Communications of the Association for Information Systems

Volume 17 Article 4

January 2006

Identification and Authentication: Technology and Implementation Issues

Moshe Zviran
Tel Aviv University, zviran@tau.ac.il

Zippy Erlich
The Open University of Israel

Communications of the Association for Information Systems

IDENTIFICATION AND AUTHENTICATION: TECHNOLOGY AND IMPLEMENTATION ISSUES

Moshe Zviran
Tel Aviv University
zviran@tau.ac.il

Zippy Erlich
The Open University of Israel

ABSTRACT

Computer-based information systems in general, and Internet e-commerce and e-business systems in particular, employ many types of resources that need to be protected against access by unauthorized users. Three main components of access control are used in most information systems: identification, authentication, and authorization. In this paper we focus on authentication, which is the most problematic component. The three main approaches to user authentication are: knowledge-based, possession-based, and biometric-based. We review and compare the various authentication mechanisms of these approaches and the technology and implementation issues they involve.

Our conclusion is that there is no silver bullet solution to user authentication problems. Authentication practices need improvement. Further research should lead to a better understanding of user behavior and the applied psychology aspects of computer security.

Keywords: information systems security, identification, authentication, authorization, passwords, question-and-answer passwords, primary passwords, secondary passwords, associative passwords, cognitive passwords

I. INTRODUCTION

The use of the Internet and other information technologies is an integral part of business strategy. With so many companies taking advantage of these technologies for their own information systems, for business exchange, and for e-commerce, the security problems that their use entails is an issue of primary concern if their potential is not to be limited. Information systems in general and Internet information systems in particular need to ensure that only the intended users can access their resources. The three main components of access control identification, authentication, and authorization, are closely related. In security systems, however, they should be operated apart. Failure to do so can lead to serious security problems [Auernheimer and Tasi, 2005].

Identification – "Who are you?" – Users supply information to identify themselves, such as name, username, and user ID. Supplying identification information does not prove that the user is who he says he is.

Authentication – "Prove your identification" – The user verifies her identity. Some examples of authentication mechanisms are user-selected passwords, system-generated passwords, passphrases, question-and-answer passwords, tokens, and various biometrics characteristics. For most systems, identification and authentication are the first line of defense to prevent unauthorized users from entering the system.

Authorization – "What you are allowed to do" – The system determines what the identified and authenticated user can actually access and what operations he is allowed to carry out. Authorization is based on predefined criteria and user profiles.

These three components of access control can be found in almost all information systems. The most problematic is the authentication component. The traditional and conventional approaches for authorization and access control [Pernul, 1995], are not appropriate for addressing the requirements of networked Internet or distributed information systems [Lopez et al., 2004]. Other technologies and approaches need to be considered [Adams and Lloyd, 1999; Ashley and Vandenwauver, 1999; Oppliger, 2002].

The traditional and by far most widely used form of authentication is the password. However, as the number of systems used by individual users grows and the number of passwords required increases, users tend to duplicate their passwords and cause the domino effect of password reuse [Ives et al., 2004], namely, all the systems with the same password are no more secure than the weakest system using this password.

In this paper we review and compare the three main approaches to authentication and their methods, as well as technology and implementation issues concerning these methods.

II. AUTHENTICATION

Most computer systems are protected through a process of user identification and authentication [Garfinkel and Spafford, 1996]. While identification is usually non-private information provided by the user to identify herself and can be known by system administrators and other system users, authentication provides secret, private information. The authentication methods can be divided into three types [Menkus, 1988]:

- What the user knows (e.g. password, PIN (personal identification number), question-and-answer), referred to as knowledge-based authentication. It is based on private information supplied by the user.
- What the user has (e.g. memory card and smart card tokens), referred to as possession-based authentication. It is based on private objects that the user possesses.
- What the user is (e.g. fingerprint, iris scan, signature dynamics), referred to as biometric-based authentication. It is based on anatomical, physiological, or behavioral characteristics.

Figure 1 describes identification and the three authentication types.

