SAMI 2015

IEEE 13th International Symposium on Applied Machine Intelligence and Informatics

PROCEEDINGS

January 22–24, 2015

Herl'any, Slovakia

elfa

Adresát:

Dátum: Registratúrne číslo: Vybavuje:

Thursday, January 23, 2015

CERTIFICATE OF ATTENDANCE

This is to certify that **drd.ing. Catalin Lupu** orally presented his paper entitled **"Security Enhancement of Internet Banking Applications by Using Multimodal Biometrics"** during the SAMI 2015 conference in Herľany, Slovak Republic.

5 elfa s.r.o.
Park Komenského 7
040 01 Košice
tel.: 055/6253839
IČO: 31648410 IČ DPH: SK2020480803

member of the international organizing committee

IEEE Catalog Number: CFP1508E-USB
ISBN: 978-1-4799-8220-2

FOREWORD

Computational Intelligence and Intelligent Technologies are very important tools in building intelligent systems with various degree of autonomous behavior. These groups of tools support such features as ability to learn and adaptability of the intelligent systems in various types of environments and situations. The current and future Information Society is expecting to be implemented with the framework of the Ambient Intelligence (AmI) approach into technologies and everyday life. These accomplishments provide the wide range of application potentials for Machine Intelligence tools to support the AmI concept implementation. The number of studies indicates that this approach is inevitable and will play essential and central role in the development of Information Society in close future.

The essential importance of the Machine Intelligence in this historically challenging effort points out the responsibility of MI community including all fields like Brian-like research and applications, fuzzy logic, neural networks, evolutionary computation, multi-agent systems, artificial life, Expert Systems, Symbolic approaches based on logic reasoning, Knowledge discovery, mining, replication and many other related fields supporting the development and creation of the Intelligent System. The importance embedding these systems in various kinds of technologies should bring profit and different role of mankind in production and in everyday life. We expect to have intelligent technologies, solution and even humanoid robots to help the mankind to improve and keep the ideas of humanity and democracy.

The role of Machine Intelligence Quotient will play an important role in the future to be able to evaluate the degree of the autonomous behavior of the designed system. It is belief that it will be domain oriented problem and should also be important to use this information for decisions made by humans e.g. in evaluation of many information system in commercial tender to pick up the system with the highest MIQ. The usefulness of this parameter will be dependent on many influences including technological, domain oriented and also commercial aspects of the CI application in various systems. The commercial need to have “intelligent” solution and products should increase the interest for MI tools.

This year number of contribution showed up from mechanical Engineering domain, control and also pure computer science. We do believe that this multidisciplinarity will be very useful to emerge more AI applications in Information Society and will help making products and solutions more “intelligent”.

This proceedings is a small contribution of knowledge dissemination and presentation of important problems and advances in Computational intelligence theory and applications. Hungary and Slovakia as members of EU will do their best to contribute to European Research Area and support the development of Computational Intelligence technology for the benefit of the mankind.

Imre J. Rudas and Liberios Vokorokos
General Chairs

COMMITTEES

Honorary Chairs

Anton Čižmár, Technical University of Košice, Slovakia
János Fodor, Óbuda University, Budapest, Hungary
Lotfi A. Zadeh, USA

Honorary Committee

C. L. Philip Chen, University of Macau
Hamido Fujita, Iwate Prefectural University, Japan
Juraj Sinay, Technical University of Košice, Slovakia

International Advisory Board

József Gáti, Óbuda University, Budapest, Hungary
Ladislav Hluchý, Slovak Academy of Sciences, Slovakia
Dušan Kocur, Technical University of Košice, Slovakia
Peter Sinčák, Technical University of Košice, Slovakia

General Chairs

Imre J. Rudas, Óbuda University, Budapest, Hungary
Liberios Vokorokos, Technical University of Košice, Slovakia

International Organizing Committee Chairs

Marián Bucko, Elfa, Slovakia
József Gáti, Óbuda University, Budapest, Hungary
Ladislav Madarász, Technical University of Košice, Slovakia

International Organizing Committee

Norbert Ádám, Technical University of Košice, Slovakia
Vladimír Gaspar, Technical University of Košice, Slovakia
Gyula Kártyás, Óbuda University, Budapest, Hungary
Ladislav Nyulászi, Technical University of Košice, Slovakia
Rita Ősz, Óbuda University, Budapest, Hungary
Michal Puheim, Technical University of Košice, Slovakia

