How to Protect Patients Digital Images/Thermograms Stored on a Local Workstation

J. Živčák, M. Roško

Abstract

To ensure the security and privacy of patient electronic medical information stored on local workstations in doctors' offices, clinic centers, etc., it is necessary to implement a secure and reliable method for logging on and accessing this information. Biometrically-based identification technologies use measurable personal properties (physiological or behavioral) such as a fingerprint in order to identify or verify a person's identity, and provide the foundation for highly secure personal identification, verification and/or authentication solutions. The use of biometric devices (fingerprint readers) is an easy and secure way to log on to the system. We have provided practical tests on HP notebooks that have the fingerprint reader integrated. Successful/failed logons have been monitored and analyzed, and calculations have been made. This paper presents the false rejection rates, false acceptance rates and failure to acquire rates.

Keywords: digital images, thermograms, biometrics, fingerprint, authentication.

1 Introduction

The Health Insurance Portability and Accountability Act (HIPAA), which was designed to ensure the security and privacy of personal health information, affects all areas of the health care. If digital (radiology) images (any kind of images, e.g., CT images or thermograms) are locally stored at workstations, they must be secured against the misuse. Nowadays, digital images and reports are distributed and accessed by authorized persons (clinicians, technologists, etc.) throughout the doctor's offices and/or by health care providers. Thus, appropriate access control, authorization and subsequent audit trails are critical [1, 2].

Common problems in securing access to patient medical information (digital images or thermograms, medical reports, and other digital data) include passwords and other sophisticated user identification and/or authentication methods, such as smart cards, biometrics, etc. [3].

To improve security and be HIPAA compliant, imaging centers and imaging departments (of hospitals, clinics) must implement security procedures and appropriate user authentication. With increasing numbers of images/thermograms being transmitted over the internet to physicians' offices, encryption also is a key component in HIPAA compliance [2].

The biometrics industry includes many hardware and software producers. Standards are emerging for a common software interface to enable the use of biometric identification in many solutions that provide security and positive identification [4]. Sharing of biometric templates and allowing effective evaluation and combination of two or more different biometric technologies is offered by IDTECK or Precise 100MC/200MC/250MC (fingerprint and Smart Card Readers) or SAGEM Morpho (fingerprint, facial and iris recognition). Interoperable biometric applications and solutions are offered by Cross Match Technologies Inc. DigitalPersona, or Precise 100MC/200MC/250MC which also offers integration with Microsoft Windows Active Directory) [5, 6, 7]. These are just a few examples of leading global biometric identity software and hardware (applications and solutions) producers.

2 Methods

We provided practical tests on 3 identical Hewlett Packard HP notebooks (model 6735b) that had Windows Vista Business operating systems installed on them, and we interconnected 3 different users in a Local Area Network (LAN), within a time frame of one month (February 2009). The biometric (fingerprint) Windows-based system environment was implemented, and the logon and authentication activity of users using a fingerprint instead of typing their password were monitored by enabling success and failure logon auditing in the Windows system's Audit policy.

The practical tests were provided within the Clinic of Plastic and Aesthetic Surgery, Porta Med, Ltd. Košice (Slovak Republic).

3 Capturing of fingerprints

Fingerprints were captured using the integrated fingerprint scanning device (reader/sensor). The scanning device is an input device that transfers the user's biometric information into electrical information and then into digital information [8, 9, 10].

In Windows, the user must authenticate before access is granted to files, folders, and/or applications (on stand-alone clients, in Active Directory setups, or some other network environment) [11].

Microsoft Windows assures security by using the following processes: authentication, which verifies the identity of something or someone, and authorization, which allows control of access to all local and network resources, such as files and printers [12].

There are four scenarios associated with the verification task. Based on whether the identity claim originates from an Enrollee or from a Fraud, the system either correctly or incorrectly accepts or rejects the identity claim [13] (Tab. 1).

Table 1: Biometric System Decision/Identity Claim

	Biometric System Decision		
Identity Claim		Accept	Reject
	Enrollee	Genuine Accept	False Reject
	Fraud	False Accept	Genuine Reject

Two steps are taken before a fingerprint is used to log on to Windows: (1) Register user's fingerprints in Credential Manager, and (2) Set up Credential Manager to log on to Windows. To register a user's fingerprints in Credential Manager, at least 2 user's fingerprints must be registered to obtain biometric samples (templates) with sufficient quality. This means that the user must swipe the same finger slowly over the fingerprint reader several times, until the finger on the screen turns green and the progress indicator displays 100 %. The biometric templates were stored locally on the hard drive of each laptop.

