BIOMETRICS USED FOR AUTHENTICATION IN INTERNET-BANKING APPLICATIONS

Eng. Cătălin Lupu, PhD Stud, ***Ştefan cel Mare University of Suceava, ROMANIA***

Valeriu Lupu, prof.dr., ***Ştefan cel Mare University of Suceava, ROMANIA***

Abstract: *Nowadays most of the banks provide internet banking services to their clients. There are multiple authentication methods used, including username and password (with the use or not of a private certificate) or username and a dynamic password (OTP – One Time Password, generated by a token (or digipass) device or received through a SMS received on a phone number registered at the bank). But there is a need for a better security in authentication process. The username, passwords or tokens can be stolen (especially through phishing/key logger methods) or lost. That's why is simpler to use something that can't be lost or stolen (although it can be spoofed, but there exists enough methods to determine its reality), like a fingerprint or an iris image. These biometric characteristics can successfully replace the ubiquitous passwords. This paper presents main authentication methods, together with the most used biometric characteristics, fingerprint and iris. These biometric characteristics are suitable to be used in an internet banking authentication process.*

Key words: *biometrics; internet banking; fingerprints; tokens.*

1. INTRODUCTION

Almost all major banks in Romania and all over the world are using their own internet banking applications. The increasingly number of transactions done by this system will lead to the necessity for an improved security concerning the authentication methods.

Nowadays there are multiple authentication methods including tokens, passwords, SMSes, private certificates. The biometrics can be used in order to replace all this kind of methods. Or – for a better security – a combination between a biometric characteristic and a token – for example – will lead to an improved method for authenticate the users to internet banking applications.

There are some biometric characteristics that can be used, for example iris, fingerprint, face, signature or voice recognition. But some biometrics are not suitable for this purpose, because: (i) the devices used to acquire them are much too expensive; (ii) the acceptance of the people who should use them; (iii) the degree of confidence is not at a very high level; (iv) the time to process information acquired from devices that can be very high for specific biometrics. The DNA, gait, vein and others can't be used for user authentication on an internet-banking application.

2. INTERNET BANKING

The main banks are offering internet banking services to their clients, in order to manage their accounts, to make payments, currency exchange, create deposits and to access information about loans.

The term “internet banking” has as synonyms “online banking”, “virtual banking” or “e-banking”. All these terms represent the same service provided by banks.

The internet banking stands for a browser web-page, delivered through a secure channel. After accessing this web-page, the user must authenticate using the authentication method(s) provided by the bank. After the successful authentication, the user can manage his/her account and can do any action that is permitted by the application.

According to [3], the concept of internet banking started in the early ‘80s, when “distance banking over electronic media” was introduced. This is the precursor of actual internet banking.

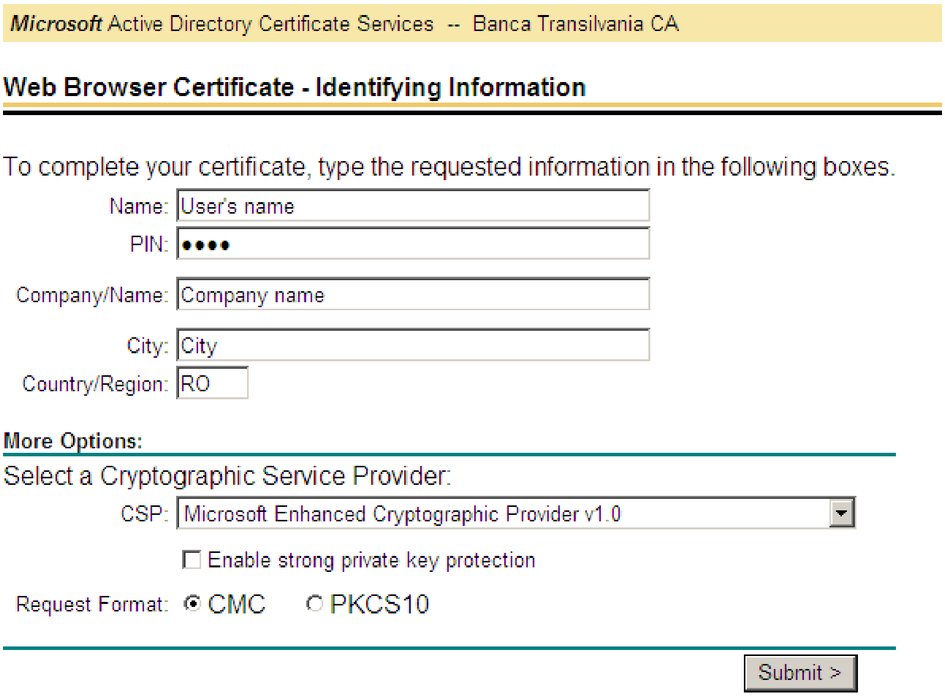
The main issue in internet banking security is represented by the authentication method chosen by bank or user. In the following sub-paragraphs different authentication methods for accessing this service will be presented.