Technical Program Committee Chairs

Szilveszter Kovács, University of Miskolc, Hungary
Ladislav Főző, Technical University of Košice, Slovakia

Technical Program Committee

Rudolf Andoga, Technical University of Košice, Slovakia
Péter Baranyi, SZTAKI, Hungary
Balázs Benyó, Széchenyi István University, Győr, Hungary
M. Bielikova, STU Bratislava, Slovakia
György Eigner, Óbuda University, Budapest, Hungary
Róbert Fullér, Óbuda University, Budapest, Hungary
Alena Galajdová, Technical University of Košice, Slovakia
Tamás Haidegger, Óbuda University, Budapest, Hungary
László Horváth, Óbuda University, Budapest, Hungary
Csaba Johanyák, Kecskemét College, Hungary
Levente Kovács, Óbuda University, Budapest, Hungary
Dušan Krokavec, Technical University of Košice, Slovakia
Vladimír Kvasnička, STU Bratislava, Slovakia
Ladislav Madarász, Technical University of Košice, Slovakia
Zoltán Mann, BME, Hungary
Vladimír Modrák, Technical University of Košice, Slovakia
Igor Mokris, SAV Bratislava, Slovakia
Endre Pap, Singidunum University, Belgrade, Serbia
Ján Paralic, Technical University of Košice, Slovakia
Marek Penhaker, VSB Ostrava, Czech Republic
Árpád Takács, Óbuda University, Budapest, Hungary
Márta Takács, Óbuda University, Budapest, Hungary
József K. Tar, Óbuda University, Budapest, Hungary
József Tick, Óbuda University, Budapest, Hungary
Zoltán Vámossy, Óbuda University, Budapest, Hungary
Annamária R. Várkonyi-Kóczy, Óbuda University, Budapest, Hungary
Teréz Várkonyi, Óbuda University, Budapest, Hungary
Mária Vircíková, Technical University of Košice, Slovakia
Jozef Živčák, Technical University of Košice, Slovakia

Secretary General

Anikó Szakál
Óbuda University, Budapest, Hungary
E-mail: szakal@uni-obuda.hu

Iveta Zamecnikova
Technical University of Košice, Slovakia
E-mail: zamecnikova@elfa.sk

TABLE OF CONTENTS

AUTHORS' INDEX

Security enhancement of internet banking applications by using multimodal biometrics

Cătălin LUPU*, Vasile-Gheorghiță GĂITAN*, Valeriu LUPU**
* "Ştefan cel Mare" University of Suceava, Faculty of Electrical Engineering and Computer Science, Romania
** "Ştefan cel Mare" University of Suceava, Faculty of Economics and Public Administration, Romania
catalinlupu@seap.usv.ro, gaitan@eed.usv.ro, valeriul@seap.usv.ro

Abstract— **The internet banking applications have become more and more complex and almost each bank has got its own service. The login and signature security vary from user/static password authentication method (that is one of the weakest way to manage one's accounts) to certificates and tokens. Also, biometrics is increasingly used in many parts of our lives, from biometric passport, airport authentication and control access. It is easier and safer to login to internet banking with something you have or are (fingerprint, face, iris etc.) than with something you remember (and that can be stolen by malicious software or people). Also, signing an order will be more secure by using a fingerprint than a code generated by a token. A combination of these two authentication methods will lead to a visible security enhancement, too. The fingerprint can be used for two purposes: to open a token device and/or login to the internet banking application or sign an order. This article will introduce some concepts about these two fields: internet banking and biometrics. It will also present a securing internet banking operations model by using biometrics. During our researches, we developed a Java application to simulate access to an internet banking web-page. This application will be briefly presented at the end of the paper.**

I. Introduction

Internet banking applications are used by more and more people all over the world. Almost each bank has its own service. Most of the banks use the user/password authentication method, with the password generated by a token device. But what happens if someone steals your token and guesses the PIN (assuming the device has got one)? The thief may access all your accounts and make transfers to some other ones, even before you notice the token was stolen. Worse, if the bank or a financial institution is not quite interested in increasing security and it uses a static password authentication method, then this is the easiest way to enter an account. The method consists in stealing login credentials, by using phishing or a malicious software program that can send the login and the password to a server (there are many possibilities: an infected computer can send the login and password directly to another computer by tracing browser actions and/or cookies, or one can use a key-logger software, for example).

