Securing Biometrics Applications

Securing Biometrics Applications

by

Charles A. Shoniregun
University of East London
UK

and

Stephen Crosier
University of East London
UK

Springer

Charles A. Shoniregun
Reader in Computing
KNURE/KSAC Distinguished Professor
School of Computing and Technology
University of East London
University Way
LONDON, UK
c.shoniregun@uel.ac.uk

Stephen Crosier
School of Computing and Technology
University of East London
University Way
LONDON, UK
Steve.crosier@ntlworld.com

Library of Congress Control Number: 2007934593

Securing Biometrics Applications by Charles A. Shoniregun and Stephen Crosier

ISBN-13: 978-0-387-69932-5
e-ISBN-13: 978-0-387-69933-2

Printed on acid-free paper.

9 8 7 6 5 4 3 2 1

springer.com

DEDICATIONS

To our families and friends

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF CONTRIBUTORS AND ORGANISATIONS

Alex Logvynovskiy	e-Centre for Infonomics, UK
Harvey Freeman	Booze Allen Hamilton, USA
Caterina Scoglio	Kansas State University, Kansas, USA
Maaruf Ali	Oxford Brooks University, UK
Victoria Repka	Kharkov National University of Radioelectronics, Ukraine
Vyacheslav Grebenyuk	Kharkov National University of Radioelectronics, Ukraine
Kia Makki	Florida International University, Miami, USA
Niki Passinou	Florida International University, Miami, USA
Ann-Sofi Höijenstam	Precise Biometrics AB
Terry Cook	City University, USA.
Jen-Yao Chung	IBM Watson Research Centre, USA
Liang-Jie (LJ) Zhang	IBM Watson Research Centre, USA
Patrick Hung	University of Ontario, Institute of Technology, Canada
Dragana Martinovic	University of Windsor, Canada
Victor Ralevich	Sheridan Institute of Technology and Advance Learning, Canada
Pit Pichappan	Annamalai University, India

InternetSecuirty.com
National Security Agency, USA
National Centre for State court, USA
Centre for Unified Biometrics and Sensors. University of Buffalo, USA
International Biometric Society, USA
CERT Coordination Centre, USA
Cisco, USA
Dell, UK
e-Centre for Infonomics, UK
InternetSecurity.org.uk, UK
Microsoft Corp, USA
Sun Microsystems, Inc., USA
University of Massachusetts, USA

PREFACE

This study investigates the security of biometric applications, the opportunities and the challenges to our society. The increasing threats to national security by terrorists have led to the explosive popularity of biometric technologies. The biometric devices are now available to capture biometric measurements of the fingerprints, palm, retinal, keystroke, voice and facial expressions. The accuracy of these measurements varies, which has a direct impacts on the levels of security they offer. With the need to combat the problems related to identify theft and other security issues, society will have to compromise between security and personal freedoms. Without doubt the 21st century has brought about a techno-society that requires more secure and accurate measures.

We have also identified the key impacts of biometric security applications and ways of minimising the risk liability of individual biometrics profile that would be kept in database. The individual identification and verification have long been accomplished by showing something you have (driving licence or a passport) and required something you know (password or a PIN). The possibility of the back-end authentication process (in a networked situation) being compromised by the passing of illegal data may represent a point of vulnerability. The authentication engine and its associated interface could be fooled. It is necessary to suggest a measure of risk to the biometric system in use, especially when the authentication engine may not be able to verify that it is receiving a bona fide live transaction data (and not a data stream from another source).

More recently, the biometric identification technologies have been adopted into upmarket devices (Laptop mobile phones, cars, building access control, national identity cards, and fast-track clearance through immigration. Thus biometrics is becoming increasingly common in establishments that require high security (government departments, public meeting places, and multinational organisations) but a highly accurate biometric system can reject authorised users, fail to identify known users, identify users incorrectly, or allow unauthorised person to verify as known users. In addition, if a third-party network is utilised as part of the overall biometric system, for example using the Internet to connect remotely to corporate networks, the end-to-end connection between host controller and back-end application server should be carefully considered. In most cases, biometric system cannot determine if an individual has established a fraudulent identity, or is posing as another individual during biometrics enrolment process. An individual with a fake passport may be able to use the passport as the basis of enrolment in a biometric system. The system can only verify that the individual is who he or she claimed to be during

enrolment. To solve these problems, we proposed the Shoniregun and Crosier Securing Biometrics Applications Model (SCSBAM).

Furthermore, the success of using biometrics technologies as a means of personal identification is more assuring and comfortable because access, authentication and authorisation is granted based on a unique feature of an individuals physiological, biological or behavioural characteristic. It is tempting to think of biometrics as being sci-fi futuristic technology that we should in the near future use together with solar-powered cars, and other fiendish devices—but who knows?

