Digital Forensic Analysis of E-Mails: A Trusted E-Mail Protocol

Gaurav Gupta♣
Senior Research Fellow
Bureau of Police Research and Development

Chandan Mazumdar
Professor
Jadaypur University

M. S. Rao
Director /Chief Forensic Scientist
Ministry of Home Affairs

Abstract

E-mail has revolutionized business, academic, and personal communication The advantages of e-mail include speedy delivery, ease of communication, cost effectiveness, geographical independence, and the portability of mailboxes. The last two are the biggest advantages over snail mail. However, with e-mail comes the threat of a genuine user being compromised through key loggers, social engineering, shoulder surfing, password guessing and other similar, though less technical, methods. This passive espionage can have a direct impact on the genuine user in terms of denial of information, loss of money, loss of time, mental harassment and an attack of personal privacy. To enable digital forensic analysis of e-mails, we propose behavioral biometric based authentication, which is analogous to a signature in paper documents. In the proposed system, if someone other than a genuine user tries to authenticate himself, then detection and fixing is possible.

Introduction

Most countries recognize e-mail as legitimate document evidence. E-mails have been used as substantial sources of evidence in cases of homicide, cyber stalking, harassment, spoofed identity and espionage. The digital forensic aspect of e-mails (e-mail forensics) requires urgent attention, due to its impact in solving most of the cases of Computer Frauds and Cyber Crimes (CFCC). To make things worse, investigative and law enforcement agencies are under-prepared to tackle the explosion of this new unseen, unheard, and innovative way of committing crime. Technologies such as quantum computing, DNA computing, and “Adaptive or Reconfigurable Computing,” [1], [16] make hardware behave flexibly and can be tailored to imitate various stipulations. The latest Wi-Fi technology and migration of wireless standards 802.11b to five times faster 802.11g [1], [16] has forced rethinking about security and authentication systems.

The evolution of sophisticated and powerful digital technological solutions needs to be matched by development of tamper proof security solutions. The existing protocols, such as kerberos, one time passwords, and methods such as encryption and steganography provide only limited security from direct and active attacks such as sniffing, analyzing traffic, breaking into servers, breaking encryption and exploiting existing protocols for replay attacks. Passive espionage attack methods, i.e.. use of key loggers, password guessing techniques, password crackers, shoulder surfing, social engineering, and other similar less technical methods for compromising the authentication token, pose a very serious threat to the integrity of the genuine user account. The existing biometrics systems, in spite of being highly reliable, lack portability and cost effectiveness and are statically bound to a fixed location. Thus, biometrics systems are not suitable for email applications where portability of mailboxes over geographical boundaries along with efficiency of cost are major driving factors. Our heavy dependency on user name and password combination to authenticate provides a window of opportunity for criminals to acquire the authentication token for malicious and unlawful gain. The direct impact of passive espionage of emails includes denial of information, loss of money, loss of valuable time, mental harassment, and an attack on personal privacy. In this paper an attempt has been made to identify the peculiar characteristics which can form a basis for the development of trusted email protocol for authentication. The major issues addressed by the study are:

- Problems associated with geographical independence, portability of mailboxes, simultaneous multiple logins, and authentic date and time stamps.
- Problems arising due to espionage on a genuine user account, i.e. violation of privacy and denial of access leads to loss of valuable information, money, time and reputation.
- Embarrassment and harassment caused by illegal use of an account, requiring the user to prove his innocence.

We propose a trusted e-mail protocol, which can provide the information of when, where and how many times the e-mail has been accessed. Simultaneously, multiple logins can be prevented. We will put forward the solution from the perspective of a digital forensic expert making use of identified behavioral biometrics characteristics of the genuine user, i.e. the keystroke dynamics and the audio-visual speech recognition **(AVSR)** for the purpose of authentication through the software layer. This will also help immensely in the cost and time effective analysis of digital forensic cases.

Previous Work

RSA [2], [3], SSL [4], PGP [5], one-time passwords [6], the Kerberos [7], [8], SSID [9], WEP [10], Open Authentication, Shared Key Authentication, and MAC Address Authentication for wireless networks [10] for secure authentication are vulnerable to passive espionage attacks. If an attacker is smart enough to break any one password of a user, then he is certain to break others, too, as they will be similar to the one the attacker cracked.

The impact of a passive attack is far more serious, as any computer literate with little knowledge of the Internet can use a script to launch an attack. A lot of work has been done to address direct attack, and many secure protocols and encryption techniques have been developed. The smart card based authentication has also been used, but it is vulnerable to tampering, and can be acquired by illegal means, such as stealing or using force.

All these problems can be countered by the use of a behavioral biometrics based authentication system. Such systems are relatively economical and if implemented properly, offer a very high level of security. The limited success of initially deployed keyboard dynamics techniques in practical implementation was mainly due to non-consideration of conditions such as illness, drunkenness, and age-related limitations. Hence we propose the following identified peculiar characteristics with associated relative weights, which will be derived considering these factors, to achieve reliable solutions with minimization of false acceptance rate (FAR), false rejection rate (FRR). We propose to broaden the points of calculation of the identified peculiar characteristics for generation of a reference template, by taking into consideration all the above-discussed factors to make the proposed system more reliable.

Basic Characteristics of Behavioral Biometric Based Authentication

Universality: The universality of characteristics means that every person should have the characteristics irrespective of geographical, religion, or any other constraining boundary. The proposed behavioral biometrics based authentication system will use keyboard dynamics and audio-visual speech recognition (AVSR). These characteristics are universal and hence, suitable for the authentication system.

Uniqueness: It is essential that no two people are the same in terms of characteristics, i.e. there should be a significant scope for differentiating one person from another. This property is achieved by keyboard dynamics and corroborative audio-visual speech recognition (AVSR)..

Permanence: Permanence requires that the characteristics are invariant with time i.e. the degree of variation should be in a range where natural variations should not result in false rejection or false acceptance.

Quantifiable: This property requires that the characteristics can be measured quantitatively.

Proposed Protocol

We propose the use of a software layer that can also be used as a plug-in, based on the identified peculiar characteristics and their weights, to generate a contemporary reference template for authenticating the genuine user. That layer would also monitor patterns of the user's work to broaden the base of characteristics and determine the possible natural variations and their permitted levels specific to each user. The proposed system has three phases. First is the enrollment of the genuine user.. The second phase is authentication of the user, using BBBA, when he or she accesses the system, Third is key generated signing of email, using keyboard dynamics and AVSR.

Keyboard Dynamics

In this paper we will put forward the mechanism for efficient and tamper proof authentication, using identified peculiar characteristics of the genuine user through keyboard dynamics and audio-visual speech recognition, to generate a “reference template” i.e. behavioral biometrics based authentication system. The proposed system will minimize the False Acceptance Rate (FAR) and False Rejection Rate (FRR), due to its ability to learn throughout its life cycle, therefore overcoming the high rate of rejection of the genuine user when he is ill, drunken, tired, injured or aging. The proposed system will also help in both detection and digital forensic analysis, as any attempt by an attacker to compromise the patterns of AVSR and keyboard dynamics will be logged with date and time stamps.

Keystroke dynamics, also referred to as typing rhythms, is considered one of the most unusual and innovative biometric technologies. It is a fairly new biometric technology and is still underdeveloped and underutilized [11], [12], and [13]. Keystroke dynamics looks at the way a person types on a keyboard. Specifically, keyboard dynamics measures two distinct variables (the identified peculiar characteristics): "dwell time," which is the amount of time a person holds down a particular key, and "flight time," which is the amount of time a person takes between keys.

Also, additional variables can be used for more reliability. These include the time taken in between every key as distinguished from every other key and the time taken between combinations of keys. Keyboard dynamics systems can measure one's keyboard input up to 1000 times per second. Keystroke dynamics requires, as with most biometrics technologies, a "reference template" [14]. This involves an initial session with a person using a keystroke dynamic system, so that the system can construct or build the "reference template" by detecting the person’s typing rhythms.

Keystroke dynamics is behavioral in nature, hence if developed and implemented properly will offer a maximum level of tamper proof secure authentication. Enrollment, as well as identification, goes undetected by the user; that is, it is passive, occurring without user knowledge. Another inherent benefit to using keystroke dynamics as an identification device is that the hardware (i.e. keyboard) is inexpensive and non-intrusive. Also even if someone has physical access to system and boots through floppy and CD drives, it is extremely difficult to remove the files and folders of the proposed system, as it is coupled with keyboard drivers. Hence if tampering occurs, the system will not work. This is not the case with other biometrics systems.

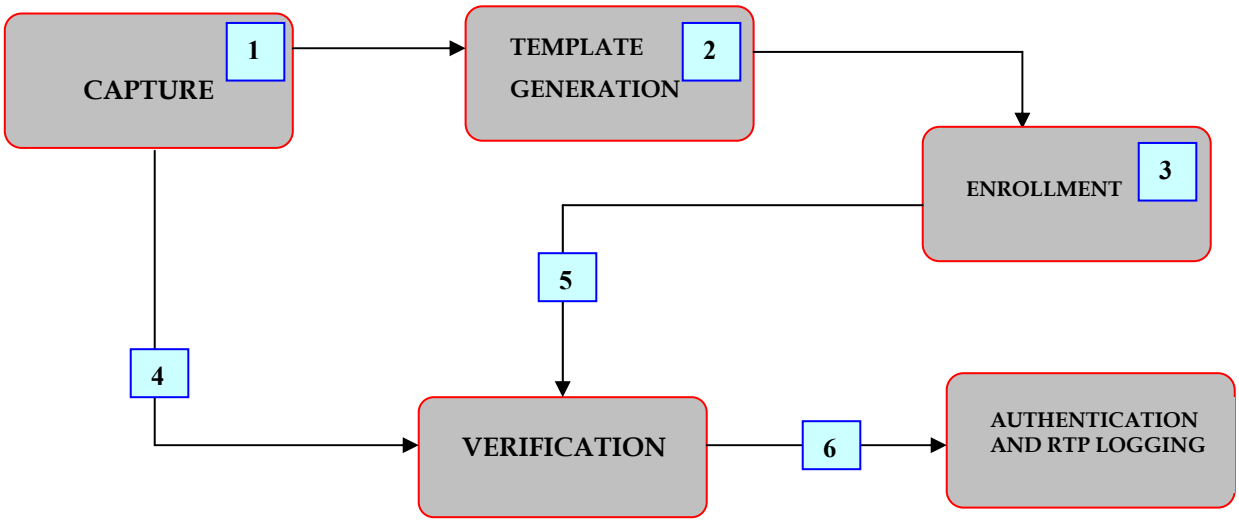

Figure 1. Four Step Mechanism of Behavioral Biometrics Based Authentication

Visual Interactivity: Audio-Visual Speech Recognition [17], [18]

Hindrances such as background noises, sore throat, and other illnesses of the genuine user posed a threat to robust speech recognition systems. These implicit problems can be over come by using the visual features of genuine user to make reliable audio-visual speech recognition systems. The use of visual features in AVSR is justified by both the audio and visual modality of the speech generation and the need for features that are invariant to acoustic noise perturbation. The speaker independent audio-visual continuous speech recognition system relies on a robust set of visual features obtained from the accurate detection and tracking of the mouth region.

Working

The proposed BBBA will be an added software layer over the existing email system and will be compatible to all types of existing email systems. The BBBA, using Keyboard Dynamics and audio-visual speech recognition (AVSR), will generate a Reference Template, which will later be used for authentication purposes, along with the user name/password combination. The reference template will be logged and will be useful for digital forensic analysis in the following scenarios:

- When a genuine person denies that he has accessed the system, i.e. to prove his innocence or otherwise.
- When somebody fraudulently uses or tries to use the system. Here two cases arise: one, when the user name/password combination is correct, but the reference template does not match, and the other, when both the user name/password combination and reference templates do not match.

We can also generate a unique key based on Keyboard Dynamics and AVSR, which could be used to sign the emails. This will help in linking the body of the email/text to the person and to tackle “man in the middle” attacks. The BBBA will help immensely in

cases where a genuine user is implicated, i.e. when a criminal uses a passive espionage attack to gain an authentication token and misuses the account of the genuine user by threatening someone, or by sending pornographic and obscene material to harm the genuine user's reputation. The proposed system can prove the innocence of the genuine user and also any intentional disguise. The RTP will log the attempted authentication template information, which can be retrieved from the server by competent authorities in order to detect and fix the espionage and to establish authentic date and time stamps (ADTS).

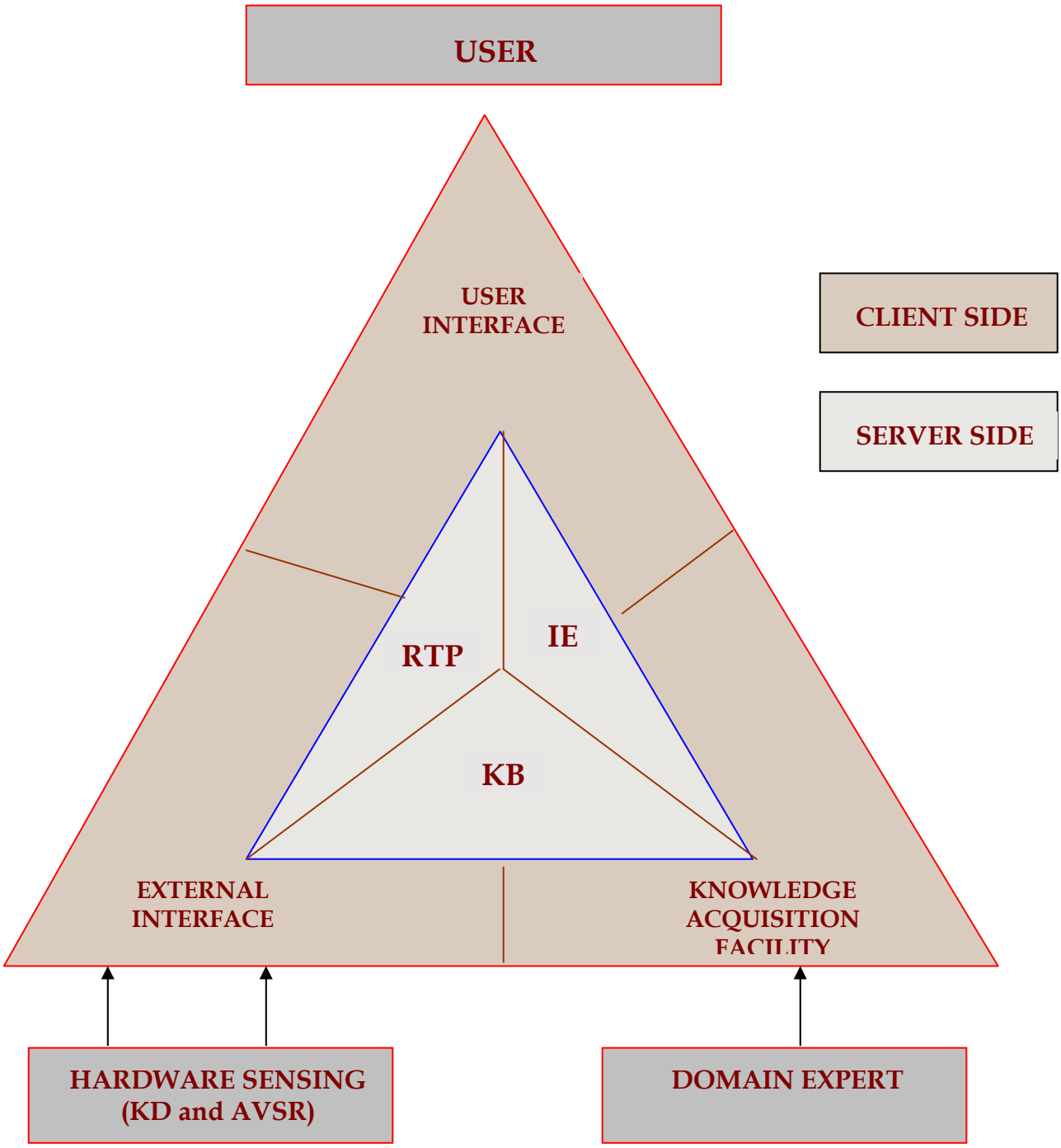

Figure2. Architecture of Behavioral Biometrics Based Authentication System

RTP: Reference template profiling for digital forensic analysis
IE: Inference engine authenticating through reference template for genuineness
KB: Knowledge base of reference templates

False Positives and False Negatives

Behavioral based biometrics systems are analogous to signatures on paper documents, as they may be known to anybody, but still extremely difficult to forge or self-disguise. With behavioral based biometrics systems, no one except the genuine user can gain entry. The identified peculiarities of keyboard dynamics and AVSR, specific to a genuine user, can form the basis for development of an expert system, which is able to monitor these patterns to establish the genuineness of the user. Because the chances of false positives and negatives are crucial to establishing the acceptance of such a system, there must be a learning capability which can adapt to gradually changing unique peculiar characteristics. The proposed system will also consider the impact of a change of systems, malfunctioning equipment, illness of user, drunken user, and effect of age, i.e. time on reliability in terms of false positives and negatives for rejection or acceptance.