The phishing method consists in entering personal data and password for a "verification" that apparently came from your bank. The web page looks similar to the one the bank uses for authentication. But, after entering personal data, even if the password isn't provided, the people that operate the phishing page can call the bank's call center (where personal data is requested) in order to claim a password change, for example, saying that they forgot it.

Using biometrics within the authentication/signature actions, problems like the ones described above will not occur anymore. The user can use his/her biometric characteristic (fingerprint, for instance) in order to authenticate or open the token device. In this case, the person that uses the device is definitely the same that is allowed to do this. There is no doubt about it, because fingerprints are likely impossible to be stolen or counterfeited. Biometrics can be used on desktop/laptop computers, but also on smartphones, many of them being equipped with a fingerprint sensor. There is still one problem with the disabled people, whose fingerprints can't be temporarily or definitively read. In this case, another biometric characteristic is necessary; for example, face or iris recognition.

The idea of using biometrics to increase the certitude that the person that is logging in is really the one he/she claims to be, was implemented many years ago, on different applications. But the usage of biometrics in internet banking wasn't much studied. There are some banks that already use biometric characteristics to authenticate their clients. For instance, fingerprint authentication is being used by UBB (United Bankers' Bank), IBC (International Bank of Commerce) from the USA and Woori Bank from South Korea. A list of worldwide banks that use biometrics in their activity (not only within internet banking, but also on branch banking, at ATMs or for access control) are presented in the article [1].

There are many software companies that offer biometric solutions for banks, for example DigitalPersona, Veridicom Intl., Imprivata (with IndentiPHI and Saflink).

The following article will introduce some concepts concerning internet banking solutions, biometrics and a combination of these techniques that will lead to a major security increase.

II. Internet Banking – Authentication and Security Concepts

A. What is Internet Banking ?

Internet banking (with its synonyms "e-banking", "online banking" or "virtual banking") stands for an online service provided by banks or financial institutions to their clients, in order to manage accounts and operate transactions. The bank will usually provide a secured

978-1-4799-8221-9/15/$31.00 ©2015 IEEE

webpage, where the client can log in using available authentication methods.

According to John Cronin ([2]), “distance banking services over electronic media” - the precursor of modern internet banking, were introduced in the early 1980s. 1983, when 4 major US banks (Citibank, Chase Manhattan, Chemical and Manufacturers Hanover) and the Bank of Scotland from UK introduced internet banking for the first time, can be considered the birthday of this concept. The trend continued and was developed, but the users were still hesitant about the system. After the exponential internet growth, namely after 1990s, the banks managed to provide this service to almost 80% of the US clients by 2000. In fact, the first services consisted in some desktop software applications and were nothing like they are today, namely by using a browser to connect to the bank.

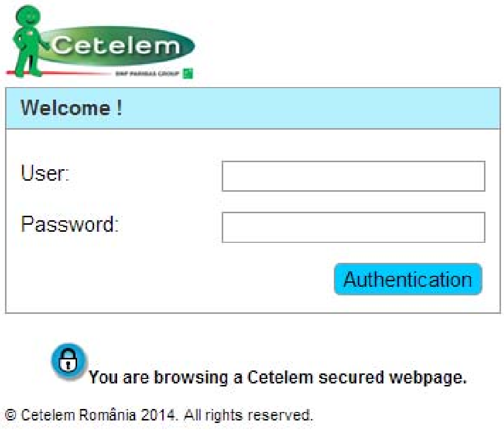
The following paragraph will present some authentication methods and concepts used for internet banking security.

B. *Authentication methods and security*

There are many possibilities to connect to an internet banking application. The most used methods consist in using a user and a password (static or dynamically generated). Three situations from two different financial institutions from Romania will be presented.

1) Username and static password

It is the weakest possible method. It was previously used by Raiffeisen Bank in Romania and many other banks. Now, the example will present the “Non-banking financial institution - Cetelem” (a subsidiary of BNP Paribas Personal Finance SA). The registration process consists in filling a form at a Cetelem desk, then receiving (after almost one week) an email from the bank to activate the access to the application. After activation, another email is sent, providing a link that must be followed in order to set the initial password. After setting the initial password, the user can login using his/her credentials. In figure 1, it is presented the login page, where the user will introduce the login credentials.