2.1. USERNAME AND PASSWORD METHOD

This authentication method is the simplest and also the weakest possible. The user has to fill a form at the bank, then receives a code by email and can choose a password. Most banks aren’t using this authentication method because the risks are too big. The password can be stolen by using phishing or a key-logger software. Also, the passwords can be written on a text file, an email or even on a paper. If the username and password are stolen, then the account can be easily compromised.

2.2. USERNAME AND PASSWORD, TOGETHER WITH A PRIVATE CERTIFICATE

A private certificate is provided by a CA (Certification Authority). The user has to enter the credentials and a PIN provided by the bank. The webpage for generating the certificate is using, for example, “Microsoft Certificate Enrollment Control” add-on (ActiveX). The main page for certificate request is presented in the figure 1.



Microsoft Active Directory Certificate Services -- Banca Transilvania CA

Web Browser Certificate - Identifying Information

To complete your certificate, type the requested information in the following boxes.

Name: User's name

PIN: ••••

Company/Name: Company name

City: City

Country/Region: RO

More Options:

Select a Cryptographic Service Provider:

CSP: Microsoft Enhanced Cryptographic Provider v1.0

□ Enable strong private key protection

Request Format: ● CMC ○ PKCS10

Figure 1. Main window for certificate request

The certificate has a validity of 1 year and can be requested on more than one computer (for example, if you would like to access your account from home, job or elsewhere). The main problem with the presented solution is that requires Internet Explorer browser, and most of the Android-based smart-phones are running other browser (Chrome, Mozilla, etc.). Also, the certificate can be requested only for desktop computers, because if someone is trying to request a certificate, even on a Windows Phone, it will fail and the certificate won’t be provided. This method is safer than the previous one because if the certificate isn’t found on the computer then the user can’t access the account, but it still using a username and a static password (together with the private certificate) for authentication. The password is changed every 3 months, but it there is still the possibility that the username, PIN and other credentials to be stolen by a phishing web-page. A certificate can be requested after stealing the user data, thus the malicious people can access the account.

2.3. STATIC USERNAME AND DYNAMICALLY GENERATED PASSWORD BY A TOKEN (DIGIPASS) DEVICE OR A SMS ON A BANK-REGISTERED PHONE NUMBER

The security of this method is stronger than the ones presented above. A token device is generating a unique password (OTP – One Time Password) based on an algorithm, which can be used for a short period of time (less than 1 minute) to authenticate to the internet-banking application. The main facility is that the internet banking services can be accessed even on a smart-phone. The main producer of these devices is VASCO. A list of the main products is presented in the web-page [4]. The digipasses can be easily personalized with the bank’s logo.

The token will be opened by entering a PIN. This is the main problem of this authentication method. The PIN can be written on the device by the user (in order not to forget them), together with the username. In case the token is lost or stolen, someone can access the account by using the credentials found on the device. If the user didn’t realize immediately the lost or stolen of the device, then the account can be compromised easily.

The SMS authentication works similar with the token method. A SMS is sent to the bank, and this will reply with an OTP code. The code can be used as a password for authentication. The main problem is represented by the fact that the phone can be lost or stolen, in this case the account integrity couldn’t be granted anymore.

The presented methods are the classical ones, but, as it could be seen, they still have weaknesses. A better method to securely authenticate such a sensitive service like internet banking is to use what user is (a fingerprint, iris, voice, etc.), and not what he/she possesses (i.e. a token) or what he/she remembers (a password).

3. MAIN BIOMETRIC CHARAC–TERISTICS SUITABLE FOR INTERNET BANKING AUTHEN–TICATION

Biometrics stands for a complex of methods intended to lead to the identification of persons by using their measurable or behavioral characteristics. The measurable and most used characteristics for personal identification are: the minutiae of fingerprints, ridges and valleys of the iris, vascularization of retina, different distances in the user’s face, voice individual patterns and many others (DNA, vein patterns, face thermogram, palmprint, ear, etc.). From the behavioral characteristics, we can mention the signature, writing dynamics, keystroke and gait.