In order to be implemented, the proposed system combines learning and updating according to user habits, and reflects even gradual change in a contemporary reference template, hence minimizing the impact of age, fatigue, illness, and time. Also the proposed system will authenticate the genuineness of the user, based on results deducted from a combined analysis of peculiar identities and characteristics, allowable natural variations, their respective assigned weights to minimize chances of false positives and negatives, and pattern recognition using keyboard dynamics and audio-visual speech recognition (AVSR). The proposed system will require a user to feed their characteristics through an initial interactive session. Experiments conducted so far, show that it is usable and provides industry-acceptable results. This inexpensive, scaleable, easy to deploy, and proactive concept adds a secure layer for raising the threshold of strong authentication.

Passwords are the most popular and firmly entrenched form of computer security and access used today. Passwords are also the most vulnerable security method, due to the ease with which they can be cracked and carelessly shared or posted. The concept presented here virtually eliminates this problem by providing an additional layer of strong user authentication to existing protocol systems. This new layer is based on the science of behavioral biometrics based authentication BBBA and can accurately determine whether the person typing and speaking is authorized to have access to the network or resource they are requesting. This method is unobtrusive as it allows the genuine user to log on in a manner with which they are familiar. The only new step is the initial enrollment process, where the legitimate user provides a series of typing and oral samples to train the proposed system to recognize their unique rhythm. The advantage of this system is that even if the user's authentication token is compromised, the user's unique pattern makes it next to impossible for criminals to get access to his/her account, much like your signature, which everyone knows, but can not execute.

The combination of keyboard dynamics and the characteristics identified using AVSR provides unique, measurable characteristics for a human being that can be used to authenticate the person. It eliminates entry gained by spuriously generated passwords through direct attacks, using mechanized methods. The proposed system, in conjunction with existing protocols, makes compromising a genuine user account next to impossible. The success rate, efficiency, implementation, effect of natural variations, and the chances of false negatives and positives have been considered and an acceptable solution level has been achieved in experimental protocol [11], [12], [13], [14] and [15].

For more efficient and user-friendly implementation, a layered approach has been devised. The specific steps necessary to establish the objectives of the protocol include:

- Identifying and defining unique peculiar characteristics of the individual user.
- Making an artificially intelligent system with a capability to learn.
- Developing an inference engine to authenticate a user with permissible natural variation.
- Collaborative authentication using AVSR capabilities to guarantee the genuineness of the user.
- Methods to deal with False Acceptance Rate (FAR) and False Rejection Rate (FRR).
- Automated filtering of peculiar characteristics and enhancement of the database depending on the changing environment .
- Establishment of standards, principles, quality, and admissibility according to law.
- Creation of appropriate tests to check the reliability of each step of the process.
- Creation of appropriate tests to determine the effect of human interaction and involvement on each step of the process.
- Measurement of the scope of error (mainly human) and ways to minimize them.
- Ways to minimize human interaction and maximize automatic detection, initialization, and control of the knowledge base involved in a digital forensic examination.

Conclusion

The proposed behavioral biometrics based authentication is based on universal characteristics, making it suitable to use for authentication. The BBBA can counter passive espionage attacks of:

- Key logger
- Social engineering
- Shoulder surfing
- Password guessing
- Password cracking tools
- Internal security breaches, including negligence
- Casual sharing of accounts.

Hence, BBBA is a less expensive and passive method which provides high security. At the same time, its use allows resources to be conserved, as there is no need to rotate and reassigns password on regular basis. The global reference template will log the reference template and location coordinates, along with defined authenticated date and

time stamps of any false attempt. Thus, the system is useful in digital forensic analysis, as it helps to locate suspects and match their samples to recorded reference templates. Because only a genuine user's reference template can be authenticated, it tackles the problem of integrity of a genuine user account, along with the question of simultaneous multiple logins.. The captured reference template of a genuine user will be transmitted in encrypted form for authentication purposes, based on a session to avoid sniffing and reply attacks. Innocence can also be proved by comparing the logged global reference template. Because behavioral biometrics based characteristics are universal in nature, they can be used for tracking and monitoring purposes and for reliable and tamper proof authentication and identification.

The key advantages are:

- The portability of implementation scores over other conventional biometrics methods such as fingerprints, electronic signatures [19], facial, voice, lip movement recognition [20], and iris recognition systems as a biometrics system requires costly hardware, which is generally not available or portable. Contrary to this, BBBA requires only a keyboard.
- Economical and efficient security without costly hardware, which can be customized.
- Its passive in nature, requiring no special skills and offering forensic aspect implementation.
- Capability for global monitoring and tracking.

The constraints are:

- Only genuine user will be allowed.
- Slight computational overhead.
- Person dependent and will fail if person is not in normal state.
- Need for improving ERR, FAR, FRR.

Future work

- Universal implementation can be used to have interconnected reference templates for multiple applications, to avoid several different points of authentication, thereby saving resources and improving efficiency.
- A global scope will help to counter the misuse of digital technologies by criminals. The Scope of Global Monitoring through the Reference Template's universality will be explored.
- A feasibility analysis and testing of similar systems for other commonly used applications, such as PIN numbers for smart cards, will be explored, as well as the quantification of the role of the proposed system in tracking criminals and digital forensic analysis.

© 2004 International Journal of Digital Evidence

About the Authors

Gaurav Gupta ♣ is a Senior Research Fellow in the Computer Forensic Division of the Bureau of Police Research and Development in Ramanthapur, Hyderabad, India. He can be reached through e-mail at gaurav_jindalin@rediffmail.com.

Chandan Mazumdar is a professor in the Department of Computer Science and Engineering at Jadaypur University in Kolkata, India. He can be reached through e-mail at chandanm@vsnl.com.

Dr. M. S. Rao is Director-cum-Chief Forensic Scientist at the Ministry of Home Affairs in the Government of India. He can be reached through e-mail at msrnd@indiatimes.com.

References

[1] The Hindu, 26th June 2003 India.

[2] Planet, Introduction to Public-Key Infrastructure, 2001, URL:

http://www.iplanet.com/developer/docs/articles/security/pki.html.

[3] Waters J. Digital Certificates, 2000. URL:

http://oden.csom.umn.edu/idsc6452/Papers/JWaters/Paper.htm.

[4] Netscape, Secure Sockets Layer, 2000 URL:

http://home.netscape.com/security/techbriefs/ssl.html.

[5] Computer Networks by Andrew S. Tanenbaum

[6] GSP Services, One-time Passwords In Everything, 2001. URL:

http://www.gsp.com/cgi-bin/man.cgi?section=4&topic=opie.

[7] Duke University, Kerberos: Strengths and Weaknesses, August 18, 1997

URL: http://www.oit.duke.edu/~rob/kerberos/kerbasnds.html.

[8] ACIS 5584, Kerberos Authentication in Windows 2000, February 4, 2001.

URL: http://filebox.vt.edu/users/hmao/project1/win2k.htm.

[9] Internet Security Systems, http://www.iss.net/wireless/

[10] RSA Security, http://www.rsasecurity.com/rsalabs/technotes/

[11] Monrose, F. Rubin, D. Keystroke dynamics as a biometric for authentication. March 3,1999,

[12] URL: http://www.cs.columbia.edu/~hgs/teaching/security/hw/keystroke.pdf.

[13] Automated Identification and Data Capture Biometrics Web Site, 2001 URL:http://www.tech.purdue.edu/it/resources/aidc/BioWebPages/Biometrics_Keystroke.html/(2001-05-02).

[14] BioPassword, 2001. URL: http://www.biopassword.com/.

[15] Government Computer News, BioPassword Security Checks User's Typing Pattern, April5, 2001 URL: http://www.washtech.com/news/software/8838-1.html.

[16] Quick Silver Technology, URL:http:// www.qstech.com

[17] Visual Interactivity: Audio Visual Speech Recognition by Ara V. Nefian, Lu Hong Liang, Xiao Xing Liu, Xiaobo Pi from http://www.intel.com/research/mrl/research/avcsr.htm#.

[18] Deravi, F. Audio-Visual Person Recognition for Security and Access Control , January 9, 1999, URL: http://www.jtap.ac.uk/reports/htm/jtap-038.html.

[19] CyberSign, 2001. URL: http://www.cybersign.com/.

[20] BioID, BioID Enterprise 3.0, 2001. URL: http://www.bioid.com