Welcome !

User:

Password:

Authentication

You are browsing a Cetelem secured webpage.

© Cetelem România 2014. All rights reserved.

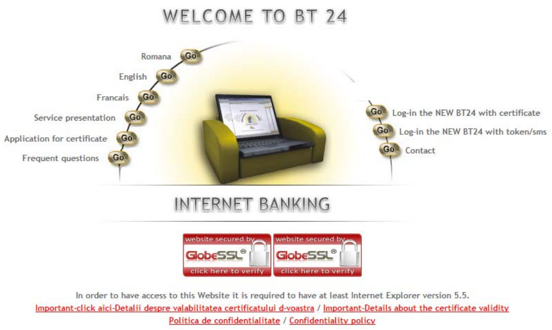
Figure 1. Cetelem authentication page, https://accounts.cetelem.ro

After entering the correct user and password, the application will redirect to the account’s main page. From here, the authenticated user can make money transfers, change personal data or view the account statement.

As shown before, there is no link to reset the password in the main page. If one loses his password, he has to call the call-center, answer some questions and then reset the password or change personal data. For instance, this can be extremely risky because of the phishing that can collect personal data and then someone that benefits from the ID theft can call the client-desk to pretend he/she is you. This method is extremely unsafe, because we usually use one password for all logins within other applications. If someone steals your password, then he/she will likely be tempted to use it on any possible application. The figure below comes from https://accounts.cetelem.ro. The page is secured with a 128 bits certificate, using the AES_128_CBC algorithm, with SHA1 and RSA. The webpage uses TLS 1.0.

2) Username and static password, when using a personal web browser certificate

This method consists of requesting a personal web browser certificate for an online banking service. The user applies for a PIN at the bank’s office and, within 1-2 weeks, an envelope containing it is delivered (using the banking internal post service). After the client receives the certificate PIN, he/she can access the internet banking webpage and request a private certificate. This can be done by accessing the “Application for certificate” link, as the following picture indicates. Then, the user must follow the instructions on the page and finally, a private certificate will be provided. The certificate is generated by Microsoft Active Directory Certificate Services, installed on the “Banca Transilvania CA”. The CA (Certification Authority) will store the user credentials and request the personal certificate within every logon into the application. This method is much more secure than the previous one, since it requires a private certificate.


WELCOME TO BT 24
Romana Go
English Go
Francais Go
Service presentation Go
Application for certificate Go
Frequent questions Go
Go Log-in the NEW BT24 with certificate
Go Log-in the NEW BT24 with token/sms
Go Contact
INTERNET BANKING
website secured by GlobeSSL click here to verify
website secured by GlobeSSL click here to verify

In order to have access to this Website it is required to have at least Internet Explorer version 5.5.
Important-click aici-Detalii despre valabilitatea certificatului d-voastra / Important-Details about the certificate validity
Politica de confidentialitate / Confidentiality policy

Figure 2. BT24 welcome page, https://bt24.btrl.ro/bt24

The private certificate provided by this CA is encrypted using a 1024 (medium) or a 2048 (high) bits key strength. The main problem is that the certificate can be only requested on the Internet Explorer browser and it becomes useless when it comes to the identification using Linux as an operating system or a smartphone with Android, iOS or even Windows Phone. Also, the certificate is computer-dependent; thus, it must be requested on every computer one wants to use this application on. It is also user-dependent, because the user only has got the PIN that can generate it.

Within the login process, in addition to the private certificate, the user must provide a username (set by the bank) and a static password.

However, the envelope with the PIN can be stolen or lost. It is highly probable that it contains the authentication password, too. Therefore, the person that uses the information from the envelope can access the certificate generating application and the login page. Yet, the password must be changed every 3 months. If the envelope containing the PIN (and possibly the password) is lost/stolen, a few days after getting it, the money from the user's account might fly to the thief's one, without having the immediate possibility to prove that one didn't really make the electronic transaction that was signed using the password.

If someone steals one's personal data, including the login username, then he/she can call the bank's call center, to request a PIN and a password change, using the credential provided by the user that fills in the fields on a phishing web page. This problem is serious, because malicious people who do that can easily convince the bank's operator to change the PIN and password, having full access to the account that is being hacked.

