

Tamara C. Smith
Background Research Report
September 27, 2006
CREU 2006 – 2007

Biometrics is expected to be incorporated in solutions to provide for Homeland Security including applications for improving airport security, strengthening the United States' national borders, in travel documents, visas and in preventing ID theft. There is a wide range of interest in biometrics across federal, state, and local governments. Congressional offices and a large number of organizations involved in many markets are addressing the important role that biometrics will play in identifying and verifying the identity of individuals and protecting national assets.

There are many needs for biometrics beyond Homeland Security. Enterprise-wide network security infrastructures, secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies. A range of new applications can be found in such diverse environments as amusement parks, banks, credit unions, and other financial organizations, Enterprise and Government networks, passport programs and driver licenses, colleges, physical access to multiple facilities and school lunch programs.

Biometric-based authentication applications include workstation, network, and domain access, single sign-on, application logon, data protection, remote access to resources, transaction security and Web security. Trust in these electronic transactions is important to the healthy growth of the global economy. Utilized alone or integrated with other technologies such as smart cards, encryption keys and digital signatures, biometrics is set to pervade nearly all aspects of the economy and our daily lives. Utilizing biometrics for personal authentication is becoming convenient and considerably more accurate than current methods. This is because biometrics links the event to a particular

individual, accurate, can provide an audit trail and is becoming socially acceptable and inexpensive.

Biometric authentication requires comparing a registered or enrolled biometric against a newly captured biometric sample. During Enrollment a sample of the biometric trait is captured, processed by a computer, and stored for later comparison. Biometric recognition can be used in Identification mode, where the biometric system identifies a person from the entire enrolled population by searching a database for a match based solely on the biometric. For example, an entire database can be searched to verify a person has not applied for entitlement benefits under two different names. This is sometimes called "one-to-many" matching. A system can also be used in Verification mode, where the biometric system authenticates a person's claimed identity from their previously enrolled pattern. This is also called "one-to-one" matching. In most computer access or network access environments, verification mode would be used. A user enters an account, user name, or inserts a token such as a smart card, but instead of entering a password, a simple touch with a finger or a glance at a camera is enough to authenticate the user. Verification is the establishment of the truth of something; it can be a claim, a state of affairs, an employer or a computer programmer. Therefore it is performed in different manner and contexts ([Wikipedia.org](https://en.wikipedia.org)).

Authentication is any process by which you verify that someone is who they claim they are. This usually involves a username and a password, but can include any other method of demonstrating identity. This can include things such as a smart card, retina scan, voice recognition, or fingerprints. Authentication is equivalent to showing

your drivers license at the ticket counter at the airport. Authorization is finding out if the person, once identified, is permitted to have the resource. This is usually determined by finding out if that person is a part of a particular group. If that person has paid admission, or has a particular level of security clearance this would be known as authorization.

Authorization is equivalent to checking the guest list at an exclusive party, or checking for your ticket when you go to the opera. Finally, access control is a much more general way of talking about controlling access to a web resource. Access can be granted or denied based on a wide variety of criteria, such as the network address of the client, the time of day, the phase of the moon, or the browser which the visitor is using. Access control is similar to locking the gate at closing time, or only letting people onto the ride who are more than 48 inches tall. It can also mean controlling entrance by some arbitrary condition which may or may not have anything to do with the attributes of the particular visitor. Because these three techniques are so closely related in most real applications, it is difficult to talk about them separate from one another. In particular, authentication and authorization are, in most actual implementations. If you have information on your web site that is sensitive, or intended for only a small group of people, the techniques in this tutorial will help you make sure that the people that see those pages are the people that you wanted to see them.

Basic authentication and digest authentication both suffer from the same major flaw. They use text files to store the authentication information. The problem with this is that looking something up in a text file is very slow. It's rather like trying to find something in a book that has no index. You have to start at the beginning, and work through it one page at a time until you find what you are looking for. Now imagine if the

next time you need to find the same thing, you don't remember where it was before. You would have to start at the beginning again, and work through one page at a time until you find it again.

Since HTTP is stateless, authentication has to be verified every time that content is requested. So every time a document is accessed which is secured with basic or digest authentication, Apache has to open up those text password files and look through them one line at a time. This will have to happen until it finds the user that is trying to log in, and verifies their password. In the worst case, if the username supplied is not in there at all, every line in the file will need to be checked. On average, half of the file will need to be read before the user is found. This process is very slow and takes a lot of time. This is not a big problem for small sets of users, but when you get into larger numbers of users this becomes very slow. In many cases, valid username/password combinations will get rejected because the authentication module just had to spend so much time looking for the username in the file. Apache will soon just get tired of waiting and return a failed authentication. In these cases, you need an alternative, and that alternative is to use some variety of databases. Databases are optimized for looking for a particular piece of information in a very large data set (wikipedia.com). It builds indexes in order to rapidly locate a particular record, and they have query languages for swiftly locating records that match particular criteria.

Authentication by username and password is only part half of the process. Frequently you want to let people in based on something other than who they are;

something such as where they are coming from. Restricting access based on something other than the identity of the user is generally referred to as access control.

Sources:

<http://www.mckinnonsc.vic.edu.au/la/it/ipmnotes/biometrics/devices.htm>

http://www.smartwatchcentral.com/Access_Control_Biometric_Fingerprint.html

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

http://www.smartwatchcentral.com/Access_Control_Biometric.html

<http://www.accesscontroldirectory.com/Lander.aspx?sessionid=ltvxyga1ycialfvjli153l45&cc=us&ns=1>

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

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

http://www.homesecuritystore.com/ezStore123/DTPProductList.asp?p=2_1_1_1_0_0_191