Global Information Assurance Certification Paper

GSEC Practical Assignment
Version 1.2b

Face the Front Please:
Face Recognition as a Viable Authentication Method

Background

For years, the computer industry has relied on alphanumeric passwords to limit access to sensitive information. Initially, passwords themselves were a fairly robust authentication method because the raw computing power necessary to propagate a successful brute force or dictionary attack was either nonexistent, or simply too expensive for the masses. In recent years, technology has advanced to the point that millions of users worldwide possess systems with the computational ability to easily launch such attacks. Advances in cryptography have helped to ease the threat of brute force password cracking, but the best cryptographic algorithm in the world is useless if the users themselves compromise their own passwords. People are notoriously bad at generating passwords and the proliferation of the Internet has exasperated the problem. Individuals now have passwords for everything from their company network login to general websites, online financial information, email, Automated Teller Machines, credit cards, etc. As a result, individuals are forced to either physically document their passwords, or as is often the case, establish easy to remember (and therefore easy to crack) passwords. In either case, the reality is that passwords can be easily compromised via cracking, theft, and especially sharing. Therefore, the future of system security must lie in the ability to authenticate users based on methods that will uniquely identify an individual securely without relying on the individual to protect the authentication medium. The solution may very well be biometrics.

What is Biometrics?

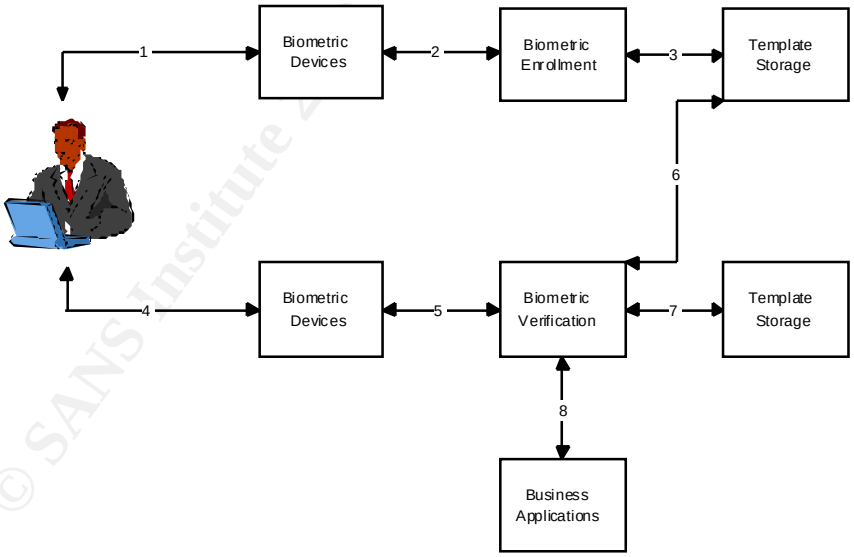
Biometrics is the use of individual's physical or behavioral characteristics to uniquely identify them for authentication purposes. Physical biometrics range from fingerprints, to hand or palm geometry, retina and iris patterns, or facial characteristics. Behavioral biometrics can include things such as signature, voice, keystroke patterns, and gait. Regardless of the type of biometrics employed, the common theme is the ability to use the individual as the authentication method. Individual characteristics can not be lost, stolen, or easily forged. For the purposes of this document, face recognition will be the only biometric technology discussed in detail.

What is Face Recognition?

Face recognition technologies uses an image captured by a digital camera or live data feeds to analyze the unique facial characteristics of an individual for security authentication purposes.

How Does Face Recognition Work?

Face recognition works by comparing a stored baseline image of a person with the image currently captured at each authentication session. Initially, during the biometric enrollment process, a digital image is captured either via a "still image" digital camera or a live video feed. Face recognition systems work in different ways, but typically, the software, scans the digital still image or data stream to locate an object that appears to be a head. Pattern matching algorithms are then employed to determine if a useable face is present. Once a face is detected, it is extracted from the background to compensate for size, lighting, expression and pose. This "normalized" face is then used to transform the facial characteristics such as the distance between the eyes, nose, and chin, as well as, general facial shape to establish a numerical facial representation known as the eigenface. The eigenface is then stored as a template in a local repository, central repository, or a portable token such as a smart card. Later, when the user attempts to authenticate with the system, a live image is captured either via a "still image" digital camera, or a live video feed. Again, the software scans the image or data stream to locate a head-like object. The software again extracts the face from the background and compensates for environmental factors as discussed above. This new "live" eigenface is then compared to the stored "template" eigenface for the individual and authentication is either confirmed or denied based on statistical comparisons of the similarities and differences noted in the two separately acquired images. This process is reproduced graphically in the figure below.