3) Username and dynamic password, generated by a token device

Token devices that generate passwords based on an algorithm are increasingly used for internet banking authentication. The main advantage is that they don't include any certificate (that expires eventually and must be replaced) and do not have to be inserted in the computer's USB port (having a cell-battery that must be changed from time to time). This is the main difference between this kind of token and the ones used for document digital signing (and that contains a certificate that eventually expires). When logging into an internet banking application, the secured webpage will request a username and a password that is generated by the token. The token also has a PIN that must be inserted every time a password is requested. It can also provide a code for electronic signature, based on the code provided by the webpage of the internet banking application. Therefore, it has two functions: to provide a login password (option 1 from its main menu) and a signature code when requested within a transaction in the webpage (option 2 from the main menu of the token). The token has a serial number that is linked to the user's account. Therefore, it can't be used to generate passwords for other accounts.

The token is presented in the following figure. The user has to enter the desired application (1 or 2) to generate a password for authentication or a signing code. The device provides a different password every time, based on an algorithm that is included in its internal software.

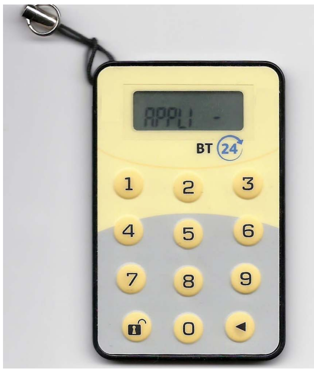


Figure 3. The BT24 authentication token

This method is more secure than the previous one, because it uses "something the user has" and not something he/she remembers (a password). This could be considered the bridge between "what the user knows" (a password) and "what the user is" (and what unique biometric characteristic he has got).

Another method, when the token is not available, is to use mobile banking. In this case, the authentication method will be SMS-OTP (SMS – One Time Password). This requires the registration of the user's phone number on his/her account. The user will fill the username and password, and then the application will send a SMS to the user's phone, containing a code that has to be filled into the login form. After this, the user can access his/her accounts.

Next, some important considerations on biometrics and its applications will be introduced.

III. Biometrics – a Grand Challenge

A. What is biometrics ?

Biometrics, a term derived from the Greek words "bios" (life) and "metrikos" (measure), stands for a complex of automation methods that should lead to personal identification using some measurable (fingerprint, iris, retina, voice, face geometry, etc.) and/or compartmental (signature, writing dynamics, etc.) characteristics of a person. According to the Webster dictionary ([3]), biometrics is defined as "the measurement and analysis of unique physical or behavioral characteristics (as fingerprint or voice patterns) especially as a means of verifying personal identity". The word "biometrics" is used for "brevity sake", because this term "has been historically used in the field of statistics to refer to the analysis of biological (particularly medical) data" ([4], [5]).

In the following paragraph, some important biometric characteristics and the sensor needed to acquire them will be presented.

B. Important biometric characteristics, sensors and their applications

There are many biometric characteristics that can be taken into account: fingerprint, iris, face, hand geometry, gait, retina, vein pattern, keystroke pattern, voice, ear, signature and many others. Some of them can be used for online authentication, but some can be only used for offline or forensic applications (such as DNA). Also, multibiometrics can be used to enhance security. The book [4] presents more data about this field.

However, we have to take into account that some individuals do not possess some of these biometric characteristics (because of a physical impairment). In this case, the system must be adapted to acquire the biometric characteristics the client is able to provide.

Biometrics is used on several applications, such as computer logon (using fingerprint, face or iris recognition), airport security (Privium System from Amsterdam International Airport – [6], Tel-Aviv "Bel Gurion" International Airport – [7], etc.), hypermarkets (Kroger – [8]), US-VISIT (United States Visitor and Immigration Status Indicator Technology – [9]) or for fun, at Disneyland World Orlando ([10]).

