December 2004

Future Security Approaches and Biometrics

Serguei Boukhonine
University of Houston

Vlad Krotov
University of Houston

Future Security Approaches and Biometrics

Serguei Boukhonine
University of Houston
sboukhonine@uh.edu

Vlad Krotov
University of Houston
vokrotov@uh.edu

ABSTRACT

Threats to both physical and information security are proliferating rapidly, placing demanding requirements on security measures used to protect tangible as well as intangible assets of both businesses and individuals. Biometric-based security technologies offer the opportunity to improve security either by use on their own, or in conjunction with other technologies. This tutorial discusses biometric technologies currently in use, their actual and potential applications, their strengths and weaknesses, performance evaluation measures, and privacy concerns associated with their potential misuse.

Keywords

Biometrics, computer security, information security, privacy.

INTRODUCTION

It was not until the mid-to-late 1980s that networked computing became sufficiently ubiquitous for penetrations to become a significant problem (McHugh, 2001). The growth of the Internet, e-commerce and other computer technologies in the 1990s and beyond magnified existing threats while giving rise to new classes of threats. Driven by these threats, new security approaches, such as virtual private networks (VPN) and public key cryptography, gained widespread popularity. Biometric technology, the subject of this paper, is one of these emerging security technologies.

Security approaches are either passive or active. Passive approaches are like a shield - they protect against a clear and present danger such as a hacker attempting to access a computer system, while active approaches are more like prevention via a preemptive strike, for instance, arresting terrorists before they plant a bomb. Traditional security technologies are mostly passive. Not many technologies are suitable for active security. The only traditional way to proactively search for and identify lawbreakers has been by massive use of manpower such as police on patrol or security guards in casinos watching closed circuit television in the hopes of identifying known cheats.

Traditional access control approaches are based on either what you know (password, PIN, etc.), or what you have (keys, cards, etc.), or some combination of both (ATM card + PIN) (Ratha, Connell and Bolle, 2001). A serious flaw associated with traditional security technologies is that anybody can use them if she or he has them. Anyone having the right key can access the locked premises. Magnetic stripe cards can be easily counterfeited (Ashbourn, 2000). Even a card or a token with the most sophisticated security mechanisms can be lost, stolen or maliciously taken away and, as a result, used by an unauthorized person. Use of PINs and passwords improves the situation somewhat, but the fundamental problem with PINs is that they identify a card rather than its user (Ashbourn, 2000). In other words, the fact that a person knows the PIN associated with the card or password associated with the username may not mean that the person is actually the owner of the card or the actual user. In addition, passwords are often easy to guess (Zviran and Haga, 1999), crack by brute force, or obtain through other means such social engineering. Obtaining the card and the PIN as well as the username and the password might be difficult, but is far from impossible. Thus, card/PIN or username/password combinations provide relatively weak network security.

THE NEXT STEP IN SECURITY TECHNOLOGIES

Biometrics, a relatively new field, holds great promise to solve many security problems. Biometrics is a method of recognizing people based on unique physical or behavioral characteristics (Ashbourn, 2000; Jain, Hong and Pankanti, 2000). Clarke (1999) provides an expanded definition of biometrics: person-identification techniques based on such difficult-to-alienate characteristics as appearance (how a person looks), social behavior (how the person interacts with others through, e.g., voice, body gestures), bio-dynamics (e.g., manner in which a signature is written, key-stroke dynamics), natural physiography (e.g., skull measurement, fingerprints sets), and imposed physical characteristics (e.g. microchips implanted under skin).

HOW BIOMETRIC TECHNOLOGIES WORK

Biometric technologies are used for both authentication and identification purposes. The objective of authentication is to determine if a particular person is who she or he claims to be, for instance to cash a check. Identification systems, by contrast, capture a person's biometric information, say at an airport boarding gate, and then compare it with templates stored in a database looking for a match. Authentication systems often require active participation by the individual.

