\equiv\ K_{ab}} \qquad (4.21)$$

Message 3 has both a ticket and authenticator. The ticket is encrypted by K_{ab}, and the session key encrypts the authenticator. As *B* is required to believe the session key (K_{ab}) to access the authenticator, it first needs to believe the ticket. This is how it is proven:

$$\frac{B \mid\equiv B \xleftrightarrow{K_{bs}} S\ ,\ B \triangleleft \left\{N_s, \{K_{ab}\}_{Sig_b}, A\right\}_{k_{bs}}}{B \mid\equiv S \sim \left\{N_s, \{K_{ab}\}_{Sig_b}, A\right\}_{k_{bs}}} \qquad (4.22)$$

$$\frac{B|\equiv \#(N_s)}{B\,|\equiv \#\{N_s,\ \{K_{ab}\}_{Sig_b},A\}_{K_{bs}}} \qquad (4.23)$$

$$\frac{(4.22)\ ,\ (4.23)}{B|\equiv\ S|\equiv \{N_s,\ \{K_{ab}\}_{Sig_b},A\}_{K_{bs}}} \qquad (4.24)$$

According to the new jurisdiction rule, if:

- B believes that S sent the ticket (equation 4.22)
- *B* believes that *S* has jurisdiction control over the session key (k_{ab}), where k_{ab} has been encrypted using Sig$_a$.
- *S* believes that *B* has jurisdiction control over Sig$_a$.

Then *B* believes the session key. Therefore *B* starts to communicate with *A* securely. Equation 4.25 shows the jurisdiction rule.

$$\frac{(4.24)\ ,\ B\,|\equiv\ S \Rightarrow \{K_{ab}\}_{Sig_b},\ S\,|\equiv\ B \Rightarrow Sig_b}{B\,|\equiv\ K_{ab}} \qquad (4.25)$$

Finally, since client *A* and *B* believe that the Key K_{ab} is sent by the server, and the server believes that *A* and *B* are the only clients that can receives the key K_{ab}, then *A* and *B* will start their communication confidently without possibly been compromised in any way by a third party.

4.6 Summary

In this chapter, logic of believes was described and how it would be used to validate protocols. Details of a tool called BAN logic used to verify the protocol were also given. It used logic of believes to do such verification. Needham Schroeder and Kerberos were equally subjected to BAN logic. As a result of the scrutiny, Kerberos protocol has a full guarantee of BAN, although it is still vulnerable to attack, as shown in last chapter. More investigations were undertaken and concluded that BAN logic is not responsive to the complacency of the user, and therefore new condition were added which can be used to check the communication channel whether it is secure or not even where users do not implement the required verification. This new form of BAN logic is called N-BAN logic. This is clearly a major contribution in respect of verification. Finally, the proposed N-Kerberos was also analysed using the N-BAN logic with the desired outcome of preventing replay attack compared to BAN logic.

Chapter 5:

Testing and Applications

5.1 Introduction

Rigorous testing of new application or product prior to its launch or going live is an important element in order to address likely teething problems that may be encountered by the end user and to ensure its validity and strength. In this chapter, details of the effect of using military signal (*P(Y)* code) in the authentication field are classified. Non incorporation of using GPS in order to verify the users' identity is described. This chapter also describes the likely beneficiaries and where this technique can be implemented. Businesses and establishments can benefit from the technology; these are organizations that accept the work only through fixed locations, such as embassies or other public sector institutions. In addition, this technique can be used to overcome one of the most undesirable attack problems called pharming attack. This chapter is set out as follows:

Section 5.2 describes different cases of testing and the using of *P(Y)* code in the authentication. Where this technique can be applied is described in section 5.3. Conclusion and summary are given in the last section.

5.2 Testing and Verification

In this section, two tests will be presented; the first one is to describe the different between Kerberos and N-Kerberos. It is to show the effect of using *P(Y)* code in case of poor performance of the user, while the second test is to check the possibility to penetrate the system from unofficial site.

In order to implement the tests, website has been designed contains two fields; password and location signature and submit push bottom to submit the information to the server as shown in Figure 5.1.

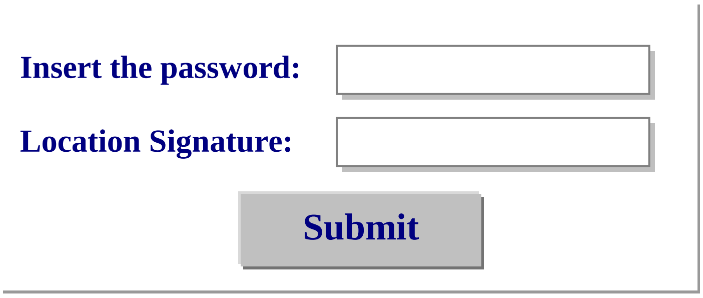


Figure 5.1 user’s identification information form

GPS receiver has been used to receive the user’s position coordinate number and then fill it manually in to the location signature field. Follow is the details of the two tests:

Test 1: the aim of this test is to demonistrate the benefit of using the GPS *P(Y)* code in authenticate the user identity. This test will show that *P(Y)* code can be used to protect the user despite the poor performance of the user in the definition of system, such as selection of a weak password or not specifying in advance the use of a specific time in the message. The steps to explain this test are as follows:

Step 1: Some pre-actions had to be performed before starting the test, which are illustrated in the following list:

1. To prepare a *GPS* receiver and install it at the site of user *A*.
2. To capture the *P(Y)* code of user *A.*
3. To hash *A*'s *P(Y)* code and save it in the server's database.
4. To prepare a tool to steal and decrypt the packet.
5. It is assumed a weakness in the setting of prior verification to the use the model such as, using a weak password to encrypt the packet and the allowed period time for sending the message is unlimited. Therefore, the message does not have a specific expiry time.

Step 2: Testing was performed and described using the following cases:

Case1: Using Kerberos protocol

In this case, the following steps were undertaken:

1. An encrypted packet was sent using Key Distributing Centre (KDC) of the PC to A's PC using a weak password and unlimited time for using this message.
2. Small software has been implemented to decrypt the signal.
3. Decrypt the message using the implemented software.

Since there is an open time to decrypt the key and the password is weak, several attempt were made with all possibilities until the key is realised.

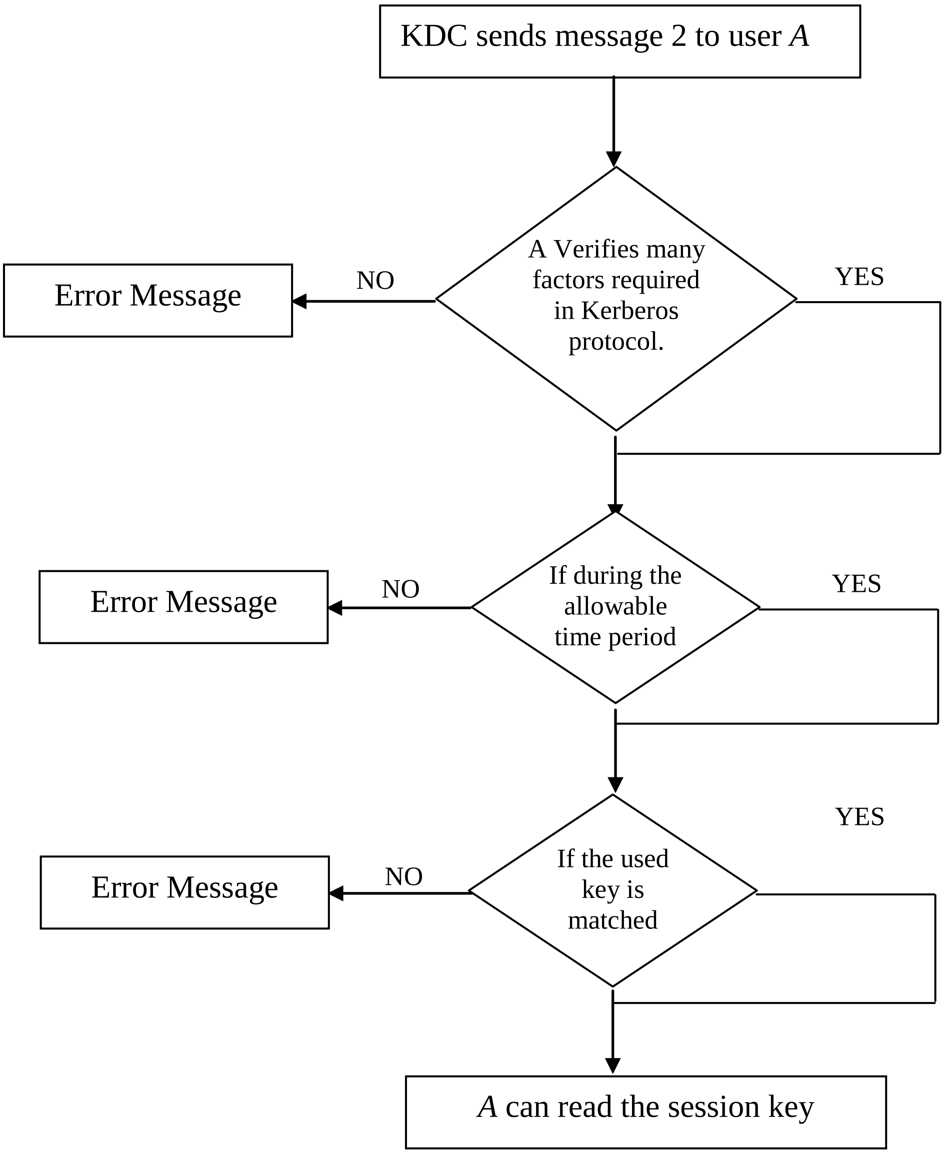
Therefore, following the testing, the code were compromised and read the session key.

Case2: Using N-Kerberos protocol

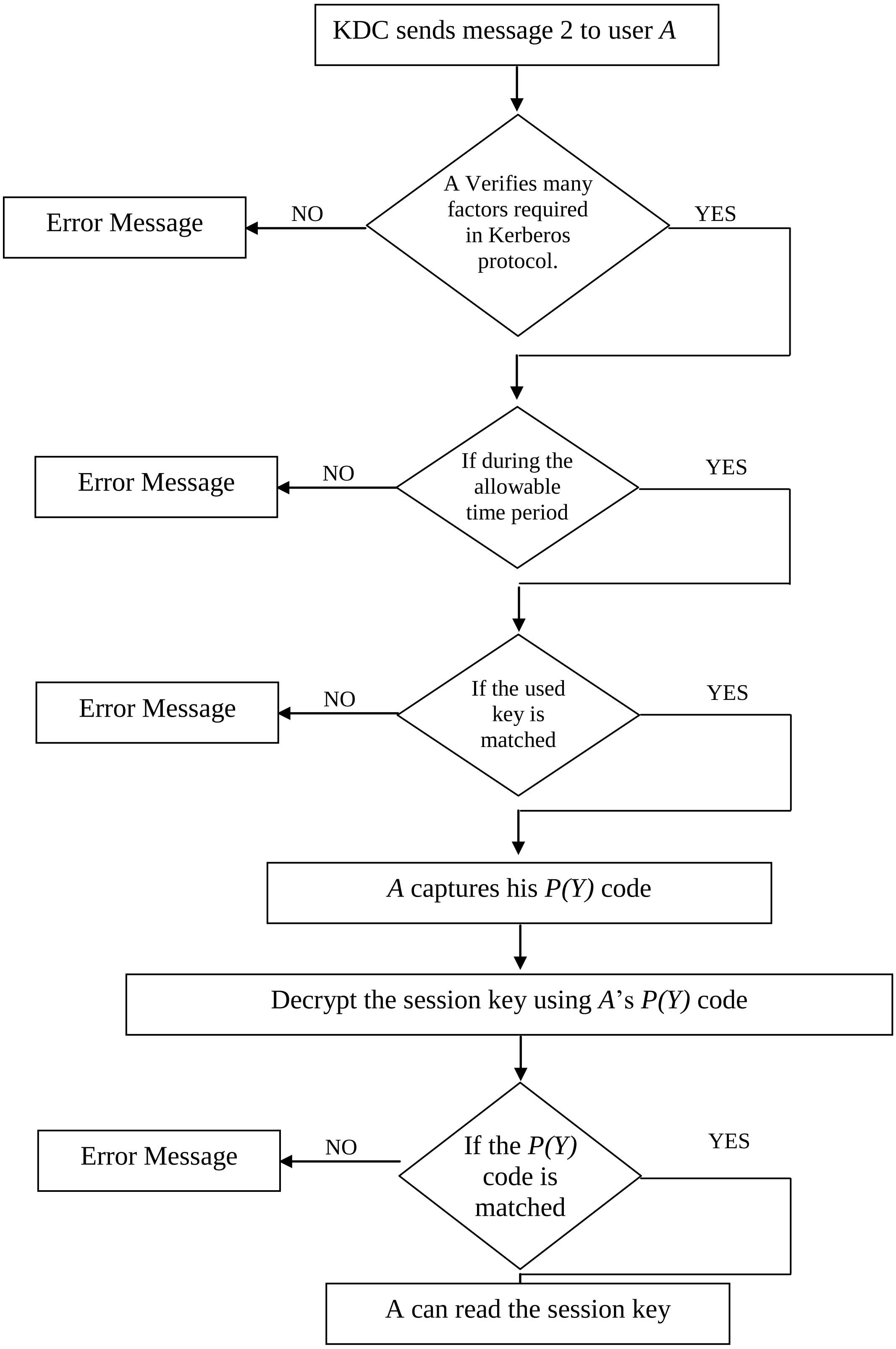
As in case 1, the same scenario was used. In case of using N-Kerberos, it is essential for hackers to penetrate different levels of protection. The first level is to breakthrough the encryption mechanism as described in the first case. The second level is to penetrate the *GPS* (*P(Y)* code) protection. This case has the following steps:

1. All the steps performed in case 1 were repeated. Despite this, it was not able to read the session key. To do so, the second level of protection (*GPS*) must be breached.
2. Many ready made decryption softwares were used in order to read the session key, but fortunately, that was not possible.

As a conclusion of this test, due to the Anti Spoof (*AS*) used in P-code, it is believed that the *P(Y)* code can be used to make the replay attack more difficult, even in the case of bad verification of the protocol. Figures 5.1 and 5.2 are to show case 1 and case 2 respectively using message 2 of Kerberos protocol.


KDC sends message 2 to user *A*
A Verifies many factors required in Kerberos protocol.
NO
Error Message
YES
If during the allowable time period
NO
Error Message
YES
If the used key is matched
NO
Error Message
YES
A can read the session key

Figures 5.2 Flaw chart of Kerberos case 1


KDC sends message 2 to user A
A Verifies many factors required in Kerberos protocol.
NO
Error Message
YES
If during the allowable time period
NO
Error Message
YES
If the used key is matched
NO
Error Message
YES
A captures his P(Y) code
Decrypt the session key using A's P(Y) code
If the P(Y) code is matched
NO
Error Message
YES
A can read the session key

Figures 5.3 Flaw chart of N-Kerberos case 2

Test 2: The aim of this test is to check the possibility to penetrate the system from unofficial site; the site which is not defined in advance in the server. Two different places have been chosen to implement this test. The steps that should be performed to do this test are as follows:

Step 1: the pre-actions that have to be performed before starting the test are described as follows:

1. To prepare a *GPS* receiver and install it in the official site (*A*).
2. To prepare a *GPS* receiver and install in unofficial site (*B*).
3. To capture the *P(Y)* code of user *A.*
4. To create a database of all *P(Y)* codes and save *A*'s *P(Y)* code on it.

Step 2: There are two cases in step 2, presented as follows:

Case 1: Access the system from the official site.

In this case, we capture the *P(Y)* code using the official site, and get access to the system.

Case 2: Access the system from unofficial site.

In this case, unofficial site has been used. Following testing, we did not get to the system because the captured *P(Y)* code from the unofficial site does not exist in the server data base.

As a conclusion of this test, the user should be in his official site in order to get access to the services. In the next section, different areas that can use the *P(Y)* code to authenticate the user identity are suggested.

5.3 Possibilities of where can it be applied?

Following intensive investigations, it is concluded that this technology would diminish the challenges and menace exposed by the scenario replicated. To illustrate this, the different areas that can be applied to this study and the benefits that could accrue from it are described.

5.3.1 Embassies

The GPS has more possibility to use in the non-variable workplace such as embassy buildings or similar security sensitive buildings. It is known that the embassies do not allow staff to transfer files to work outside the perimeter of the embassy. In such system, it is suggested creating a security network based on the GPS signal in order to authenticate the user identity. This may increase the level of data transfer protection. For example, Jordanian embassies in two different places have been chosen to ascertain the possibility of how the system using GPS signal works. Note that next example is not a real implementation, it is just a possibility. The pre-required steps to implement the system in Jordanian embassies are presented below:

1. Install GPS receiver in the two embassies sites (*X*, *Y*).
2. Install GPS receiver in the key Ministry building in Jordan (*M*).
3. Capture the *P(Y)* code of sites *X* (Sig_x) and *Y* (Sig_y).
4. Save all the captured embassies' signatures in a database in the server located in the key Minister building in Jordan.

Case1: *X* communicates with *M*

When embassy *X* asked *M* to send data, the following procedures must be followed to send the required data:

1. *X* sends his request to *M*

2. *M* requires Sig$_{x}$ from the database.
3. *M* prepares (*X*-request).
4. *M* builds two different protection layer; inner and outer levels. The inner is encrypting *X*-request using Sig_x and the outer is encryption of all messages using the shared key. Note that the message has been signed by time stamp.
5. *X* receives the message from *M*.
6. Encrypt the message by the shared key.
7. *X* captures his *P(Y)* code (Sig$_{x}$) from the GPS receiver.
8. *X* Decrypts (*X*-request) using Sig$_{x}$.

$$\boxed{P \rightarrow X :\{N,\{X - request\}_{Sig_x}\}_{K_{px}}}$$

Figures 5.4. The content of P’s responds

The requested data are protected using two level of protection instead of one. The inner level is using a very well encrypted code based on user physical location as shown in Figure 5.3.

Case2: *X* communicates with *Y*

When embassy *X* needs data from embassy *Y*, the following procedures must be adhered to:

1. *X* sends his request from *Y* to *M*.
2. *M* requires Sig_x and *Sig*$_{y}$ from the database.
3. *M* sends *Y* the request of *X* and Sig_x encrypted by the shared key between *M* and *Y*. as shown in figure 5.4

$$\boxed{P \rightarrow X : \{N, \{K_{xy}\}_{Sig_x}, \{request, K_{xy}, Sig_x\}_{Sig_y}\}_{K_{px}}}$$

Figures 55. *P* sends *Y* *X*'s request

4. *X* receives the message from *M*.

5. Encrypt the message by the shared key (K_{px}).

6. *X* captures his *P(Y)* code (SIG_x) using his *GPS* receiver.

7. *X* Decrypts the shared key using SIG_x.

8. *X* sends the ticket ($\{request, K_{xy}, SIG_x\}_{SIG_y}$) in addition to his personal information encrypted by his signature ($\{N, K_{xy}\}_{SIG_x}$) to *Y* as shown in figure 5.5.

$$\boxed{X \rightarrow Y : \{request, K_{xy}, SIG_x\}_{Sig_y} \{N, K_{xy}\}_{Sig_x}}$$

Figures 5.6. *X* sends *Y* *X*'s request

9. *Y* prepares the request of *X* (*X*-request), and encrypt it using *X*'s signature and the shared key as shown in figure 5.6.

$$\boxed{Y \rightarrow X : \{N, \{X - request\}_{Sig_x}\}_{K_{xy}}}$$

Figures 5.7. *X* sends *Y* *X*'s request

10. *X* receives the message from *Y*.

11. Encrypt the message using the shared key K_{xy} ,

12. *X* captures his signature using his GPS receiver, and encrypts his request.

5.3.2 Pharming Attack

In recent years, phishing appears to be one of the prominent criminal activities pertaining to computer security. Unscrupulous groups target gullible users and direct them towards bogus websites in order to defraud. Hackers have adopted this method based on the fact that most computers users are not astute and savvy enough to identify phony and fake websites. In Pharming attack, the attacker redirects the user to a fake website; when a user sends a domain name asking to get access web page, the domain name will be translated to an IP address using Domain Name System (DNS). Then, the web browser connects to the server and loads the page which is equivalent to this IP address. In Pharming attack, the attacker targets the local host file and converts the URLs to different numbers and then, the users will be redirected to the dummy websites. Users may then deal with these fake websites as a trustworthy entity without knowing it. The aim of the hacker is acquiring sensitive information such as user name, password and credit card details. The attackers target the DNS server, which would mean millions of internet users will be affected [59, 120].