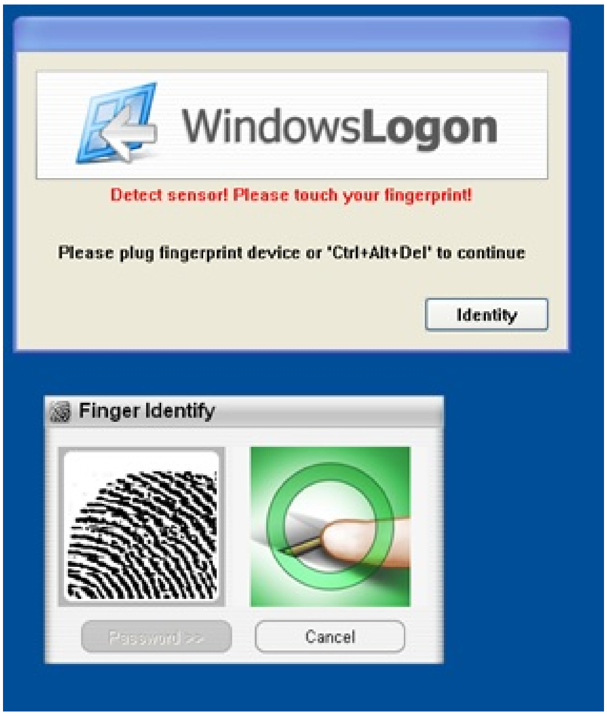
In the following paragraphs, some important biometric characteristics will be introduced.

1) Fingerprint identification

Fingerprints were one of the first studied biometric characteristics. They are used to authenticate persons or for forensic purposes. Besides other biometric characteristics, fingerprints remain at the crime scene, because of the natural grease that exists on fingers. Therefore, ever since 1892, Francis Galton determined the uniqueness of fingerprint characteristics and described some methods and algorithms in a book ([11]) which can be considered one of the first books in biometrics. Fingerprinting was introduced as an identification method in the UK Police in 1897, by Sir Richard Edward Henry ([12]).

Fingerprint identification methods and algorithms have been widely described in the book [13] and many other articles and books.

The computer logon process using fingerprint (which is also suitable for internet banking authentication) is presented in the figure 4.


WindowsLogon

Detect sensor! Please touch your fingerprint!

Please plug fingerprint device or 'Ctrl+Alt+Del' to continue

Finger Identify

Figure 4. Windows Logon using author’s fingerprint

Many devices can be used to capture the image of a fingerprint. According to [13], the main sensors to do this job can be: optical (FTIR - Frustrated Total Internal Reflection, optical fibers), solid-state (capacitive, thermal, electric field, piezoelectric), ultrasound. The touching method is one of the most used nowadays. But the sweep method consists of a cheaper device and can be easily integrated into a mouse or a smartphone. This method implies that the user should sweep his finger on a sensor. The image of the fingerprint from figure 4 is obtained by using the sensor on the mouse presented in figure 5. The mouse comes with the software for Windows logon, in addition to the driver of the fingerprint sensor. Programmatically, libraries provided by the software can be used to develop other online or desktop applications.