The general process for authentication systems is outlined in Figure 1. The authentication process starts with an individual inserting a smart or magnetic card into a reader (instead of a card, the user may key in his or her username). If it is a smart card, the reader reads a biometric template from the card. Otherwise, the reader reads the username. Afterwards, the user's live biometric information is captured and compared with the template either read from the smart card or obtained from the database. If the system determines that the individual is who she or he claims to be, access is granted. Otherwise, access is

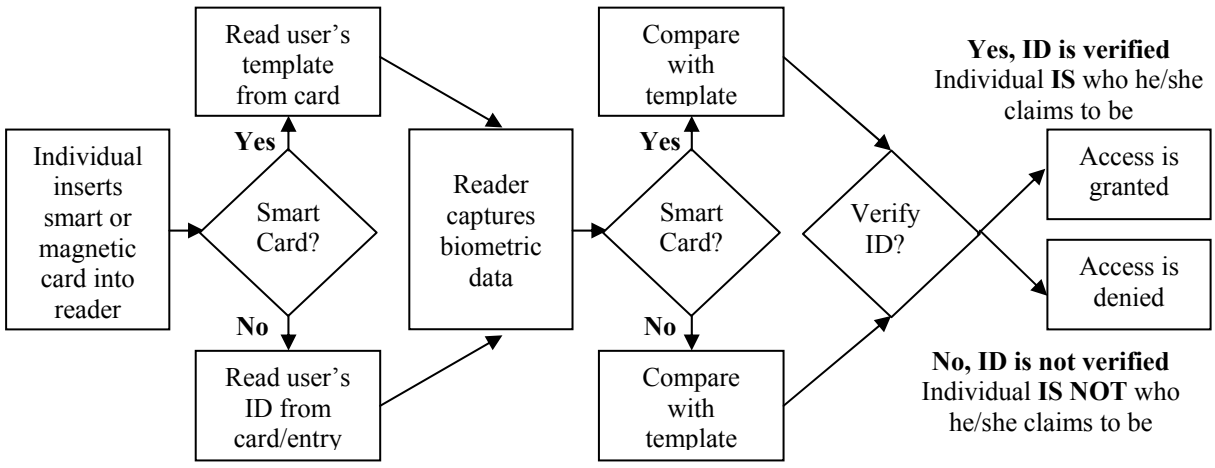

Figure 1. Biometric Authentication Algorithm

denied. While the authentication process looks like today's common security systems, biometric systems differ in several respects: 1) biometric information identifies the user of the card not the card; 2)one cannot forget biometrics as you might a PIN; 3) each person's biometrics are unique.

Identification systems are either passive to the individual (meaning they can be used without knowledge of a user) or they require the individual to provide biometric data. Figure 2 shows the process for identification systems. The individual does not identify himself or herself—the data is captured into the system and the database determines if the system knows or does not know the individual. If the individual is known, then action results, otherwise, the captured biometric data is deleted. The process of identification is also known as "one-to-many" comparison (Ashbourn, 2000). Identification systems differ from authentication systems in two ways: 1) The ability to actively look for potentially harmful individuals without their knowledge, and 2) The individual does not need to carry a card or key in the username.

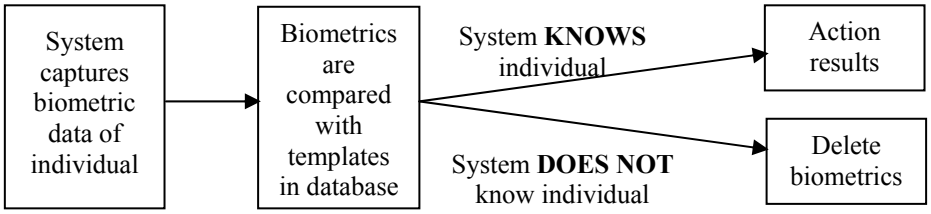

Figure 2. Biometric Identification Algorithm

TYPES OF BIOMETRIC TECHNOLOGIES

Biometric technologies can be classified according to the input data source they rely on for authentication and identification. Some of the most common body parts that are scanned by biometric systems are faces, eyes, and hands. Voice has also been widely used in such applications as automated call centers. The table below gives a brief overview of these biometric technology types.

Body Part	Type	How it works	Advantages	Disadvantages	Use Examples
Face	Face Recognition	Face recognition captures characteristics of a face either from video or still image and translates them into digital form	Suitable for identification applications; relatively unobtrusive	Prone to errors caused by environmental influences (e.g. light), sunglasses, facial hair, etc. Expensive	Identification (law enforcement) uses as well as identity authentication uses
Eyes	Retina Scanning	Captures unique pattern of blood vessels. It is extremely secure and accurate.	Secure and accurate	Expensive; requires perfect alignment: usually the user must look in monocular or binocular receptacle	Suitable for high security applications in controlled environment
	Iris Scanning	Captures unique patterns of an iris	Secure; does not need physical contact and non-intrusive	Expensive; sensitive to environmental conditions	
Voice	Voice Recognition	Captures unique characteristics of voice	Easy to use and understand; non-intrusive	Sensitive to background conditions such as noises	Automated call centers
Hands	Hand Geometry	Captures up to 90 unique hand characteristics	Easy to use and inexpensive	Balky and sensitive to environment	Access control, computer access
	Fingerprinting	Uses unique patterns known as loops, arches, and whorls.	Easy to use, inexpensive; fingerprints databases are already available	Less reliable than retina or iris scanning	Access control, computer access control.

Table 1. Human Body and Types of Biometric Technologies (based on Ashbourn, 2000)

In addition to these major techniques, other biometric techniques include vein pattern scanning, use of individual scent, measuring earlobes, facial thermograms, individual keystroke dynamics, and signature verification (Ashbourn, 2000; Schneier, 1999; Jain et al.,2000). These methodologies are less developed and are not widely used. Individual keystroke dynamics, such as speed of typing, pauses between words, and intervals between individual characters, could potentially provide on-going identity verification rather just one-time verification at the beginning of a session.

CURRENT AND FUTURE APPLICATIONS OF BIOMETRIC TECHNOLOGY

Active (Identification) Applications

Biometrics can be active or passive. An example of a system with the potential for active security is face recognition, which will allow law enforcement agencies to increase surveillance, tracking and apprehension of criminals to a previously unimaginable degree. For instance Newham, a borough in London installed 206 surveillance cameras feeding information to the FaceIt® Surveillance, a face recognition technology (Identix Inc., 2004). Images of people are constantly matched against a database of suspects and known criminals. The system was installed in November 1998. A year later assaults were down 21 percent and burglaries and vehicle related crime dropped by 39 percent.

In the wake of the September 11, 2001 attacks, the United States government began exploring new technologies for preventing acts of terror. Biometrics is one of the technologies currently used by the Department of Homeland security to identify people who might be a threat to national security. Everyone entering the United States with a visa now has fingerprints and photographs taken and scrutinized (BBC News, 2004). The American government is also planning to build a biometric identification system for America's embassies and consulates abroad so that travelers can be screened before they reach U.S. borders (Jones, 2004). This increased demand for biometric technologies may translate into a multi-billion dollar injection into the industry, bringing biometrics technologies to a higher level of efficiency with likely consequent improvements in unit costs and more widespread application. Biometrics may also be useful for active security applications in places such as casinos, shopping malls, and at sporting events.

Passive (Authentication) Applications

In addition to the active applications, passive applications include:

- *Physical access control*. Reliability of such systems will be significantly increased
- *Time and attendance monitoring*. Biometrics can cut down on cheating such as clocking in for other people
- *Benefit payment systems*. Biometrics can reliably verify the identity of a benefits recipient. It will also prevent "double dipping" when an individual uses multiple identities to defraud the system
- *PC/Network access control*. Biometrics can reliably verify user identity, preventing unauthorized access
- *ATM applications*. Biometrics will drastically reduce losses banks and consumers suffer because of ATM fraud
- *National identity cards*. The U.S., Canada. U.K., China, Hong Kong, Thailand, Philippines, Oman, and European Union are either already adopting or are planning to adopt biometric national identifiers (Cline, 2004). Eventually, biometric technologies may eliminate physical id documents, debit and credit cards, keys, and similar devices.
- *Internet verification for e-commerce and home workers*. Identity theft problem can be decreased, allowing consumers to shop on the Internet with confidence
- *Tracking cattle*. Biometrics is not only for humans. In response to the mad-cow disease, officials are reportedly considering ways to track cattle, possibly using retinal or iris scanning (Jones, 2004)

BIOMETRIC SYSTEM PERFORMANCE

Biometrics is still an emerging concept – thus requiring organizations considering implementation of the technology to assess the performance of biometric solutions more critically than would be necessary if the technology was more mature. Performance of a biometric security system can be evaluated in terms of its accuracy, storage requirements, and speed (Jain et al. 2000).