The main diagram for biometric authentication is presented in the figure 2. A sensor is used to acquire the biometric characteristic, then the samples are evaluated and if they are proper then the process will evolve to characteristics extraction module. If the sample is not acceptable, then the user’s characteristics will have to be re-acquired. On the “Characteristics extraction module”, if the user is using the application for the first time and an enrollment is needed, then the system will go to the “Template generation” module. After the templates are generated, they are stored in a database.

Samples are verified with the templates in the database and if the match score is behind the established threshold, then the user is accepted to use the application, otherwise it will be taken the decision to reject the user from using it.

3.1. ENROLLMENT, VERIFICATION AND IDENTIFICATION

The presented system can be used in three different modes: enrollment, verification and identification.

At the enrollment, the user will provide the biometric characteristic to a sensor, the quality of the image is evaluated and if this is proper for use then features are extracted from the acquired image. After this step, a template is generated and is stored in a database.

The verification supposes that the user provides the identity and the system will verify if the person is who pretends to be.In the identification mode, the system will acquire a biometric characteristic and search in a database for a positive match. If no match is found then the user is unknown and has two possibilities: to enroll into the system or to repeat the entire process, because – probably – the acquired sample wasn’t satisfactory for the system.

The most important two biometric characteristics that are suitable for authentication in an internet-banking service will be presented in the following sub-paragraphs: fingerprints and iris.

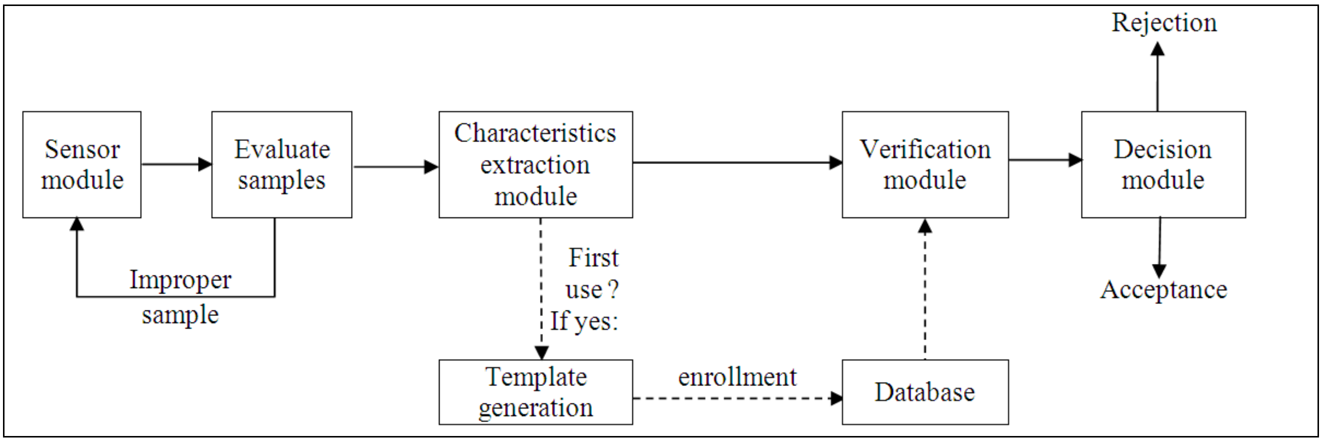


Figure 2. Biometric authentication diagram

3.2. FINGERPRINTS

Fingerprints were used for forensic purposes since the 19th century.

The main challenge is to determine the minutiae that form a fingerprint.

The minutiae can be classified in: arches, loops (the most common, approx. 60% from all minutiae), cores, deltas, etc.

In the figure 3 are presented 8 different types of sensors for fingerprint acquisition.

According to [5], the sensors are classified in: optical (FTIR – Frustrated Total Internal Reflection, optical fibers), solid-state (capacitive, thermal, electric field, piezoelectric), ultrasound.

