Global Information Assurance Certification Paper

Biometrics: Fingerprint Authentication
Zeena Merchant
January 19, 2001

How secure are passwords? With the numerous passwords that an individual has to remember, they are often forgotten, misplaced, or stolen. Think of how many different passwords you have to remember: computer passwords, internet site logons and passwords, PIN numbers for the ATM and for credit cards, the list goes on. Most of the time, users end up writing down their various passwords in order to remember all of them. We have all been places where we have seen passwords written on a sticky piece of paper and attached to the side of the computer. What is the risk there? How can it be prevented? Enforcing password policies will certainly help in controlling access to computers, but often times it is just not enough.

One alternative to conventional security methods is in Biometrics. Biometric devices use personal characteristics to verify a user's identity. These characteristics can include face recognition, fingerprint or eye scans and voice or signature identification. Any of these traits can be used to uniquely identify an individual and could become an alternative to passwords for security. Biometric methods cannot be stolen or lost; and in using biometrics, an individual does not have to memorize many different confusing passwords or pin codes. This paper will be concentrating on biometric authentication through the use of fingerprints.

Authentication

Identification and authentication are important aspects of security. Identification deals with recognition of a unique individual while authentication is how this identity is verified. This keeps unauthorized users from obtaining restricted information. For example:

Joanne needs to get some jewelry out of her safe deposit box. When she arrives at the bank, she introduces herself to John Doe (the bank clerk) and asks him to help access her box. Before assisting Joanne in her need, she is asked for proof of her identity. She presents her driver's license to John, which verifies her identity, and the transaction can then continue.

Identification and authentication are much more difficult than presenting your driver's license when dealing with computer access and on-line transactions. There are three different types of items used for identification and authentication:

- Something the person has (identification card, token card, smartcard)
- Something the person knows (user name, password, pin number)
- A physical characteristic of the person (fingerprint, retina)

Unlike an identification card or password, it is much more difficult for an unauthorized user to obtain a person's physical characteristic. That is why biometrics is becoming a highly sought option for security.

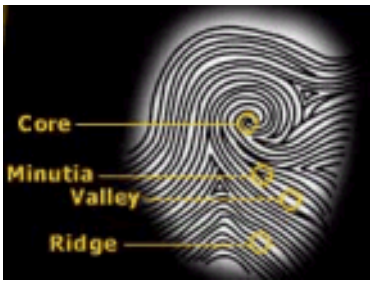
Fingerprint Biometrics

Every person's fingerprint is unique and is a feature that stays with the person throughout his/her life. This makes the fingerprint the most reliable kind of personal identification because it cannot be forgotten, misplaced, or stolen. Fingerprint authorization is potentially the most affordable and convenient method of verifying a person's identity.

As with any technology, fingerprint authorization requires a means by which to scan and recognize the print. Currently, the fingerprint is the only method that can be adopted and used for authorization on personal computers. Packages that check users' prints include American Biometrics' BioMouse Plus, Biometric Access' SecureTouch 98, Mytec Technologies' Touchstone and NEC's TouchPass. All of these tools scan the user's fingerprint and analyze the print to ensure a match.

The lines that create a fingerprint pattern are called ridges and the spaces between the ridges are called valleys. It is through the pattern of these ridges and valleys that a unique fingerprint is matched for verification and authorization. The fingerprint scanner works by taking a mathematical snapshot of a user's unique biological traits and saving the snapshot as a minutia file. The minutia file that is stored in the database cannot ever be reconverted back to the original fingerprint image.

Image Capture



There are two approaches for capturing the fingerprint image for matching: minutia matching and global pattern matching. Minutia matching is a more microscopic approach that analyzes the features of the fingerprint, such as the location and direction of the ridges, for matching. The only problem with this approach is that it is difficult to extract the minutiae points accurately if the fingerprint is in some way distorted. The more macroscopic approach is global pattern matching where the flow of the ridges is compared at all locations between a pair of fingerprint images; however, this can be affected by the direction that the image is rotated.