Since biometrics rely on unstructured data input, mistakes are always possible; the system can accept an impostor as a valid individual (a false match) or reject a valid individual (a false no match) (Jain et al. 2000). These types of mistakes constitute two important variables for assessing performance of the systems: false nonmatch rate (FNR) and false match rate (FMR). These two variables are correlated negatively, making it necessary to seek a balance between these two measures along the Receiver Operating Characteristics (ROC) line (the line in Figure 4) , which is a model for system accuracy in a given test environment (Jain et al. 2000).

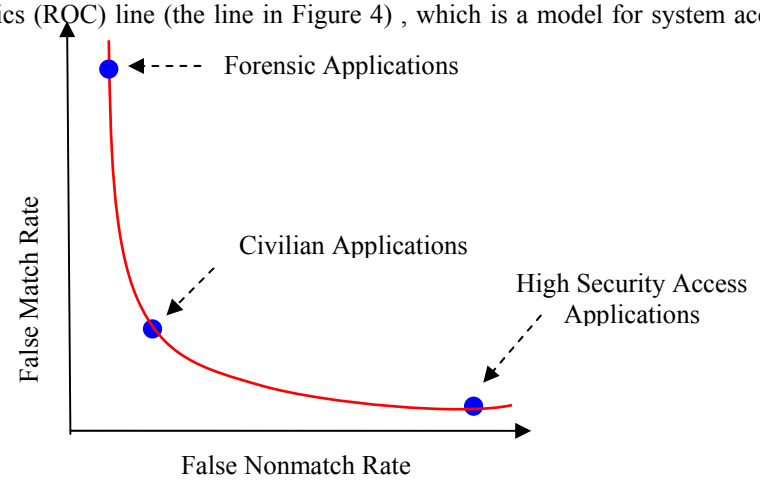

Figure 4. Receiver Operating Characteristics (adopted from Jain et al. 2000)

Biometric technologies may demand additional storage, bandwidth, and processing requirements. Storing digitized human body patterns requires more computer memory than is required, for instance, for storing passwords. Transferring scanned biometrics also requires expanded network bandwidth. Moreover, the computer processing power requirements for matching a user name and a password with a particular record in a database of logins and passwords is nothing like applying complex pattern recognition algorithms to biometric input. These increased requirements for computer capacity are closely related to system speed. Unless sufficient computer resources are provided, a biometric system may not function at an acceptable performance rate.

In addition to system performance, such system evaluation measures as acceptability and circumvention (Jain et al. 2000) need to be considered. Acceptability is the extent to which people are willing to accept a biometric solution in their daily lives. Indeed, some of the scanning techniques may be perceived as invasive and troublesome, which may cause organizational resistance. Circumvention refers to how easy it is to fool a system through fraudulent methods.

CURRENT AND EMERGING BIOMETRIC SOLUTIONS

Most biometric technologies are already commercially available. Fingerprint technology is the most widely available and the cheapest. All kinds of fingerprint readers, mice, trackballs and cards are available with prices of around one hundred dollars for devices such as ID Mouse Professional. Hand geometry readers, voice recognition, iris and retina scanning and face recognition technologies are all available from a number of vendors. Dropping hardware prices in conjunction with improved software will increase the popularity of biometrics system and put them within reach of most businesses and consumers. For example, an iris-scanning device currently sells for less than $200 in retail.

In addition to improvements to currently available technologies, futurists predict use of instant DNA testing and brain wave pattern scanning for authentication and identification purposes. In 10 to 20 years these technologies may present a practical alternative for instant identity verification. DNA testing is extremely accurate but currently requires specially equipped laboratories and takes time. It is extensively used for both identification and authentication purposes in law enforcement but currently is not a practical option for real time security applications. However, scientists claim to have already developed an instant DNA identification technique which will eventually be built into a handheld device (Connor, 2002).

Iowa-based neuroscientist Lawrence Farwell invented a technique called "brain fingerprinting" that may help establish innocence or guilt in a courtroom (Wen, 2001). His method focuses on a specific electrical brain wave, called a P300, which activates when a person sees a familiar object. The subject wears a headband of electrodes and faces a computer screen, which flashes photos. This technique provides a potential window into someone's past visual experience. If a person looks at random pictures of weapons, without activating a P300 wave, these objects are presumably unknown to him. But if the murder weapon is shown, and a P300 wave activates, then the person clearly has some experience with that weapon. Kirsch (2001) proposes use of brain scanning in conjunction with iris scanning for identification of terrorists. Here's how the proposed system works: after an individual's identity is established by a biometric such as iris scanning, the individual would be shown a series of pictures presumably familiar to terrorists such as weapons while his brain is being scanned.

