Global Information Assurance Certification Paper

GIAC Level One Certification Practical: Internet Research Project

Allison Miller

March 29, 2000

Risks in Biometric-based Authentication Schemes

Allison Miller

Introduction

> "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)

It is true that password-based and token-based systems are subject to attacks that wouldn't work on biometric-based authentication schemes. However, one would not want to assume biometric identification systems are impervious to attack, as this is definitely not the case. While biometric authentication methods may provide stronger security than simple passwords, the authentication mechanism can still be successfully compromised. Weaknesses in biometric authentication schemes exist and should not be overlooked during a risk analysis evaluation.

Authentication

Authentication is used to determine the identity of a person/user. Authentication is a very important concept in security, because many critical security services are dependant on authenticating users.

For example:

> The authentication mechanism facilitates the generation of reliable audit trails (actions are tracked to distinct and known users)
> Authentication is required for non-repudiation in communications (the identities of participants in a transaction/communication session are known and provable)
> Authentication is inherent in preserving confidentiality (controlling access to protected data requires that the authorized users are known and defined). (Dam)

In general, methods of authentication fall into three categories:

> Something the user knows (passwords, PINs)
> Something the user has (i.e. Tokens: ID Cards, smartcard)
> Something the user is (i.e. Biometrics: voiceprint identification, retinal scanners, fingerprint readers) (Wu)

Passwords, or other "things the user knows", are by far the most widely used method of authenticating users to a system. Authentication is handled by the software and (other than a keyboard or keypad) requires no extra hardware components. Deployment is cheaper than other authentication mechanisms.

Unfortunately, passwords are vulnerable to a number of attacks that make them weaker than tokens (something the user has) and biometrics (something the user is). For example,

> Users often pick poor passwords like ordinary words easily found in a small dictionary, or passwords based on personal, easy to guess information like family members' names, Date-of-Birth, or favorite sports team.
> Other systems that don't allow users to change their own passwords may create passwords that are difficult to guess; unfortunately this makes them difficult to remember as well. Users often disclose these kinds of passwords (by writing them down).
> Passwords are also subject to brute-force attacks. Once a password file is obtained, the contents can be subjected to software tests that try every possible combination of input characters until they finds a match. No matter how good the password is it will be broken eventually by the automated cracking tools. (Good passwords can make password cracking computationally infeasible, but never impossible)

Organizations face several compelling issues that are forcing them to re-evaluate and strengthen their authentication practices. For example, the trend of internetworking both internal and external systems to realize gains in productivity has resulted in more sensitive being available to more people. This is fine, as long as the availability of the information is limited to the right people. Also an important point, the boundaries of an organization's systems have become less defined with the proliferation of external VPN connections, remote users, outsourced network services, and other third-party connections into the organizational network. Since the perimeter may include semi-trusted or untrusted connections, it is important that the activity within an organization is controlled; authentication mechanisms can mitigate the risk to the organization by providing a level of control.

Token-based (something you have) and biometric-based (something you are) authentication mechanisms are the subject of a great deal of interest, as they clearly provide a stronger solution to the problem of authenticating users. In fact, token-based and biometric-based authentication can already be found in many highly secure environments. The higher cost of deployment is justified when the security requirements call for strict access control (high-security government & military installments, correctional facilities, banks).

The use of multi-factor authentication solutions is also a popular technique to satisfy sophisticated security requirements. These authentication schemes "employ at least two of these three factors [something the user knows, something the user is, or something the user has], such as the PIN number and the smart card which combine to produce a one-off password which immediately becomes obsolete." (Robb) Multi-factor authentication is an efficient way to increase the security available on existing infrastructure.

Biometrics

Biometrics "is the automated technique of measuring a physical or behavioral characteristic of an individual, and then comparing it with one that has been previously stored to determine if the characteristics are similar enough to confirm identity." (Woodward)

Biometric authentication systems use physical (things we are) and behavioral (things we do that are unique to us) characteristics for identifying individuals, and verifying their authorization to use a given

system. People have a number of biometric identifiers, and several are unique enough to provide reasonable "proof" of identity. For example, authentication systems using the following characteristics exist in the market today:

> Physical: chemical composition of body odor, facial features and thermal emissions, features of the eye, fingerprints, hand geometry, skin pores, vein measurement
> Behavioral: handwritten signatures, keystrokes/typing patterns, and voiceprints

Of these distinguishing characteristics, only the retina, the iris, and fingerprints are considered truly unique to the individual. (Woodward) The other characteristics are relatively unique (unique enough to provide reasonable proof of identity). Some of the systems (e.g. fingerprinting) may allow the administrator to "tighten" or "loosen" the relativity of a match (the "proof") based on an acceptable (reasonable) false positive rate.

Risks

There are several weak points in the current biometric authentication mechanisms, these vulnerabilities tie into the security of the input mechanism, the digital representation of the biometric indicator, and the unarity of the biometric indicators.

Security of Input Mechanism

As in any authentication system, "..a limitation [to biometric authentication systems] is the need for security of the capture medium. For example, biometric authentication data offered by a personal computer could have been generated by the presumed scanning device or it could be a bit string supplied by an attacker. Thus, to the extent that it is possible to generate bit strings that appear to be valid biometric data, these systems are vulnerable." (Schneider) Since biometric capture requires specialized hardware systems, this becomes very important in the design of a secure authentication mechanism. Supervised authentication (in front of a third-party, like a guard) provides less opportunity for tampering than unsupervised authentication (to a desktop system, for example).

Digital Data

It is true that biometrics identifiers are difficult to forge. However, since the biometric information is converted into digital data (usually a cryptographic hash) and passed onto a system that does the authentication, "An attacker won't try to forge [a user's] real thumb, but will instead try to inject her digital thumbprint into the communications." (Schneier)

Biometrics are unique to the individual and non-transferable, but once the information is interpreted and converted into digital format, it is easily copied and sent anywhere. "Moreover, possession of the template needed to validate a biometric scan, plus knowledge of the algorithm used to create that template, probably provides enough information to generate such bit strings (for any user whose template is compromised)…" (Schneider)

Unary Characteristics

Biometric indicators are not only unique to the individual, they are unary; "A biometric is a unary identity: All of us have only one left thumbprint." (Moskowitz) This becomes a problem for two reasons, one is the threat of losing the indicator (akin to forgetting a password), the other is the threat of disclosure of the biometric indicator to unauthorized parties (akin to unauthorized disclosure of a password).

> Losing the biometric indicator means authorized individuals cannot be authenticated. "There's the risk of lost access for example, a person may have an accident and lose the ability to

activate the thumbprint on his or her computer." (Moskowitz)
Disclosure of the biometric indicator means that unauthorized users may able to be authenticated under false pretenses. "Once someone steals your biometric, it remains stolen for life; there's no getting back to a secure situation." (Schneier) Unfortunately, it can very difficult to reset a biometric, what with having relatively limited body parts, and all. Also, "..disclosure of template data stored at any biometric authentication server could compromise use of that biometric technique for the affected users, forever!" (Schneider)

Other Potential Issues

In general users are encouraged to pick unique passwords between systems, the rationale is that if one password is broken or disclosed, you don't want the security of all of your information on other systems suddenly available to a hostile party. With biometrics this becomes a bit more complicated, because "biometrics are unique identifiers, but they are not secrets." (Schneier) You literally wear your biometric indicators every day. Biometric authentication systems are already being deployed by banks (at ATMs), correctional facilities, and at other high-security environments. The threat of system compromise will increase as users share their biometrics with multiple parties.

Biometric sharing is a privacy issue for users as well as a security issue for system managers: "How will you separate your work identity from your private identity?…[T]here is [currently] significant risk that your private activities (buying habits, entertainment preferences, political activities) will be inextricably connected to your work activities." (Moskowitz) Privacy issues are not unique to biometrics or to authentication, as data aggregation, sharing, and profiling continue to be an issue in our computerized information age.

Conclusion

To provide important security services like audit capability, confidentiality, and non-repudiation in transactions, authentication mechanisms are essential. To authenticate, or "prove" one's identity to a system, three methods of authentication have been developed, based on criteria composed of: something you know (passwords or PINs), something you have (tokens), or something you are (biometrics). Passwords and PINs are currently the most inexpensive and commonly used methods of authentication although biometric-based and token-based systems provide more security. However, the industry will probably see more sophisticated types of authentication being deployed as organizations require more robust system security and tokens, and biometrics are becoming less expensive.

Biometric authentication schemes are generally stronger than password-based authentication schemes, however, no system is impervious to attack. The method of implementation is very important. The specific characteristics and issues related to biometrics have an impact on their usefulness as user identification. Specifically, "[b]iometrics are powerful and useful, but they are not keys. They are not useful when you need the characteristics of a key: secrecy, randomness, the ability to update or destroy." (Schneier) The limitations of biometric identifiers should be evaluated in constructing an Identification and Authentication infrastructure.

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).

Moskowitz, Robert. "Are Biometrics Too Good?" Network Computing. 25 January 1999, Issue: 1002. URL:http://www.techweb.com/se/directlink.cgi?NWC19990125S0017. (21 March 2000).

Office of Information Technology. "Security of Electronic Information: Authentication Guideline". URL: http://www.oit.nsw.gov.au/guide/autheng/autheng.asp. (21 March 2000).

Robb, Guy. "Internet Security: The Business Challenge". Telecommunications Online. October 1996. URL:http://www.te.ecoms-mag.com/marketing/articles/oct96/guyrobb.html (21 March 2000).

Schneider, Fred B., Editor. "Trust in Cyberspace." Committee on Information Systems Trustworthiness. 22 December 1998. URL:http://cryptome.org/tic.htm. (21 March 2000).

Schneier, Bruce. "Biometrics: Uses and Abuses." Inside Risks 100, Communications of the ACM, vol 42, n 8, August 1999. URL:http://www.counterpane.com/insiderisks1.html. (21 March 2000).

Woodward, John D. "Believing in Biometrics". Information Security Magazine. February 1998. URL:http://www.infosecuritymag.com/biometrics.htm. (21 March 2000).

Wu, Thomas. "The Secure Remote Password Protocol." 22 Nov. 1997. URL:http://jafar.stanford.edu/srp/ndss.html. (21 March 2000).

Yasin, Rutrell. "Authentication With More Smarts." Internet Week. 5 March 1999. URL:http://www.internetwk.com/news0399/news030599-5.htm. (21 March 2000).