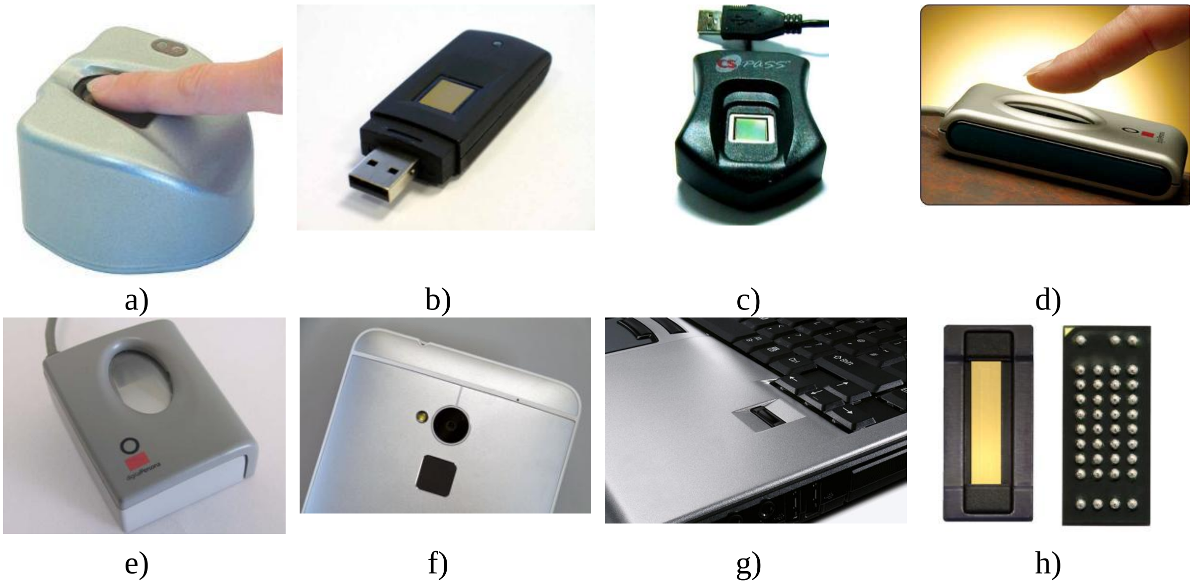


Figure 3. Sensors and scanners for aquiring fingerprints: (a) Lumidigm, Inc. - Venus Series Biometric Fingerprint Sensor, (b) Kingston USB Fingerprint flash drive, (c) CS PASS, (d,e) digitalPersona, U.are.U, (f) HTC One with fingerprint sensor below the camera , (g) UPEK - TCS5 TouchStrip Fingerprint Sensor , (h) AuthenTec - AES1711

The fingerprint sensors presented above are really cheap and can be used for authentication in an internet banking application. Fingerprints are easily acquirable thru non-invasive methods, have a great acceptance to the people and the methods for processing them can be automated really simply.

Fingerprints can be used for many purposes, especially for access control (in buildings, cars (paper [6]), computers, etc.), at ATMs, for cryptography and many others domains.

The main problem with fingerprints is that there are some disabled people that don’t have fingers or hands, or they cannot use them in order to provide a good image needed for recognition. Also, around 3-7% of the population doesn’t have legibly fingerprints. Also, the fingerprints can be altered, by mistake or deliberate. Other problem consists in the fact that moulds can be produced in order to fool the system. Several measures have to be taken into the account when acquiring biometric features, in order to fully avoid the spoofing, which is like the phishing for the username/password method.

Methods for processing fingerprints and extracting features and templates are described at largely in the book [5].

3.3. IRIS – ONE OF THE NEWEST BIOMETRIC CHARACTERISTIC

Iris was taken into account as a biometric since 1987, when Leonard Flom and Aron Safir discovered that it possess characteristics that are suitable for personal identification (as it can be seen in the patent [7]). But the real contribution on the standardization of methods was the John Daugman’s patent from 1994, “Biometric personal identification system based on iris analysis”, which is presented in [8]. After that, most of the researches were made based on this patent.

The camera used for acquiring the iris pattern is presented in the figure 4. It consists in fact from 2 cameras, one for iris acquiring and the other can be used as a webcam (suitable to be used in getting other biometrics, like face, lips or ear). This camera also has a infra-red beam (on the bottom), that is activated when the iris image is acquired.

The images of the iris in infrared have better characteristics, because in the case of dark-brown or near-black eyes, in natural light, the acquired data won't be satisfactory for a personal identification or verification.

The infrared beam isn't dangerous for the eyes and it is no need to wear special equipment in order to provide the iris image.