"Brain fingerprinting" can be used for identity verification. An individual might be shown a series of unique pictures that would be not be seen by anyone else (e.g. randomly generated by a computer). In the process if authentication, these pictures could be played back to the individual. Only the authorized person's brain would emit the right response.

PRIVACY ISSUE

Altman (1975, p.24) defined privacy as "…the selective control of access to the self," while Richard Mason (Mason, 1986), defines it as:

> *information about one's self or one's association must a person reveal to others, under what conditions and with what safeguards? What things can people keep to themselves and not be forced to reveal to others?*

In light of the above definitions, biometrics-based identification technologies, such as facial recognition, appear to pose the greatest privacy risk. A security camera does not ask for one's consent before capturing one's image. Control over personal information is therefore weakened. Philip E. Agre (2003), a strong opponent of facial recognition, presents a comprehensive list of arguments against its widespread adoption and use.

> *… automatic face recognition in public places, including commercial spaces such as shopping malls that are open to the public, should be outlawed. The dangers outweigh the benefits…The potential for abuse is astronomical. Pervasive automatic face recognition could be used to track individuals wherever they go… The information from face recognition systems is easily combined with information from other technologies. Among the many "biometric" identification*

> *technologies, face recognition requires the least cooperation from the individual… The technology is hardly foolproof…Among the potential downsides are false positives, for example that so-and-so was "seen" on a street frequented by drug dealers… Yet the conditions for image capture and recognition in most public places are far from ideal. Shadows, occlusions, reflections, and multiple uncontrolled light sources all increase the risk of false positives… Face recognition is nearly useless for the application that has been most widely discussed since the September 11th attacks on New York and Washington: identifying terrorists in a crowd…*

While identification systems invoke Orwellian or, more currently, Minority Report images of a total surveillance society, authentication systems pose a threat of their own. Bruce Schneier, a well-known cryptologist and computer security expert, warns (Schneier, 1999).

> *Biometrics don't handle failure well. Imagine that Alice is using her thumbprint as a biometric, and someone steals the digital file. Now what? This isn't a digital certificate, where some trusted third party can issue her another one. This is her thumb. She has only two. Once someone steals your biometric, it remains stolen for life; there's no getting back to a secure situation.*

Identities can be stolen if biometrics are used without proper safeguards. Identity theft is a major privacy invasion and the fastest growing crime in America; according to an FTC survey, there were 9.9 million victims of identity theft in America in 2003 (FTC, 2003).

On the other hand, many in the biometrics industry believe that properly deployed biometrics will increase privacy, since if you have somebody's biometric, you do not need other information such as race, gender, or social security number. The problem is the underlying database management, not biometrics (Winter, 2000). This sentiment is not limited to the biometrics industry. The well-known sociologist Amitai Etzioni (1999) believes that benefits of privacy should be weighed against its costs and that biometric technologies may bring about huge benefits to consumers and businesses as well as enhance privacy. Etzioni (1999) believes Big Brother fears are overstated:

> *…contrary to popular belief, new identification technologies do not usher in totalitarian governments, but once totalitarian governments take over, they use whatever means of control they can usurp. Strengthening the foundations of civil society is the best defense against totalitarianism, not trying vainly to return the genie of biometrics into the bottle from which it already has escaped.*

Still, it privacy concerns must be addressed and those concerns seem only likely to increase with future adoptions of technologies such as DNA fingerprinting. The biometrics industry and privacy advocates both favor adoption of comprehensive regulations to prevent possible biometric abuses and protect privacy and civil rights while allowing the industry to develop. They disagree, however, on the source of those regulations. Many privacy advocates favor government regulation, contending that industry self-regulation will fail. Clarke (2004) laments "…self-regulation means protection of the sheep by the wolves; and funnily enough the wolves pay more attention to their own objectives than to those of the sheep."

CONCLUSION

Various applications of biometric technology are currently in use. While a number of issues, such as privacy concerns, are still largely unresolved, biometric technology, if implemented and used correctly, has significant potential to counter the growing threat to physical and information security.

