Assignment 1
Biometric authentication

Internet Security and Privacy
2G1704

Alexandre Fustier
Vincent Burger

Professor : Johan Montelius Autumn Semester 2005

Introduction:

Biometric is one authentication method. It consists in identifying people by recognizing one or several physicals characteristics. It is probably one of the future main solutions for providing authentication. There are several types of authentication, based on different aspects of a user. As Matt Bishop say in his book "Introduction to Computer Security "[1], authentication can be based on:

- What this user has, for example a key.
- What this user knows, for example a password.
- Where this user is, for example IP-address.
- What this user is: biometrics methods.

Each of these methods has some advantages and drawbacks. Depending on what you want to provide, you have to think of what is the best method for your specific case. You maybe want something cheap, or easy to use, or really secure. You have to reach a compromise between these aspects.

For example, passwords are really cheap and easy to use, but if a password is not strong enough, it is not a secure authentication method.

In this document, we will provide an overview of the different biometrics methods and see which ones are used. Then, we will discuss the advantages and drawbacks of the biometric among the authentication methods.

I. Types and description of biometrics

Biometrics techniques can be divided in two main sets: physiological or behavioral. A physiological biometric method is something that is physical, and that belongs to you. The behavioral biometric consists in something that you do in your everyday life. Some information about these different methods are taken from [1], [2] and [5].

1. Physiological biometric

a. Fingerprints

This is the most known method that belongs to this category. It is also the oldest biometric authentication approach. It is based on the recognition of someone's fingerprint, by analyzing its characteristics. There are two different techniques to capture fingerprints. The first is by scanning optically the finger. The other method is by using electrical charges, that determines which parts of the finger are directly in contact with the sensor and which are not. Each fingerprint has some characteristics, such as curves, bifurcations, deltas. One set of these characteristics is unique for each person. Moreover, if your finger is little dirty, or if cut yourself, it will work as well, because the main characteristics of your fingerprint are not changed. A vulnerability of this method is reproducing a fingerprint for example with silicone. For the optical devices, even a picture of a fingerprint can fool the device. Fingerprints are commonly used in a lot of organization. Moreover you can find fingerprints readers easily.

b. Eyes

There are two methods using the eyes characteristics for authentication. The first is based on the retinal recognition. The user has to look in a device that performs a laser-scanning of his retina. The device analyzes the blood vessels configuration of the acquired retinal picture. By the way, it authenticates the user. This blood vessels configuration is unique for each eye. The device is not friendly, because you have to fix a point while a laser is analyzing your eye. It seems difficult to fool the authentication system.

The second method is based on the iris recognition. The scan is done by a camera. Unlike the retinal method, you don't need to be close to the device to be authenticated. The acquired picture is analyzed by the device, and contains 266 different spots. It is said that it is the most reliable biometric authentication method. Moreover iris is stable through the whole life. The 266 spots are based on characteristics of the iris, such as furrows and rings. Like for the retinal recognition, the iris recognition seems difficult to be fooled.

Both methods are currently in developing state. Some prototypes are already available.

c. DNA

This method is based on a DNA analysis. To perform a DNA analysis the user has to give some of his cells, for example by giving a hair, or some skin. Analyzing DNA takes a long time. That's why it is not used as an authentication method. It is a shame that it can not be used easily, because it would have provided an excellent authentication, because everyone is unique through his DNA. But it can be easily fooled, because anyone can steal a hair of somebody else. Maybe researchers will find a good way to implement such devices, and it will maybe become the most efficient way of authenticate people.

d. Face

This method is based on the faces recognition. The device is a simple camera; even a web cam with low resolution is enough. The user stands in front of the camera, and then the device computes a digital representation based on some features of the face. The representation is compared with one which is stored in a database, and if there is a match, the user is authenticated. It is easy to setup, and cheap to implement because all you need is a cheap camera and a well-done software. With good software, it provides you a good authentication method with unique recognition, except for twins. But the problem is that it is easy to fool, because all what you need is a single photo of a user's face.

e. Handprints

This method is based on the recognition of the handprints. The device is a scanner that extracts a picture of a user's hand. Some characteristics like length of the fingers, distance between them or their relative position are computed, based on the picture. These characteristics are used to match with an entry in the database. With these characteristics, you define a unique entity. That provides you unique recognition except in case of twins or even with same family members. To fool the system, you can either have a mould of the hand or just a picture of it. This method is used in some places because it is not so complex to implement.

f. Voice

This method is based on the recognition of someone's voice. The user speaks in a microphone, and voice is recorded and computed. It is done by using some frequency analysis of the voice. This analysis is based on how you speak and not on what you say. It can be useful to authenticate someone through a telephone, and it allows users to work on a remote location. It is less accurate than other biometrics authentication methods, and some errors can occur. This authentication method can be easily fooled by recording someone's voice. The voice recognition is used in many systems because it is cheap and easy to setup. But it can't be used as a single authentication method: you have to combine it with another method (biometric or not).

There are several others physiological biometrics, such as lips or earlobes recognition, sweat ore odor analysis, blood analysis and so on. These biometric methods are less used and have to improve before they can be used. Some biometrics, such as the voice can also be considered as a behavioral authentication method, and that leads us to the analysis of the second type of biometric.

2. Behavioral biometric

a. Signature

The analysis of signature is also a biometrical authentication solution. The device is a tactile screen. The user performs a signature with a "pen" on this tactile screen. The parameters that are computed for the authentication are the shape of the signature, the time taken to do it, the stroke order and the pen pressure. With the computation of these parameters, the system provides to you a unique authentication method. It is virtually impossible to reproduce in the same way somebody else's signature. This method is not deployed today, but it will be more used in the future. It is easy to implement and it will be standardize, so it will become quite cheap.

b. Gait

Another behavioral biometrics is the authentication by the gait. It works by analyzing how a person is walking. A camera films the user walking, and by computing some mathematical function on the inclination of the legs, the frequency of the balancing of the body, it gives you a good authentication method. You can use this at distance, and then it can be use as a security system. The technology is quite new, and the researchers have to improve it, because it is not able to provide a unique recognition method. It is not used at this time, and if it becomes a standard, it will be used preferably as a detection system more than as an authentication method. The good aspect of this biometric is that you can "authenticate" a person even in a crow, because you can use it far from the subject and target a specific target.

c. Keystrokes

Keystrokes analysis is also a behavioral biometric, and provides an authentication method. It works more or less like the signature biometric, by analyzing the way a user is typing on a keyboard. It measures how long a user holds a key, and how long it takes to the user to switch from one key to another. It provides a good authentication method in term of uniqueness, but the problem is that a user can have different keystrokes if he is stressed, or tired. But it is a comfortable authentication method (more comfortable than an iris or retinal scanner). It is the easiest biometrics authentication method to implement because all you need is a little software, and no hardware (just a keyboard).

All theses methods follow a common scheme: Some part or behavior of someone is digitalized, transforms in data that follows a template so it can be compared to entries in a database and then authenticate or not a user. The size of this template is a part of the strength of a biometrics. For example fingerprints have templates at least of 150 bytes, and iris gives a template of 512 bytes.

The database has to be created at the beginning: when you want to add users to your system, you have to take their biometrics measures and add these entries in the database. This is called enrollment.

II. Advantages of the biometric authentication

The Biometric authentication has several advantages. First, the biometrics authenticates only people. It can not authenticate computer as the classical authentication methods which are based on IP address or public key. The biometric characteristics that are used in authentication systems are unique for each person.

The major advantage of the biometrics is that you have always with you your way to authenticate yourself. For example, you can forget a password or lost an access card. It is impossible to forget your fingerprint, your gait, your signature…

Biometric is more practical for the user as to remember several password for example. It can reduce the cost of password and access-card administration. As soon as the biometric system is set up, there is only a few of administration.

In most of the case, it is more difficult to attack a biometric authentication system as attacking an authentication system based on password or access-card. You can guess a password or steal an access card. It seems more difficult to fool a good biometric authentication system. Furthermore biometric makes possible to know exactly who has been authenticated and where. A password or an access card can have been borrowed by someone. With a biometric authentication system, it can not happen.

There are a lot of interesting advantages but also some drawbacks to the biometric authentication.

III. Drawbacks of the biometric authentication

The first drawback of biometric authentication is that some methods can't work for some people [5]. For example, it is impossible to use fingerprint authentication for someone who has no hands. Some behavioral authentication methods can't work if something is changed in your life. For example if you have new shoes, perhaps your gait will change, and it can be a problem to authenticate you. Furthermore if one of your fingers is severely hurt, the fingerprints authentication will not work. Some characteristics as your face can also changed with the age [6]. Moreover, most of the biometrics authentications systems are still in developing state and it can be expensive to install them. As shown in the first part, someone can fool the biometric authentication.

Some biometrics authentication systems are not really user-friendly such as DNA or retinal recognition. It can be also not very clean. It is possible that users don't want to use such system [3].

Biometrics authentication raises also the problem of respect of privacy. It is worrying if your fingerprints are asked everywhere that you want to go or if every time that you speak, someone can identify you by analyzing your voice. Some movies are based on a world leading by biometric, and it is really frightening. If biometric is widespread in our every day life and all your activities are stored in database, there is no more privacy. Personal information taken by biometrics device can be misused. We must decide in which system we must authenticate by biometrics and in which system we must not. Using biometric authentication should be a choice for a user not an obligation. Laws have to be done in order to limit the use of biometrics information in a reasonable way.

Conclusion:

There are several types of biometrics, and each has its advantages and drawbacks. Depending on what level of security and what do you want to provide, you have to make the good choice. Biometrics implies that you have to face some ethics and law considerations. But if you can go through this problem, it can provide you a very good, secure and easy way of authenticate people.

We think that with the improvement of the actual techniques, it will become one of the standards in the authentication methods in a close future.

Nevertheless, without a control by some laws, it would be a mess, because commercial company could use biometric to target people (as it is done actually on Internet), and even sell information to other companies.

Biometrics is the tomorrow authentication's method, but a lot of work has to be done on both technical and ethical sides.

References:

Books:

[1] Introduction to Computer Security (Matt Bishop)

[2] Network Security- Private Communication in a public world (Charlie Kaufman, Radia Perlman, Mike Spenicer)

Web:

[3] http://en.wikipedia.org/wiki/Biometrics

[4]http://www.biometrics.dod.mil

[5]http://www.eff.org/Privacy/Surveillance/biometrics/

[6]http://www.globalsecurity.org/security/systems/biometrics.htm