In addition, audit account logon events was placed. This governs auditing each instance when a user logs on with a swipe of his/her finger over the fingerprint reader. Auditing fingerprint logon attempts generates security events, depending on whether the audit of successes or failures, or both (in our case we audited both), is enabled. Success auditing generates an audit entry when an account logon process is successful. Failure auditing generates an audit entry when an attempted account logon process fails.

The events recorded in Event Viewer were used to track each user's logon attempt that occurred on each HP notebook locally. The number of entries in Event Viewer, when the accounts logon process was successful and/or the accounts logon process failed, were counted and analyzed.

4 Results

We have already mentioned that the system correctly or incorrectly accepts or rejects the identity claim on the basis of an identity claim. Thus we experience four situations, as per Tab. 1: (1) True Positive – Genuine accept an Enrollee, (2) False Positive – False reject an Enrollee, (3) False Negative – False accept a Fraud, and (4) True Negative – Genuine reject a Fraud [13].

A measure of the performance of the biometric system is its error rate, described by the *False Acceptance Rate FAR* (the probability that a biometric system incorrectly identified an Enrollee or failed to reject a Fraud), and the *False Rejection Rate FRR* (the probability that a biometric system failed to identify an Enrollee, or verified a legitimate identity claim as a Fraud) [14, 15].

The False Acceptance Rate FAR is defined as:

$$FAR = \frac{Number\ of\ False\ Acceptances}{Number\ of\ Fraud\ Recognition\ Attempts} \quad (1)$$

The False Rejection Rate FRR is defined as:

$$FRR = \frac{Number\ of\ False\ Rejections}{Number\ of\ Enrollee\ Recognition\ Attempts} \quad (2)$$

At the point where FAR and FRR are equal, this value is called the *Equal Error Rate* (*ERR*). This value does not have any practical use, so we did not calculate it. However, it is an indicator of the accuracy of the device. For example, if we have two devices with error rates of 5 % and 10 %, we know that the first device is more accurate (it makes fewer errors) than the other. However, such comparisons are not straightforward in reality [15, 16].

The number of entries from Event Viewer, in this case fingerprint logon attempts, when the accounts logon process was successful and/or the accounts logon process failed (for each user on each notebook) were collected, counted and analyzed. Tab. 2 and Tab. 3 show the calculated FRR rates from the real environment of three different computers (but with the same type of fingerprint sensor/scanner), and three users.

Although the error rates quoted by manufactures (typically FAR < 0.01, FRR < 0.1, ERR < 1) may indicate that biometric systems are very accurate, the real situation is rather different, namely the FRR is very high (over 10 %). In our case, the FRR values expressed as a percentage are in the range of 9.5 % to 18.5 % (Tab. 4). This can sometimes prevent a legitimate user (enrollee) gaining access. Thus we must be very careful when interpreting such numbers/measurements.

Table 2: Number of logins (successful, failed) for each user/per computer (notebook), and calculated False Rejected rates FRR

Notebook 1	Total logins		FRR
	Successful	Failed	
User 1	46	8	0.142
User 2	57	7	0.109
User 3	66	7	0.095
Total	169	22	0.115
Notebook 2	Total logins		FRR
	Successful	Failed	
User 1	99	12	0.108
User 2	44	10	0.185
User 3	133	22	0.141
Total	276	44	0.137
Notebook 3	Total logins		FRR
	Successful	Failed	
User 1	65	8	0.109
User 2	71	9	0.112
User 3	89	14	0.135
Total	225	31	0.121

Table 3: Total successful and failed logins (user/per computer), and False Rejection Rates FRR

	Total logins		FRR
	Successful	Failed	
User 1	210	28	0.117
User 2	172	26	0.131
User 3	288	43	0.129
Total	670	97	0.126

Tab. 4 shows the FRR rates for each user and each computer/notebook (expressed as a percentage) out of the total of authorized and failed access attempts (fingerprint used to log on to Windows).

