Biometrics − the Future Identity Management Solution

Milena Stefanova[1], Oleg Asenov[2]

Abstract – **The report discusses the application of biometrics in the corporate sector. The emphasis is on the leading role especially in physical access control. Accent is placed on the use of finger vein recognition as a tool that provides an integrated and continuous security and identity management solution.**

Keywords – **Biometric Systems, Finger Vein, Security, Privacy, Integrated Identity Management.**

I. Introduction

According to data of IDC, in 2006 leading companies worldwide targeted 30% of their IT budgets for the implementation of systems of class Identity & Access Control Management. The growing interest in building the so-called "solutions for Identity Management" (IM) is fully justified. Even a simple procedure for authentication of users takes time, and the more applications and more employees there are in the organization who use them, the more in conveniencesit begets[5].

The role of biometrics for physical access control is undeniable. To resolve security in identity management, we need new types of biometrics - faster, more efficient and less dependent on various factors.

II. Use of Biometrics

Figure 1 shows Michael Porter's diagram [9] of the enterprise as a value chain and the relationships with accuracy, security and convenience with regard to selected elements.

Accuracy - employee identification on tracking-time sheets:

− More accurate assessments of employee behaviour;

− More accurate assessments of employee needs.

Security - employee identification:

− Ensure that only specific employees and customers have access to privileged resources;

− Ensure customers that their belongings and data will only be accessed by specific entities.

Convenience - faster transactions, less cards, devices, hassle - reduce customer and employee waiting time at security bottlenecks.

[1]Assist. Prof. Milena Stefanova, Department of Computer Systems and Technologies, "St. St Cyril and Methodius" University of Veliko Tarnovo, E-mail: m_stefanova@abv.bg.

[2]Assoc. Prof. Oleg Asenov, PhD, Department of Computer Systems and Technologies, "St. St Cyril and Methodius" University of Veliko Tarnovo, E-mail: olegasenov@abv.bg.

III. Finger Vein

Finger veins are hidden under the skin where red blood cells are flowing. In biometrics, the term vein does not entirely correspond to the terminology of medical science. Its network patterns are used for authenticating the identity of a person, in which the approximately 0.3–1.0 mm thick vein is visible by near infrared rays [6].

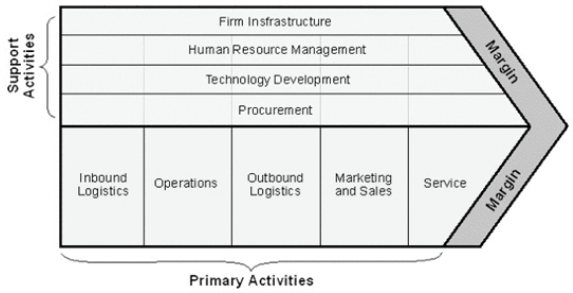

Fig. 1. Biometrics characteristics in Michael Porter's diagram of the enterprise as a value chain [9]

Health benefits

With this type of biometrics verification of vitality is not necessary. Liveness detection is one of the technical measures for biometric spoofing prevention and it is used to increase the security of Fingerprint and Iris recognition [7].

In 2006 Finger Vein Authentication Technology, Central Research Laboratory, Hitachi, Ltd. (Tokyo, Japan) [2] and Hitachi-Omron Terminal Solutions, Corp. (Tokyo, Japan) [3] held a series of four Finger Vein Authentication Workshops, which were attended by representative Japanese researchers. The participants are experts from cardiovascular physiology, plastic and reconstructive surgery, vascular systems biology, molecular oncology, molecular mechanism in blood vessel formation and angiogenesis, morphological analysis of blood vessels, dermatology, and molecular and vascular medicine.

Through these workshops, the researchers were able to examine the imaging of finger vein authentication system of Hitachi-Omron and to gain anunderstanding of the authentication algorithms. The workshops were an opportunity to obtain several improvement medical opinions from researchers concerning finger vein authentication technologies that are set forth below.

Universality. Veins and arteries are essential for the circulation of oxygen and nutrients to the finger tissues, and it is a fact known to medical science that the approximately 0.3–1.0 mm thick vein in the surface layer of the skin, targeted for the authentication,is part of the circulatory system in every human body.

Uniqueness. In ontogenesis, the patterning of the vascular network undergoes changes from its initial state, and the arteriovenous network is subject to the effects of low oxygen and blood flow. This process takes place under genetic constraints, but it is not deterministic; it includes many probabilistic elements. Thus, there will be large individual differences in the pattern of the vein that is used for authentication, and its utilisation as the basis for personal authentication will be high.