(1) Capture the chosen biometric; (2) process the biometric and extract and enroll the biometric template; (3) store the template in a local repository, a central repository, or a portable token such as a smart card; (4) live-scan the chosen biometric; (5) process the biometric and extract the biometric template; (6) match the scanned biometric against stored templates; (7) provide a matching score to business applications; (8) record a secure audit trail with respect to system use. Source: "A Practical Guide to Biometric Security Technology"

Types of Face Recognition Searching

Different systems employ different searching techniques to determine which faces are a matched pair. Some systems employ one-to-many searching, while others perform one-to-one matching. One-to-many searching involves comparing the current "authentication" image with a database of authorized user baseline or "template" images. If the software finds an acceptable match between the authentication and template images, then the individual is granted access. This type of matching is desirable because users are required only required to establish an initial baseline image; they have no information to remember and need not carry any type of physical identification. The other common type of matching employs one-to-one matching. In one-to-one matching, the numeric representation of the template image is stored on a smart card or magnetic stripe card. The user is required to use this card to load the template image in the system. The loaded template image and the newly captured authentication image are then directly compared to determine if the match is acceptable. One-to-one matching requires less computational resources than one-to-many matching because the software does not have to compare the authentication image to a conceivably large database of template images. In addition, one-to-one matching allows for the hybrid combination of biometrics and smart card technology. By storing the template on a smart card, users are responsible for maintaining the integrity of their own template, which eliminates the possibility of an attacker compromising the central repository. Furthermore, combining smart cards with face recognition enhances the user's privacy because the template is not stored in a central location that is subject to compromise. The tradeoff with one-to-one matching as compared to one-to-many searching is that the user is required to possess a physical identifier, and the user must actively initiate the verification process by loading the template image.

Limitations of Face Recognition Technology

Although face recognition technology presents some very promising potential uses, there are several concerns that must be appropriately addressed if face recognition technology is to gain widespread acceptance in the future. Specifically, it is necessary to address concerns such as privacy, false acceptance, false rejection, and technology standards.

Privacy

The issue with face recognition technology and privacy was discussed above briefly, but bears revisiting. Users are typically wary of giving companies access to digital representations of their personal physical traits. Although face recognition templates are not nearly as invasive as fingerprint authentication methods, there is nevertheless concern expressed by users of this technology. The privacy issue can be greatly reduced by implementing the hybrid biometric and smart card security methods discussed above.

False Acceptance

False acceptance occurs when an unauthorized individual is authenticated as authorized by the biometric system. False acceptance rates vary depending on the particular biometric software

being used, and the templates stored on the system. The FAR is increased in one-to-many searching systems because of the potential for several users to have similar eigenfaces stored in the central repository. This risk is greatly reduced in one-to-one matching systems because the possibility of similar eigenfaces confusing the authentication process is eliminated. Despite the type of searching/matching employed, in general, face recognition biometrics achieve a FAR of less than 1%.

False Rejection

False rejection occurs when an authorized individual is inappropriately denied access by the biometric system. Like FAR, false rejection rates also vary depending on software being used and the desired level of matching accuracy. In addition, environmental factors such as lighting, age, facial hair, and glasses can result in a higher FRR. Face recognition biometrics are typically prone to false rejection more often than false acceptance by design. However, like FAR, FRR for face recognition biometrics is still less than 1% in most configurations.

Technology Standards

Like any new technology, standards are a very important consideration when choosing an authentication method, due to concerns related to integration with future systems and product support long-term. Unfortunately, there are very few standards for biometric authentication systems presently. While the image-capturing medium is fairly standardized, the proprietary algorithms that generate the numerical eigenface representations are far from standard. Several initiatives are currently underway by various agencies to attempt to develop a standard for generating eigenfaces. These standards are essential to ensuring biometrics place in the future of authentication systems. Without standards, biometric systems will not be able to work with each other to provide the strong layered security structure that they were designed to accomplish.

How Much Will Face Recognition Cost?

Implementing biometric security is not without costs. The cost components that must be considered include:

- Digital cameras or other specifically designed products to capture the user's image
- Hardware and processing power to store the templates and process the matching function
- Software licenses
- Installation
- Maintenance
- User education and assimilation and the productivity costs involved with the initial transition
- Exception processing when users can no longer rely on their template due to physical changes caused by injury or aging

Perhaps the most significant of these costs to be considered involves user education and assimilation and exception processing. User acceptance of biometric technologies has been

mixed at best. Many users have expressed serious concerns about companies capturing and storing their biometric information. Educating users about company policies related to biometric security systems is perhaps the most important aspect of gaining user acceptance of a biometric security implementation. Users must be ensured that the digital representation of their personal identity will be handled with respect and care. If a central repository is employed for the storing of digital templates, users must be confident that the security infrastructure of the company properly protects the privacy of their information. The hybrid combination of smart cards and biometric devices can be used to ease the concern users have about companies maintaining stored copies of their digital traits. Exception processing can also quickly become a significant cost of a biometric system if care is not taken to properly establish the confidence interval required by the system. Obviously, higher confidence intervals lead to tighter security, but they also increase the potential for increased false rejection rates. Biometric systems can quickly become very costly to an organization if the confidence interval is set unreasonably high and users are consistently denied access to the system. Conversely, confidence intervals set inappropriately low increases the false acceptance rate compromising the security of the system. An important hurdle for every company utilizing face recognition is to establish a confidence interval that will provide the level of security desired at the least possible exception handling cost.

Uses of Face Recognition

Biometrics is more than just a replacement for password authentication. Currently, the primary use for biometrics such as face recognition is physical access security. Unlike identification cards that must be verified by security personnel, face recognition technologies permit unmanned access control. In addition, face recognition can be used for surveillance purposes to monitor the presence of individuals, and compare them to a database via a many-to-many search. For example, face recognition software and a live video feed can be used to continuously monitor a server room for the presence of any unauthorized individuals. Such continuous monitoring could be used to prevent authorized individuals from bringing unauthorized individuals into a secure environment. In addition, face recognition technologies are currently being employed by the United States Immigration and Naturalization Service to expedite the verification process of non-resident aliens who work in the U.S. but live in Mexico and therefore cross the borders daily. The INS has found that such technology has greatly reduced their costs associated with verifying the identity of such workers. Finally, face recognition can be used as a password replacement/supplement at the system or application level and can be layered to provide additional levels of security when necessary. For example, there are numerous systems currently in production that can be used to protect the screen saver function on Windows machines, which is usually simply password protected and amazingly easy to compromise.

Conclusion

Biometric security measures are not necessarily a brand new technology; they have been employed in maximum-security installations for decades. Until recently, the prohibitive cost of such systems has resulted in their limited use thus far. However, recent advances in digital

imagery and computational power have made biometrics affordable for everyday installations. Biometrics are not and never will be the "cure all" for application security issues, but used appropriately and in conjunction with a strong security model, they provide the potential for revolutionizing the way security is managed in organizations both large and small. The future potential uses for biometrics are vast and varied, which will likely be one of the driving factors that will ensure its survival when other authentication methods fail. After all, the idea of access control is to limit access to specific individuals. Short of planting a microchip in every individual in your organization, is there really a better and more unique authentication method than the physical traits of an individual?

References

Avanti: The Biometric Reference Site
URL: http://homepage.ntlworld.com/avanti/

Baback Moghaddam and Alex Pentland “Beyond Eigenfaces: Probabilistic Matching for Face Recognition.” International Conference on Automatic Face and Gensture Recogntition, Nara, Japan, April 1998

“Probabilistic Modeling for Face Recognition.”
URL: http://www.merl.com/projects/face-rec/

Simon Liu and Mark Silverman, "A Practical Guide to Biometric Security Technology" IT Professional, January-February, 2001.
URL: http://www.computer.org/itpro/homepage/Jan_Feb/security3.htm. (21 March 2000).

The Face Recognition Homepage
URL: http://www.cs.rug.nl/~peterkr/FACE/face.html

Visionics Corporation: FaceIT
URL: http://www.visionics.com/faceit/

Woodward, J.D. “Biometrics: Privacy's Foe or Privacy's Friend?” Proceedings of the IEEE, 85(9):1480-1492.