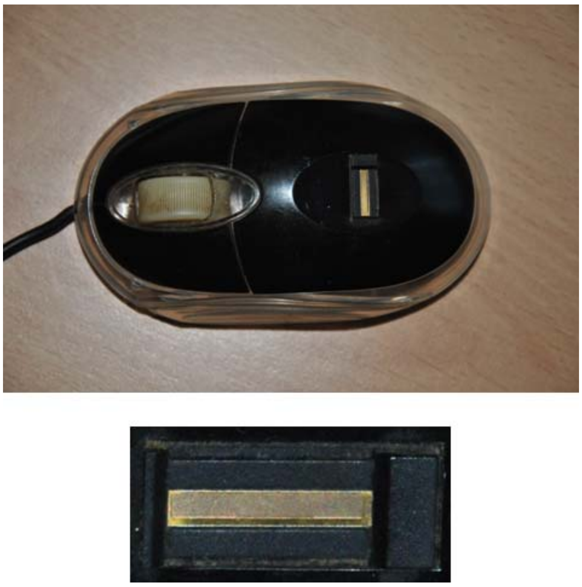


Figure 5. Mouse with a sweep fingerprint sensor and the detail of the sensor

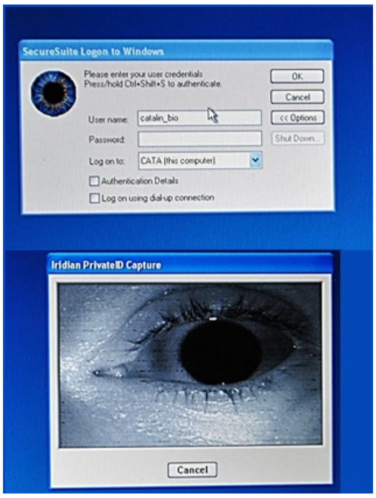
2) Iris recognition

This method is new and was still being developed since 1987, when two ophthalmologists (Leonard Flom and Aron Safir – [14]) discovered that the human iris possesses some characteristics that can be used for personal identification or people verification. The iris is usually confused with retina, but they are two different components of the human eye, one being acquired relatively easily, using an infrared camera (the iris) and the other needing special equipments to be acquired (the retina). The main contributions in iris recognition were John Daugman’s studies, starting from 1994, when the US Patent no. 5.291.560 was issued ([15]). The patent is called “Biometric personal identification system based on iris analysis” and was issued for Dr. John Daugman from Cambridge University. The main contribution of this patent is the fact that iris recognition can be mathematically described.

Iris recognition can be used (as a fingerprint) for computer logon applications and can also be integrated into an internet banking authentication process. In the picture 6, the Windows login page and the author’s right eye will be presented.

The software “SecureSuite” is provided with a “Panasonic BM-ET100US” camera that will be shown in the figure 7.

The camera has two objectives, the upper one being used for iris capture and the lower one - as a webcam. Thus, this device can also be used for facial, ear or gait recognition. In the lower part of the camera, it can be seen three formations that consist in an infra-red beam that activates every time the iris is being captured. It is better to do iris capture using infra-red, because this method will provide a better image to be processed in order to determine the iriscode (the code generated for an iris, using Daugman’s algorithm described in [15], [16] and other articles).



Please enter your user credentials
Press/hold Ctrl•Shift•S to authenticate.

User name: catalin_bio
Password:
Log on to: CATA (this computer)
□ Authentication Details
□ Log on using dial-up connection

Figure 6. Iris recognition login

Figure 7. Panasonic BM-ET100US camera

3) *Combining multiple biometrics*

Multiple biometric characteristics can be combined in order to provide a higher level of security. In the following picture, an embedded system will be described, that consists of using a special camera for iris recognition (like the one described in figure 7) and a fingerprint sensor installed on a mouse (described in figure 5). The author uses a laptop with an iris and fingerprint recognition software. The system can be used to develop a various number of applications for control access, internet banking or anything else that requires a great level of security.

IV. Using Biometrics in Internet-Banking Applications for Security Enhancement

As shown above, the degree of login or signing process security can be increased by using biometrics. Biometrics can be used for at least two purposes: to open the token instead of using a PIN and/or to actively interfere in the login or signing process. Biometrics can be used alone, or in combination with another authentication methods, such as a token.

Also, biometrics must not be imposed to the client, but the front-desk bank officer must explain the customer the advantages of this technology. Some clients are still reticent to this authentication method, but if the advantages are clearly explained, then they will be more receptive to this matter. The solution below must be presented especially to those people that really fear the possibility of their ID theft.

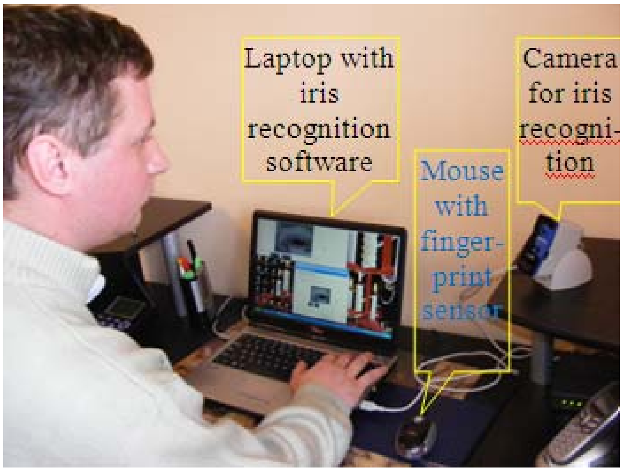

Laptop with iris recognition software
Camera for iris recogni-tion
Mouse with finger-print sensor

Figure 8. Multibiometric system, that consists of an iris recognition camera and a fingerprint sensor installed on a mouse

The first possibility is to integrate the fingerprint sensor on the token in order to replace the PIN of this device. The user will scan his/her fingerprint and the token will continue to function as though the user has inserted the PIN. All the other functions of the token remain unchanged. In the following picture, the idea will be graphically described.