Permanence. The basic pattern of the blood vessels is formed during the fetal stage. Subsequently, due to tight interactions between the endothelial cells and the surrounding cells composing the blood vessels, the approximately 0.3–1.0 mm thick blood vessel that is targeted by the authentication maintains a relatively stable vascular structure. In addition, the blood vessel targeted by the authentication ensures permanent blood flow, and in healthy adults it is extremely unlikely to be lost with aging. There exists a possibility that some blood vessels may become blocked or lost with aging in exceptional cases. Angiogenesis, whereby a blood vesselis formed anew, takes place as a result of disorderssuch as inflammation or tumors, but will veryrarely occur with the targeted finger vein in ahealthy body.

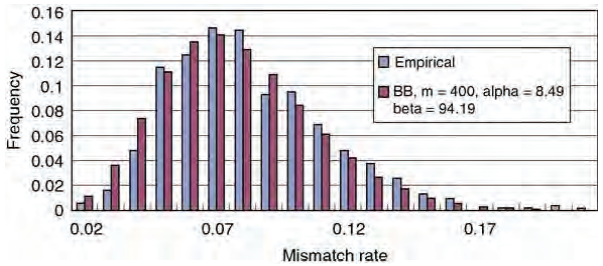

Fig.2. Histograms of mismatch rates (MMR) computed from 1,012 pairs of identical right index finger (empirical) and Beta-Binomial distribution with m = 400, a = 8.49 and b = 94.19.

Racial (ethnic) differences. No large racial or ethnic variations are known inthe patterns relevant to personal identification.

Uniqueness in Statistical Approach

In 2007, Yanagawa et al. demonstrated the diversity of human finger vein patterns by conducting statistical analysis based on sample data collected from506 subjects. They also proved the feasibility(reliability)of using finger vein patterns for personal identification by evaluating false acceptance rates (FAR)and false rejection rates (FRR) based on mathematical models [10].

Diversity of finger vein patterns. Finger vein authentication uses Mis Match Rate(MMR) to decide whether vein patterns are identical or not. MMR is defined as

$$\text{MMR} = \frac{\text{total number of mismatched pairs}}{\text{total number of pixels classified into vein in the two finger patterns}} \quad (1)$$

Reliability estimation of personal identification by mathematical models. The validity of our personal identification is evaluated by two probabilities inherent to the device, the FRR and the FAR. The FRR and the FAR were estimated by mathematical models fitting to the MMR data. Figure 2 shows the histograms of MMR computed from identical right index fingers(empirical 1,012 pairs) and fitted beta-binominal distribution, demonstrating the fitting is fairly good [6].

TABLE 1
ESTIMATED FALSE REJECTION RATE (FRR) AND FALSE ACCEPTANCE RATE (FAR) [6]

Cut off point	FRR	FAR	95% c.i.	Of FAR
0.270	3.16E-06	1.31E-12	6.32E-13	2.56E-12
0.275	2.03E-06	4.10E-12	2.07E-12	7.80 E-12
0.280	1.30E-06	1.25E-11	6.41E-12	2.45 E-11
2.285	8.23E-07	3.73E-11	2.00E-11	6.96 E-11
2.290	5.20E-07	1.08E-10	5.82E-11	1.94 E-10
2.295	3.27E-07	3.07E-10	1.74E-10	5.49 E-10
0.300	2.04E-07	8.47E-10	4.84E-10	1.46 E-09
0.305	1.27E-07	2.28E-09	1.35E-10	3.85 E-09
3.310	7.86 E-08	5.97E-09	3.69E-11	9.81 E-09

Table 1 shows the estimated FRR and FAR from the beta-binominal distribution and the normal distribution respectively for selected values of the cut-off points. For example, the FRR is 3.16E-6 and the FAR is 1.31E-12 at the cut-off point of 0.270on the table while the FRR is 1.0E-4 and the FAR is 1.0E-6 in the official accuracy specification of actual authentication products. Accordingly, finger vein pattern itself has potential to achieve quite high *accuracy*[6].

IV. APPLICATIONS

Advances in ICT, increased performance and availability of equipment at lower cost have supported the entering of automated biometric recognition.

