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.

Biometrics: Technology That Gives You a Password You Can't Share

User passwords have always been a big issue for administrators and for users. For administrators, it creates a huge workload to administer passwords. Users have a hard time memorizing their password, which creates a big security problem. This paper examines biometrics as a means for making user authentication more secure based on a unique identifier, the fingerprint. New and affordable biometric products are popping up in the market and fingerprint recognition provides the most reliable method of identification because...

Copyright SANS Institute

Author Retains Full Rights

AD

Automate more Web application scanning.

watchfire

Yevgeniy Libov

BIOMETRICS: TECHNOLOGY THAT GIVES YOU A PASSWORD YOU CAN'T SHARE

Version 1.2e

07/09/01

Introduction

User passwords have always been a big issue for administrators and for users. For administrators, it creates a huge workload to administer passwords. Users have a hard time memorizing their password, which creates a big security problem. For example, people making their passwords easy to remember thus their passwords making easier to crack. But as we all know - any password can be cracked. To make user authentication more secure, user should be identified not by "what he/she knows" but by "who he/she is"-a unique identifier, which cannot be easily hacked and cannot be passed to another user. Biometrics makes this technology possible.

Biometrics is the ability to automatically recognize a person using distinguishing traits such as fingerprints, face, retina or iris from the eye, voice, or hand geometry. Now since biometric technology is becoming cheaper, it is becoming heavily used in information technology. Fingerprint recognition is the most popular method of biometric recognition. It's not very expensive and it's very accurate. The cost of fingerprint recognition systems continues to decline. Where fingerprint recognition systems cost over $1000 several years ago, consumers can now buy a system for under $100 per seat. New and affordable biometric products are popping up in the market and fingerprint recognition provides the most reliable method of identification because no person's prints are identical to those of another individual. Even identical twins have different fingerprints. In most cases, fingerprints remain the same throughout a person's lifetime. The ridges on the fingertips change only as a result of surgery, disease, or an accident.

Background

Many people assume that use of fingerprints for identification is a new technology. First use of fingerprint as a identifier date back to 2nd century B.C. China, where the identity of the sender of an important document could be verified by his fingerprint impression in the wax seal. The fact that fingerprints were unique to each individual and therefore could be used to accurately identify an individual was known back in 17th century. The 19th century introduced systematic approaches to matching fingerprints to certain individuals. The Henry classification system is one systematic approach based on patterns such as loops and whorls, is still used today to organize fingerprint card files. It was developed by a British policeman during the British occupation of India in the 1800's.

Now, the traditional "inking" of one's fingerprint and pressing it against a paper card is still the standardized way of capturing an individuals fingerprint.
The fingerprint scanners are proven to be the most successful biometric device. Fingerprint recognition devices/applications account for nearly 80 percent of the total worldwide biometrics market.

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

Australia was the first country to adopt a national computerized form of fingerprint imaging, which implemented fingerprint imaging/recognition technology into its law enforcement system back in 1986.

How does it work?

Fingerprint recognition device captures the unique pattern of lines on the tip of a finger. These unique pattern of lines can either be in a loop, whorl, or arch pattern.

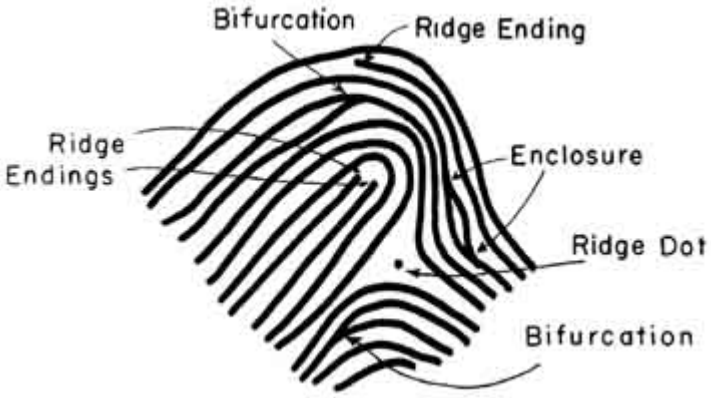
Arch
5% of all prints

Loop
65% of all prints

Whorl
30% of all prints

The loop form can be found in 65% of all the prints, whorl in 30% and arch only in 10%. A loop pattern can be detected when the ridges start on one side of the finger, reach the center of the finger and then go or loop back to the same side. A whorl pattern can be identified as the concentric circles that are formed by the ridges in the center of one's finger. The remainder of these ridges shape themselves around this whorl pattern. Finally, the arch pattern is where the ridges start at one side of the finger and span themselves across the center of the finger to the other side.