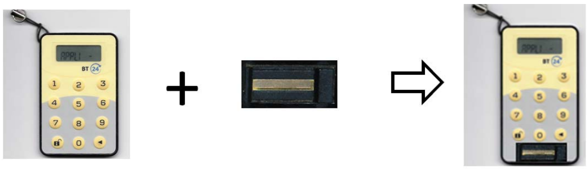


Figure 9. Token + fingerprint sensor will lead to a token that operates using this sensor

When registering the application for the token, a fingerprint or a set of them is/are scanned and stored in the internal memory of the token. Each time the user wants to use the token, he/she has to sweep the finger registered on the token.

Another solution is to use the integrated fingerprint reader – token device in order to login or sign an order. The user must first open the token (using a PIN or a registered fingerprint, as one could see above) and the authentication page of the internet banking webpage, and, in addition to the username and the code generated by the token, he/she should enter the fingerprint again. This solution requires that the device should be connected to the computer through the USB port or by other communication method (Bluetooth, WiFi, etc.).

At least, but not at last, the user can use only a username and his/her fingerprint in order to enter the internet banking application. This would be ideal, but the two solutions presented above have, in our opinion, a greater level of security.

During 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 store the template in a MySql database; (iii) do 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 above.

We chose Java to implement this application because it is compatible and can be easily integrated with most of the devices (desktop/laptop computers, tablets, smartphones, etc.).

This application is still being developped, because we use only one fingerprint sensor (SunPlus USB Fingerprint), placed on an optical mouse. There are a lot of sensors and the communication with them is made by the functions in its software or driver. The aim is to make a universal application that can work with any kind of fingerprint sensor.

V. Conclusions and Future Trends

The topic of this article can be more developed and first of all, one must take into account that some impaired people can't provide a fingerprint, so the system must be adapted in order to satisfy this requirement, too. We chose this combination token/fingerprint sensor because these devices are still cheap enough (less than €30 for all of them). A more secure system shall use iris or other biometric characteristics, but in this case, the price of the device will increase (a camera such as the one presented in figure 7 costs around $100).

The two fields presented in this article (internet banking and biometrics) are really wide and the research on combining them can lead to better solutions and higher levels of security.

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 the Sectorial Operational Program Human Resources 2007-2013.

References

[1] S.S. Hoseini and S. Mohammadi, *"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, Part III 2(9), September 2012, pp. 9152-9160, http://www.textroad.com/pdf/ JBASR/J.%20Basic.%20Appl.%20Sci.%20Res.,%202(9)9152-9160,%202012.pdf

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

[3] Webster dictionary, http://www.merriam-webster.com/dictionary/biometrics

[4] A. Ross, K. Nandakumar, A.K. Jain, *"Handbook of multibiometrics"*, Springer, 2006, ISBN 978-0-387-22296-7

[5] J.L. Wayman, A.K. Jain, D. Maltoni, D. Maio, "*Biometric systems: technology, design and performance evaluation*", Springer, 2005, ISBN 978-1-84628-064-1

[6] Schipol's Privium service, http://www.schiphol.nl/Travellers/ AtSchiphol/Privium.htm

[7] Tel-Aviv's Ben Gurion Airport, http://www.iaa.gov.il/en-US/airports/bengurion/Pages/About.aspx

[8] Kaplan, D., "*Shoppers can now pay with fingerprint at Kroger*", http://www.chron.com/business/article/Shoppers-can-now-pay-with-fingerprint-at-Kroger-2058416.php

[9] Office of Biometric Identity Management, the USA's Department of Homeland Security, http://www.dhs.gov/obim

[10] My Disney Experience – Frequently Asked Questions, https://disneyworld.disney.go.com/faq/my-disney-experience/privacy-policy/

[11] Galton, F., "*Finger-prints*", Macmillan, 1892, http://galton.org/books/finger-prints/index.htm

[12] G. Pasescu, I.R. Constantin, "*Secretele amprentelor papilare*", Editura National, 1996, ISBN 973-97574-0-5

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

[14] L. Flom, A. Safir, "*Iris recognition system*", United States Patent no. 4.641.349, 1987

[15] J. Daugman, "*Biometric personal identification system based on iris analysis*", United States Patent no. 5.291.560, 1994

[16] J. Daugman, "*How iris recognition works*", Proceedings of 2002 International Conference on Image Processing, Vol. 1, pp. 33-36, ISSN 1522-4880