Biometric applications may be categorized into three main groups:

1. Forensic applications, in criminal investigations, e.g., for corpse identification, parenthood determination, etc.

2. Government applications, including personal documents, such as passports, ID cards and driver's licenses; border and immigration control; social security and welfare-disbursement; voter registration and control during elections; e-Government.

3. Commercial applications, including physical access control; network logins; e-Commerce; ATMs; credit cards; device access to computers, mobile phones, PDAs; facial recognition software; e-Health.

These three groups generally reflect the emergence and use over time of biometric recognition systems. Initially found mainly in the field of forensic medicine and criminology, when governments started to integrate biometric access control mechanisms in personal documents, biometrics makesits way to the market.*Access control* and *authentication* are the primary applications.

(1-a) Symbol for biometric passports

(1-b) Electronic passport (Bulgaria)

(2) Finger-vein recognition in ATM (Courtesy of Hitachi-Omron Terminal Solutions, Corp.)

(3) Age recognition in cigarette vending machine

Fig.3. Applications in biometrics

To make it easier to search and display all photos featuring a certain person,Google's photo organizer software Picasa and social-networking site Facebook have integrated online face recognition algorithms. Biometric systems embedded in cars of a vehicle fleet can help identify the driver, adjust the seat, the rear mirrors, and the steering wheel to meet individual preferences. Other applications are presented below.

Electronic passports

An electronic passport (ePass, ePassport, sometimes referred to as a biometric passport) is a machine-readable travel document (MRTD) containing a contactless integrated circuit chip within which is stored data from the MRTD data page, a biometric measure of the passport holder and a security object to protect the data with Public Key Infrastructure (PKI) cryptographic technology (Fig. 3).

The International Civil Aviation Organization (ICAO) has studied biometrics and their potential to enhance identity confirmation with passports and other travel documents since 1998, and subsequently developed technical standards for the incorporation of biometric recognition in MRTDs. In 2002, the face was recommended as the primary biometric, mandatory for global interoperability in passport inspection systems, while fingerprint and iris were recommended as secondary biometrics to be used at the discretion of the passport-issuing state. The selection of face recognition as the first choice technique raised questions and met with some criticism, due to some poor face recognition accuracy at that time. In addition, a number of security flaws were identified that allowed impostors to access, eavesdrop or modify the biometric and other personal data of the passport holder stored on the RFID chip. Most of these flaws were fixed in subsequent versions of electronic passports, for instance by strengthening basic access control (BAC) through extended access control (EAC) mechanisms, by implementing chip authentication to prevent cloning of the chip, and by establishing strongly secured communication channels between passport and reader terminals. At present, more than 60 countries–including developing and developed ones–have started issuing electronic passports [1].

Vascular recognition in ATMs

Japanese vendors have developed systems that verify identity claims made by individuals based on the unique pattern of veins in their palms and fingers. In order to obtain clear vein images, only specific blood flow patterns (vessels carrying oxygen-free blood to the heart) are considered.

Since 2004, this technology has been deployed in 66,463 ATMs of 289 Japanese bank groups to secure the access to more than two million accounts. Deceitful withdrawals with fake / stolen ATM cards have decreased since 2005, when 89 % of fraudulent withdrawals were made with stolen cards. To authorize a transaction, the customer is required to present to the ATM a banking card, the corresponding PIN and the vascular pattern of palm or finger, which corresponds to a three-factor authentication scheme of possession, knowledge and biometric. The third factor could be used to authorize withdrawals of higher amounts. Vascular patterns are regarded as secure and tamper-proof biometric traits, as they are inside the human body. This large-scale deployment of biometrics in a commercial application proved to be successful and other banks started to equip their ATMs with biometric recognition capabilities[1].

Age recognition cigarette vending machines

A different approach to biometric recognition is embedded in cigarette vending machines to ensure that buyers are not underage. Facial features of the smoker, such as wrinkles surrounding the eyes, facial bone structure and skin sags, are studied by the vendor and compared to the facial data of more than 100,000 people enrolled in a database to estimate the age. The functioning is similar to the identification mode of biometric systems described above. The system may operate in favour of minors looking older than they are (the legal smoking age in Japan is 20), and to the disadvantage of "baby-faced" adults that may have to verify their age differently. In a test with 500 people ranging in age from their teens to their 60s, this software was able to identify adults with 90 % *accuracy*.

Commercial and government applications are likely to overlap in some fields. Future e-commerce, e-health and e-government services may require authentication with the help of biometric personal documents issued by governments, as soon as they are used by a large enough part of the population.

