

Biometrics Research:

Access Control, Authentication, & Verification



Lindsey Bertugli
Fall 2006

CREU 2006-2007

Background Research on Biometrics

Biometric devices have become society's newest answer to an age old problem; that of preventing people from being where they are not supposed to be and doing things that they are not supposed to do. The devices themselves are designed to address the three closely interrelated concepts of access control, authentication, and verification. Access control is the process of properly identifying someone, then verifying their identity through some kind of authentication process. Its main objective is to preserve and protect the confidentiality, integrity, and availability of information, systems, and resources (Access Control 101).

Biometric devices are used in two types of access control. The first is physical access control (Building Access Control). Some of the mostly widely used systems in physical access control are access cards, usually smart cards, and PIN numbers. These are readily available to many people, including students at state universities like Indiana University of Pennsylvania or Slippery Rock University. However, it seems as though most of those who use these systems are not even aware that they are considered biometrics.

The purpose of physical access control is to prevent people from being somewhere they should not be in order to protect what is supposed to be there. Whatever you are trying to protect is often referred to as a "target". Physical access control is

generally placed on the entrances of a building that contain a target and on the entrance to the room containing the target. For example, at the University of Oregon there are card readers that require a swiped card and a PIN to open a door into a building. On the doors to computer lab inside that building, which contains the target hardware and data, there are locks that require a PIN (Building Access Control).

However, no one would depend entirely on physical access control to protect important data on a computer or network. That is where the second type of access control becomes useful. It is, of course, system access control, which is the process of determining whether or not a user or process may access a system or file (Wikipedia: Access Control). Such access control systems can include things like file permissions to determine who can read, write, and access information, program permissions to allow certain users to run a certain program, or the right to edit or access data in a database (Definition of Access Control).

There are three main types of system access control. The first type is DAC, or Discretionary Access Control, and allows the owner of the data to determine who can read, write, or execute any given file or service (Access Control 101). Therefore, DAC requires that every file have an owner. If a file does not have an owner, then it is essentially unprotected (Wikipedia: Access Control). Mandatory Access Control, or MAC, is the second type and only allows administrators to determine, or pre-determine, who can access or modify data, systems, or resources (Access Control 101). MAC evolved into two more complex types of control. One is Rule-Based, which is similar to Role-Based, which will be mentioned shortly, and the other is Lattice-Based, which is the

most complex of the three MAC types. However, very few systems implement the Mac forms of control (Wikipedia: Access Control). The last type is Role-Based Access Control, which evolved from Discretionary Access Control (Wikipedia: Access Control). This systems allows user to access information and systems based on their roles within the organization (Access Control 101). Role-Based Access Control provides a lot of flexibility through its use of groups. These are very similar to groups as defined in Linux operating systems. Using these access groups, you can confine certain privileges to certain sets of users in much the same way that you can limit the use of the “su” command to only root users.

No matter which type of access control is used, access cannot be determined simply by authentication. There are times when you will want to consider other aspects of a user when deciding whether or not they should be able to gain access to something. For example, if you have very sensitive data stored in a particular file on a system, you may not want to allow access a user access to that file if they are connected to the system remotely. On the other hand, you would want to allow access if they were using a secure on-site terminal. Simply stated, “Restricting access based on something other than the identity of the user is generally referred to as Access Control,” (Authentication, Authorization, and Access Control).

While authentication is not all there is to access control, it is an important aspect of it. Authentication is the process of verifying a user’s identity and is based on at least one of three factors: something known, something possessed, or something physical. Something known usually refers to a password or Pin (Wikipedia: Access Control). This

is the most common form of authentication (Authentication). Something possessed refers to objects like smart cards and other non-implantable RFID devices. Finally, something physical refers to a physical characteristic, or biometric measurement, such as a fingerprint, voice, or retina (Wikipedia: Access Control). Sometimes it is better to use more than one method, such as requiring a smart card and a PIN. This is known as multifactor authentication (Wikipedia: Authentication). Outwardly, it seems like an excellent way to extend remote access to users, indeed it remains one of the most secure ways to do so, but there are certain things that need to be considered. One is how secure you need your system to be. The other is your users. They need to understand why your system needs to be so secure and to consent to using a form of biometric every time they access it (Two-Factor Authentication Grows UP).

Authentication and verification are so closely related that if you look up the definition of verification, you can actually find it defined as authentication (Wiktionary: Verification). In particular, biometric verification can be defined as, “any means by which a person can be uniquely identified by evaluating one or more distinguishable biological traits,”. Such traits include fingerprints, hand geometry, earlobe geometry, retina patterns, iris patterns, voice waves, DNA, and signatures (Biometric Verification).

In today’s security focused society, biometric devices have become the leading edge of technology. More and more they are taking the place of current access control systems in an attempt to provide increased protection in this time of ever increasing danger. Like every leading edge, biometrics have met with strong resistance based

primarily on people's fear for their privacy. We have the need and the technology, but whether or not people will be willing to use it remains to be seen.

Resources

Access Control 101. *Intranet Journal*,

http://www.intranetjournal.com/articles/200311/ij_11_10_03a.html.

Authentication. *100 Best Web Hosting*,

<http://www.100best-web-hosting.com/glossary28.html>.

Authentication, Authorization, and Access Control. *Apache*,

<http://httpd.apache.org/docs/1.3/howto/auth.html#access>.

Biometric Verification. *SearchSecurity.com*,

http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci789799,00.html.

Building Access Control. *University of Oregon*,

http://safetyweb.uoregon.edu/general/access_control.htm.

Definition of Access Control. *M-Tech*,

http://mtechit.com/concepts/access_control.html.

Two-Factor Authentication Grows UP. *SearchSecurity.com*,

http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci862681,00.html.

Wikipedia: Access Control. *Wikipedia*,

http://en.wikipedia.org/wiki/Access_control.

Wikipedia: Authentication. *Wikipedia*,

<http://en.wikipedia.org/wiki/Authentication>.

Wiktionary: Verification. *Wiktionary*,

<http://en.wiktionary.org/wiki/verification>.