There are several methods in accomplishing the process of identifying one's fingerprint. The most common method involves recording and comparing the fingerprint's minutiae points. Minutiae points are the points where print ridges come together or end. Minutiae points can be considered the 'uniqueness' of an individual's fingerprint. Minutiae points are referred to as 'points' because the fingerprint scanner assigns locations to the minutiae using X, Y and directional variables.



Here is the list of characteristics of minutiae points :

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

1. Bifurcation-the point at which a ridge splits into multiple ridges, called branches
2. Divergence-this is the point where parallel ridges either spread apart or come together
3. Enclosure-occurs when a ridge splits into two branches and then comes together again shortly thereafter
4. Ending-occurs when a ridge terminates
5. Valley-spaces or gaps that are on either side of a ridge

Usually, fingerprint that has been scanned by a fingerprint identification system, there are generally between 30 and 40 minutiae. FBI has found that no two individuals can have more than eight common minutiae points.

Other methods of identifying a person's fingerprint include counting the number of ridges between points, processing the fingerprint image and recording the print's sound waves. Fingerprint recognition technology is based on two electronic capturing methods: optical and capacitive. Optical fingerprint technologies require the user to place his or her finger on a glass substrate at which point an internal light source from the fingerprint device is projected onto the fingerprint. The image is then captured by a charge-coupled device. Optical methods have been used extensively and have been in existence for the past decade. They are proven but are on the expensive side and are not always reliable due to environmental conditions. A build up of dirt, grime, and oil from one's finger can leave a "ghost" image which is referred to as a "latent image". As a result, their employment has been confined to specific criminal justice and military installations.
On the other hand, capacitive imaging looks to make fingerprint recognition available to the masses by making fingerprint imaging devices (hardware) more compact in size, less expensive, and more reliable. Capacitive systems analyze one's fingerprint by detecting the electrical field around the fingerprint using a sensor chip and an array of circuits. When a person's fingerprint is initially captured, a template is constructed and stored in a data storage system or database. This template is then used to compare against a person's fingerprint for each subsequent time he or she scans their finger. The fingerprint requires one of the largest data templates in the biometric field. The finger data template can range anywhere from several hundred bytes to over 1,000 bytes depending upon the level of security that is required and the method that is used to scan one's fingerprint.
The identifying power of fingerprint recognition systems seems to show that they tend to reject over three percent of authorized users while maintaining false accept rates of less than one in a million.

Real-Life example

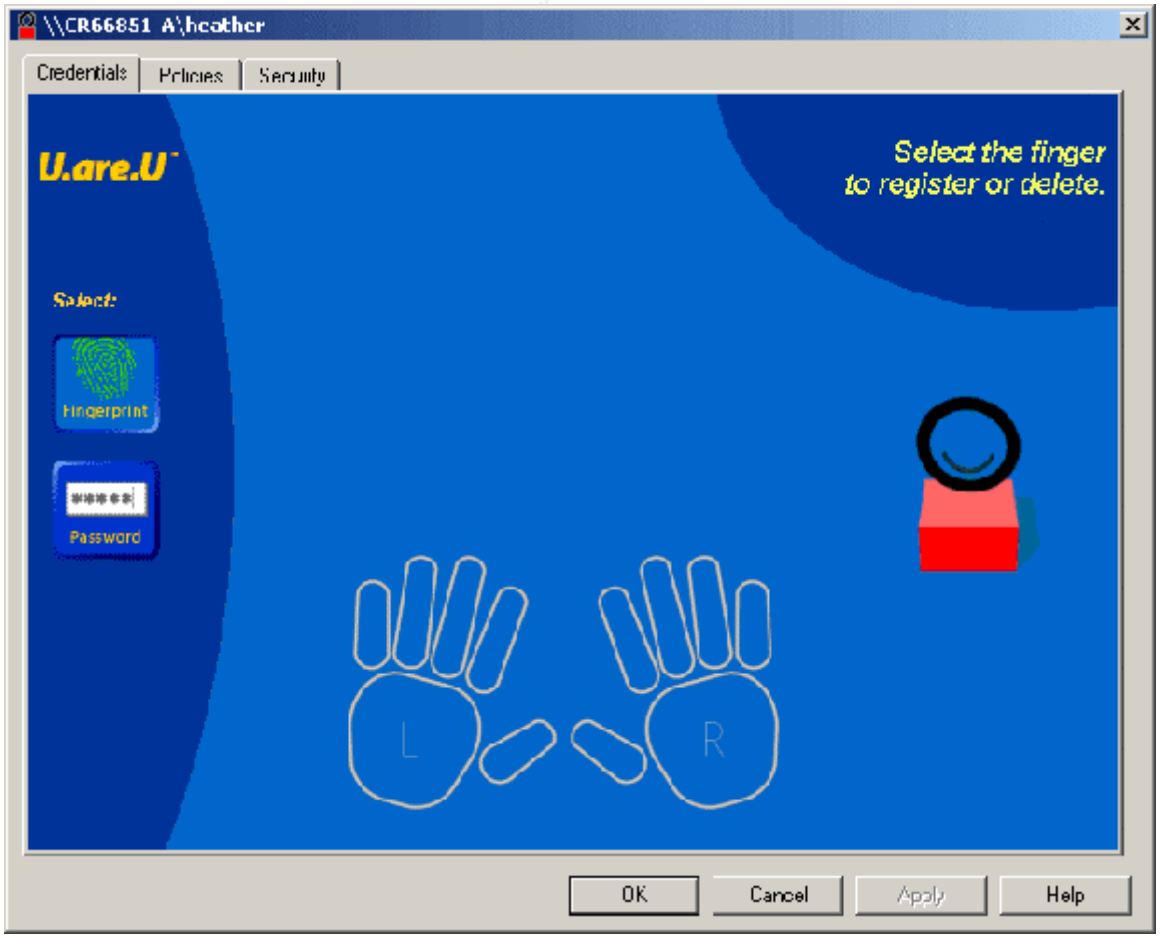
Digital Persona is a company that is forging ahead with the need for user recognition equipment. Their product, U.are.U, is making this technology easy to understand and use.

U.are.U is the product developed by Digital Persona. This product allows a user to login to the domain or locally using your fingerprint instead of the password. There are three different packages available: U.are.U Deluxe is the simplest package designed for home and small office users, U.are.U Pro for corporate usage and U.are.U online for the Internet usage. All packages includes software and hardware device. The fingerprint

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

recognition device is plug-and-play, connected to the USB port and does not require a power supply.

The Deluxe package provides you with the software that is installed locally on their workstation and recognition device that connects to the USB port. After installation the user can scan their fingers and can use fingerprints instead of the password. The first person to login after the installation becomes the administrator. The program automatically determines the optimal moment for capturing. Each finger is scanned four times for accuracy.



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

While scanning, sensors extract fingerprints in more then 70 points and store this mathematical template in a numeric 256-byte file. It's nearly impossible to recreate the fingerprint from this file, insuring that the user's identity cannot be cloned.
During the login process the fingerprint compared to the template stored in the file. To prevent play back attacks, U.are.U establishes a challenge-response link with the PC prior to sending a fingerprint. If for some reason the user cannot login using their fingerprint, the username and password can be used to gain access but this feature can be disabled. Administrators can add another layer of security by requiring user to use two or more fingers for authentication.

The product includes some additional features: One Touch Password, One Touch Screensaver, U.are.U Software Development Kit and Private Space. One Touch Password enables users to replace their password, user name, and other identification associated with an Internet site or computer applications. U.are.U Software Development Kit allows programmers to protect any software with fingerprint security. One Touch Screensaver enables users to unlock their screensaver with their fingerprints. Private Space Dedicates a portion of the local or network drive as secure space for sensitive applications and confidential data, which are automatically encrypted and accessed with a fingerprint. When enabled, user can specify the amount of space and location of the Private Space. All data in space is encrypted and cannot be viewed by an unauthorized user. To gain access to the files in the Private Space the user has to authenticate using their fingerprint. U.are.U Pro comes in two parts Server and Workstation. Server includes additional capabilities: user roaming, secure server-based administration, backup domain controller support and enhances user administration. User roaming allows user to login from any workstation on the domain by providing centralized storage of user personal credentials. Secure server-based administration maintains strict adherence to the Windows NT Security Architecture for networked environments that include less secure Microsoft Windows 95/98 systems. And, the backup domain controller support allows U.are.U data replication to the BDC, if the PDC is unavailable.