ACKNOWLEDGEMENTS

We thank Dr. Blake Ives of the University of Houston for his insightful comments and suggestions, which have been indispensable in the preparation of this paper. We also wish to thank Dr. Andy Schwartz, currently on the MIS faculty at the LSU, for his part in preparing a previous version of this paper for presentation to the Information Systems Research Center at the University of Houston.

REFERENCES

1. Agre, P. (2003) "Your Face Is Not a Bar Code: Arguments Against Automatic Face Recognition in Public Places,"
2. http://polaris.gseis.ucla.edu/pagre/bar-code.html (current Feb. 20, 2004).
3. Altman, I. (1975) The environment and social behavior, Brooks/Cole, Monterey, California.
4. Ashbourn, Julian, "Biometrics: Advanced Identity Verification," Springer-Verlag, 2000.
5. AuthenTec, Inc (2004). www.authentec.com (current Fen. 20, 2004).

6. Clarke, R. (2004). Interview, http://www.biometricsinstitute.org/ bi/passprot/clarkeinterview1.htm (current Feb. 20, 2004).
7. Clarke, R.(1999). "Introduction to Dataveillance and Information Privacy, and Definitions of Terms". http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html (current Feb. 20, 2004).
8. Cline, J. (2004) "Get Ready for the U.S. National ID Card," Computerworld.com,
9. http://www.computerworld.com/governmenttopics/government/policy/story/0,10801,89491,00.html (current Feb. 20, 2004).
10. Connor, S. (2002) "Instant DNA Fingerprinting Turns Sci-Fi into Reality," http://www.nanotechnology.northwestern.edu/press/independent%20february%202002.PDF (current Feb. 20, 2004).
11. Etzioni, A. (1999) "Biometrics Are Coming! Biometrics Are Coming!," SpeakOut.com,
12. http://speakout.com/activism/opinions/3808-1.html (current Fen. 20, 2004).
13. FTC. (2003) **"**FTC Releases Survey of Identity Theft in U.S. 27.3 Million Victims in Past 5 Years, Billions in Losses for Businesses and Consumers," http://www.ftc.gov/opa/2003/09/idtheft.htm (current Feb. 20, 2003).
14. IdentityTheft.org (2004) "Identity Theft Prevention and Survival," http://www.identitytheft.org/ (current Fen. 20, 2004).
15. Identix Inc. (2004) http://ww.visionics.com (current Fen. 20, 2004).
16. Jain, A., Hong, L. and Pankanti, S. (2000) "Biometric Identification," *Communications of the ACM,* 43, 2, 91-98.
17. Jones, R. (2004) "Homeland Security Seen Spurring Biometrics," http://www.msnbc.msn.com/id/3999879/ (current Feb. 20, 2004).
18. Kirsch, S. (2001) "Identifying Terrorists Before They Strike by Using Computerized Knowledge Assessment (CKA),"
19. http://www.skirsch.com/politics/plane/ultimate.htm (current Feb. 20, 2004).
20. Mason, R.O.(1986) "Four Ethical Issues of the Information Age," *MIS Quarterly,* 10, 1, 4-12.
21. McHugh, J. (2001) "Intrusion and Intrusion Detection," *International Journal of Information Systems*, 1,1, 14 - 35.
22. Ratha, N.K., Connell J.H., Bolle R.M. (2001) "Enhancing Security and Privacy in Biometrics-Based Authentication Systems," IBM Systems Journal, http://www.research.ibm.com/journal/sj/403/ratha.html (current Feb. 20, 2004).
23. Schneier, B. (1990) "The Uses and Abuses of Biometrics," *Communications of the ACM,* 42, 8, 136.
24. Wen, P. (2001) "'Brain Fingerprints' May Offer Better Way to Detect Lying," National Geography News,
25. http://news.nationalgeographic.com/news/2001/07/0705_wirelies.html (current Feb. 20, 2004).
26. "US Fingerprint Foreign Visitors" (2004), BBC News, http://www.news.bbc.co.uk/2/hi/americas/3367893.stm (current Feb. 20, 2004).
27. Winter, C. (2000) "Biometrics: Safeguard or Invasion of Privacy?" *Sun-Sentinel*, October 29.
28. Zviran, M. and Haga, W.J. (1999) "Password Security: An Empirical Study," *Journal of Management Information Systems,* 15,4, 161-186.