

ICTN 4040

Section 601

Communication Security

Biometrics: 21st Century Security

Stan Smith

East Carolina University

Biometrics: 21st Century Security

Since September 11 2001 security has been in the forefront of American concerns. Granted, the general population is most concerned with personal physical security, which basically translates to physical security at the work place. We all hear of the horrible stories of disgruntled employees who bring a gun to work to kill fellow coworkers. That is not to mention the dangerous world we live in this day and time with terrorism. I think biometrics will be the biggest security tool used in the 21st century to protect the physical attributes of a company or its assets. I have decided to write my paper on this intriguing subject and how it relates to security of information networks.

Biometrics is a process used to identify or authenticate an individual's identity using any of a series of physical or behavioral characteristics. These characteristics can include but are not limited to fingerprints, hand or palm geometry, retina and iris scans, facial mapping, signature or writing style, and more recently, DNA maps. While relatively new, biometrics is rapidly advancing and growing in acceptance and use. The importance of this emerging technology does not necessarily lie in learning the intricacies of how biometric science works, but in exploring the management of the exposures biometrics present to individuals, businesses, and governments. This process begins with identifying the cyber risk exposures that biometrics makes possible.

System vulnerabilities are weak points that are identified in various internal network entry points and integral components such as workstations, employee

awareness, servers, databases, mainframes, mobile users and remote users. In addition, external network influences that pose weak points include vendors, customers, and partners.

System circumvention involves using systems in ways they were not intended. For example, hackers can gain access to a system using hardware and software weaknesses. Once a system's weakness has been found, it gives intruders the ability to use, sell, alter or destroy the data stored on it. The weakness could be from inadequate network security, or leaked or stolen passwords. Hackers may include terrorists, stalkers, abusive ex-spouses, blackmailers or organized crime. There is no single profile that encompasses all hackers, either by the methods they use or by their motives for invading data systems.

Verification fraud involves circumvention of the system during the process of verification itself that can be achieved in a number of ways. A perpetrator may be able to force an individual with registered biometrics to provide his biometric sample, enabling entry to the network.

Enrollment fraud. Are you who you say you are? Persons will enter an organization under the guise of employment service with the malicious motivation of system infiltration. This is accomplished through providing biometric information just like every other employee, which allows full access to security, premises and information systems. What constitutes authentic information? Can that information be tampered with?

Strong network security is the first concern a Chief Information Security Officer (CISO) must ensure when working with biometrics. Employment of

appropriate firewalls, routers, antiviral and anti-Spam methods will help to reduce the impact of a system breach by a hacker.

A verification process must be in place to ensure the right people are getting in to the right places. It is not enough to assume absolute verification with biometrics alone, but rather as part of a well designed security implementation that considers strong two factor authentication, such as a PIN or digital signature.

As biometrics become more critical in the protection of civil infrastructure, they will have to become more interoperable, scalable, usable, reliable, and secure. That will require comprehensive biometric standards. The more you know about proposed biometric standards, the better equipped you will be to evaluate the biometric products you are considering for your own systems.

In the following paragraphs are examples of some of the biometric products available today.

The Facekey Standard Biometric Access Control System combines face recognition and fingerprint recognition to provide the highest level of security. There is no need for cards, keys, or keypads. The combination of two biometrics makes it possible to have security with an error rate approaching zero. Each unit of the Biometric Access Control System can control up to two doors and multiple units can be networked to connect multiple doors at multiple sites in the US or internationally. The Facekey Standard Biometric Access Control System integrates a controller with a fingerprint reader and camera. Readers that accept proximity cards, swipe cards, or keypads can be added for an additional charge. A standard

UPS protects against power failures. The system uses technology to identify an individual based upon both his or her face and fingerprints. The system works by converting information about the individual's face and fingerprints into a unique code. Users register or enroll into the system by recording their facial and fingerprint patterns. As the user approaches the door, his or her live face and fingerprints are matched with the stored patterns. Face recognition requires proper lighting at each access point. When access has been granted, the unit will produce a signal to open the door and the name of the user, the location, and the date will be logged. If an unauthorized person attempts access, the door does not open and that event is recorded as an "unknown user." If an enrolled user attempts to access a location that he or she is not authorized to access, that person's name, the location, and the date will be logged. If communication with the server is lost, the controller will continue to identify authorized users, grant access, and record the events. The server will be updated with information collected at the door when communication is restored.

Recognition Systems' biometric HandReaders simultaneously analyze more than 31,000 points and instantaneously records more than 90 separate measurements of an individual's hand, including length, width, thickness, and surface area to verify that the person using the device is really who he or she claims to be. The HandReader compares this information with a "template" of the individual's hand that has previously been stored in the reader, on a server, or on a card. Once the person has been identified as a valid user, a door can be

opened, access can be provided, or time recorded. The reading and verification process takes less than a second with impeccable reliability.

Once the stuff of James Bond movies, fingerprint reading sensors have gone mainstream as a way to log on to your computer, or on to web sites you visit. Even if they are used mainly as a convenience, fingerprint readers can contribute to security, because people using them are less inclined to adopt insecure methods for remembering passwords, like writing them on visible Post-it Notes, or using the simple password again and again. The Fujitsu fingerprint reader is very sophisticated compared to other fingerprint recognition devices, as it will not work unless it detects blood coursing through the veins in your finger. It is much more difficult to imitate another person's internal structure, since it can not be viewed by the naked eye, nor can it be lifted from a surface, like fingerprints.

By the end of 2005, the US government is expected to announce that Personal Identity Verification cards must use a mathematical, minutiae-based template of fingerprint images of cardholders' two index fingers instead of compressed images of the prints themselves. Vendors are excited because the standard would allow faster authentication with less data and more privacy. This new template will stimulate the industry to have more companies providing products to meet this standard, which is a major step forward for the biometric industry. PIV cards are a mandate from President Bush that all federal employees and contractors have secure credentials for physical access to federal facilities and networks.

References

- Arnone, Michael. "Feds to use Faster, Safer Fingerprint Standard,"
<http://proquest.umi.com.jproxy.lib.ecu.edu/pqdlink?index=62&did=953585241&SrchMode=1&sid=2&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1145222179&clientId=15121>
- Barton, Bruce. "The Emerging Cyber Risks of Biometrics,"
<http://proquest.umi.com.jproxy.lib.ecu.edu/pqdlink?index=45&did=913086311&SrchMode=1&sid=1&Fmt=4&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1145216279&clientId=15121#fulltext>
- Boehret, Katherine. "The Mossberg Solution: Using a Fingerprint to Log on to your PC,"
<http://proquest.umi.com.jproxy.lib.ecu.edu/pqdlink?index=4&did=1003524561&SrchMode=1&sid=2&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1145217829&clientId=15121>
- O'Leary, Tim. "Expanding Biometric Applications,"
<http://proquest.umi.com.jproxy.lib.ecu.edu/pqdlink?index=2&did=1018956871&SrchMode=1&sid=2&Fmt=4&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1145217829&clientId=15121>
- Ryan, Russ. "Setting the Standard on Biometrics,"
<http://proquest.umi.com.jproxy.lib.ecu.edu/pqdlink?index=11&did=1015548611&SrchMode=1&sid=2&Fmt=4&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1145218879&clientId=15121>