Charles A. Shoniregun
Stephen Crosier

Securing Biometrics Applications

Springer

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.

© 2008 Springer Science+Business Media, LLC.
All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer Science+Business Media, LLC, 233 Spring Street, New York, NY 10013, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now know or hereafter developed is forbidden.
The use in this publication of trade names, trademarks, service marks and similar terms, even if the are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

9 8 7 6 5 4 3 2 1

springer.com

DEDICATIONS

To our families and friends

TABLE OF CONTENTS

Dedications i
List of contributors and organisations ix
Preface xi
Acknowledgements xiii
Chapter 1
Research overview and biometric technologies
1. Introduction 1
2. Research rationale 2
3. Research hypothesis 3
4. Conceptual research context 7
5. Current technology for biometrics 16
6. Enrolment 17
7. Standards 20
8. The European commission 27
9. Summary of chapter one 28
References 29
Chapter 2
Biometrics measurements
1. Introduction 31
2. Related work 31
3. Biometric methods 37
4. Multimodal biometrics 65
5. Biometric encryption 66
6. Summary of chapter two 67
References 67
Chapter 3
Applications of biometrics
1. Introduction 71
2. Economy of scale 71
3. Security access 72
4. Police and prison services 74
5. Patient management in hospitals 75
6. Casino facial recognition 77
7. Enterprise network security and web access 78
8. Conceptual client requirements 79
9. Other areas of application 103
10. Summary of chapter three 111
References 112

Chapter 4
Securing biometrics applications
1. Introduction 113
2. Methods and methodology 114
3. Case studies 114
4. Classifications and taxonomy of biometrics applications 127
5. Laboratory test 129
6. Alternative international networks 132
7. Shoniregun and Crosier secured biometrics applications model (SCSBAM) 135
8. Result summary of hypotheses 139
9. Summary of chapter Four 141
References 142
Chapter 5
Critical evaluation and discussion
1. Introduction 143
2. The European Commission's Joint Research Centre (JRC) 143
3. Technological enhancement 149
4. Ethical implications 156
5. Impacts of biometrics on world governments 160
6. Impacts of future biometrics technologies 170
7. Summary of chapter five 176
References 177
Chapter 6
Conclusion
1. Operational issues of biometrics 181
2. Recommendation 184
3. Contribution to knowledge 184
References 185
Index 187

LIST OF FIGURES

Figure 1–1. Generic biometric system process 6
Figure 1–2. Generic biometric system model 9
Figure 1–3. Enrolment: identification and verification 19
Figure 2–1. Hand and palm-vein pattern 38
Figure 2–2. Hand recognition enrolment system 39
Figure 2–3. Access process for hand biometric 39
Figure 2–4. Fingerprint patterns 45
Figure 2–5. Six universal expressions 49
Figure 2–6. Distance transform 50
Figure 2–7. Understanding iris recognition 52
Figure 2–8. Retina recognition 56
Figure 2–9. Voice verification process 57
Figure 2–10. Voice identification system 58
Figure 2–11. The functional units of the brain 62
Figure 2–12. A neural-network with input pre-processing 64
Figure 3–1. Enrolment procedure, for passports and identity cards 81
Figure 3–2. Verification procedure for passports and identity cards 82
Figure 3–3. Card reader 83
Figure 3–4. Verification link 84
Figure 3–5. Detailed enrolment procedure 85
Figure 3–6. Immigration identification procedure 86
Figure 3–7. Traffic police verification 87
Figure 3–8. Identity police verification update 88
Figure 3–9. Benefits agency identification procedure 89
Figure 3–10. Health service identification 90
Figure 3–11. Combined system 104
Figure 4–1. Biometrics database connections between countries 132
Figure 4–2. International hub 133
Figure 4–3. International hub 134
Figure 4–4. Overview of Shoniregun and Crosier secured biometrics applications model(SCSBAM) 136
Figure 4–5. SBAC initial enrolment 137

LIST OF TABLES

Table 1–1. Validity of biometric accuracy 3
Table 1–2. Seven pillars of biometric wisdom 11
Table 1–3. Fingerprint 13
Table 1–4. Face recognition 13
Table 1–5. Hand geometry 14
Table 1–6. Palm print 14
Table 1–7. Iris recognition 15
Table 1–8. Vascular pattern 15
Table 1–9. Speech verification 15
Table 1–10. Dynamic signature recognition 16
Table 1–11. Selected biometrics standards 26
Table 4–1. Classification and taxonomy of biometrics 127
Table 4–2. Summary of hypotheses tested and results 140
Table 5–1. BioPrivacy application impact framework 174

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	SheridanInstituteofTechnologyandAdvanceLearning, 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).