Some of the current scanners available for image capture include:

- Optical Scanner - captures a fingerprint image using a light source refracted through a prism
- Thermal Scanner - very small sensor that produces a larger image of the finger and is contrast-independent
- Capacitive Scanner - uses light to illuminate a finger placed on a glass surface and records the reflection of this light with a solid-state camera

Each of these devices use light to measure the ridges and non-ridges, take an original fingerprint image, capture the minutia points and create an identifying template from the minutia points.

Image Processing

Following the image capture, image processing is performed to achieve a definitive match on the individual. At this stage, image features are detected and enhanced for verification against the stored minutia file. Image enhancement is used to reduce any distortion of the fingerprint caused by dirt, cuts, scars, sweat and dry skin.

Image Verification

At the verification stage, the image of the fingerprint is compared against the authorized user's minutia file to determine a match and grant access to the individual.

Potential Issues

Fingerprint authentication is becoming a popular method for authorization but is still met with some resistance from the public. Although fingerprint biometrics maintains a high level of security and is easy to use, it still faces some issues including:

- Privacy
- False Rejection
- False Acceptance
- Accuracy
- Setting Standards

Privacy

Comparison and storage of unique biological traits makes some individuals feel that their privacy is being invaded. Many associate fingerprint scanning with the fingerprinting of alleged criminals and are therefore hesitant to accept this technology.

False Rejection Rate (FRR)
False rejection occurs when a registered user does not gain access to the system. This person has then been falsely rejected from access.

False Acceptance Rate (FAR)
False acceptance is when an unauthorized user gains access to a biometrically protected system.

Accuracy
Although fingerprints are unique to an individual, there are instances where a fingerprint may become distorted and authorization will not be granted to the user. As discussed above in image processing, dirt, cuts, scars, sweat and dry skin can cause fingerprint distortion.

Setting Standards
According to the International Computer Security Association 1999 Biometrics Survey, more than 330 fingerprint authentication products are marketed by vendors. This raises concerns over standards, integration with existing systems and long-term support.

Conclusion
The speed and cost of data scanning, storage, and retrieval technology has progressed to the point that the use of fingerprint recognition for security is now a feasible and affordable alternative to conventional security practices. A good system will combine "what you are" with "what you know" or "what you have." Fingerprints are the general biometric option of choice because of their decreasing cost, increasing popularity and continued integration into the desktop environment. Properly implemented, fingerprints offer potential for high accuracy and eliminated duplication, theft, forgetfulness and loss. Some of the future applications of fingerprint authentication, in addition to computer system authorization, may include: internet access, payment services, credit card and payment transactions, automotive anti-theft devices, travel, etc. The potential is endless.

> *"Stronger authentication methods often involve hardware -- a tangible object or artifact -- that must be associated with authorized users and that is not easily duplicated. (The ultimate `hardware' involved might well be biometric in nature: a person's handprint, a fingerprint, or a retinal pattern.) Of course, except in the case of biometric identifiers, all authentication systems can be compromised if the secret or the hardware token belonging only to the proper party is passed on to unauthorized parties." (Dam)*

References

Dam, Kenneth W. and Lin, Herbert S., Editors. "CRISIS: Cryptography's Role In Securing The Information Society." NRC Project on National Cryptography Policy. 1996.
URL: http://www.nap.edu/readingroom/books/crisis/frontmatter.txt. (21 March 2000).

"Fingerprint Authentication." National Security Agency.
URL: http://www.nsa.gov/programs/tech/factshts/fingrpnt.html

Fingerprint Authentication – The time has finally arrived." Veridicom.
"URL: http://www.veridicom.com/technology/fingerprint.htm

Seifried, Kurt. "WWW Authentication." Security Portal. January 28, 1999.
URL: http://www.securityportal.com/research/www-auth

"Securing Your WebSpeed Application with an Authentication and Authorization Product." Progress Software.
URL: http://www.progress.com/webspeed/whitepapers/securing_authentication.htm

"What is Biometric Authentication?" American Biometric Company.
URL: http://www.biomouse.com/whitepapers/biometric.htm

Williams, Charles Williams. "Who Goes There? Authentication in the On-Line World." The Business Forum.
URL: http://www.bizforum.org/whitepapers/cylink002.htm

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor