

# Network Security: Biometrics - The Password Alternative

by

Ronald G. Wolak  
wolakron@scis.nova.edu

A paper submitted in fulfillment of the requirements  
for DISS 740 - Assignment Four, Task One

School of Computer and Information Sciences  
Nova Southeastern University

December 1998

An Abstract of a Paper Submitted to Nova Southeastern University  
in Fulfillment of the Requirements for DISS 740 - Assignment Four, Task One

## Network Security: Biometrics - The Password Alternative

by  
Ronald G. Wolak

December 1998

Passwords are the primary means of authenticating network users. However, network administrators are becoming concerned about the limited security provided by password authentication. Many administrators are now concluding that their password-based security systems are not all that secure. User passwords are routinely stolen, forgotten, shared, or intercepted by hackers. Another serious problem is that computer users have become too trusting. They routinely use the same password to enter both secure and insecure Web sites as well as their networks at work. In response to the proven lack of security provided by password authentication, network administrators are replacing network passwords with smartcards, biometric authentication, or a combination of the three. Smart cards are credit card-size devices that generate random numbers about every minute, in sync with counterparts on each entry point in the network. Smart cards work well as long as the card isn't stolen. A better choice to ensure network security is the use of biometrics. In the following pages, this paper investigated the different biometric techniques available to determine a person's identity. Also described, were the criteria for selecting a biometric security solution. In conclusion, efforts to establish biometric industry standards (including standard application program interfaces (APIs)) were discussed.

## Network Security: Biometrics - The Password Alternative

Passwords are the primary means of authenticating network users. However, network administrators are becoming concerned about the limited security provided by password authentication. Many administrators are now concluding that their password-based security systems are not all that secure. User passwords are routinely stolen, forgotten, shared, or intercepted by hackers. In a recent example of the limitations of passwords, a group of hackers from Europe broke into the e-mail system at [Stanford University](#), stole thousands of student and staff passwords, and went undetected for three weeks (Bloomberg News, 1998). Another serious problem is that computer users have become too trusting. They routinely use the same password to enter both secure and insecure Web sites as well as their networks at work.

In response to the proven lack of security provided by password authentication, network administrators are, in growing numbers, replacing network passwords with smartcards, biometric authentication, or a combination of the three. Smart cards are credit card-size devices that generate random numbers about every minute, in sync with counterparts on each entry point in the network. To log on to a computer, users enter a password and the number that appears on the smart card's LED window. Smart cards work well as long as the card isn't stolen. A better choice to ensure network security is the use of biometrics. Biometric verification provides a much higher level of security vs. traditional solutions such as passwords, smart cards, or tokens by verifying that the user is who he claims to be and not merely the holder of a card, token or password.

Biometrics, a science and business, identifies people by their physical characteristics. These characteristics include fingerprints, retinal prints, face prints, handprints, speech patterns, and even DNA profiles. One of the primary uses of biometric verification technology is to control access to computer networks. In 1998, analysts predict that total expenditures to create biometric security systems will reach \$100 million (Millman, 1998). Governments will spend approximately \$62 million and corporations \$38 million. In 1999, biometrics is expected to continue to grow, and total corporate spending for biometric hardware and software will increase to \$50 million. Spending will increase to \$1 billion in the year 2000.

In fact, many analysts predict that the rush to install biometric security systems will replace the Year 2000 computer crisis as the most pressing high-tech project once the millennium arrives (Bloomberg News, 1998). In the following pages, this paper investigates the different biometric techniques available to determine a person's identity. Also described, are the criteria for selecting a biometric security solution. In conclusion, efforts to establish biometric industry standards (including standard application program interfaces (APIs)) are discussed.

## Biometric Techniques

### Face

Face recognition is one of the newest biometric technologies. Specialized recognition software coupled with a video camera allows these systems to recognize people's faces. [Visionics](#), one of the industry leaders, developed a product called FaceIt (Garfinkel, 1998). FaceIt is a software engine that consists of advanced pattern recognition algorithms for automatically locating faces in complex scenes. FaceIt technology works either from a static image or from a video feed. The software is able to find human faces anywhere in the field of view and at any distance. It is also able to continuously track them and crop them out of the scene.

Once located, a facial image is transformed into an internal representation using an algorithm called Local Feature Analysis (LFA). This algorithm represents the image in terms of local, statistically pre-derived features from specific regions of the face. This representation (i.e. face print) is resistant to changes in lighting, skin tone, eyeglasses, facial expression, and hair. It also compensates for pose variations of up to 35 degrees in all directions. Next, in order to determine a person's identity, FaceIt computes the degree of overlap between the live face print and those associated with known individuals stored in a database of facial images.

### Fingerprint

Fingerprint identification systems have been in use by the criminal justice community for more than 30 years. They are a "minutiae based" system as the algorithms locate and measure actual features in the fingerprint and equate them into minutiae template. The minutiae points measured are ridge endings and bifurcations. According to research company [Frost & Sullivan](#), fingerprint identification systems account for nearly 80 percent of the global biometric sales (Millman, 1998).

Recently, [Hewlett-Packard](#) (HP) announced its plans to implement biometric security features into its product line next year (Hagendorf, 1998). Fingerprint scanners able to authenticate users will ship with HP's OmniBook laptop line by early 1999. HP is offering the technology as an accessory for laptops first and will follow-up shortly with desktop systems.

[Identix](#) of Sunnyvale, California is the world's largest fingerprint security firm. [Compaq](#) recently began offering Identix fingerprint recognition technology as a stand-alone peripheral for enhanced computer security on their desktop systems. Identix also provides a large number of high-end verification solutions for such strategic applications as Oracle's security package for its global customers. These customers store more than half the world's known data.

## **Hand**

The typical hand geometry recognition system is comprised of a smart camera and computer hardware and software. Systems are able to measure the 3D geometry of a user's hand or fingers and confirm their identity within one second. Hand geometry recognition systems are perhaps the most accepted of the biometric technologies. Users like them because they are not intrusive and only have a .1 percent false reject rate (FRR) - one of the lowest in the industry. They are heavily used in the nuclear and defense industries due to their low false acceptance rate (FAR) of .1 percent. Also, they are reliable and low cost.

[Recognition Systems](#) is the worldwide leader in hand geometry biometric devices. However, [BioMet Partners](#) (an up and coming competitor) successfully applied the technology to perhaps the most difficult application for any biometric product. Their systems are now used at the visitor entry turnstiles at Disney World. On the average, 10,000 people register there every day. No other biometric has come close to breaking this record.

## **Iris**

Iris recognition technology identifies individuals by computer analysis of the patterns found in the iris of the human eye. The iris is the most mathematically unique feature of the human body - even more unique than fingerprints. It is even claimed that the human iris can identify a person more accurately than DNA. Iris recognition technology is considered the ultimate personal identifier.

Iris scanning is the most secure of the "productized" authentication techniques currently available. However, most products are too expensive for general use and have prices in the four- to five-digit range per device. In response, [IriScan](#), the major patent holder for iris recognition systems, is working on new products that will decrease the per-device cost by a factor of 10 or more. Shortly, iris-scanning devices will be available for less than \$500.

## **Signature**

Signature recognition systems require the user to sign his/her name with a stylus on a touchpad. Differences in basic styles, plus stroke speed and pressure, allow the system to differentiate and certify users with a high degree of accuracy. One example of a Windows-based signature recognition product is Quintet's SignLock. This technology is most appropriate at point-of-sale terminals.

## **Voice**

Voice recognition systems require the user to "enroll their voice", so that the system has a record of the user's voiceprint on file. This is accomplished by responding to prompts. The prompts can be visual prompts displayed on a screen, or audio played through PC

speakers and over the telephone. To authenticate the identity of the user, his/her voiceprint is compared to the voiceprint stored during the enrollment process. Voiceprints can reliably identify someone 90 to 99 percent of the time (Garfinkel, 1998). Voice authentication is most prevalent in the telephony industry for obvious reasons.

## Selection Criteria

Prior to selecting one of the above biometric authentication techniques, network administrators must understand the application, the user base, and the characteristics of the biometric device itself. The following are a few of the factors to be considered.

### User Acceptance

Some biometrics techniques (e.g. fingerprint identification) are perceived as an invasion of privacy. Biometric device manufacturers are careful to point out that they are not associated with the FBI's fingerprint recognition system ([Automated Fingerprint Identification System \(AFIS\)](#)), that most devices are unable to store raw fingerprints, and that fingerprints cannot be reconstructed based upon the data stored within the system. Another factor affecting user acceptance is the intrusiveness of the device. Users consider some biometric device types, particularly retinal scanning systems, to be quite intrusive.

### False Reject Rate

The false reject rate (FRR) is the rate at which a valid user is rejected from the system. This factor is less critical in the high-security environments that biometrics usually protect, but it can be a crucial factor with other applications. For example, Walt Disney World replaced tickets with hand-geometry devices because of the technology's very low FRR and its general acceptance by its customers (Willis, 1998). The company chose this technology because it would rather let a few fake hands in than offend valid customers with false rejects.

### False Acceptance Rate

The false acceptance rate (FAR) is the rate at which an intruder is identified as a valid user. The false acceptance rates of most devices are calculated by mathematically extrapolating field trial data. This practice makes it difficult to compare biometric technologies based upon quoted FAR numbers. FARs become critical when attempting to authenticate a user based on biometrics, instead of a trying to verify a person with a one-to-one or one-to-few operation. For example, according to [IriScan](#), if the probability of a false match between a known pair of biometrics is .001, then the probability of finding the wrong person in a database of only 200 people is .181. This increases quickly to .86 with a population of 2,000. Iris recognition trials show a much lower false acceptance probability of .000000000001. This is equivalent to searching a database of everyone on the planet and having only a .01 probability of a false acceptance.

## Calibration

A few fingerprint recognition systems require careful calibration by a trained technician. Also, voice recognition systems require extensive user training, especially at higher sensitivity levels.

## Users

Some users have difficulty using biometric devices. For example, people with light ridge definition in their fingers have difficulty using fingerprint recognition systems. Also, people working with abrasives can have their ridges worn away. Other problems arise from substantial physical differences resulting from age, gender, and ethnicity. Another consideration is users with excessively dry, wet, or dirty hands when using finger and hand recognition systems. Also, people wearing gloves are not able to use these systems. However, newer ultrasonic-based systems have been able to detect fingerprints through thin latex gloves.

## Data Security

The security of the connections between the biometric device and the host (as well as the host and any back-end verification systems) is very important in preventing wire snooping and playback attacks. Devices using standard cameras, microphones, and other equipment should encrypt or sign data packets on the wire. Also, in a domain environment, communications between client and server PCs should be encrypted. In addition to being protected during transfer, biometric template data should also be encrypted where it is stored.

## Conclusion

The [Gartner Group's](#) Business Technology Journal named the biometric techniques described above as one of the ten emerging technologies to watch in 1998 (Festa, 1998). In addition, industry revenues are expected to reach \$1 billion in the year 2000. Recognizing these facts, leading companies in the biometric industry (e.g. [Recognition Systems](#), [Identicator, Inc.](#), and [IriScan](#)) formed the [International Biometric Industry Association](#) (IBIA) in September of this year. The task of the organization is to advance, advocate, defend, and support the collective international interests of the biometric industry.

Two other organizations related to the field of biometrics are the U.S. government sponsored [Biometric Consortium](#) and the [International Customer Service Association](#) (ICSA) (on the commercial side). Both of these groups are chartered to promote biometric standards. Also, [IBM](#) and [The National Registry, Inc.](#) (both leaders in biometric application APIs) are working closely with these standards organizations to promote generic APIs. Biometric APIs would enable developers to swap biometric devices and algorithms as required. Such "swap-ability" is mandatory if the industry is going to meet revenue numbers projected in the next couple of years (Lange, 1998).

A closing note - under normal circumstances, common industry standards and APIs would be considered desirable. This is not the case when dealing with the politics of biometric authentication. Many groups want just the opposite. For example, the Metro Toronto Department of Social Services (prior to a recent biometric purchase) wanted to be assured that the system's biometric information was not standard and therefore could not be exchanged. The department insisted upon this requirement in order to protect its clients.

## Reference List

- Bloomberg News. (1998, November 18). Biometrics moves to the fore.  
*CNET News.com*. <http://www.news.com/News/Item/0,4,29020,00.html>
- Festa, P. (1998, January 27). 10 technologies to watch in 1998. *CNET News.com*.  
<http://www.news.com/News/Item/0,4,18540,00.html?st.ne.bp..bphed>
- Garfinkel, S. (1998, September). Body blocks: The future of security is biometrics.  
*PC World Magazine*.  
[http://www.pcworld.com/current\\_issue/article/0,1212,7548+5+0,00.html](http://www.pcworld.com/current_issue/article/0,1212,7548+5+0,00.html)
- Hagendorf, J. (1998, November 23). New notebooks: HP adds biometric security.  
*Computer ResellerNews*.  
<http://www.techweb.com/se/directlink.cgi?CRN19981123S0013>
- Lange, L. (1998, February 9). API's reach out and touch human-ID systems.  
*EETimes*. <http://www.techweb.com/se/directlink.cgi?EET19980209S0021>
- Millman, H. (1998, June 29). The one and only you. *InfoWorld*, 20(26), 87-88.
- Willis, D. (1998, June 1). Let your fingers do the logging in. *Network Computing*.  
<http://www.techweb.com/se/directlink.cgi?NWC19980601S0021>