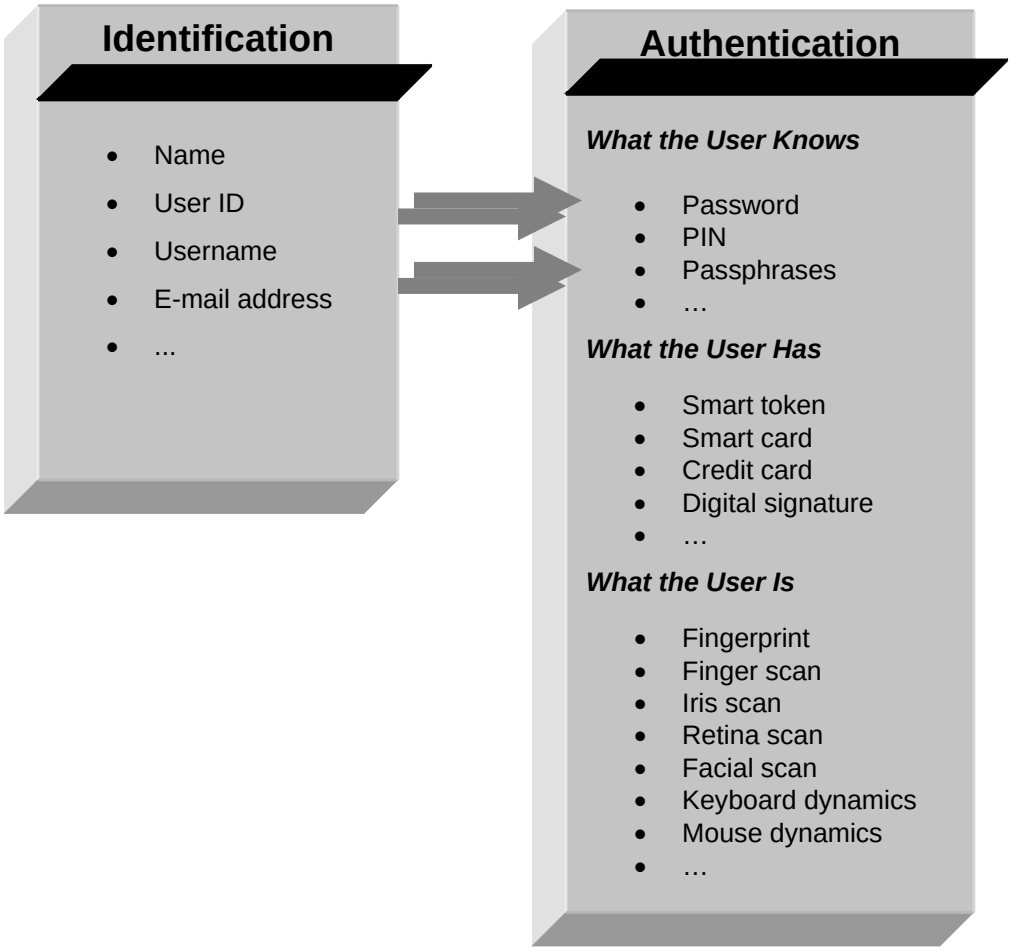

Figure 1. Identification and Authentication Types

While it may appear that any of these types can provide efficient authentication, each exhibits its own benefits and drawbacks. Tradeoffs need to be made among security, ease of use, and ease of administration.

The authentication types can be used alone or in combination. If one type is being used, it is referred to as one-type or single-factor authentication; if two types are used, it is two-type or two-factor authentication; and if all three types are used, it is referred to as three-type or multi-factor authentication. For the authentication process to be considered strong, it must be at least two-type.

KNOWLEDGE-BASED AUTHENTICATION

The most widely used type of authentication is knowledge-based authentication. Examples of knowledge-based authentications are passwords, pass-phrases or pass-sentences [Spector and Ginzberg, 1994], graphical passwords [Blonder, 1996; Davis et al., 2004; Thorpe and van Oorschot, 2004; Wiedenbeck et al., 2005], pass-faces [Brostoff and Sasse, 2000] and PINs. The traditional and by far most widely used form of authentication based on the user's knowledge is the password [Cooper, 1989; Zviran and Haga, 1993].

A password is conceptually simple for both system designers and end users. It consists of a secret series of characters according some predefined rules. The user ID and password pair serves for user identification and authentication to ensure that unauthorized users do not access the system and to block unauthorized access to the computing resources. In most systems it can provide effective protection if it is used correctly.

However, passwords are known to suffer from several pitfalls due to human information processing limitations [Jobusch and Oldehoeft, 1989a, 1989b; Hitchings, 1995; Adams and Sasse, 1999; Sasse et al., 2001; Carstens et al., 2004: Yan et al., 2004, 2005].

1. The tradeoff between memorizing and safety. Passwords should be difficult to guess and easy to remember [Barton and Barton, 1984; Pfleeger, 1989]. Unfortunately, difficult to guess and crack passwords are difficult to remember and easy to remember passwords are easy to guess and crack. That poses a dilemma in the generation of passwords. The most secure password is a random string of characters, such as qktPew3# [Porter, 1982; Wood, 1983; Barton and Barton, 1984; Garfinkel and Spafford, 1996]. Such passwords are difficult to guess by others, but are difficult to remember. To remember them, users write them down [Paans and Herschberg, 1987], which reduces their secrecy. Moreover, most users have multiple passwords for different systems and applications, forcing them to remember several passwords [Adams and Sasse, 1999]. To help them remember, they usually choose meaningful strings such as name, nickname, or initials [Barton and Barton, 1984; Menkus, 1988; Riddle et al., 1989; Adams and Sasse, 1999], which are easy to remember but also easy to crack.

2. Follow rules. To improve password security, the following rules are suggested for choosing and maintaining passwords [Smith, 2002]:

- *Non-dictionary and no-name passwords* – a non-dictionary word prevents the use of dictionary-based attacks. The only way to identify non-dictionary or no-name passwords is by using brute force, which requires testing all the possible combinations of characters for every length of password.

- *Long enough passwords with mixed types of characters* – passwords with at least eight characters with upper and lower case letters, numbers and special symbols. Long passwords with mixed types of characters increase the number of possible combinations that need to be tested in the brute force method.

- *Password aging and not reusing* – periodic changing and not reusing passwords forces the intruder to identify a new password each time. Thus, it is good practice to establish a password aging policy that forces users to change passwords periodically, but not too frequently, to avoid irritating users.

- *Complex yet easy to remember passwords* – passwords based on data structures that users are accustomed to remembering, like creating acronyms from a personal sentence known only to the user [Carstens et al., 2004; Yan et al., 2005], or the use of certain elements such as rhymes that make the password more memorable. Yan et al. [2005] observed that passwords based on mnemonic phrases are just as hard to crack as random passwords yet are just as easy to remember as naïve user selections.

- *Passwords should not be shared and should not be written* – writing down or sharing passwords harms their secrecy.

Passwords that follow these suggestions are more effective, more difficult to identify, and harder to determine by cracking utilities. To improve their security, the strength of passwords should be verified by the system administrators using password cracking programs like dictionary attack programs and/or brute force attack programs. It is common practice for system administrators to invoke reactive password checkers to identify weak passwords or to use proactive checkers to filter out certain classes of weak passwords when the user inputs the password for the first time

[Bishop and Klein, 1995]. Also, password files should be protected properly and the passwords should be encrypted or hashed.

3. Human authentication. Some mechanisms ensure human authentication and protect against automated programs used by attackers. An example of such a mechanism is the one used by Microsoft Hotmail™, which introduces a picture with some character set and asks the user to identify the character set in the picture, as shown in Figure 2. This mechanism is based on the presumption that in most cases an automated program cannot recognize the characters in the picture.

One way to overcome the problem of sniffing passwords when authentication is done over the Internet is by one-time password which can be implemented using smart cards – a possession-based authentication discussed below.

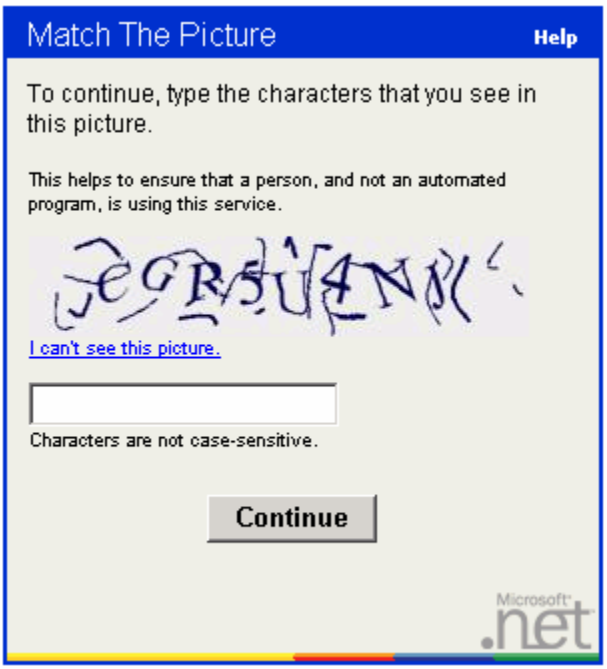

Figure 2. Microsoft Hotmail™ Check to Ensure Human Identification

TYPES OF PASSWORDS

Password types are categorized in several ways. One categorization is into primary and secondary passwords, according to their level of authentication.

Primary and Secondary Passwords

Passwords that are used as the first level of authentication, allowing access to the information system resources through the operating systems, are commonly referred to as primary passwords [Ahituv et al., 1987; Pfleeger, 1989]. Passwords that are used as the second level of authentication, for further control and protection of multilevel access to segments of these resources, sensitive applications, or data files, are commonly referred to as secondary passwords [Haga and Zviran, 1991; Zviran and Haga, 1993]. While the mechanisms employed in primary passwords are determined by the operating system manufacturer, information systems designers can select any password mechanism for secondary passwords.

The format of primary passwords determined by the operating system manufacturer uses system-generated passwords or user-generated passwords with some predefined rules. With system-generated passwords, a password is automatically generated by the operating system and assigned to a user. User-generated passwords are shown to be easier to remember but less secure than system-generated passwords because they are easier to guess [Lopez et al., 2004].

Question-and-Answer Passwords

Question-and-answer passwords are also called secret questions or security questions. Used mostly as a secondary password, they involve a dialogue between the user and the system where the user responds to a set of brief questions about personal facts, opinions, and cues.

Thus, in Microsoft Hotmail™, when a user opens a new account, after entering the primary password, she must also enter the question-and-answer password (the secret question), as shown in Figure 3. This password is mainly used when the user forgets her primary password and wants the system to help her to recall it.

Question-and-answer passwords were suggested as a method of overcoming the difficulty of remembering passwords. In a typical question-and-answer session, a user is presented with several randomly selected questions from a set of questions stored in his profile in the operating system. Access to a system or a particular application is granted only upon a match between the user's answers and those stored in the profile.

The two main methods of question-and-answer passwords are: cognitive passwords and associative passwords, also called word association passwords [Smith, 1987; Haga and Zviran, 1991; Zviran and Haga, 1993; Bunnell et al., 1997; Pond et al., 2000].

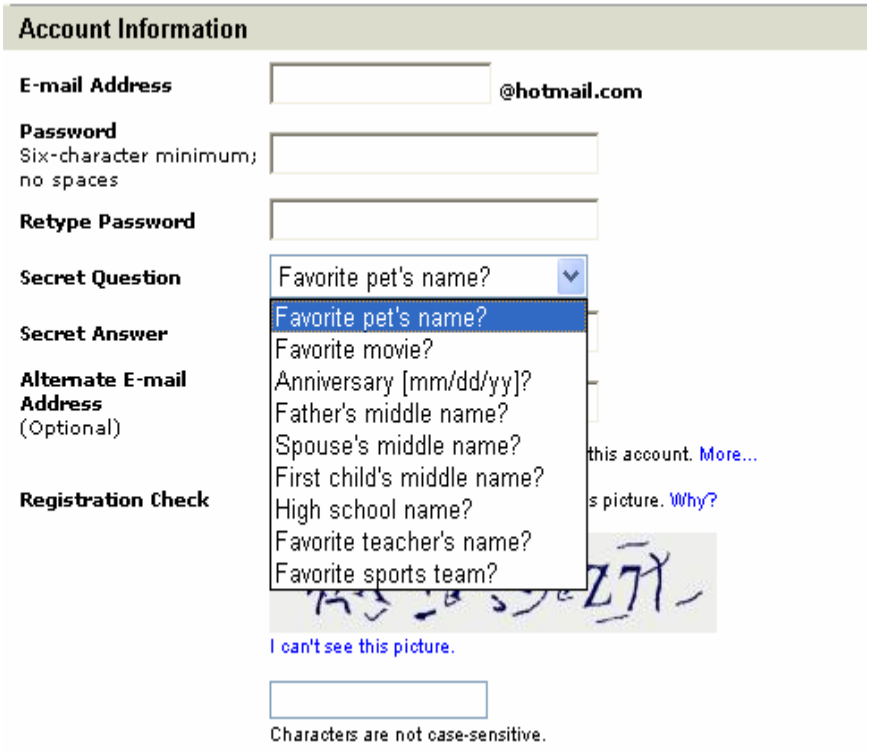

Figure 3. Microsoft Hotmail™ Secondary Question-And-Answer Password

Cognitive passwords. A cognitive password is something the user need not try to remember, he just knows it. In cognitive passwords, the user provides the system with answers to personal fact-based or opinion-based questions [Haga and Zviran, 1989], such as the user's mother's maiden name (fact-based) or user's favorite type of music (opinion-based). Because cognitive passwords were found to be easier to recall than conventional passwords and difficult to guess when selected properly, they are recommended as a way to overcome the difficulty of composing effective passwords [Zviran and Haga, 1990a, 1990b, 1993].