This problem has come to the attention of many researchers and computer security professionals because of its significant adverse effects. Several researches have been proposed to overcome this menace. But unfortunately, the problem still exists. “It is estimated that businesses lose $2 billion dollars per year when their clients are targeted by phishing scams. Meanwhile 3.6 millions were conned out of $3.2 billion between August 2006 and August 2007; figures like these are expected to rise”[4]. The technique in this thesis may used to reduce the affects of pharming attack; since the DNS server has a fixed place, the DNS’s physical position can be used as a key condition in order to

[4] http://www.brighthub.com/computing/smbsecurity/articles/64476.aspx#ixzz0n0Ptat4j

authenticate the user's identity. In other words, the hacker has to get access to where the DNS computer exists physically in order to change the host addresses.

5.3.3 Other Places

This methodology can be used in the areas which use fixed location in their work procedures such as embassies as explained above in details. List of other areas are presented below:

1. **Universities.**

   The Student in the university uses password to get access to the university's services such as access to their account; printer, library, financial account academic record where applicable and many other services. Most students do not take adequate precaution regarding the level of password strength because they are distant from the security area. Therefore, using the location signature will be appropriate for those people. In order to overcome the limitation problem, the administrator can add an option to the student's profile which they can enable or disable the using of the location signature based on the importance or the confidentiality of the requested service, in case of using student's account accessing the computer system off campus.

2. **Multiple Sites.**

   There are many companies that have several sites spread over different locations in various parts world. The positions of these sites are fixed. Therefore, the position signature can be used to protect the transmitted documents among these sites. For example, Banks branches needs to send and receive important documents and figures through online transactions.

3. Safety Communication.

Since state and public institutions are fixed in terms of their location, this technology will help in the transfer of sensitive data that require secure medium to transfer between different State institutions.

5.4 Summary

In this chapter, the effect of using the *P(Y)* code is tested. Two different cases have been implemented to show the advantage of using the military signal *P(Y)* code in increasing the authenticity strength of the user's identity. It has been concluded that despite using a weak password, another layer of protection using *P(Y)* code can protect the system. Different cases that show where this technique can be implemented are described. Furthermore, it is concluded that pharming attack can be eliminated using the user's position signature (*P(Y)* code) to authenticate the identity of the administrator.

Chapter 6:

Conclusion, Limitations and Future Work

6.1 Introduction

This thesis assessed the level of protection when data is transmitted between users and computer networks. It critically examined the identification of the user in what is referred to as authentication. Various methods were appraised to confirm the identity of the user and also constraints pertaining to data protection issues. The main aim was to minimise the ability of hackers to interfere with computer systems. To this end, several available methodologies were appraised and also reviewed considerable number of international report pertaining to same. Particular methods were examined and the level of data protection used in their algorithm. As a result of the rigorous analysis, an enhanced and robust algorithm is developed with superior level of security to shield the user identity.

In order to achieve more secure communication channel, N-Kerberos protocol is proposed. N-Kerberos uses the user's physical address, obtain by the GPS signal, as a new authentication factor to verify the identity of the user. In addition, a special evaluation tool called N-BAN logic is proposed in order to detect whether the N-Kerberos protocol are secured or not.

The reminder of this chapter is set out follows; Section 6.2 is to demonstrate details of the main contributions. The limitations are described in section 6.3. Suggestion for future work is provided in section 6.4.

6.2 Conclusion

As a result of the findings of this study, a non-conventional method of technologies of data protection needs to be developed; improvement in the encryption code is not sufficient solution, since it might be cracked by more competent hacker. Therefore, this study proposed a situation where the user is compelled to be more vigilant; in addition to relying on used codes. The details of the main contributions are as follows:

1. **Literature review about the authentication.**

   The importance of clarity of the user's identity and the challenges associated with it were reviewed. Numerous studies which attempted to protect the user's privacy in a coherent manner were examined to determine if they provide adequate and acceptable level of protection.

2. **Proposed N-Kerberos protocol.**

   A new form of Kerberos that is called N-Kerberos is proposed. The user's physical position address as a new authentication factor is considered in order to achieve a robust protection level. To achieve this, the military GPS signal (*P(Y)* code) is picked. Then, *P(Y)* is used to encrypt the key before sending it online. N-Kerberos is characterizing for two main major points as compared with Kerberos protocol, as listed below:

a. In Kerberos protocol, only one key has been used. Moreover, choice of this key relies on the users themselves. In other words, the message might easily be decrypted, as a result of choosing a weak password. While N-Kerberos protocol uses another level of protection, in addition to Kerberos's key. The new protection level is relying on the location signature which is very hard to be decrypted as oppose to relying on the user.

b. Kerberos protocol is not mindful of how users are implementing the Kerberos's required verifications before using the system. This may facilitate decoding the message in the case of the use of inaccurate definitions. While in N-Kerberos, users are saved even in cases of using inaccurate definitions, because they are required to use their location signature which is an encrypted very strongly.

3. Proposed N-BAN Logic

A special tool is used to detect whether the security protocols are secured or not, this tool is called BAN logic. The modified BAN logic is a group of logical operations and is referred to as N-BAN logic. BAN logic is not sensitive to the non-discipline of the users. While N-BAN focused on follow-up to the user's performance, a new condition to the jurisdiction rule in BAN logic is added. This new modification requires the user to use their position during the manufacture of the key. In other words, a new condition has been added and is considered to be a logical operation in order to believe that the sent message is protected.

4. **Implementation.**

   An experiment was conducted to test the strength and quality of the GPS receiver. It is confirmed that in practice it is possible to use the power of this signal in raising the level of verification the identity of the user.

6.3 Limitations

In some cases, three distinct disadvantages are identified, and these are as follows:

1. Costly

In N-Kerberos protocol, the organisation needs to buy a GPS receiver for every single employee. This will increase the cost of implementing the strategy.

2. Fixed location

User must use his official and authorised location in order to have the key. This is considered a limitation. For instance, where an employee travels out of his authorised nominated location they would be denied access.

3. Poor Signals.

In the likely event of adverse weather conditions, the user may not capture good quality signal. One practical example is the recent explosion of volcanic ashes in Iceland that affected most of west and northern Europe. Moreover, It has been noted that GPS receiver needs to be viewed by 3 or 4 GPS satellites in order to calculate the location or capture the *P(Y)* code. Therefore, the GPS receiver may not work in a basement or in an underground location, and also where the signals are obstructed.