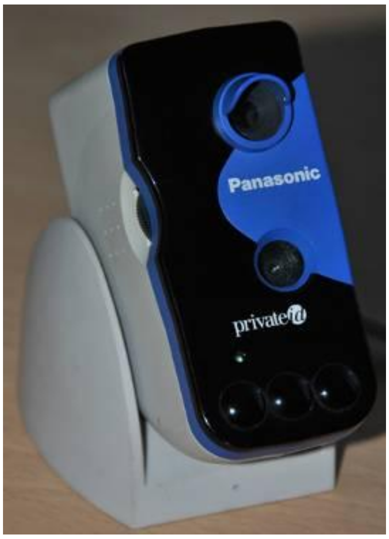


Figure 4. Panasonic BM-ET100US camera for iris and/or face recognition

The template generated for the iris (called IrisCode) has a length of only 1024 bytes per iris, as it can be seen on a dump – [9] – from the Daugman's algorithm.

The main advantage for iris is that the similarity between two different irises is almost zero, because of its randomly generated patterns (ridges and valleys).

Disadvantages consist in the higher price for the camera and the fact that some people don't possess this biometric characteristic or they aren't accepting this authentication method.

4. USING BIOMETRICS TO IMPROVE INTERNET BANKING AUTHENTICATION

As it could be seen in the above paragraphs, biometrics has some advantages and disadvantages. But, compared with classic authentication methods, improved security can be provided through these methods. Biometrics can be used for at least two purposes: (i) to unlock the token device, by swiping the finger on a sensor; in this case it won't be necessary anymore a PIN that can be forgotten or stolen; (ii) to authenticate in the internet banking application, using a fingerprint or the iris, without the need to use a digipass. In the first case, the fingerprint is registered on the device at the enrollment, at the bank that provided it. In the second case, the fingerprint or iris is registered in the bank's database and when the user wants to authenticate, he/she provides a username and the password is replaced by the biometric characteristic.

In our researches in this field, we developed a Java application that is able to: (i) acquire the fingerprint from the user; (ii) do the enrollment and to store the template in a MySql database; (iii) make the verification of a user.

After the verification, the bank's internet banking application is opened. But, in the future, the main page of the internet banking can be changed in order to introduce only the username and a fingerprint for the logon process, using the application described

We choose Java for implementation of this above application because it is compatible and can be easily integrated with most of the devices (desktop/laptop computers, tablets, smart-phones, etc.). This application is still in developing process, because we use only one fingerprint sensor (SunPlus USB Fingerprint), placed on an optical mouse. There exist a lot of sensors and the communication with them is made by functions in its software or driver. The aim is to make a universal application that can work with any kind of fingerprint sensor.

5. CONCLUSIONS

The use of fingerprint as the main biometric in our researches was caused by the fact that the sensor is really cheap and the acceptance of the final user is really high. The universality, uniqueness, permanency, acquiring, simplicity, reduced cost, convenience and precision of the fingerprints recommend them to be used alone in such a sensitive domain like internet banking services.

There are many other applications that can use the biometric characteristics, for example cryptography (it’s easier to use a fingerprint than to remember a password in the case of an archived file (RAR or ZIP); however such an archive can’t be sent to another user because will not be able to extract the content).

The use of biometric characteristics and methods will lead to a higher level of security and privacy when they are used for authentication in internet banking services.

ACKNOWLEDGMENT

This paper was supported by the project "Sustainable performance in doctoral and post-doctoral research - PERFORM - Contract no. POSDRU/159/1.5/S/138963", project co-funded from European Social Fund through Sectorial Operational Program Human Resources 2007-2013.

REFERENCES

[1] Hosseini, S., Mohammadi, S., Review Banking on Biometric in the World’s Banks and Introducing a Biometric Model for Iran’s Banking System, Journal of Basic and Applied Scientific Research, 2(9) p. 9152-9160, 2012

[2] Tassabehji, R., Kamala, M.A., Improving E-Banking Security with Biometrics: Modelling user attitudes and acceptance, 3rd International Conference on New Technologies, Mobility and Security (NTMS), p. 1-6, 2009, DOI: 10.1109/NTMS.2009.5384806

[3] Cronin, M.J., Banking and Finance on the Internet, John Wiley and Sons, ISBN 0-471-29219-2, p. 41, 1997

[4] https://www.vasco.com/products/client_products/esignature_digipass/esign.aspx

[5] Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S., Handbook of fingerprint recognition, Springer,2005, ISBN 0-387-95431-7

[6] Lupu, C., Lupu, V., Multimodal biometrics for access control in an intelligent car, ISCIII, p. 261-267, 2007

[7] Flom, L., Safir, A., Iris recognition system, United States Patent No. 4.641.349, 1987

[8] Daugman, J., Biometric personal identification system based on iris analysis, United States Patent No. 5.291.560, 1994

[9] http://www.cl.cam.ac.uk/~jgd1000/afghanscreendump.txt