Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Biometric Technology Stomps Identity Theft

The yearly cyber crime cost in the United States is over 300 million and rising. As always, the crucial security mission is access control to systems and key installations to keep out intruders and identity thieves. However, with the rise of identity theft it has become more difficult to prevent unauthorized access to information resources and installations. Methods of positively verifying and authenticating people may mitigate the current identity theft crisis. Biometric technologies--applications that use the physiol...

Copyright SANS Institute
Author Retains Full Rights

AD

Biometric Technology Stomps Identity Theft

By Seyoum "Zeg" Zegiorgis

Abstract: The yearly cyber crime cost in the United States is over 300 million and rising. As always, the crucial security mission is access control to systems and key installations to keep out intruders and identity thieves. However, with the rise of identity theft it has become more difficult to prevent unauthorized access to information resources and installations. Methods of positively verifying and authenticating people may mitigate the current identity theft crisis. Biometric technologies—applications that use the physiological and behavioral attributes of a living person for the purpose of positively verifying the identity--may be the answer. Until now biometric technology products were crude resulting in high error rates of authentication and verification. Because of recent advances in computer science, biometric technology products (BTPs) have become more reliable and less expensive to own. With a BTP--such as an iris analyzer--a living person's identity can be positively authenticated and verified making it difficult for imposters to access resources by stealing someone else's identity. This paper discusses the benefits of implementing a biometric technology product—one more tool for safeguarding the information assets and key installations of an organization—the privacy issues associated with the deployment of a BTP.

The Battlefield

Information security is being fought on several fronts—three of them being the ones where the battle is raging the most. On the confidentiality front, information security officers are battling with intruders and information bandits to safeguard the confidentiality of information. In the integrity front, the battle is being waged between security professionals and hackers to guarantee the authenticity of data and information from malicious adulteration while in storage or in transit. On the third front, battle is raging between information security forces and those who are trying to deny the availability of services and systems to authorized users. The yearly cost of cyber crime in the United States is over 300 Million and rising.

The Silicon Valley/San Jose Business Journal (12 March 2001) reports,

> "The threat from computer crime and other information security breaches continues unabated and the financial toll is mounting, according to the sixth annual "Computer Crime and Security Survey," by San Francisco-based Computer Security Institute."

The business journal continues to report that

> "About one-third of the respondents put a dollar sign to their losses -- a total of $377.83 million for the 186 respondents who would put a dollar value on their losses. In contrast, the losses from 249 respondents in 2000 totaled only $265.59 million while the average annual total over the three years prior to 2000 was $120.24 million, according to the survey results."

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

What is the primary cause of such staggering loss? The sixth annual Computer Crime and Security Survey puts "theft of proprietary information" and "financial fraud" to be the prime causes. Both are results of unauthorized access to resources either through social engineering, identity theft or direct hacking.

The "Due Diligence" Burden

As an information security practitioner, the thought of some intruder breaking into or posing as an authorized user and accessing the network always must make the information security officer chill to the bones. The thought of someone stealing the organization's information assets when management is supposed to show "due diligence" in protecting such assets should make all involved in the custody of information assets paranoid. Their paranoia is supported by the FBI/CSI survey of computer-related crime that cost the US a stiff 377.8 million. The fact that 90% of computer crimes are committed by insiders and those who pose as authorized users makes one wish there was a way of positively authenticating and verifying users to keep out identity thieves out of secured resources.

Not only information managers have to show "due diligence," but also fulfill several legislative mandates dictated by such laws as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) that is to sweep the country in year 2003. All those who collect personal information—especially health care providers, health plan administrators and insurers—are required to ensure the privacy of such information in storage and transit. They are required to deploy information security tools and mechanisms to ensure the security of such information or risk fines of up to 250,000 dollars.

Financial services are also required to safeguard financial privacy including financial transactions, data, assets, and customer's non-public information to fulfill requirements of the Financial Services Modernization Act of 1999. This Act requires that financial services ensure the protection of databases, positively identify customers and tellers using appropriate security tools, including pattern analyzers.

The Solution

Biometry is a statistical analysis of patterns obtained by compiling readings of physiological characteristics (found in a person's palm, finger, iris and voice, shown below) or behavioral characteristics (found in a person's handwriting or keyboard keystrokes) for positively identifying a living person. They were first introduced in the 70s and early 80s. Biometric Technology tools gather those unique physiological or behavioral attributes of a person for storing it in a database or comparing it with one already found in a database. The technology can be used in all access control instances—

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

physical or logical--where there is a need for a living person to be positively identified and authenticated.

The reasons for using BTPs include the positive authentication and verification of a person, ensuring the confidentiality of information in storage or in transit. Other reasons are the non-repudiation of acts or transactions, deterrent of identity theft, convenient, safe, non-intrusive, and reduced administration costs compared to passwords. The effectiveness of BTPs are increased if biometric solutions are implemented in combination with Smart Cards and PKI.

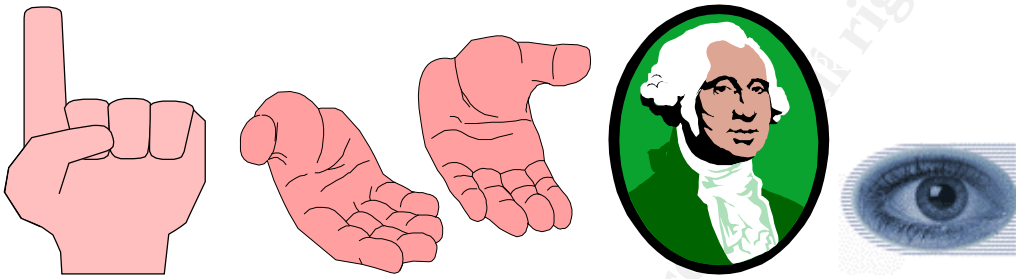

Figure 1--Physiological attributes of a living person

Before resorting to verification or authentication, however, the physiological or behavioral attributes of the living person have to be collected and when there is a need for identification, similar attributes from a living person are read and compared with the ones in the database. If a match between the two sets of data is found, then the person is said to be positively identified (verified) and authenticated for who he or she claimed to be. This process is used in the identification and authentication of living persons because

Figure 2--Stage One in BTP Reading

biometric applications do not process the data collected on dead people.

Biometrics goes from an enrollment or adaptation role—the initial stage where information is read or stored for future use—to recognition (verification) and to the identification stages. While passwords can be stolen or sometimes cracked, someone's fingerprint, voice-print and iris scan are unique to an individual. Biometric products store a kind of digital hash of a fingerprint, iris scan or voice-print--not the actual image—in a database for later comparison. The data can be collected voluntarily or through surveillance involuntarily.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

A BTP—such as a fingerprint scanner—performs authentication and verification in stages.

- The enrollment stage, a mechanism will scan and capture the ridges and undulations of your fingertip
- The voluminous data is then compressed to make it suitable for database storage

Figure 3--Stage TWO of BTP Process

- The BTP then goes through the comparison/evaluation stage where a processor compares newly captured data with similar data already stored in a database
- The final stage is the presentation stage where similar or not similar message is returned using an interface of an application. .

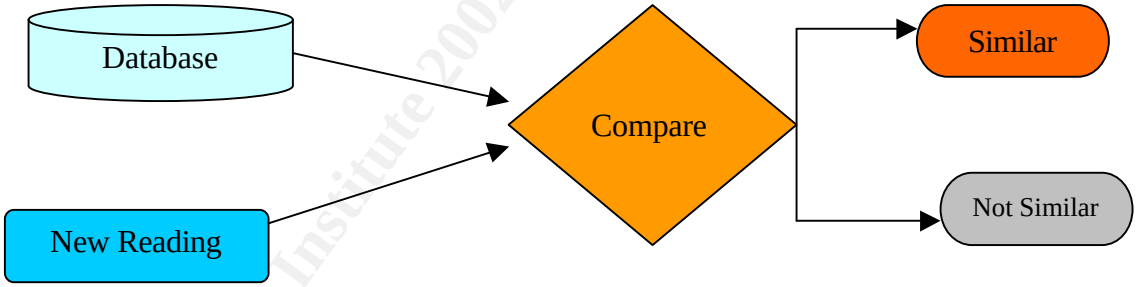

Figure 4--Final Stage of the BTP Process

Put simply, a BTP resolves a pattern recognition problem by separating the original from the forged using comparisons. The mode of comparison is classified as a "one-to-one" or "one-to-many." In a one-to-one comparison, a pattern of the living person is compared to the one and only one that already exists in the database to authenticate a claimant of an identity. In a one-to-many comparison, the pattern of an identity is compared against all patterns already stored in the database with the purpose of identifying whose identity is the current pattern.

The mission

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

When all fingers pointed to lax of security in the September 11 attacks, when the responsibility of protecting information or other assets lies on custodians of such assets, and when the burden of proof that "due diligence" has been taken to protect critical resources is on the security professional, the mission of safeguarding security focal points and resources becomes paramount. It calls for keeping both intruders and identity thieves at bay using whatever tools that accomplish the mission. While reactive security tools such as Intrusion Detection Systems, Firewalls and other perimeter or boarder protection tools may help to send an alert of suspicious activity by intruders, they may be ineffective against insider attack by authenticated users or by identity thieves. It is reasonable, then, to assume that proactive security tools such as Biometric Technology Products (BTPs) are well suited to stomp out imposters.

Benefits of using BTPs

Biometric technologies are well matched to statutory privacy mandates such as the protection of:

- Information in databases including customers and teller identification using fingerprint, iris, and facial recognition
- ATM access using iris and facial recognition.
- Transactions in transit over the telephone using voice recognition
- Computer-aided online transactions using voice, iris, fingerprint, and facial recognition
- Point of sale (POS) transactions using signature dynamics and fingerprint
- B2B, C2B and VPN transactions

Several branches and agencies of the Federal government have embraced Biometric Technology right from the introduction of the technologies in the 70s and 80s. The Department of Defense has created the U.S. Army's Biometrics Department whose goal is to replace passwords with Biometric tools such as fingerprint scans and other body-based authentication that would allow defense personnel to gain access to computer networks. The September 11 WTC and Pentagon Terrorist attacks, too, have created a rising interest in biometric technology.

The Federal government and many other organizations are using biometric tools that identify people by fingerprints, face and eye scans and other physical traits. While pursuing terrorists, Federal officials are "beefing-up" security at airports and other key installations by implementing biometric tools. Additionally, they are encouraging biometrics companies to increase production of biometric tools while fine-tuning their accuracy.

Also, interest is fueled by the rise in hacker activities. The September 11 terrorists identity theft, for example, has heightened awareness, and the 150 or more firms that make up the industry are fine-tuning their products to minimize error rates and increase speed.

Concerns for Using BTP

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Despite biometrics' promises, obstacles to immediate and successful deploy still linger: opposition by civil libertarians for fear of the invasion of privacy; the prohibitive costs of these high-tech security systems, and the high "false positive" rate of the technology.

Recently, the ACLU condemned the use of face-recognition systems deployed in some airports by sighting experiments and studies done by both public and private organizations. The ACLU argues the studies proved Biometric tools are mostly inaccurate . One other objection to the use of Biometric Technology is the concern "how protected is the private data collected on people?" Is a person able to control the information gathered on himself/herself? Is the person able to avoid "tracking"—the ability to search records about a person and to monitor a person's activities in real time? How about "function creep?" This concern relates to using information for purposes other than the original propose for which it was collected (whether it is positive or negative).

The error rate (1% to 3%) is high in the list of concerns. Physiological biometrics (palm, finger, iris scan, etc.) have higher "false authentication rates (FAR)." This is the rate of wrongly identifying an imposter to be the real person. Behavioral biometrics, on the other hand, have higher "false recognition rates (FRR)." This is the rate of failing to recognize the real person and wrongly saying the person is not who he purports to be. Some contact lenses, for instance, could throw off eye-scanning devices, and criminals can fake fingerprints using silicon imprints made from wax molds.

Lack of an industry standard is also cited as a drawback of BTPs. It is just recently that a group of high-tech corporations including Microsoft, Novell, IBM and Compaq teamed up into the BioAPI Consortium to develop standards for hardware and software that is used in Biometrics. Other objections to the use of BTPs range from physical security-the ability to prevent intrusion into a person's space (to avoid the stigma of criminal connotations) to religious objections ("Mark of the Beast" in Revelation 13: 16-18).

In spite of these objections, Biometric technology is emerging as a potential pillar for "homeland security," and the Biometrics market--$66 million in 2000--is expected to reach $900 million by 2006.

Summary

Preventing unauthorized access to IT resources and other security-sensitive areas is every security professional's mission. Biometric Technology is providing the answer to many of the access management problems we have, especially the positive verification and authentication of people. It uses physiological attributes on palms, fingers, iris, voice and behavioral attributes such as keystrokes that are unique to each person. The numerous ridges and undulations on the palm or finger of a person, the 250 or more kinks in the iris of a human eye, the voice inflections or the key strokes learned over the years, can be used to verify a person's identity claims.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Because of the recent terrorist attacks, interest in Biometric Technology, the number of public/private organizations engaged in it, and the quality and number of products produced and deployed have increased dramatically. Investor interest in Biometric Technology companies is also at an all time high. The industry is also showing growth with some companies gaining larger market shares over others. Legislative requirements in the area of privacy have added fuel to the need for positive identification and authorization.

While numerous benefits can be listed for deploying Biometric Technology products, there are few concerns that need to be addressed to ensure total acceptance of the technology by users. Though some concerns could be legitimate, others are not. In spite of the concerns, however, Biometric Technology products are being deployed in local, regional and national security checkpoints thus bringing our identity theft woes to an end in the immediate future. It is safe to assume that if Biometric Technology tools were in place in our airports, the September 11 terrorists would have been identified as imposters and thus prevented from carrying out their horrendous acts.

