Too Many Passwords…

William J. Lawson, Ph.D.
Technical PM/Advisory Board, ICDRI
AT&T Global Network Services
WilliamJLawson@ieee.org
August 16, 2002

Introduction

Ever since the implementation of the first enterprise network, organizations have continuously searched for the most impregnable method(s) available to keep corporate knowledge and personal privacy (data) secure from the unauthorized intrusion, violation, or destruction of prying eyes. Traditionally, the most dominant methods of securing a companies' infrastructure is to merge an employee's username with a password, personal identification number (PIN), or a secure token (Nanavati, Thieme, & Nanavati, 2002).

However, passwords and PINs can be hacked, shared, or guessed; and secure tokens can be lost (Corcoran, Sims, & Hillhouse, 1999). It is therefore not uncommon for employees of large companies to have numerous, long, and unbelievably complicated passwords to remember. Many times the passwords are so ambiguous that the employees become stressed and the passwords are easily forgotten. To add to the frustration, an employee must then contact the helpdesk or network administrator to have the encrypted password reset or changed (Quintanilla, 2000).

The function of a biometric authentication system is to facilitate controlled access to applications, networks, personal computers (PCs), and physical facilities. A biometric authentication system is essentially a method of establishing a person's identity by comparing the binary code of a uniquely specific biological or physical characteristic to the binary code of an electronically stored characteristic called a biometric template. The defining factor for implementing a biometric authentication system is that it cannot fall prey to hackers; it can't be shared, lost, or guessed. Simply put, a biometric authentication system is an efficient way to replace the traditional password based authentication system (Ashbourn, 2000).

A Biometric Authentication System Will Allow for Integration of Non-homogenous Systems.

Developers of biometric authentication systems continuously track industry standards and have developed comprehensive toolkits known as software development kits (SDK) to address issues involving the integration of non-homogenous software and hardware (Nanavati et al.).

To allow for maximum integration of non-homogenous systems and legacy systems, manufacturers of biometric authentication systems adhere to standards called the Biometric Application-Programming Interface (BioAPI). The standards set forth in the BioAPI were developed by the BioAPI Consortium and is an open-systems standard that not only simplifies the integration of hardware and software, but the standards also contribute to interoperability, scalability, versatility, and the administration of all other systems (BioAPI Consortium, 2001).

An equally important biometric standard developed by the National Institute of Standards and Technology (NIST), the National Security Agency (NSA), and the Biometric Consortium is the Common Biometric Exchange File Format (CBEFF). The CBEFF was recently approved in February 2002 by The American National Standards Institute; the purpose of the CBEFF is to further promote interoperability, easy of integration, adaptability, and scalability of biometric technologies by standardizing the exchange format of a biometric template. CBEFF has accomplished this by defining a common set of data elements necessary to support the authentication of users and the employment of multiple biometric technologies within the infrastructure of an organization (CBEFF Website, n.d.).

A Biometric Authentication System Can Be Universally Applied to All Areas of the Company.

The system can be applied to areas requiring logical access solutions, and it can be used to access applications, personal computers, networks, financial accounts, human resource records, the telephone system, and invoke customized profiles to enhance the mobility of the disabled (Nanavati et al.).

In a business-to-business scenario, the biometric authentication system can be linked to the business processes of a company to increase accountability of financial systems, vendors, and supplier transactions; the results can be extremely beneficial (Ashbourn, 2000).

The global reach of the Internet has made the services and products of a company available 24/7, provided the consumer has a user name and password to login. In many cases the consumer may have forgotten his/her user name, password, or both. The consumer must then take steps to retrieve or reset

his/her lost or forgotten login information. By implementing a biometric authentication system consumers can op to register their biometric trait or smart card with a company's business-to-consumer e-commerce environment, which will allow a consumer to access their account and pay for goods and services (e-commerce). The benefit is that a consumer will never lose or forget his/her user name or password, and will be able to conduct business at their convenience (Nanavati et al.).

A biometric authentications system can be applied to areas requiring physical access solutions, such as entry into a building, a room, a safe or it may be used to start a motorized vehicle. Additionally, a biometric authentication system can easily be linked to a computer-based application used to monitor time and attendance of employees as they enter and leave company facilities (Nanavati et al.).

The Overall Security and Cost Benefits of a Biometric Authentication System are Currently Without Comparison.

Security of the enterprise has always been a major concern for executives and information technology professionals of companies. A biometric authentication system that is correctly implemented can provide unparalleled security, enhanced convenience, heightened accountability, superior fraud detection, and is extremely effective in discouraging fraud (Nanavati et al.).

Controlling access to logical and physical assets of a company is not the only concern that must be addressed. Companies, executives, and security managers must also take into account security of the biometric data (template) (Walder, 1997).

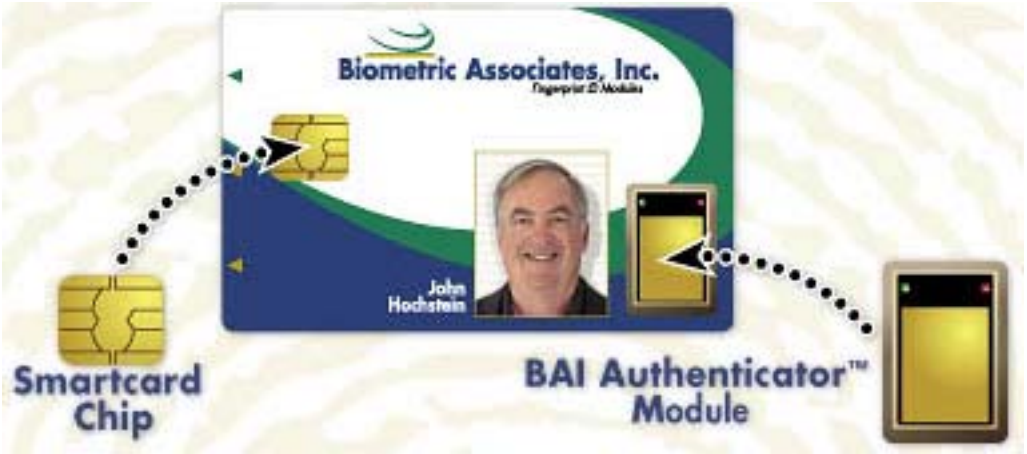
The Americans Civil Liberties Union (ACLU) is only one of many local, state, federal, and international organizations with legitimate concerns about the security (privacy) or misuse of the biometric data collected by the government and private companies (Winter, 2000). The aforementioned concerns are of such importance that two organizations were formed to address the concerns, the first is the International Biometric Industry Association (www.ibia.org), which is sponsored by the National Institute of Standards and Technology (NIST) and the second is the Bioprivacy Organization (www.bioprivacy.org), which is sponsored by the International Biometric Group (www.biometricgroup.com) (Woodlands Online, n.d.).

The biometric data can be stored in a number of ways, either in a centralized database or in a distributed system. Examples of a distributed system would be an optical card, memory card, proximity card, or a smart card. No matter what storage method is used, the biometric data must be encrypted to ensure that security requirements are met (Biocentric Solutions Inc., n.d.).

The most common standardized encryption method used to secure a company's infrastructure is the Public Key Infrastructure (PKI) approach. This approach consists of two keys with a binary string ranging in size from 1024-bits to 2048-bits, the first key is a public key (widely known) and the second key is a private key (only known by the owner). However, the PKI must also be stored and inherently it too can fall prey to the same authentication limitation of a password, PIN, or token. It too can be guessed, lost, stolen, shared, hacked, or circumvented; this is even further justification for a biometric authentication system (Corcoran et al.).

Per Walder (1997) the best overall way to secure an enterprise infrastructure, whether it be small or large is use a smart card. A smart card is a portable device with an embedded central processing unit (CPU). The smart card can either be fashioned to resemble a credit card, identification card, radio frequency identification (RFID), or a Personal Computer Memory Card International Association (PCMCIA) card (Biocentric Solutions Inc., n.d.). The smart card can be used to store data of all types, but it is commonly used to store encrypted data, human resources data, medical data, financial data, and biometric data (template). The smart card can be access via a card reader, PCMCIA slot, or proximity reader; it is therefore in compliance with section 508 of the Americans with Disabilities Act (ADA) (Walder, 1997).

A smart card is a must when implementing a biometric authentication system; only by the using a smart card can an organization satisfy all security and legal requirements (Biocentric Solutions Inc., n.d.). Corcoran et al. (1999) stated, "This process irrefutably authenticates the person presenting the card as the same person to whom the cryptographic keys belong and provides the necessary tight binding between cryptographic key storage and the authorized user of the cryptographic keys." (p. 5).



A perfect example of a Biometric Smart Card
(Source: www.biometricassociates.com)

When implementing a biometric authentication system the managers of a company must take into account many elements related to the company's infrastructure. Some of these elements will be easily identifiable, while others may be as illusive as the fountain of youth. The easiest elements of the infrastructure to identify are those that are heavily used and would most likely have been a commercially purchased product, such as the hardware and software of the biometric authentication system itself. Whereas the illusive elements of the company's infrastructure may be seldom used and may or may not have been commercially purchased. For example, a legacy system may have been purchased commercially, yet seldom used. We must also take into account issues related to the environment in which the system will be deployed (logical, physical or both), system integration, platform, distributed systems, biometric trait, front-end devices, front-end processing, back-end devices, back-end processing, level of security required, user education, remote access users, initial productivity losses, scalability, and exception processing (Ashbourn, 2000).

If a biometric authentication system is properly implemented and managed effectively the cost savings benefits, related to the help desk, administration, increased convenience, productivity of users, decreased fraud, reduction of stress, and increased security can far out weigh the cost of implementation (Biocentric Solutions Inc., n.d.).

The BioNetrix Corporation (2001) has composed a paper in which it has cited reports from the Gartner Group, META Group, Network Applications Consortium (NAC), Security Industry Association, Computer Security Institute (CSI), and the Federal Bureau of Investigations (FBI). The report from the Gartner Group proclaims that it will cost from $14 to $25 for a corporate helpdesk to reset an employee's password, further more an employee is most like to forget his/her password an average of four times in a year. When the cost of resetting a password is applied to thousands of employees it becomes astronomical.

Implementing a biometric authentication system can decrease the administration cost of an organizational network and increase user convenience and productivity. On the average, a user spends 12.5 hours a year logging onto just one application a day, when you multiple this by the total number of application access by a user it is easy to see the cost savings. A welcomed side effect is increased user convenience and productivity (BioNetrix Corporation, 2001).

The increased security of a biometric authentication system directly contributes to the reduction of financial losses due to fraud and security breaches. CSI reported in a survey they conducted that 50% of the 186 companies that responded claim to have 10-20 incidents per year, with an average per year cost of $142 thousand per incident (BioNetrix Corporation, 2001).

Many Governmental Agencies and Private Companies have Adopted Biometric Technologies with Excellent Results the Growth will continue.

In recent years, many governmental and commercial market sectors have adopted the use of biometric technologies as a proven method for authenticating a users access to valuable data or physical structures. The market sector that have seen the largest increase of implementation are the law enforcement sector, government sector, financial sector, healthcare sector, travel sector, and the immigration sector, these market sectors are referred to as biometric vertical markets (Nanavati et al.).

Just about 1,000 city employees of Oceanside, CA have been using a biometric authentication system that was installed by at the workstation level by BioLogon. According to the Information Technology Director of Oceanside, Michael Sherwood many of the helpdesk calls were to reset password, since the system was installed the number of helpdesk calls have dropped by approximately 60%. Additionally, Sherwood has deemed the biometric authentication system as a time-saver and a worthy investment (Quintanilla, 2000).

Physical access for employees to secure areas of airports in San Francisco, Hawaii, O'Hare's in Chicago, Charlotte/Douglas International and Frankfurt, Germany are controlled by a biometric authentication system. All reports describe the system as being highly effective (Nanavati et al.).

Governments around the world have implemented biometric technologies to protect live, civil liberties, individual privacy. The Otay Mesa, CA border crossing between Mexico and the United States employs a facial geometry biometric to authenticate the crossing of 3,000 commuters. The Sheriff's Department in Los Angeles, CA uses facial geometry to compare a composite sketch to a database of 350,000 mug shots (Woodlands Online, n.d.).

Health care centers must comply with what is referred to as the HIPPA legislation and one of the principles of HIPPA is to safeguard access to patient data. Health care centers like New York State Office of Mental Health, St. Vincent Hospitals, and Health Care Centers have adopted a biometric authentication system as the preferred method (Nanavati et al.).

Conclusions

Governmental agencies and commercial companies must remain eternally vigilant and continually seek out the most up-to-date method of securing the technological assets of an enterprise. But, let us not forget that as we seek to secure, hackers seek to invade.

Implementing a biometric authentication system is a very efficacious method of galvanizing the technological assets of an enterprise against the fanatical onslaught of internal and external threats. When implementing a biometric authentication system companies must be ecologically aware that as the required level of authentication increases, so does the cost.

It is best to think of a biometric authentication system as a key! Yes… As a key, it can open physical doors for you, provides logical security to data, and keep others out. It is a key that can be customized to an individual's access needs or it can be used to invoke a customized profile to aid physically challenged individuals.

I would like to close with a quote from Microsoft's Bill Gates' in PC WEEK Online October 8, 1997 stated, "Biometric technologies – those that use human characteristics such as fingerprint, voice and face recognition – will be the most important IT innovations of the next several years".

References

Ashbourn, J. (2000). Biometrics: Advanced identity verification. London: Springer-Verlag London Limited.

BioAPI Consortium. (2001, March 16). BioAPI specification version 1.1. Retrieved July 19, 2002, from http://www.bioapi.org/bioapi1.1.pdf

Biocentric Solutions Inc. (n.d.). White paper: Why use a biometric and a card in the same device? Retrieved July 3, 2002, from http://www.biocentric solutions.com/media/whitepaper.pdf

BioNetrix Corporation. (2001, June 18). BioNetrix authentication suite: Cost justification for implementing an enterprise-wide authentication management infrastructure. Retrieved July 3, 2002, from http://www.bionetrix.com

Corcoran, D., Sims, D., & Hillhouse, B. (1999, March 1). Smart cards and biometrics: Your key to PKI. Linux Journal. Retrieved July 3, 2002, from http://www.linuxjournal.com/article.php?sid=3013

Nanavati, S., Thieme, M., & Nanavati, R. (2002). Biometrics: Identity verification in a networked world. New York: John Wiley & Sons, Inc.

National Institute of Standards and Technology. (n.d.). Common Biometric Exchange File Format (CBEFF) Website. Retrieved July 23, 2002, from http://www.itl.nist.gov/div895/isis/bc/cbeff/

Quintanilla, F. (2000, July 5). Fingerprint as password: Your fingerprint could be your one password for life. Retrieved July 3, 2002, from http://www. biometricgroup.com/a_press/office/office.htm

Walder, B. (1997). Smart cards: The use of “intelligent plastic” for access control. Bedford, England: NSS Group Network House.

Winter, C. (2000, October 29). Biometrics: Safeguard or invasion of privacy. Sun-Sentinel. Retrieved July 3, 2002, from http://www.biometricgroup.com/ a_press/SunSentinelarticle_Oct2000.htm

Woodlands Online. (n.d.). Biometric emerges as a solution for security. Retrieved July 3, 2002, from http://www.biometricgroup.com/a_press/ woodland.htm