Table 4: FRR rates in [%] (NB – notebook)

	NB 1	NB 2	NB 3
User 1	14.2	10.8	10.9
User 2	10.9	18.5	11.2
User 3	9.5	14.1	13.5

The numbers of refused acquired attempts for each user were counted in advance, and the *Failure to Acquire Rate FTA* was calculated, as below [16]:

$$FTA = \frac{Number\ of\ refused\ acquirement\ attempts}{Number\ of\ all\ acquirement\ attempts} \quad (3)$$

All acquirement refusals mean the inability of the fingerprint reader (sensor) to deliver the output data. No software or log files were used to count these refused acquirement attempts. Manual counting was arranged by each user to count refused acquirement attempts by the respective fingerprint reader (sensor).

The numbers of refused logon attempts for each user (false reject of an enrollee) are shown in Tab. 5. These are only informative results indicating how many fingerprint logon attempts were not enrolled. The *Failure to Acquire Rates* (*FTA*) were also calculated, and are shown in Tab. 5.

Table 5: FTA rates

	Acquired attempts		FTA
	Total/Success. and Failed	Refused	
User 1	238	40	0.168
User 2	198	32	0.161
User 3	331	52	0.157
Total	767	124	0.161

Tab. 6 shows the numbers of genuine acceptances and false rejects and/or false acceptances and genuine rejects in association with User 1 and notebook 1. A false reject of an Enrollee is referred to as a type 1 error of identity claim or a False Positive, and/or False acceptance of a Fraud is referred to as a type 2 error of an identity claim, or a False Negative [13].

Table 6: The number of accepted and rejected attempts associated for User 1 and notebook 1 (Note: the numbers of accepted and rejected attempts of Enrollee/User 1 were used from Tab. 1)

	Accepted	Rejected
Enrollee	46 True Positive (Genuine Accept)	8 False Positive (False Reject)
Fraud	1 False Negative (False Accept)	49 True Negative (Genuine Reject)

False Acceptance of a Fraud (False Negative) is a possible error in the statistical decision process that fails to reject enrollment when it should have been re-

jected. In real-life applications, one type of error may have more serious consequences than the other [7].

We measured the False Acceptance Rate FAR parameter for one user only (User 1) during his/her 50 login (recognition) attempts, when the user, instead of enrolling with his "registered" fingerprint (we used index fingers) provided some other "not registered" finger(s). (Note: a not registered finger means that the biometric samples/templates of the fingerprints had not been captured). In accordance with this part of the test, User 1 passed the authentication (was not rejected) once, which represents 2 % of the total Fraud login attempts.

The False Acceptance Rate (FAR), as we mentioned above, is typically FAR < 0.01. As we have shown in our measurements, where the FAR rates were calculated as per (1), we had one false acceptance Fraud only (False Negative), which represents 2 % of the total number Fraud login attempts, thus in this case the False Acceptance Rate FAR $= 0.02$.

Related calculations [13] from Tab. 6:

$$\textit{False Positive rate} = \frac{\textit{False Positive}}{(\textit{False Positive} + \textit{True Negative})} \quad (4)$$

$$\textit{False Negative rate} = \frac{\textit{False Negative}}{(\textit{True Positive} + \textit{False Negative})} \quad (5)$$

then

$$\text{False Positive rate} = \frac{8}{(8+49)} = 0.14 \text{ [or 14 \%]} \quad (6)$$

$$\text{False Negative rate} = \frac{1}{(46+1)} = 0.02 \text{ [or 2 \%]} \quad (7)$$

5 Conclusions

Utilizing fingerprints for personal authentication is becoming convenient and considerably more accurate than current methods, such as the utilization of passwords. Fingerprints cannot be forgotten, shared or misplaced. We have shown experimentally that the use of biometric techniques (fingerprint biometrics) is not yet perfect, but is reliable and secure enough to be used in log on to, e.g., personal computers (workstations) and/or networks to obtain proper data access.

Some factors influence our results for authentication reliability (dryness or wetness of fingerprints, pressure, speed of finger swiping over the fingerprint reader, etc.) These factors influence the generation of a unique template for use each time an individual's biometric data is scanned and captured. Consequently (depending on the biometric system), a person may need to present biometric data several times in order to enroll.

As regards fingerprint-based methods, note that the stored fingerprint templates should not enable reconstruction of the full fingerprint image. In this way, the system can comply perfectly well with privacy rules, so that it can only be used in co-operation with the person who is enrolled.

Acknowledgement

This paper is an outcome of the VEGA project No. 1/0829/08: "Correlation of input parameters and output thermograms changes within infrared thermography diagnostics" carried out at the Technical University of Košice, Faculty of Mechanical Engineering, Department of Biomedical Engineering, Automation and Measurement.

We thank MUDr. Viliam Jurášek and his staff from the Clinic of Plastic and Aesthetic Surgery, Porta Med, Ltd. Košice, Slovak Republic, for their assistance with data collection.

References

[1] Gate, L.: PACS Integration and Work Flow. *Radiologic Technology*, 2004, Vol. **75**, No. 5, pp. 367–377. The American Society of Radiologic Technologists, 2004.

[2] Lehman, J.: HIPAA's impact on radiology. *Radiology Management*, 2003. Vol. **25**, No. 1, pp. 45–46.

[3] Ross, A., Prabhakar, S., Jain, A.: *An Overview of Biometrics*, [on-line]. [cit. 3–23–2010]. http://biometrics.cse.msu.edu/info.html

[4] Chang, Kyong I., Bowyer, Kevin W., Flynn, Patrick J., Chen, Xin: Multi-biometrics Using Facial Appearance, Shape and Temperature. *6^{th} IEEE Int. Conf. on Automatic Face and Gesture Recognition FG'04*, Seoul, Korea, May 17–19, 2004, pp. 43–48.

[5] *Public Attitudes Toward the Uses of Biometric Identification Technologies by Government and the Private Sector. Summary of Survey Findings. Prepared by ORC International.* 2002. [on-line]. [cit. 3–23–2010] http://www.ece.unh.edu/biometric/biomet/public_docs/Biometricsurveyfindings.pdf

[6] Mullaney, J.: *Biometric authentication a choice for banks*. Software Quality News. 12 Oct 2006. [on-line]. [cit. 3–23–2010]. http://searchsoftwarequality.techtarget.com/news/article/0,289142,sid92_gci1222998,00.html

[7] Liu, S., Silverman, M: A practical guide to biometric security technology. *IT Professional*, 2001, **3**, pp. 23–32. [on-line]. [cit. 3–23–2010]. http://www.computer.org/itpro/homepage/Jan_Feb/security3.htm

[8] Ratha, N. K., Connell, J. H., Bolle, R. M.: Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 2001, Vol. **40**, No. 3, pp. 614–634.

[9] Keith, Rhodes A.: *Information Security. Challenges in Using Biometrics. Applied Research and Methods.* 2003. [on-line]. [cit. 1–20–2009] http://www.gao.gov/fraudnet/fraudnet.htm

[10] Maltoni, D., Maio, D., Jain, A. K., Prabhakar, S.: *Handbook of Fingerprint Recognition.* Springer Verlag, New York, 2003. [on-line]. [cit. 1–22–2009] http://bias.csr.unibo.it/maltoni/handbook

[11] HP Protect Tools. *Security Manager Reference Guide.* [on-line]. [cit. 2–2–2009] http://www.hp.com/notebook

[12] *Understanding Logon and Authentication.* Published: November 2005. [on-line]. [cit. 1–25–2009] http://www.microsoft.com/technet/prodtechnol/

[13] Lehman, E. L., Romano, Joseph P.: *Testing Statistical Hypotheses* (3 ed.). New York, Springer. ISBN 0387988645.

[14] Association for Biometrics, International Computer Security Association: *Glossary of Biometric Terms.* 1999. [on-line]. [cit. 1–20–2009] http://www.afb.org.uk/docs/glossary.htm

[15] Roško, M.: Biometrics: Fingerprint Verification and/or Authentication in Windows-Based System Environment. In: *Crisis Management*, 02/2007, p. 6. University of Žilina, (Faculty of Special Engineering), Žilina. ISSN 1336-0019.

[16] Říha, Z., Matyas, V.: *Biometric Authentication Systems.* Masaryk University (Faculty of Informatics). Technical Report (FIMU-RS-2000-08), p. 46. November 2000.

Dr.h.c. prof. Ing. Jozef Živčák, PhD.
Phone: +421 556 022 381, Fax: +421 556 022 363
E-mail: jozef.zivcak@tuke.sk
Technical University of Košice
Faculty of Mechanical Engineering
Department of Biomedical Engineering
Automation and Measurement
Letná 9/A, 042 00 Košice, Slovak Republic

Ing. Milan Roško
Phone: +14 164 696 333, Fax: +14 164 696 615
E-mail: milan.rosko@gmail.com
Toronto East General Hospital
825 Coxwell Ave., M4C 3E7, Toronto, Canada