ACKNOWLEDGEMENTS

It is difficult to acknowledge all the people that have directly or indirectly contributed to this book. But some names cannot be forgotten —many thanks to our editor Susan Lagerstrom-Fife, publishing director Jennifer Evans and Rudiger Gebauer for their support. Indeed, those kind reminders and useful comments from Susan and Sharon are all appreciated.

A special thank you to Dr Alex Logvynovskiy of e-Centre for Infonomics, for his never-ending contribution.

Undoubtedly, our reflection to past experiences both in the commercial sector and academia has help to bridge the gap in our understanding of the impacts of biometric security applications and ways of minimising the risk liability of individual biometrics profile. We would also like to acknowledge our appreciation to the following organisations: Precise Biometrics AB, IR Recognition systems Inc, Bio-key International, Identix, SAF Solution Enterprise, Wonder Net and Executive Agent for Biometrics.

Our sincere thanks to all the organisations that voluntarily participated in our search for knowledge.

Chapter 1

RESEARCH OVERVIEW AND BIOMETRIC TECHNOLOGIES

1. INTRODUCTION

The purpose of this study is to identify the key impacts of biometric security applications and ways of minimising the risk liability of individual biometrics profile that would be kept in the database system/server. The term biometrics was derived from the Greek words bio (life) and metric (to measure). The concept of biometrics is dated back to over a thousand years where potters in East Asia placed their fingers on their wares as an early form of branding. In the 14th century explorer Joao de Barros reported that the Chinese merchants were stamping children's palm prints and footprints on paper with ink to distinguish the young children from one another. This is one of the earliest known cases of biometrics in use and is still being used today.

> 'Degrees of freedom represent the number of independent varieties of a deviation. If 100 shred strips of paper were randomly dropped from the same distance, for example the end result would differ each time, and the likelihood of getting the same result is almost impossible.'
>
> —Chirillo J, and Blaul S, 2003

In different parts of the world up until the late 1800s, identification was largely relied upon by photographic memory and biometrics has moved from a single method (fingerprinting) to more than ten discreet methods. As the industry grows however, so does the public concern over privacy issues. Laws and regulations continue to be drafted and standards are beginning to be developed. Biometrics is rapidly evolving technology which has been widely used in forensics, but presently it is adopted in broad applications used in Banks, electronic commerce, access control welfare, disbursement programme to deter multiple claims, health care, immigration applications, national ID Card to

provide a unique ID to citizens and passport, airport terminals to allow passengers easy and quicker check-in and also to enhance security. Other technologies are seen as cutting-edge, but their accuracy remains questionable.

2. RESEARCH RATIONALE

The Department of Defence (DOD) set out Password Management Guideline in 1985. The Guideline codified the state of the use of passwords at that time, the Guideline provided recommendations for how individuals should select and handle passwords. As a result of DOD Password Management Guideline, computer users are told to periodically change their passwords. Many systems expire a user's password after an established period of weeks or months when they prompt user to change the password, however some users tend to forget and they are logged out, and the only way for them to get back in the system was a call to the IT helpdesk, which can be flooded with calls. The help desk staff may end up spending a disproportionately large amount of time fixing problems with passwords. Some systems tend to use password hashing for obscuring a password cryptographically; conversely, hashing makes it impractical to retrieve a user's password once forgotten.

Insecure authentication methods often leads to loss of confidential information, denial of services, lack of trust and issues with integrity of data and information contents. The value of a reliable user authentication is not limited to just computer access only, but to many other interconnected systems. The existing techniques of user authentications (user ID cards, passwords, chip and pin) are subject to several limitations. For example the main security weakness of password and token-based authentication mechanisms is that the awareness or possession of an item does not distinguish a person uniquely. The authentication policy based on the combination of user id and password has become inadequate. The biometric can provide much more accurate and reliable user authentication method by identifying an individual based on their physiological or behavioural characteristics (inherent features, which are difficult to duplicate and almost impossible to share) (see Tables 1–1 and 1–2 for further details). Using biometrics makes it possible to establish an identity based on `who you are', rather than the validity of biometric accuracy by 'what you possess' (photo ID or credit cards and passport) or 'what you remember' (password) (Campbell et al, 2003).

Table 1–1. Validity of biometric accuracy

Biometric system	Accuracy	Ease of use
Fingerprint	High	Medium
Hand Geometry	Medium	High
Voice	Medium	High
Retinal	High	Low
Iris	Medium	Medium
Signature	Medium	Medium
Face	Low	High

The biometric systems establish an aspect of user convenience that may not be possible using traditional security techniques. For example, users maintaining different passwords for different applications may find it challenging to remember the password of each specific application. In some instances, the user might even forget the password, thereby requiring the help desk to intervene and perhaps reset the password for that user while the biometric link an event to a person, which prevents any form of impersonation.

3. RESEARCH HYPOTHESIS

To identify and minimise the security of biometric applications a number of leading research questions were emerged to test the hypotheses:

i. What precisely constitutes biometrics?

ii. Is classification and taxonomy of biometrics possible?

iii. What are the impacts of biometrics on society?

iv. What constitutes the failure of biometrics technology?

v. Is security an issue for biometrics users?

However, knowledge can be very hypocritical at the beginning but always satisfactory when results are achieved. The following hypotheses have been formulated based on the above questions and the literature review (which includes ongoing access to online resources and laboratory experiments). All

we can say is that we do not have evidence to reject or accept the emerging hypothesis.

Hypothesis 1:

- Null hypothesis (H_0^1): Classification and taxonomy of biometrics are unattainable.
- Alternative (H_A^1): Classification and taxonomy of biometrics are attainable.

Hypothesis 2:

- Null hypothesis (H_0^2): Biometrics is not complementary to generic security approach.
- Alternative (H_A^2): Biometrics is complementary to generic security approach.

Hypothesis 3:

- Null hypothesis (H_0^3): Absolute security is unattainable on biometrics
- Alternative (H_A^3): Absolute security is attainable on biometrics.

On a serious note, making biometrics applications secured has been a hot debate for many years. The key issues in securing biometrics applications are contained in the generic architecture of the technologies that are adopted. The generic security implementations such as password and keys have been in place for a long time but unlike today, the intermediate systems at the time had no requirement to access multi-platform and millions of interconnected technologies. As the technology advances much more sophisticated system have been introduced, the deployment of biometrics has raises some issues, which must be addressed. These issues are the rediscovery of where and when do we require biometrics technology. There has been an increase in the number of devices that interoperates with biometrics to ensure that compliant implementations include the services and management interfaces needed to meet the security requirements of a broad user population.

Generally speaking, wherever there is a password or PIN used in an application or system, it could be possibly replaced by biometrics. But it varies

according to the application requirements. However, applications can be characterised by the following characteristics Nalini, et al., 1999:

- Attended vs. unattended.
- Overt vs. covert.
- Cooperative vs. non-cooperative.
- Scalable (means that the database being scalable with no appreciable performance degradation) vs. non-scalable
- Acceptable vs. non-acceptable.

The biometrics technologies can be used to verify (*identification:* who am I?) or to identify (*verification* or *authentication:* am I whom I claim to be?) an individual. The biometrics identification determines who a person is. It involves measuring individual's characteristics and mapping it with users profile stored in the database. The main purpose of positive identification is to prevent multiple users from claiming a single identity. In positive identification method, the user normally claims an identity by giving a name or an ID number, and then submits a biometric measure. Once submitted, it's matched with the previously submitted measure to verify that the current enrolled user is under the claimed identity (Wayman, 2000). These tasks can be achieved through many non-biometric alternatives in such applications as ID cards, PINs and passwords. Depending on the situation or the environment where it's installed, positive identification biometric method can be made voluntary and those not wishing to use biometrics can verify identity in other ways. The biometrics identification method can require a large amount of processing power especially if the database is very large. It is often used in determining the identity of a suspect from crime scene information. There are two types of identification: positive and negative. Positive identification expects a match between the biometric presented and the template, it is designed to make sure that the person is in the database. While the negative identification is set up to ensure that the person is not in the database, more so, it can take the form of watch list where a match triggers a notice to the appropriate authority for action.

On the other hand, biometrics *verification* or *authentication* is determines that an individual is who they say they are. It involves taking the measured characteristic and compares them with previously recorded data of the person. The main function of negative identification in an organisation is to prevent

claims of multiple identities by a single user. In negative identification, the user who enrols for biometric authentication claims that he or she have not been previously enrolled and submits a biometric measure, which is compared to all others in the system database. If the user's claim of non-enrolment is verified, that means a match is not found (Wayman, 2000). At the moment there are no reliable non-biometric alternatives in such applications, hence the use of biometrics in negative identification applications must be mandatory in places where it's important. The biometrics *verification* or *authentication* method requires less processing power and time. It is often used for accessing places or information, depending on the application domain; a biometric can either be an online or an offline system. To verify an individual's identity a 1:1 check is made between the biometric data and the biometric template obtained during enrolment (see Figure 1–1 for diagrammatic illustration). For any biometric system to be effective the data should be stored securely and not be vulnerable to theft, abuse or tampering. The data should also be free of errors to prevent false positive and negative results, and the user must be confident that the system is reliable and secure.

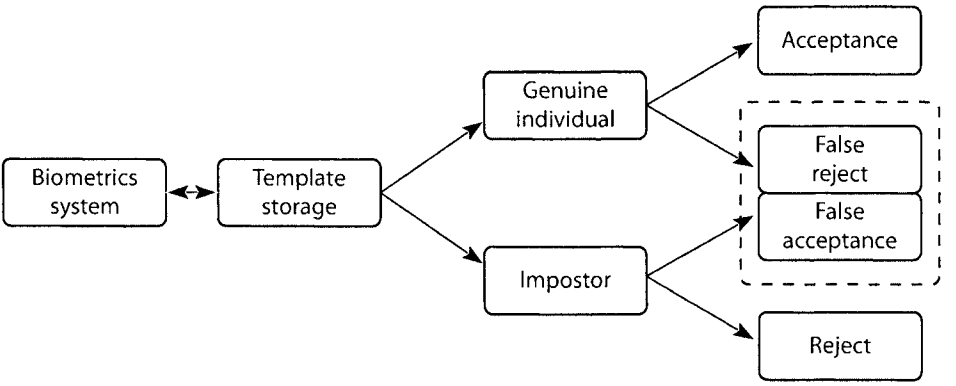

Figure 1–1. Generic biometric system process

The vast amount of data that is now held on everyone and the increases forecast for the future means that it is conceivably possible for people whereabouts to be traced through their use of information. With the need to combat the increasing problems related to identity theft and other security issues, the society will have to make a choice between security and personal freedoms. Biometrics can be incorporated at the point of sale, thereby enabling consumers to enrol their payment options (cheques, loyalty cards, credit and debit cards) into a secure electronic account that is protected by, and accessed with, a unique physical attribute. All biometric systems require an authorised user to register with the system. This involves the person supplying the relevant

biometric information needed by the system, which is then converted to data that can be stored on a database. For biometrics to be globally adopted there is a need for international standards compatibility.

4. CONCEPTUAL RESEARCH CONTEXT

From the late 1990's, governments and private organisations have developed a particular interest in biometrics and are actively funding projects involving biometrics technology. Hence, biometrics became an independent research field. It has been observed that the identity established by biometric is not an absolute 'yes' or 'no', instead it is gives a level of confidence. The Law enforcers department, matching finger images against criminal records has always been an important way to identify criminals or trace a person to a crime that that has been committed. But the manual process of matching is difficult and takes time. The Federal Bureau of Investigation (FBI) in late 1960s began to automatically check fingerprint images, and by the mid-1970s a number of automatic finger scanning systems were in operation (Zhang, et al., 2006). The Identimat pioneered the application of hand geometry and set a path for biometrics technologies as a whole. The developments in hardware, with faster processing power and high memory capability have led to advancements in the biometrics technology evolution.

With rapid growth in electronic transactions, there has been an absolute demand for biometrics technologies that enabled secure transactions but if biometrics are to become widely implemented by government and the private sectors, the public must trust that their privacy cannot be compromised and the information will not be misused. When biometric data is provided to an organisation the public should be made aware of who can access their data and how it can be used. One question would be, if fingerprints were provided for identity cards and passports— *would another government agency (such as the police) have unrestricted access to the database?* In the United State the fingerprints taken at immigration are automatically added to the FBI database. Therefore, organisations most trusted to control private data were government agencies and banks, so if biometric systems are introduced a number of questions needs to be answered:

- Who will administer biometrics profile?
- How should it be administered?

- What features should be required?

- What should be done to create awareness of trust?

In 2006 a survey was conducted by UNISYS on public perceptions of identity management. The study looked at Europe, North America, Latin America and the Asia-Pacific regions, there was a willingness amongst the respondents to share personal data in order to prove or verify their identity. The rates of acceptance vary between the regions. The findings are summarised as follows:

- In North America and Asia-Pacific respondents were more likely to share more personal data with both a trusted private business and with government, than were the respondents in Europe and Latin America.

- Respondents in Europe, North America and the Asia-Pacific regions were more willing to share personal information with governments, while in Latin America the reverse was true.

- In all regions individuals were more willing to share substantially more personal data in order to receive enhanced verification capabilities, e.g., for a multi-purpose identity credential which could be used for a number of functions.

- The data which people would be most willing to share are name, address and telephone number, but they were not willing to give information about race, religion or credit card number.

- The most important functions of a multi-functional identity credential were to access buildings, Internet accounts and immigration.

- Most individuals would prefer the data to be held on a chip on an identity card. There was also acceptance for incorporating data as a biometric within a cellular phone. When asked about the chip being implanted within the body, the acceptance rate was very low.

- It is also important that the multi purpose identity criteria should be interoperable across borders.

The UNISYS survey revealed that, the most accepted biometrics profile were fingerprints and voice, with iris being the least accepted. There is no