Bunnell et al. [1997] and Zviran and Haga [1990a, 1990b, 1993] found similar high recall rates for fact-based and opinion-based cognitive items. They also found similar low guessing rates for opinion-based cognitive items. However, Bunnell et al. [1997] found a guessing rate for fact-based items to be much higher than that obtained by Zviran and Haga [1990a, 1993], which led them to the conclusion that guessability for such items is too high unless items are carefully selected. Podd et al. [1996] also found high recall rates for cognitive items similar to those obtained by Zviran and Haga [1990a, 1990b, 1993]. They found unacceptably high guessing rates for fact-based cognitive items and acceptable guessing and recall rates for the best of the opinion-based items. Bunnell et al. [1997] found that fact-based cognitive items were better recalled than opinion-based items.

Thus, carefully selected cognitive items can yield acceptable recall and guessing rates. In tandem with a conventional password, they could improve security.

Associative passwords. In associative passwords, new users are asked to provide the system with a set of word associations, consisting of both cues and their unique associated responses [Smith, 1987]. To access the system, users must provide the correct associated responses to rotating cues sampled from the set of cues that were provided to the system. Smith [1987] argued for improved security with a secondary technique, like an associative password, rather than increasing password complexity. Research, however, yielded inconsistent results about recall and guessing associative passwords [Pond et al., 2000].

Pond et al. [2000] studied the effect of three different formulation techniques of associated passwords on recall rates:

- *Response only* – respondents are provided with cue words and are required to generate an associated response for each cue;
- *Cues and responses* – respondents generate both cues and associated responses;
- *Theme* – respondents generate both cue and response words having first decided upon a theme for their word association.

No statistically significant differences in recall and guessing rates were found among the three techniques, leading to the tentative conclusion that the effect of these formulation techniques on ease of recall is small.

Associative passwords require more research to isolate the best method of generating them [Bunnell et al., 1997; Pond et al., 2000].

Comparison of Knowledge-based Passwords

This subsection compares the findings of three studies of knowledge-based passwords.

In measuring the recall of self-generated passwords, system-generated passwords, passphrases, cognitive passwords, and associative passwords, Zviran and Hega [1993] found that the recall rate of associative passwords was more than double the recall rate for the other three. In addition, cognitive passwords resulted in a slightly higher recall rate than associative passwords.

In comparing recall and guessing rates for conventional, cognitive, and associative passwords, Podd et al. [1996] found that associative passwords produced low guessing rates but also low

recall rates, whereas cognitive passwords produced the highest recall rates but also a high guessing rate.

Recall and guessing rates for several types of knowledge-based passwords were studied by Bunnell et al. [1997]. They examined:

- conventional passwords (including user self-generated and assigned system-generated)
- cognitive passwords (including fact-based and opinion-based), and
- associative passwords.

They found that conventional self-generated and assigned system-generated passwords resulted in relatively high recall rates coupled with relatively low guessability rates. The guessability rates for the fact-based and opinion-based cognitive items were high. The fact-based cognitive items yielded the highest recall rates but their guessability rate was much too high. However, the best fact-based and opinion-based items resulted in relatively low guessability and reasonably high recall rates. On the other hand, associative items produced low guessability rates but also relatively poor recall rates.

POSSESSION-BASED AUTHENTICATION

Authentication based on what the user has is referred to as possession-based or token-based authentication. It makes use mainly of physical objects that a user possesses, like tokens. However, presentation of a valid token does not prove ownership because it may have been stolen or duplicated by sophisticated fraudulent means [Svigals, 1994]. Tokens also create problems of administration and are inconvenient for users to carry around.

Types of Tokens

Tokens are usually divided into memory tokens and smart tokens.

Memory tokens. Memory tokens store information but do not process it. Special devices are needed to write and read the data to and from the tokens. The most common type of memory token is the magnetic card, which is used mostly for authentication together with a knowledge-based authentication mechanism such as the user's PIN. Memory tokens are inexpensive to produce. Using them with PINs provides significantly more security than PINs or passwords alone.

Smart tokens. Unlike memory tokens, smart tokens incorporate one or more embedded integrated circuits which enable them to process information. Like memory tokens, most smart tokens are used for authentication together with a knowledge-based authentication mechanism such as the user's PIN. Of the various types of smart tokens, the most widely used are those that house an integrated chip containing a microprocessor. The smart cards are used in the identification and authentication processes, both in networked and stand-alone computer systems. Their portability and cryptographic capacity led to their wide use in many e-commerce applications [Juang, 2004]. When using smart cards for authentication, the card must first be physically presented to the computer system. Then authentication of the card by the system is performed, a process that usually involves execution of cryptological algorithms.

Authentication schemes proposed for enhancing the efficiency and security of smart cards include:

1. Timestamp-based authentication schemes to prevent malicious replay attacks in networks [Yang and Shieh, 1999; Chan and Cheng, 2000; Hwang and Li, 2000; Sun, 2000; Lee, Li and Hwang, 2002; Lee, Hwang and Yang, 2002; Chan and Cheng, 2002; Fan et al., 2002; Wu and Chieu, 2003; Jiang et al., 2004; Wu and Chen, 2004; Yang and Wang, 2004].

2. Juang [2004] suggested an efficient password authenticated key agreement using smart cards. The main merits of his scheme are:

- no password or verification table is required in the server;
- users can freely choose their own passwords;
- communication and computation costs are low;
- it requires mutual authentication (user-server); and
- it incorporates a key agreement mechanism by generating a session key agreed on by the user and the server.

Due to their complexity, smart tokens are more expensive than memory tokens but they provide greater flexibility and security and are more difficult to forge. Because of their high security level, smart tokens are also used for one-time passwords for authentication across an open network.

BIOMETRIC-BASED AUTHENTICATION

We refer to authentication based on what the user *is* as *biometric-based* authentication; namely, automatic identification using certain anatomical, behavioral, and physiological features and characteristics associated with the user [Kim, 1995; Prabhakar et al., 2003].

Biometric authentications are based on physiological or behavioral characteristics that reliably distinguish one person from another. Thus, it is possible to establish an identity based on who the user is, rather than by what the user possesses or knows and remembers. Biometrics includes both the collection and the comparison of these characteristics. A biometric system can be viewed as a pattern recognition system consisting of three main modules:

- the sensor module,
- the feature extraction module, and
- the feature matching module.

The users' personal attributes are captured and stored in reference files to be compared for later authentication to determine if a match exists. The biometric system is composed of biometric data of the captured users' personal attributes necessary to perform user authentication and the software and hardware required to collect, store, and process the biometric data.

Biometric authentications are technically complex and usually expensive because they require special hardware. They are quite secure, but are not widely accepted by users because they are perceived to be intrusive and an encroachment on personal privacy through automated means. They also raise ethical issues [Alterman, 2003], such as potential misuse of the personal biometrics for tracking and monitoring productivity [Deane et al., 1995]. Their main use is in systems requiring a high level of security.

The emergence of biometrics addressed the problems that plague traditional verification methods. They provide the most effective and accurate identification method because they cannot easily be stolen or shared. Biometric systems also enhance user convenience by alleviating the need to design and remember passwords. However, while convenient, the digital scan or pattern is vulnerable to network analysis and once stolen, cannot be used any more [Ives et al., 2004].

All biometric technologies inherently suffer from some level of false match or false non-match [Matyas and Stapleton, 2000]. False match is a type II error –accepting a match when there is no match. False non-match is a type I error –rejecting the match when there is a match. Biometric

errors can occur for several reasons: the capture device might be dirty, the lighting might be poor, and the system might not adjust well to different environmental factors such as sun, cold, or glare [O'Gorman, 2003], and also due to the user's physiological changes because of surgery and other conditions. Thresholds of acceptance for any of the biometric techniques depend on the level of security required by the computer system. A high-security system, like a finance or health system, will minimize the false match (type II error) rate at the expense of increasing the false non-match (type I error) rate. A low-security system will minimize the false non-match rate at the expense of increasing the false match rate.

Physiological and Behavioral Biometrics

Biometrics are usually divided into two main categories: *physiological and behavioral biometrics.*

Physiological biometrics

Physiological biometrics are based on the user's stable physical attributes. The best known are:

Fingerprint – a computerized version of the traditional fingerprint identification system, based on the surface of curves formed by the ridges on a fingertip. It generates much information, which requires a large amount of storage [Roddy and Stosz, 1997]. Biometric devices that read fingerprints and plug into USB ports are widely available [Auernheimer and Tasi, 2005].

Finger scan – based on the extract of specific features from finger print data, they store and use selective points on the fingerprint. Finger scan collects and uses a smaller amount of data than fingerprint data.

Hand geometry – based on measures of the physical shape and dimensions of the hand. The method uses a small camera.

Iris scan – based on the unique pattern, rings, and corona in the iris using a snapshot of the iris, taken by a camera. It requires the camera to be properly placed so that the sun does not shine into its aperture.

Retina scan – based on the pattern of the blood vessels on the backside of the eyeball. The iris scan is more acceptable than the retina scan because it requires only a glance while the retina scan blows air into the eye.

Facial scan – based on attributes of the face, bone structure, nose ridges, and eye width [Li and Jain, 2005].

Fingerprints continue to be the most widely used physiological characteristic in systems that automatically recognize a user's identity [Jones, 2000; Maltoni et al., 2003; Wayman et al., 2004; Ratha and Bolle, 2005]. An example of one of its up to date applications is the use of fingerprint-based identification and authentication to support on-line, web-based course examinations [Auernheimer and Tasi, 2005].

Behavioral biometrics

Behavioral biometrics are based on user behavioral attributes that are learned movements. The best known are:

Keystroke or keyboard dynamics and *signature dynamics* – based on the different typing dynamics, they try to capture the electrical signals for speed and movements while users are typing or signing [Obaidat and Sadoun, 1997].

Mouse dynamics is similar to keyboard and signature dynamics in that users can be identified by the way in which they use the mouse. This method was found to be less effective than keyboard and signature dynamics [Guven and Sogukpinar, 2003].

Speech or voice verification – based on the user's voice pattern, when speaking into the computer's microphone, it recognizes subtle differences in speech sounds and patterns. Speech is usually categorized as behavioral because it is a product of learned behavior, although the underlying body feature upon which speech is based is a vocal apparatus, which is physical and relatively stable [O'Gorman, 2003].

III. COMPARING THE THREE AUTHENTICATION TYPES

The factors that need to be considered when choosing an authentication method are [Furnell et al., 2000]:

- effectiveness,
- ease of implementation,
- ease of use, and
- user attitude and acceptance.

The knowledge-based authentication method is inexpensive and easy to implement and change. Unfortunately it is also the easiest to compromise and is less secure than tokens or biometric-authentication methods, which are inherently more secure. On the other hand, tokens and biometric-authentication methods are more expensive to implement. User's prefer knowledge-based authentication and do not like biometric-based authentication.

Table 1 shows the ranking of the three authentication types according to the four factors.

Table1. Authentication Types and Their Ranking

Type of authentication	**Effectiveness**	**Ease of implement-ation**	**Ease of use**	**User attitude**
Knowledge-based	Low	High	High	High
Possession-based	Medium	Medium	Medium	Medium
Biometric-based	High	Low	Low	Low

Because knowledge-based authentication is less effective than the other two types, it is recommended that it be used as part of a two-type authentication. For example, authentication can be based on a password and token or it can be based on a password and keystroke [Furnell et al., 2004, Yu and Cho, 2004].

IV. SUMMARY AND CONCLUSIONS

No silver bullet solution exists to user authentication problems. Computer systems are protected by three main types of authentication methods: knowledge-based, possession-based, and biometric-based. Each of these offers both benefits and drawbacks. Multiple layers of protection provide substantially better security. When choosing an authentication method, the tradeoff

among security effectiveness, ease of implementation, ease of use, and user attitude and acceptance needs to be considered.

As long as passwords are comparatively inexpensive, simple to use, and attractive to users, they will probably continue to be employed in low to medium security information systems for the foreseeable future. When properly managed in a controlled environment, they can provide effective security.

Further research is needed on the three authentication types to improve and enhance their technologies and to enable the design of more usable and effective security systems.

REFERENCES

Adams, A. and M. A. Sasse (1999) "Users are Not the Enemy: Why Users Compromise Security Mechanisms and How to Take Remedial Measures," *Communications of the ACM,* 42(12), pp. 40-46.

Adams, C. and S. Lloyd (1999) *Understanding Public-Key Infrastructure: Concepts, Standards and Deployment Considerations*, Indianapolis, IN: Macmillan Technical Publishing,

Ahituv, N., Y. Lapid, and S. Neumann (1987) "Verifying the Authentication of an Information System User," *Computers and Security*, 6(2), pp. 152-157.

Alterman, A (2003) "A Piece of Yourself: Ethical Issues in Biometric Identification", *Ethics and Information Technology*, 5(3), pp. 139-150.

Ashley, P. and M. Vandenwauver (1999) *Practical Intranet Security: Overview of the State of the Art and Available Technologies*, Norwell, MA: Kluwer Academic Publishers.

Auernheimer, B. and M. J. Tasi (2005) "Biometric Authentication for Web-based Course Examinations," *Proceedings of the 38th Annual Hawaii International Conference on System Science* (HICSS'05), pp. 294-300.

Barton, B. F. and M. S. Barton (1984) "User-Friendly Password Methods for Computer-Mediated Information Systems," *Computers and Security*, 3(3), pp. 186-195.

Bishop, M. and D. Klein (1995) "Improving System Security Through Proactive Password Checking," *Computers and Security*, 14(3), pp. 233-249.

Blonder, G. E. (1996) Graphical Passwords. United States Patent 5559961.

Brostoff, S. and M A. Sasse (2000) "Are Passfaces more Usable than Passwords? A Field Trial Investigation," in S. McDonald, Y. Waern, and G. Cockton (Eds.), *People and Computers XIV - Usability or Else*! *Proceedings of HCI2000*, Sunderland, Springer, UK, pp. 405-424.

Bunnell, J., J. Podd, R. Henderson, R. Napier, and J. Kennedy-Moffat (1997) "Cognitive, Associative and Conventional Passwords: Recall and Guessing Rates," *Computers and Security*, 16(7), pp. 629-641.

Carstens, D. S., P. R. McCauley-Bell, L. C. Malone, and R. F. DeMara (2004) "Evaluation of the Human Impact of Password Authentication Practices on Information Security," *Information Science Journal*, 7(1), pp. 67-85.

Chan, C. K. and L. M. Cheng (2000) “Cryptanalysis of a Remote User Authentication Scheme Using Smart Cards,” *IEEE Trans. Consumer Electronic,* 46(4), pp. 992-993.

Chan, C. K. and L. M. Cheng (2002). "Cryptanalysis of a Timestamp-based Password Authentication Scheme," *Computer Security*, 21(1), pp. 74-76.

Cooper, J. (1989) *Computer and Communications Security*, New York: McGraw-Hill.

Davis, D., F. Monrose, and M. Reiter (2004). “On User Choice in Graphical Password Schemes,” *Proceedings of the 13th USENIX Security Symposium*, San Diego, CA.

Deane, F., K. Barrelle, R. Henderson, and D. Mahar (1995). "Perceived Acceptability of Biometric Security Systems," *Computers and Security* 14(3), pp. 225-231.

Fan L., J. H. Li, and H. W. Zhu (2002) "An Enhancement of Timestamp-based Password Authentication Scheme," *Computers and Security*, 21(7), pp. 665-667.

Furnell, S. M., P. S. Dowland, M. H. Illingworth, and P. L. Reynolds (2000) "Authentication and Supervision: A Survey of User Attitudes," *Computers and Security* 19(6), pp. 529-539.

Furnell, S. M., I. Papadopoulos, and P. S. Dowland (2004) "A Long-Term Trial of Alternative User Authentication Technologies," *Information Management and Computer Security*, 12(2), pp. 178-190.

Garfinkel, S. and G. Spafford (1996) *Practical Unix and Internet Security*, Sebastopol, CA: O'Reilly & Associates,.

Guven, A. and I. Sogukpinar (2003) "Understanding Users' Keystroke Patterns for Computer Access Security," *Computers & Security,* 22(8), pp. 695-706.

Haga, W. J. and M. Zviran (1989) "Cognitive Passwords: From Theory to Practice," *Data Processing and Communications Security*, 13(3), pp. 19-23.

Haga, W. J. and M. Zviran (1991) "Question-and-Answer Passwords: An Empirical Evaluation," *Information Systems*, 16(3), pp. 335-343.

Hitchings, J. (1995) "Deficiencies of the Traditional Approach to Information Security and the Requirements for a New Methodology," *Computers and Security*, 14(5), pp. 377-383.

Hwang, M. S. and L. H. Li (2000) "A New Remote User Authentication Scheme Using Smart Cards," *IEEE Transactions on Consumer Electronics,* 46(1), pp. 28-30.

Ives, B., K. R. Walsh, and H. Schneider (2004) "The Domino Effect of Password Reuse," *Communications of the ACM*, 47(4), pp. 75-78.

Jiang, R., L. Pan, and J. H. Li (2004) "Further Analysis of Password Authentication Schemes Based on Authentication Tests," *Computers and Security*, 23(6), pp. 469-477.

Jobusch, D. L. and A. E. Oldehoeft (1989a) "A Survey of Password Mechanisms: Weaknesses and Potential Improvements, Part 1," *Computers and Security***,** 8(7), pp. 587-604.