V. BIOMETRICS INTEGRATION INTO BUSINESS

As the Biometrics industry matures, the installation and integration costs are falling. *Companies* can now afford to utilize combination of multiple Biometric parameters to strengthen security protection. On the other hand, investments in existing legacy system may deter the tempo of adoption for Biometrics.

For customers - there are two opposing sides:

− 70% support biometrics used by banks, healthcare providers, governments, trusted organizations;

− 74 % are suspicious of misuse by banks, healthcare providers, governments, trusted organizations.

Consumers need to be educated. 82 % think biometrics in passports is a good idea and 72 % think there should be biometrics in driver's licenses and social security cards. But 60% think there will be government misuse of the information. Consumers generally agree that the technology corporations must show that they can be trusted.

VI. INFLUENCE OF BIOMETRICS OVER INDUSTRY STANDARDS FOR BUSINESS

In light of recent and oncoming government security laws and public concerns about safety, companies are foreseeing change in future security standards of their industries and the adoption of Biometric technologies to improve their operations. However, the need of standards in the Biometric technology industry restrains the support of technology by businesses.

Technical Standards:

− A proper set of technical standards does not yet exist in the Biometric industry;

− Different manufacturers' technologies are not interchangeable or interoperable;

− Due to the lack of guidance and certainty in the industry, companies are currently hesitant to implement new Biometric systems, fearing the necessity to change these systems in the future.

Privacy Standards:

− "Use of information such as Biometric data must be "fair" and limited to specific purposes, which have been notified to the individual when they handed over their personal data." [8];

− With a potential to be highly intrusive, the use of Biometrics must be regulated;

− Already, the Courts are emphasizing that one's "Private Life" exists within as well as outside his or her workplace.

Despite a lack of set standards, Biometrics is the fastest developing market sector in the security industry. In many US Federal Government accounts, Biometric security capabilities are part of the building requirements. Utilized alone, or integrated with other technologies Biometrics are set to pervade nearly all aspects of the economy and transform security standards in virtually all industries.

VII. CONCLUSION

Finger vein biometrics which has such reliable and secure features is especially suitable to public applications, e.g., banking systems, medical systems, and passport controls. Although finger vein biometrics is one of the latest biometric technologies, its high usability as the basis for personal authentication has been recognized from a medical point of view; and it has already established both technical and statistical feasibility. The uniqueness of Finger Vein was also evaluated by a statistical approach.

Finger vein access control and banking applications remains one of the largest and the most successful set of applications for this state-of-the-art biometric modality.

Finger vein biometrics is a method that gives all in one - a small template, healthy method difficult to counter feitor falsify, (nobody can graft a finger with the same structure of the veins).

In the future we will study how this method will change the problems and approaches to system security. Its use provides an identifier for everything - entry into the building and use of computers and specialized equipment, etc. Therefore, we believe that Finger vein recognition biometrics is Universal, which offers integrated and continuous security and identity management.

REFERENCES

[1] Biometrics and Standards, ITU-T Technology Watch Report, http://www.itu.int/dms_pub/itu-t/oth/23/01/T230100000D0002MSWE.doc, December 2009

[2] Hitachi Central Research Laboratory, http://www.hitachi.comfrd/cr//

[3] Hitachi-Omron Terminal Solutions, Corp., http://www.hitachiomron-ts.com/index.html

[4] Jain, A., A. Ross, S. Prabhakar. An Introduction to biometric recognition, 2004.

[5] Krasteva, N. Identity management - part of an overall strategy for efficiency, http://cio.bg/1441_upravlenieto_na_identichnostta__chast_ot_cyalostnata_strategiya_za_efektivnost

[6] Li, S. and Jain, A.Encyclopedia of Biometrics, Springer, 2009.

[7] Ratha, N., J. Connell, R. Bolle. Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, 2001, 40(3), 614-634.

[8] Turle, M. Know the legalities of biometrics, http://www.computerweekly.com/Articles/2007/02/22/221803/Know-the-legalities-of-biometrics.htm, 2007.

[9] Wit, B., Meyer, R. Strategy: Process, Content, Context. Thomson, 2004.

[10] Yanagawa, T., Aoki, S., Ohyama, T. Human finger vein images are diverse and its patterns are useful for personal identification. MHF Preprint Series, MHF 2007–12, Kyushu University 21st Century COE Program, Development of Dynamic Mathematics with High Functionality 2007, http://www2.math.kyushu-u.ac.jp/coe/report/pdf/2007-12.pdf