6.4 Future Work

Inserting the *P(Y)* code signature into the user device is proposing in the future work. The device may not need to use the GPS receiver every time to be protected. GPS receiver may be just a time in a factory and push those signatures in the devices. Figure 6.1 shows the how inserting the P(Y) code is going to be.

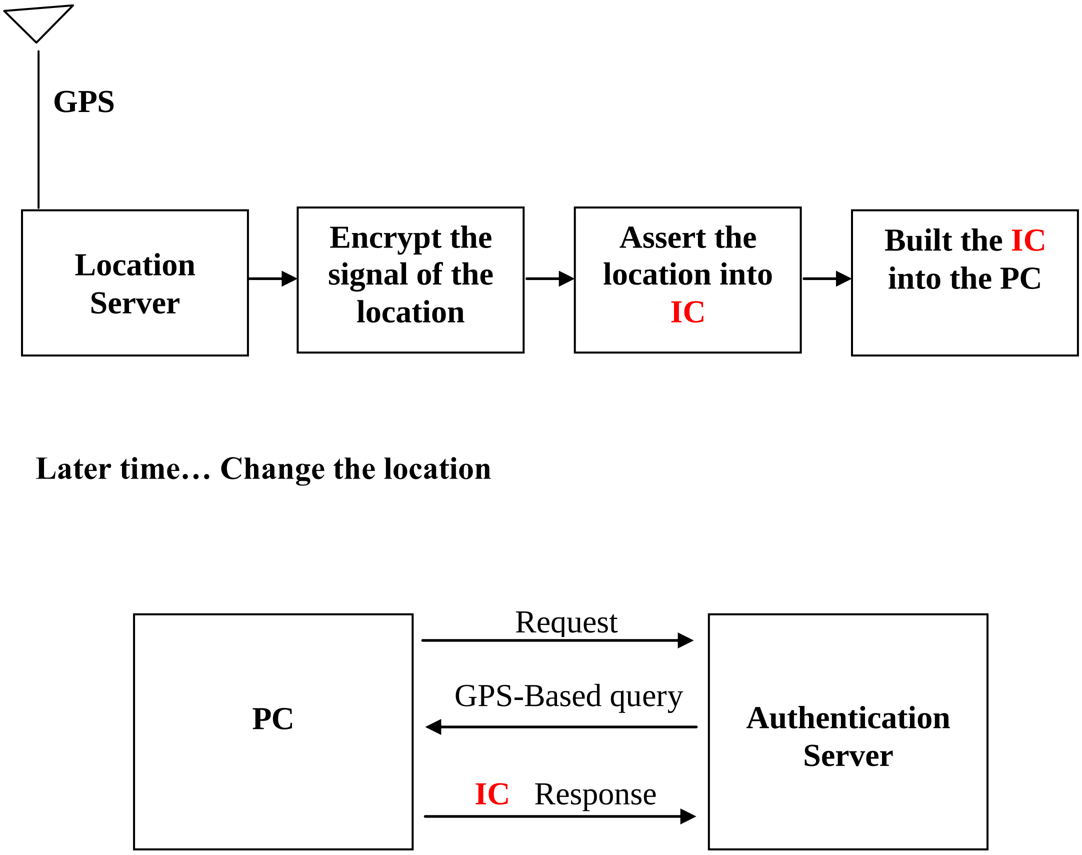


Figure 6.1 Assert the P(Y) code into the devices

If the *P(Y)* code of every single employee is engraved in their device, all the limitation mentioned above will be overcome as follows:

- **Cost:**

The organisation will use only one GPS receiver used in all employees' offices to capture the signatures and engrave them to the employees' devices. Therefore there would no to be a need to buy a GPS receiver for every single employee. The cost will be reduced.

- **Fixed Location**

Users can hence travel and use their devices without needing to use the official sites in order to connect to the system because the address has been engraved in their devices. This will eliminate the limitation of using fixed locations.

- **Poor signals**

To overcome constrains of poor signal in a basement building, signature details of a particular spot in the desired building with a strong signal world then be engraved in the devices of employees in the affected area.

REFERENCES

1. Abadi, M. and R. Needham, *Prudent engineering practice for cryptographic protocols.* Software Engineering, IEEE Transactions on, 1996. **22**(1): p. 6-15.

2. Akyildiz, I.F., et al., *Wireless sensor networks: a survey.* Computer networks, 2002. **38**(4): p. 393-422.

3. Ang, G., et al. *A Hierarchical Authentication Scheme for the Different Radio Ranges Sensor Networks*. in *Computational Science and Engineering, 2009. CSE '09. International Conference on*. 2009.

4. Bellovin, S.M. and M. Merritt, *Limitations of the Kerberos authentication system.* ACM SIGCOMM Computer Communication Review, 1990. **20**(5): p. 119-132.

5. Bertino, E. and M. Kirkpatrick. *Location-Aware Authentication and Access Control Concepts and Issues*. in *Advanced Information Networking and Applications, 2009. AINA '09. International Conference on*. 2009.

6. Bicakci, K. and N. Baykal, *One-time passwords: Security analysis using ban logic and integrating with smartcard authentication.* Computer and Information Sciences-ISCIS 2003, 2003: p. 794-801.

7. Brumley, D.B., D., *Remote timing attacks are practical.* Computer Networks, Elsevier, Stanford University, USENIX Association Berkeley, CA, USA, 2005. **48**(5): p. 701-716.

8. Bryant, B., *Designing an authentication system: a dialogue in four scenes*. 1988, Draft February: Project Alhena internal document.

9. Bunnell, J., et al., *Cognitive, associative and conventional passwords: Recall and guessing rates.* Computers & Security, 1997. **16**(7): p. 629-641.

10. Burrows, M., M. Abadi, and R. Needham, *A logic of authentication.* ACM Transactions on Computer Systems (TOCS), 1990. **8**(1): p. 18-36.

11. Cannon, J.M., J.A. Johanson, and P.D. Mooney, *Enhanced wireless network security using GPS*. 2006, Google Patents.

12. Carlucci Aiello, L. and F. Massacci, *Verifying security protocols as planning in logic programming.* ACM Transactions on Computational Logic (TOCL), 2001. **2**(4): p. 542-580.

13. Chia-Mu, Y., L. Chun-Shien, and K. Sy-Yen. *A Constrained Function Based Message Authentication Scheme for Sensor Networks*. in *Wireless Communications and Networking Conference, 2009. WCNC 2009. IEEE*. 2009.

14. Chong, F. and Z. Zhi-Liang. *An Efficient Implementation of RSA Digital Signature Algorithm*. in *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on*. 2008.

15. Chown, P., *Advanced encryption standard (AES) ciphersuites for transport layer security (TLS)*. 2002, RFC 3268, June 2002.

16. Clulow, J. and J.S. Clulow, *The design and analysis of cryptographic application programming interfaces for security devices.* Masterthesis, University of Natal, Durban, Südafrika, 2003.

17. Common Criteria for Information Technology Security Evaluation, P., *Security Functional Requirements*. 1999, Available: http://www.commoncriteria.org/docs/PDF/CCPART2V21.

18. Coppersmith, D., *The Data Encryption Standard (DES) and its strength against attacks.* IBM journal of research and development, 1994. **38**(3): p. 243-250.

19. Corcoran, D., D. Sims, and B. Hillhouse, *Smart cards and biometrics: Your key to PKI.* Linux Journal. Retrieved July, 1999. **3**: p. 2002.

20. David B. Johnson, D.A.M., Yih-Chun Hu, and Jorjeta G. Jetcheva. *The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks*. 2002.

21. Davis, D. and R. Swick, *Workstation services and Kerberos authentication at Project Athena*, Technical Memorandum TM-424, MIT Laboratory for Computer Science (February 1990).

22. Delaune, S. and F. Jacquemard. *A theory of dictionary attacks and its complexity*. 2004: Citeseer.

23. Deng, J., R. Han, and S. Mishra. *Defending against path-based DoS attacks in wireless sensor networks*. 2005: ACM.

24. Denning, D.E. and P.F. MacDoran, *Location-based authentication: Grounding cyberspace for better security.* Computer Fraud & Security, 1996. **1996**(2): p. 12-16.

25. Diffie, W. and M.E. Hellman, *Special Feature Exhaustive Cryptanalysis of the NBS Data Encryption Standard.* Computer, 1977. **10**(6): p. 74-84.

26. Doherty, L., K.S.J. pister, and L. El Ghaoui. *Convex position estimation in wireless sensor networks*. in *INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*. 2001.

27. Ehrsam, W.F., et al., *A cryptographic key management scheme for implementing the Data Encryption Standard.* IBM Systems Journal, 1978. **17**(2): p. 106-125.

28. Fan, Y., et al., *Statistical en-route filtering of injected false data in sensor networks.* Selected Areas in Communications, IEEE Journal on, 2005. **23**(4): p. 839-850.

29. Feng, Z., M. Mutka, and L. Ni. *PrudentExposure: a private and user-centric service discovery protocol*. in *Pervasive Computing and Communications, 2004. PerCom 2004. Proceedings of the Second IEEE Annual Conference on*. 2004.

30. Furnell, S.M., et al., *Authentication and supervision: A survey of user attitudes.* Computers & Security, 2000. **19**(6): p. 529-539.

31. Germain, R.S., A. Califano, and S. Colville, *Fingerprint matching using transformation parameter clustering.* Computational Science & Engineering, IEEE, 1997. **4**(4): p. 42-49.

32. Gong, L., R. Needham, and R. Yahalom. *Reasoning about belief in cryptographic protocols*. in *Research in Security and Privacy, 1990. Proceedings., 1990 IEEE Computer Society Symposium on*. 1990.

33. Goyal, V., et al., *Founding cryptography on tamper-proof hardware tokens.* Theory of Cryptography: p. 308-326.

34. Gritzalis, S., D. Spinellis, and P. Georgiadis, *Security protocols over open networks and distributed systems: Formal methods for their analysis, design, and verification.* Computer Communications, 1999. **22**(8): p. 697-709.

35. Gustafson, D., J. Dowdle, and K. Flueckiger. *A high anti-jam GPS-based navigator*. 2000.

36. Habib, A. and D. Roy. *Steps to defend against DoS attacks*. in *Computers and Information Technology, 2009. ICCIT '09. 12th International Conference on*. 2009.

37. Han, K. and K. Kim. *Enhancing privacy and authentication for location based service using trusted authority*. 2007: Citeseer.

38. Harter, A. and A. Hopper, *A distributed location system for the active office.* Network, IEEE, 1994. **8**(1): p. 62-70.

39. Harter, A., et al., *The anatomy of a context-aware application.* Wireless Networks, 2002. **8**(2): p. 187-197.

40. Hightower, J., R. Want, and G. Borriello, *SpotON: An indoor 3D location sensing technology based on RF signal strength.* UW CSE 00-02-02, University of Washington, Department of Computer Science and Engineering, Seattle, WA, 2000.

41. Hopper, A., A. Harter, and T. Blackie. *The active badge system (abstract)*. in *Conference on Human Factors in Computing Systems*. 1993. Amsterdam, The Netherlands: ACM.

42. http://wellcometoshareknowledge.blogspot.com/2010/02/hackers-steel-card-data.html.

43. http://www.kowoma.de/en/gps/positioning.htm.

44. Hu, Y.C. and D.B. Johnson. *Caching strategies in on-demand routing protocols for wireless ad hoc networks*. in *In Proceedings of the Sixth Annual IEEE/ACM International Conference on Mobile Computing and Networking*. 2000: ACM.

45. Hu, Y.C., A. Perrig, and D.B. Johnson. *Packet leashes: a defense against wormhole attacks in wireless networks*.

46. Hu, Y.C., A. Perrig, and D.B. Johnson. *Packet leashes: a defense against wormhole attacks in wireless networks*. in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*. 2003.

47. Hu, Y.C., A. Perrig, and D.B. Johnson. *Rushing attacks and defense in wireless ad hoc network routing protocols*. 2003: ACM.

48. Huang, H., S. Zhong, and J. Tan. *Browser-Side Countermeasures for Deceptive Phishing Attack*. 2009: IEEE Computer Society.

49. information, E.S.D.I., *Securing your digital life.* 2005.

50. Jain, A., L. Hong, and S. Pankanti, *Biometric identification.* Communications of the ACM, 2000. **43**(2): p. 98.

51. Jain, A.K., R. Bolle, and S. Pankanti, *Biometrics: personal identification in networked society*. 1999: Kluwer Academic Publishers.

52. Jain, A.K., A. Ross, and S. Pankanti, *Biometrics: a tool for information security.* IEEE transactions on information forensics and security, 2006. **1**(2): p. 125-143.

53. Jakobsson, M. and S. Myers, *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*. 2006: Wiley-Interscience.

54. Jobusch, D.L. and A.E. Oldehoeft, *A survey of password mechanisms: Weaknesses and potential improvements. part 1.* Computers & Security, 1989. **8**(7): p. 587-604.

55. Johnson, D.B. *Routing in Ad Hoc Networks of Mobile Hosts*. in *In Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications* 1994.

56. Johnson, Y.-C.H.a.D.B. *Implicit Source Routing in On-Demand Ad Hoc Network Routing*. in *In Proceedings of the Second Symposium on Mobile Ad Hoc Networking and Computing* 2001.

57. Kai, F., L. Hui, and W. Yue. *Security Analysis of the Kerberos Protocol Using BAN Logic*. in *Information Assurance and Security, 2009. IAS '09. Fifth International Conference on*. 2009.

58. Kaplan, E. and C. Hegarty, *Understanding GPS: Principles and Applications Second Edition.* Artech House, 2006.

59. Karlof, C., et al. *Dynamic pharming attacks and locked same-origin policies for web browsers*. 2007: ACM.

60. Kasslin, K., A. Tikkanen, and T. Virtanen, *Kerberos V Security: Replay Attacks.* Enhancing Trust, 2003: p. 191.

61. Katz, J. and Y. Lindell, *Introduction to modern cryptography*. 2008: Chapman & Hall/CRC.

62. Kaufman, C., R. Perlman, and M. Speciner, *Network security: private communication in a public world.* 2002.

63. Kenneth R. Allendoerfer, N.H.F.G., ATO-P, Shantanu Pai, L-3 Communications, Titan Corporation, *Human Factors Considerations for Passwords and Other User Identification Technique, Part 2: Field Study, Results and Analysis*, W.J.H.T.C. Federal Aviation Administration, Atlantic City International Airport, NJ 08405, Editor. 2006.

64. Kim, M.J., et al., *An algebraic watchdog for wireless network coding.* Arxiv preprint arXiv:0901.2913, 2009: p. 1159 - 1163.

65. Kirda, E. and C. Kruegel, *Protecting users against phishing attacks.* The Computer Journal, 2006. **49**(5): p. 554.

66. Klein, L.A. and L.A. Klein, *Millimeter Wave and Infrared Multisensor Design and Signal Processing*. 1997: Artech House, Inc. Norwood, MA, USA.

67. Kocarev, L., M. Sterjev, and P. Amato. *RSA encryption algorithm based on torus automorphisms*. 2004.

68. Kocher, P. *Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems*. 1996: Lecture Notes in Computer Science, Springer-Verlag, London, Uk.

69. Kohl, J. and C. Neuman, *The Kerberos network authentication service (v5)*. 1993, Citeseer.

70. Krauss, C., M. Schneider, and C. Eckert. *An Enhanced Scheme to Defend against False-Endorsement-Based DoS Attacks in WSNs*. in *Networking and Communications, 2008. WIMOB '08. IEEE International Conference on Wireless and Mobile Computing*. 2008.

71. Kuhn, M.G. *Eavesdropping attacks on computer displays*. in http://www.cl.cam.ac.uk/_mgk25/. 1985. 15 JJ Thomson Avenue, Cambridge CB3 0FD, United Kingdom: Citeseer

72. Kwon, T. and J. Song, *Clarifying straight replays and forced delays.* ACM SIGOPS Operating Systems Review, 1999. **33**(1): p. 47-52.

73. Ladd, A.M., et al., *Robotics-based location sensing using wireless ethernet.* Wireless Networks, 2005. **11**(1): p. 189-204.

74. Lefebvre, F., J. Czyz, and B. Macq. *A robust soft hash algorithm for digital image signature*. in *Image Processing, 2003. ICIP 2003. Proceedings. 2003 International Conference on*. 2003.

75. Lehtinen, M., A. Happonen, and J. Ikonen. *Accuracy and time to first fix using consumer-grade GPS receivers*. in *Software, Telecommunications and Computer Networks*. 2008.

76. Liu, D. and P. Ning, *Multilevel TESLA: Broadcast authentication for distributed sensor networks.* ACM Transactions on Embedded Computing Systems (TECS), 2004. **3**(4): p. 800-836.

77. Liu, S. and M. Silverman, *A practical guide to biometric security technology.* IT Professional, 2001. **3**(1): p. 27-32.

78. Malliga, S., A. Tamilarasi, and M. Janani. *Filtering spoofed traffic at source end for defending against DoS / DDoS attacks*. in *Computing, Communication and Networking, 2008. ICCCn 2008. International Conference on*. 2008.

79. Maltz, D.B.J.a.D.A., *Dynamic Source Routing in Ad Hoc Wireless Networks*, e.b.T.I.a.H.K. In Mobile Computing, chapter 5, Editor. 1996, Kluwer Academic Publishers. p. 153–181.

80. Marra, D.A., *A Strong Authentication Mechanism for Consumer-Facing Online Transactions.* 2005.

81. Marti, S., et al. *Mitigating routing misbehavior in mobile ad hoc networks*. 2000: ACM.

82. Matosevic, M., Z. Salcic, and S. Berber, *A Comparison of Accuracy Using a GPS and a Low-Cost DGPS.* Instrumentation and Measurement, IEEE Transactions on, 2006. **55**(5): p. 1677-1683.

83. Menezes, A.J., P.C. Van Oorschot, and S.A. Vanstone, *Handbook of applied cryptography*. 1997: CRC.

84. Miller, S.P., et al., *Kerberos authentication and authorization system.* In Project Athena Technical Plan Section E.2.1, MIT, 1987.

85. Mills, D., *Network Time Protocol (Version 3) specification, implementation and analysis*. 1992, RFC 1305, March 1992.

86. Mirkovic, J., et al., *Internet Denial of Service: Attack and Defense Mechanisms (Radia Perlman Computer Networking and Security)*. 2004: Prentice Hall PTR Upper Saddle River, NJ, USA.

87. Mirkovic, J. and P. Reiher, *A taxonomy of DDoS attack and DDoS defense mechanisms.* ACM SIGCOMM Computer Communication Review, 2004. **34**(2): p. 39-53.

88. Morris, R.T., *A weakness in the 4.2 BSD Unix TCP/IP software.* Computing science technical report, 1985. **117**.

89. Mukhamedov, A. *Full agreement in BAN kerberos*. in *Security and Privacy for Emerging Areas in Communication Networks, 2005. Workshop of the 1st International Conference on*. 2005.

90. Mutlugun, M. and I. Sogukpinar. *Multi-level Authentication Scheme Utilizing Smart Cards and Biometrics*. in *Emerging Security Information, Systems and Technologies, 2009. SECURWARE '09. Third International Conference on*. 2009.

91. Needham, R.M. and M.D. Schroeder, *Using encryption for authentication in large networks of computers.* Communications of the ACM, 1978. **21**(12): p. 999.

92. O'Gorman, L., *Comparing passwords, tokens, and biometrics for user authentication.* Proceedings of the IEEE, 2003. **91**(12): p. 2021-2040.

93. OUT-LAW.COM, *Phishing attack targets one-time passwords*. 12th October 2005, http://www.theregister.co.uk/2005/10/12/outlaw_phishing/.

94. Pankanti, S., R.M. Bolle, and A. Jain, *Biometrics: The future of identification.* Computer, 2000. **33**(2): p. 46-49.

95. Pankanti, S., R.M. Bolle, and A. Jain, *Biometrics:The future of identification.* Computer, 2000. **33**(2): p. 46-49.

96. Patarin, J., *Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of Asymmetric Algorithms; Eurocrypt'96.* Springer LNCS, 1996. **1070**: p. 33-48.

97. Peng, X. and H. Zhao. *An "Attacker Centric" Cyber Attack Behavior Analysis Technique*. in *Advanced Communication Technology, The 9th International Conference on*. 2007.

98. Perrig, A., et al., *The TESLA broadcast authentication protocol.* RSA CryptoBytes, 2002. **5**(2): p. 2-13.

99. Perrig, A., et al., *SPINS: Security protocols for sensor networks.* Wireless networks, 2002. **8**(5): p. 521-534.

100. Pond, R., et al., *Word association computer passwords: The effect of formulation techniques on recall and guessing rates.* Computers & Security, 2000. **19**(7): p. 645-656.

101. Postel, J., *Transmission control protocol*. 1981, STD 7, RFC 793, September 1981.

102. Postel, J., *User datagram protocol*. 1980, Citeseer.

103. Postel, J. and K. Harrenstien, *Time protocol.* DARPA Network Working Group Report RFC-868, USC Information Sciences Institute, 1983.

104. Qinghan, X. *Security issues in biometric authentication*. in *Information Assurance Workshop, 2005. IAW '05. Proceedings from the Sixth Annual IEEE SMC*. 2005.

105. Qiong, P. and Z. Xiuying. *Montgomery Exponentiation with No Final Comparisons: Improved Results*. in *Circuits, Communications and Systems, 2009. PACCS '09. Pacific-Asia Conference on*. 2009.

106. Ramachandran, A.V. and N. Feamster. *Authenticated out-of-band communication over social links*. 2008: ACM.

107. Rayanchu, S., et al. *Diagnosing Wireless Packet Losses in 802.11: Separating Collision from Weak Signal*. in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*. 2008.

108. Ren, K., W. Lou, and Y. Zhang. *LEDS: Providing Location-Aware End-to-End Data Security in Wireless Sensor Networks*. in *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*. 2006.

109. Rivest, R., *RFC1321: The MD5 message-digest algorithm.* RFC Editor United States, 1992.

110. Sanchez-Reillo, R. *Securing information and operations in a smart card through biometrics*. in *Security Technology, 2000. Proceedings. IEEE 34th Annual 2000 International Carnahan Conference on*. 2000.

111. Schmid, A., *Positioning Accuracy Improvement With Differential Correlation.* Selected Topics in Signal Processing, IEEE Journal of, 2009. **3**(4): p. 587-598.

112. Schneier, B., *Applied cryptography: protocols, algorithms, and source code in C*, ed. 2nd. 2007: A1bazaar. 429–459.

113. Schultz, E.E., *A framework for understanding and predicting insider attacks.* Computers & Security, 2002. **21**(6): p. 526-531.

114. Sencun, Z., et al. *An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks*. in *Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on*. 2004.

115. Shaheen, J., et al. *Confidential and Secure Broadcast in Wireless Sensor Networks*. in *Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium on*. 2007.

116. Sherman Lo, D.D.L., Dennis Akos, Paul Bradley, *Signal Authentication A Secure Civil GNSS for Today.* Inside GNSS, http://www.insidegnss.com/auto/sepoct09-Lo.pdf, 2009: p. 30-39.

117. Smith, R.E., *Authentication: from passwords to public keys*. 2002: Addison-Wesley. 255–284.

118. Soh, B. and A. Joy. *A novel Web security evaluation model for a one-time-password system*. 2003.

119. Stallings, W., *Cryptography and Network Security: Principles and Practice (2nd).* CRYPTOGRAPHY AND NETWORK SECURITY: PRINCIPLES AND PRACTICE, XX, XX, 1998: p. 163-205.

120. Stamm, S., Z. Ramzan, and M. Jakobsson, *Drive-by pharming.* Information and Communications Security: p. 495-506.

121. Steiner, J.G., C. Neuman, and J.I. Schiller. *Kerberos: An authentication service for open network systems*. in *in Proc. Winter USENIX conference*. 1988. dallas: Citeseer.

122. Takagi, H. and L. Kleinrock, *Optimal Transmission Ranges for Randomly Distributed Packet Radio Terminals.* Communications, IEEE Transactions on, 1984. **32**(3): p. 246-257.

123. Takesue, M. *A Protection Scheme against the Attacks Deployed by Hiding the Violation of the Same Origin Policy*. in *Emerging Security Information, Systems and Technologies, 2008. SECURWARE '08. Second International Conference on*. 2008.

124. Tan, H., et al. *Secure multi-hop network programming with multiple one-way key chains*. 2008: ACM.

125. Tao, P., et al. *Wireless LAN location-sensing for security applications*. 2003: ACM.

126. Ting-Chao, H. and L. Victor, *Transmission Range Control in Multihop Packet Radio Networks.* Communications, IEEE Transactions on, 1986. **34**(1): p. 38-44.

127. Tong, Z. and K. Chakrabarty. *Authentication of sensor network flooding based on neighborhood cooperation*. in *Wireless Communications and Networking Conference, 2006. WCNC 2006. IEEE*. 2006. In Proc. of ACM MOBIHOC'05.

128. Walter, C.D. *Longer keys may facilitate side channel attacks*. in 2004: Springer.

129. Want, R. and A. Hopper, *Active badges and personal interactive computing objects.* Consumer Electronics, IEEE Transactions on, 1992. **38**(1): p. 10-20.

130. Want, R., et al., *The active badge location system.* ACM Transactions on Information Systems (TOIS), 1992. **10**(1): p. 102.

131. Wayman, J.L., *Error rate equations for the general biometric system.* Robotics & Automation Magazine, IEEE, 1999. **6**(1): p. 35-48.

132. Wen-Chung, K. and L. Yung-Cheng. *Attack and Improvement on the One-Time Password Authentication Protocol Against Theft Attacks*. in *Machine Learning and Cybernetics, 2007 International Conference on*. 2007.

133. Wen, H.H., P. Y. R. Dyer, J. Archinal, A. Fagan, J. *Countermeasures for GPS signal spoofing*. 2005.

134. Wood, A.D. and J.A. Stankovic, *Denial of service in sensor networks.* Computer, 2002. **35**(10): p. 54-62.

135. Xin, S., et al., *Research on DoS Atomic Attack Oriented to Attack Resistance Test.*

136. Xue, F. and P.R. Kumar, *The number of neighbors needed for connectivity of wireless networks.* Wireless Networks, 2004. **10**(2): p. 169-181.

137. Yahaya, Y.H., M. Isa, and M.I. Aziz. *Fingerprint Biometrics Authentication on Smart Card*. in *Computer and Electrical Engineering, 2009. ICCEE '09. Second International Conference on*. 2009.

138. Yang, H., et al. *Toward resilient security in wireless sensor networks*. 2005: ACM.

139. Yih-Chun Hu, M.J.a.A.P., *Efficient Constructions for One-Way Hash Chains*in *Applied Cryptography and Network Security*, L.N.i.C. Science, Editor. 2005, Springer Berlin / Heidelberg. p. 423-441.

140. Zhu, F., M.W. Mutka, and L.M. Ni, *A private, secure, and user-centric information exposure model for service discovery protocols.* IEEE Transactions on Mobile Computing, 2006: p. 418-429.

141. Zogg, J.M., *GPS Basics–Introduction to the System, Application Overview.* u-blox AG, 2002.