Jobusch D. L. and A. E. Oldehoeft (1989b) "A Survey of Password Mechanisms: Weaknesses and Potential Improvements, Part 2," *Computers and Security***,** 8(8), pp. 675-689.

Jones, G. W. (2000) *Introduction to Fingerprint Comparison*, Springer, New York.

Juang, W. S. (2004). "Efficient Password Authenticated Key Agreement Using Smart Cards," *Computers and Security*, 23(2), pp. 167-173.

Kim, H. J. (1995). "Biometrics, Is it a Viable Proposition for Identity Authentication and Access Control?," *Computers and Security*, 14(3), pp. 205-214.

Lee, C. C., L. H. Li, and M. S. Hwang (2002) "A Remote User Authentication Scheme Using Hash Functions," *ACM Operating Systems Review,* 36(4), pp. 23-29.

Lee, C. C., M. S. Hwang, and W. P. Yang (2002) "A Flexible Remote User Authentication Scheme Using Smart Cards," *ACM Operating Systems Review,* 36(3), pp. 46-52.

Li, S. Z. and A. K. Jain (Eds.) (2005) *Handbook of Face Recognition*, New York:Springer.

Li, S. Z., J. Lai, T. Tan, G. Feng, and Y. Wang (Eds.) (2004) "Advances in Biometric Person Authentication", *5th Chinese Conference on Biometric Recognition, SINOBIOMETRICS 2004*, Guangzhou, China, Proceedings Series: Lecture Notes in Computer Science, New York: Springer.

Li, S. Z., Z. Sun, T. Tan, S. Pankanti, D. Chollet, and D. Zhang (Eds.) (2005) "Advances in Biometric Person Authentication," *International Workshop on Biometric Recognition Systems, IWBRS 2005*, Beijing, China, Proceedings Series: Lecture Notes in Computer Science, Vol. 3781, Springer, NY.

Lopez, J., R. Oppliger, and G. Pernul (2004) "Authentication and Authorization Infrastructures (AAIs): A Comparative Survey," *Computers and Security*, 23(7), pp. 578-590.

Maltoni, D., D. Maio, A. K. Jain, and S. Prabhakar (2003) *Handbook of Fingerprint Recognition*, New York" Springer.

Matyas, S. M. and J. Stapleton (2000) "A Biometric Standard for Information Management and Security," *Computers and Security*, 19(5), pp. 428-441.

Menkus, B. (1988) "Understanding the Use of Passwords," *Computers and Security*, 7(2), pp. 132-136.

Obaidat, M. and B. Sadoun (1997) "Verification of Computer Users Using Keystroke Dynamics," *IEEE Transactions on Systems, Man, and Cybernetics. Part B: Cybernetics,* 27(2), pp. 261-269.

O'Gorman, L. (2003) "Comparing Passwords, Tokens, and Biometrics for User Authentication," *Proceedings of the IEEE*, 91(12), pp. 2019-2040.

Oppliger, R. (2002) *Security Technologies for the World Wide Web* (2nd ed.), Artech House Publishers, Norwood, MA.

Paans, R. and I. S. Herschberg (1987) "Computer Security: The Long Road Ahead," *Computers and Security*, 6(5), pp. 403-416.

Pernul, G. (1995) "Information Systems Security: Scope, State-of-the-Art, and Evaluation of Techniques," *International Journal of Information Management*, 15 (3), pp. 242-256.

Pfleeger, C. P. (1989). *Security in Computing*, Englewood Cliffs, NJ: Prentice-Hall.

Podd, J., J. Bunnell, and R. Henderson (1996) "Cost-Effective Computer Security: Cognitive and Associative Passwords," in J. Grundy & M. Apperley (Eds.), Proceedings of the Sixth Australian Conference on Computer-Human Interaction (OZCHI '96), pp. 304-305.

Pond, R., J. Podd, J. Bunnell, and R. Henderson (2000) "Word Association Computer Passwords: The Effect of Formulation Techniques on Recall and Guessing Rates," *Computers and Security*, 19(7), pp. 645-656.

Porter, S. N. (1982) "A Password Extension for Improved Human Factors," *Computers and Security*, 1(1), pp. 54-56.

Prabhakar S., S. Pankanti, and A. K. Jain (2003) "Biometric Recognition: Security and Privacy Concerns," *IEEE Security and Privacy Magazine*, 1(2), pp. 33-42.

Ratha, N. and R. Bolle (Eds.) (2005) *Automatic Fingerprint Recognition Systems*, New York: Springer.

Riddle, B. L., M. S. Miron, and J. A. Semo (1989) "Passwords in Use in a University Timesharing Environment," *Computers and Security*, 8(7), pp. 569-579.

Roddy, A. R. and J. D. Stosz (1997) “Fingerprint Features: Statistical Analysis and System Performance Estimates,” *Proceedings of the IEEE*, 85(9), pp.1390-1421.

Sasse, M. A., S. Brostoff, and D. Weirich (2001) "Transforming the 'Weakest Link': A Human/Computer Interaction Approach to Usable and Effective Security," *BT Technology Journal*, 19(3), pp. 122-131.

Smith, S. L. (1987) "Authenticating Users by Word Association," *Computers and Security*, 6(6), pp. 464-470.

Smith, R. E. (2002) *Authentication: From Passwords to Public Keys*, Boston, MA: Addison-Wesley,.

Spector, Y. and J. Ginzberg (1994) "Pass-sentence: A New Approach to Computer Code", *Computers and Security*, 13(2), pp. 145-160.

Sun, H.-M. (2000) “An Efficient Remote User Authentication Scheme Using Smart Cards,” *IEEE Transactions on Consumer Electronics,* 46(4), pp. 958-961.

Thorpe, J. and P. van Oorschot (2004) "Graphical Dictionaries and the Memorable Space of Graphical Passwords," *Proceedings of the 13th USENIX Security Symposium*, San Diego, CA.

Wayman, J., A. K. Jain, D. Maltoni, and D. Maio (Eds.) (2004) *Biometric Systems: Technology, Design and Performance Evaluation*, New York: Springer.

Wiedenbeck, S., J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon (2005) "PassPoints: Design and Longitudinal Evaluation of a Graphical Password System," *International Journal of Human-Computer Studies*, 63(1-2), pp.102-127.

Wood, C. C. (1983) "Effective Information System Security with Password Controls," *Computers and Security*, 2(1), pp. 5-10.

Wu, W. C. and S. M. Chen (2004) “Weaknesses and Improvements of an Efficient Password Based User Authentication Scheme Using Smart Cards”, *IEEE Transactions on Consumer Electronic,* 50(1), pp. 204-207.

Wu, S.-T. and B.-C. Chieu (2003) "A User Friendly Remote Authentication Scheme with Smart Cards," *Computers and Security*, 22(6), pp. 547-550.

Yan, J., A. Blackwell, R. Anderson, and A. Grant (2004) "Password Memorability And Security: Empirical Results", *IEEE Security and Privacy*, 2(5), pp. 25-31.

Yan, J., A. Blackwell, R. Anderson, and A. Grant (2005) "The Memorability and Security of Passwords," in L. Cranor & S. Garfinkel (Eds.), *Security and Usability: Designing Secure Systems That People Can Use*, Sebastopol, CA: O'Reilly & Associates, pp. 121-124.

Yang, C.-C. and R.-C. Wang (2004) "Cryptanalysis of a User Friendly Remote Authentication Scheme with Smart Cards," *Computers and Security*, 23(5), pp. 425-427.

Yang, W. H. and S. P. Shieh (1999) "Password Authentication Schemes with Smart Card", *Computers and Security*, 18(8), pp. 727-733.

Yu, E. and S. Cho (2004) "Keystroke Dynamics Identity Verification - Its Problems and Practical Solutions", *Computers and Security*, 23(5), pp. 428-440.

Zviran, M. and W. J. Haga (1990a) "Cognitive Passwords: The Key to Easy Access Control", *Computers and Security*, 9(8), pp. 723-736.

Zviran, M. and W. J. Haga (1990b) “User Authentication by Cognitive Passwords: An Empirical Assessment”, *Proceedings of the IEEE Jerusalem Conference on Information Technology 1990: Next Decade in Information Technology*, pp. 137–144.

Zviran, M. and W. J. Haga (1993) "A Comparison of Password Techniques for Multilevel Authentication Mechanisms", *Journal of Computing*, 36(3), pp. 227-237.

GLOSSARY OF TERMS

Associate password: A question-and-answer password in which the user provides the system with associated responses to rotating cues.

Authentication: Users verify their identity. The three main approaches to user authentication are knowledge-based, possession-based, and biometric-based.

Authorization: The system determines what the identified and authenticated user can actually access and what operations s/he is allowed to carry out. Authorization is based on predefined criteria and user profiles.

Biometric-based authentication: Authentication based on what the user is, such as fingerprints and signature dynamics. It is based on anatomical, physiological or behavioral characteristics.

Cognitive password: A question-and-answer password in which the user provides the system with answers to personal fact-based questions such as the user’s mother’s maiden name, or opinion-based questions such as the user’s favorite type of music.

Identification: Users supply information to identify themselves, such as name, username, and user ID.

Knowledge-based authentication: Authentication based on what the user knows, such as password, PIN, and question-and-answer. It is based on private information supplied by the user.

Password: Knowledge-based authentication consisting of a secret series of characters according to some predefined rules. It is the most widely-used mechanism of authentication.

Possession-based authentication: Authentication based on what the user has, such as memory cards and smart card tokens. Possession-based authentication is also referred to as token-based authentication. It is based on private objects that the user possesses.

Primary password: Password that is used as the first level of authentication, allowing access to the information system resources through the operating system.

Question-and-answer password: A session in which a user is presented with several randomly selected questions from a set of questions stored in the user’s profile in the operating system. The user’s answers are compared to those stored in the profile. Used mostly as a secondary password. The two main types of question-and-answer passwords are cognitive passwords and associative passwords.

Secondary password: Password that is used as the second level of authentication, for further control and protection of multilevel access to segments of resources, sensitive applications, or data files.

System-generated password: Password that is automatically generated by the operating system and assigned to a user.

Token-based password: See possession based authentication.

User-generated password: Password that is generated by the user according to some system predefined rules.

ABOUT THE AUTHORS

Moshe Zviran is Associate Professor of Information Systems in the Faculty of Management, The Leon Recanati Graduate School of Business Administration, Tel Aviv University. He received his B.Sc. degree in mathematics and computer science and the M.Sc. and Ph.D. degrees in information systems from Tel Aviv University, Israel, in 1979, 1982 and 1988, respectively. He previously held academic appointments at Claremont Graduate University, California, the Naval Postgraduate School, California, and Ben-Gurion University, Israel. His research interests focus on the management of the information resource and information systems security. Prof. Zviran's research is published in *MIS Quarterly, Communications of the ACM, Communications of AIS, Journal of Management Information Systems, IEEE Transactions on Engineering Management, Information and Management, Omega, The Computer Journal and other journals*. He is co-author (with N. Ahituv and S. Neumann) of *Information Systems for Management* (Tel-Aviv, Dyonon, 1996) and *Information Systems – from Theory to Practice* (Tel-Aviv, Dyonon, 2001).

Zippy Erlich is on the faculty of the Computer Science department at the Open University of Israel and served as the head of the department for four years. She developed curricula for undergraduate and graduate programs of study in Computer Science and headed development teams for a variety of B.Sc. and M.Sc. courses. She received her B.Sc. degree in mathematics and statistics, M.Sc. in applied mathematics – both from Tel-Aviv University, and Ph.D. in computer science from University of California, Los-Angeles. Before joining the Open University, she headed the Data Processing department of the Israeli Navy Computer Center. Her research interests include measurement of information systems success and user satisfaction, data mining, social networks, and e-learning.

Communications of the Association for Information Systems

ISSN: 1529-3181