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

U.are.U Pro Workstation includes all features of the Deluxe package in addition to the One Touch Internet and Administration Tools. One Touch Internet allows the user with single sign-on capabilities to business applications and forms. It recognizes and securely fills in all fields (such as password, username, credit card #, etc.) of any Web or Windows-based form with the touch of your finger. Administration Tools provides the ability for remote installation and configuration.

U.are.U Online allows you to use the product for the web applications and web page authentication. Fingerprint templates are stored in '3rd-party deposit box', and it works as the e-signature solution. U.are.U Online Service Integration Pack allows developers to easily and securely enable their service with U.are.U Online.

Conclusion

Biometric technology adds another layer of security, by insuring secure identification and authentication. The main advantage of this technology is that fingerprint unlike password is almost impossible to hack or to pass to another person. Use of solutions such as U.are.U eliminates a lot of administrative and users work. For example, resetting user passwords, making password scans to eliminate unsecured passwords and users do not have to memorize them. This solution also has its disadvantages. It requires software installation on the client, slows down the login process, and it costs extra money.

The future of biometric technologies is promising. Biometric devices and applications continue to grow worldwide. Biometric technologies will soon be the common way to gain access into your personal computer system. There are several other factors that will push the growth of biometric technologies. A major inhibitor of the growth of biometrics has been the cost to implement them. That is beginning to change as computer hardware and software as well as manufacturing prices fall in price. One can now go and purchase a fingerprint recognition system for under $100. Also, increased accuracy rates are and will play a big part in the acceptance of biometric technologies. The development and research into biometric error testing, false reject (false non-match)

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

and false accept (false match), has been of keen interest to biometric developers. How well do biometrics keep the "bad guys" out and let the "good guys" in will always be a question that is asked when customers look to implement a biometric technology. Both false match and false non-match error rates continue to improve and it is the balance between the two that will be critical when implementing a biometric technology.

Finally, new applications and new markets are expanding the deployment of biometric technology. Biometric applications that were once reserved for just military and other government applications are now finding their way into our daily lives. Biometric applications are surfacing in child day-care centers, health clubs, universities, and ATM's. The explosion of the Internet and Intranet's are also fueling the presence of biometrics. As e-commerce continues to develop as a mode of communication, many corporations and individuals are becoming concerned with security issues.

References

Chang, David "Fingerprint Recognition Through Circular Sampling"
http://www.cis.rit.edu/~dxc0331/web_thesis/thesis.html

"U.are.U Biometric Authentication Systems", Digital Persona, 2001
http://www.digitalpersona.com

Thomas, Keir "Peripherals review: fingerprint scanner", published in October 1999 issue of PC Direct.
http://www.zdnet.co.uk/pcdir/reviews/1999/10/uru/

http://netsecurity.about.com/compute/netsecurity/cs/biometrics1/

http://www.biometrics.org

Biometrics
http://netsecurity.about.com/compute/netsecurity/gi/dynamic/offsite.htm?site=http%3A%2F%2Fwww.sacman.com%2Findex.htm

"Let Your Finger Do the Login", CRN Testing Center, 12/31/00
http://winmag.techreviews.com/sections/topics/article/TT20010120S0002

Brown, Bruce "First Looks", July 9th 1999.
http://www.zdnet.com/pcmag/firstlooks/9807/f980709a.html,

Plain, Stephen W. "Digital Persona U.are.U Deluxe", from February 23rd 1999 issue of PC Magazine
http://www.zdnet.com/pcmag/features/biometrics/387166.html

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

Biometrics Technology: Frequently Asked Questions (FAQ)
http://www.ecfirst.com/biometricsfaq.html

Biometric Systems Performance and Security
http://www.mytec.com/02/bio-02-06.shtml

© SANS Institute 2002, Author retains full rights.

Last Updated: May 26th, 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**