Key Terms and Phrases in Biometrics

The following terms are adapted from "Association for Biometrics and International Computer Security Association Glossary of Biometric Terms"

Biometry is defined as the statistical analysis of biological observations and phenomena (Merriam Webster Dictionary).

Biometric Technologies are tools used to identify a living person by comparing that person's finger, palm, iris, and facial attributes with a previously stored similar information about living persons.

Biometric System is an automated system capable of capturing a biometric sample from an end user, extracting biometric data from that sample, comparing the biometric data with that contained in one or more reference templates (databases), deciding how well they match, and indicating whether or not an identification or verification of identify has been achieved.

Biometric Taxonomy is a method of classifying the role of biometrics within a given biometric application such as: cooperative vs. non-cooperative user, overt vs. covert Biometric System, Habituated vs. Non-Habituated user, Supervised vs. unsurprised user, and standard environment vs. non-standard environment.

False Acceptance is when a biometric system incorrectly identifies an individual or incorrectly verities an impostor against a claimed identify. Also known as a Type II error.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

False Acceptance Rate (FAR) is the probability that a biometric system will incorrectly identify an individual or will fail to reject and imposter. Also known as Type II error rate.

FAR = NFA / NIIA or FAR = MFA / NIVA (where FAR is the false acceptance rate, NFA is the number of false acceptance, NIIA is the number of impostor identification attempts, and NIVA is the number of impostor verification attempts).

References

Ashbourn, Julian. "Implementing Biometric Systems." Association For Biometrics. 1998.

Association for Biometrics and International Computer Security Association. "Glossary of Biometric Terms," 1998.

Association for Biometrics. "Biometrics for User Authentication in E- and M-Commerce: The 3rd Arm of the Triangle with Encryption and Smart Cards." Hayes, Middlesex. 14 October 1999.

Bowman, Erik J. "Overview of the Biometric Identification Technology Industry," Defending Cyberspace 99.

Campbell and et al. "Government Applications and Operations" The Biometric Consortium. http://www.biometrics.org/REPORTS/CTSTG96/ (1996).

CardTech/SecurTech 2000. "Biometrics and the Financial Services Modernization Act of 1999: Using Biometric Technologies to Safeguard the Privacy of Financial Customers, Transaction, Data and assets," May 3, 2000.

Davies, Simon G. "Touching Big Brother: How biometric technology will fuse flesh and machine." http://www.privacy.org/pi/reports/biometric.html (1994).

Dupont, Daniel G. "Seen Before: To guard against terrorism, the Pentagon looks to Image-recognition technology," Scientific American. December 1999.

Fuller, Clinton C. Hearing on Biometrics and the Future of Money, Subcommittee on Domestic and International Monetary Policy, Committee on Banking and Financial Services, May 20, 1998.

Gunnerson, Gary. "Are You ready for Biometrics? Biometric ID systems bring tighter security to networks and greater convenience to users." PC Magazine Online. http://www.zdnet.com/pcmag/features/biometrics/intro.html (23 Feb 1999).

Jain and et al. "Biometrics: Promising frontiers for emerging identification market" Computer. http://www.cse.msu.edu/cgi-user/web/tech/document?ID=436 (Feb 2000)

Liu, Simon, and Mark Silverman. A Practical Guide to Biometric Security Technology" IT Pro-Security.. http://www.computer.org/itpro/homepage/Jan_Feb/security3.htm (Jan-Feb 2001).

Mannix, Margaret. "Stolen names, Stolen lives: Fake Ids helped the terrorists; but don't expect a quick fix for identity theft." U.S. News & World Report. (12 Nov 2001).

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

O'Sullivan, Orla. "Biometrics comes to life" ABA. http://www.banking.com/aba/cover_0197.htm (19 Sept 2001)

Page, Douglas. "Biometrics: What's Ahead." High Technology Careers Magazine. http://www.hightechcareers.com/doc198/ahead198.html

PC Labs Reviews. "Biometric Security: How it works." PC Magazine Online. http://www.zdnet.com/pcmag/features/biometrics/how.html

Silicon Valley/San Jose Business Journal. "Cyber Crimes Soar." http://bizjournals.bcentral.com/sanjose/stories/2001/03/12/daily14.html (12 Mar 2001).

The Biometric Consortium.

Whitted, Lori and Joe Loughran. "Making a Market in Biometrics: A presentation to the IBIA," The McLean Group, McLean, VA. September 15, 1999.

Wirtz, Bridgitte. "Biometric Systems 101 and Beyond: An Introduction to and Evaluation of the Technology and an Overview on Current Issues."

Woodward, Jr., John D. "On 'Biometrics and the Future of Money', " Testimony for the Hearing of the Subcommittee on Domestic and International Monetary Policy, Committee on Banking and Financial Services, U.S. House of Representatives, One Hundred Fifth Congress. May 20, 1998.

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 24th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced