BIOMETRIC USER AUTHENTICATION FOR IT SECURITY

From Fundamentals to Handwriting

Advances in Information Security

Sushil Jajodia
Consulting Editor
Center for Secure Information Systems
George Mason University
Fairfax, VA 22030-4444
email: jajodia@gmu.edu

The goals of the Springer International Series on ADVANCES IN INFORMATION SECURITY are, one, to establish the state of the art of, and set the course for future research in information security and, two, to serve as a central reference source for advanced and timely topics in information security research and development. The scope of this series includes all aspects of computer and network security and related areas such as fault tolerance and software assurance.

ADVANCES IN INFORMATION SECURITY aims to publish thorough and cohesive overviews of specific topics in information security, as well as works that are larger in scope or that contain more detailed background information than can be accommodated in shorter survey articles. The series also serves as a forum for topics that may not have reached a level of maturity to warrant a comprehensive textbook treatment.

Researchers, as well as developers, are encouraged to contact Professor Sushil Jajodia with ideas for books under this series.

Additional titles in the series:

IMPACTS AND RISK ASSESSMENT OF TECHNOLOGY FOR INTERNET SECURITY:Enabled Information Small-Medium Enterprises (TEISMES) by Charles A. Shoniregun; ISBN-10: 0-387-24343-7
SECURITY IN E-LEARNING by Edgar R. Weippl; ISBN: 0-387-24341-0
IMAGE AND VIDEO ENCRYPTION: From Digital Rights Management to Secured Personal Communication by Andreas Uhl and Andreas Pommer; ISBN: 0-387-23402-0
INTRUSION DETECTION AND CORRELATION: Challenges and Solutions by Christopher Kruegel, Fredrik Valeur and Giovanni Vigna; ISBN: 0-387-23398-9
THE AUSTIN PROTOCOL COMPILER by Tommy M. McGuire and Mohamed G. Gouda; ISBN: 0-387-23227-3
ECONOMICS OF INFORMATION SECURITY by L. Jean Camp and Stephen Lewis; ISBN: 1-4020-8089-1
PRIMALITY TESTING AND INTEGER FACTORIZATION IN PUBLIC KEY CRYPTOGRAPHY by Song Y. Yan; ISBN: 1-4020-7649-5
SYNCHRONIZING E-SECURITY by Godfried B. Williams; ISBN: 1-4020-7646-0
INTRUSION DETECTION IN DISTRIBUTED SYSTEMS: An Abstraction-Based Approach by Peng Ning, Sushil Jajodia and X. Sean Wang; ISBN: 1-4020-7624-X
SECURE ELECTRONIC VOTING edited by Dimitris A. Gritzalis; ISBN: 1-4020-7301-1
DISSEMINATING SECURITY UPDATES AT INTERNET SCALE by Jun Li, Peter Reiher, Gerald J. Popek; ISBN: 1-4020-7305-4
SECURE ELECTRONIC VOTING by Dimitris A. Gritzalis; ISBN: 1-4020-7301-1

Additional information about this series can be obtained from http://www.springeronline.com

BIOMETRIC USER AUTHENTICATION FOR IT SECURITY

From Fundamentals to Handwriting

by

Claus Vielhauer
Universität Magdeburg, GERMANY

Springer

Claus Vielhauer
Universität Magdeburg
Magdeburg, GERMANY

Library of Congress Cataloging-in-Publication Data

A C.I.P. Catalogue record for this book is available
from the Library of Congress.

Biometric User Authentication for IT Security
From Fundamentals to Handwriting
by Claus Vielhauer
Universität Magdeburg, GERMANY

Advances in Information Security Volume 18

ISBN-10: 0-387-26194-X e-ISBN-10: 0-387-28094-4
ISBN-13: 978-0-387-26194-2 e-ISBN-13: 978-0-387-28094-3

Printed on acid-free paper.

Printed in the United States of America.

9 8 7 6 5 4 3 2 1 SPIN 11369356, 11534648

springeronline.com

Contents

Preface

Biometric user authentication techniques have evoked an enormous interest by science, industry and society in the recent past. Scientists and developers have constantly pursued the technology for automated determination or confirmation of the identity of subjects based on measurements of physiological or behavioral traits of humans. Many biometric techniques have been implemented into authentication systems of apparently mature functionality. Although all biometric systems are subject to an intrinsic error-proneness, vendors argue for the accuracy of their systems by presenting statistical estimates or error probabilities, which suggest to be reasonably low for particular applications. With intentions like an expected integration of biometric features in travel documents in the near future, large-scale application of biometrics is becoming reality and consequently, an increasing number of people working in the IT domain will be confronted with biometric technology in the future. Thus, with the increasing diverseness of the different techniques, it is becoming more and more important for academic teachers, students and researchers as well as for practitioners, application designers and decision-makers in the IT security domain to understand the basic concepts, problems and limitations of authentication by biometrics. The goal and the uniqueness of this book are to impart knowledge to these people by expanding in two dimensions.

The **horizontal dimension** will educate the reader about the common principles in system design and evaluation of biometric systems in general, over the spectrum of the most relevant biometric techniques. Here, we will introduce to the state-of-the-art in biometric recognition across the variety of different modalities, including physiological traits such as fingerprint and iris recognition, as well as behavior such as voice or handwriting, and put them in context of the general theory of user authentication in IT security. For the system design part, we look at the systematic development of a generic process model, and provide an overview of implementation examples, along with references to selected signal and image processing methods, as well as classification techniques. The part on evaluation discusses the fundamental causes of inaccuracy of biometric systems and introduces mechanisms for experimental determination of quantitative figures in terms of error rates. Specifically for the most relevant biometrics, state-of-the-art recognition rates and references to technical details are presented for physiological methods based on face, fingerprint, iris, retina, ear and hand modalities, as well as for behavior-based approaches for voice, handwriting, gait, lip movement and keystroke dynamics. This comparative discussion will enable the reader to differentiate technical principles, potential applications and expected recognition accuracy across the zoo of different biometric schemes

Away from the scientific disciplines of signal processing and pattern recognition, biometrics can also be viewed from the perspective of IT security. Here, biometrics represents just another possibility for user authentication, besides well-established possession and knowledge-based methods. For taking care of this aspect, the book will provide insights in a formal model for the user authentication problem, as well as security requirements within all types of authentication systems. As one of the view publications in this area, it will be demonstrated how biometrics fit into this IT security-based model and where security problems can be found here.

In the **vertical dimension**, the book expands into very detailed algorithm designs and evaluation methodology for active biometric modalities on the specific example of handwriting dynamics. These parts of the book present a new approach to systematic testing of biometric algorithms, based on modeling of different types of sensor hardware and a forgery classification of attacks. Furthermore, algorithm examples for user verification and cryptographic key generation from handwriting dynamics are presented mathematically and explained in detail. It will be discussed in a very detailed manner, how experimental evaluations in various parameterizations can be performed. While in these excursions, we expand on one single modality, online handwriting, the underlying concepts are by no means limited to handwriting and these reflections are thus relevant to other biometric methods as well.

Both dimensions of the book convey true novelties both in educational and in scientific aspects. The **perception of biometric user authentication from IT security** unveils very descriptively the necessity for not considering biometrics as a black box tool to achieve security in IT, but also the requirement of **securing biometric systems in themselves**. The presentation of a **new evaluation methodology** shows the reader how **experimental scenarios can be designed to simulate real-world scenarios** of skilled forgeries and varying sensor types. **Scientifically**, as well as relevant for application designers, the main novelties of the book consist of new findings on the **impact of forgery efforts and sensor characteristics** to the recognition accuracy of biometric systems and the presentation of a **new algorithm to secure biometric references**.

Acknowledgments

Writing a book is a project, which requires a lot of work, energy and resources over a long period of time. It requires passive and active support by numerous persons additional to the author, and I attempt to give credit to those, who have helped me most in my research activities and during the long months of writing.

My overall thanks go to my wife and family for their understanding, support and patience. A scientist working in author mode may become a very strange behaving creature at times, with very limited time for family business.

Further, Klara Nahrstedt and Ralf Steinmetz have given me incredible support in reviewing my Ph.D. thesis, and by pushing me to expand my work on the subject of biometrics. Substantial parts of this book are based on the work presented in this thesis ([Viel2004]), particularly the discussions on the user authentication system model in Chapter 3, as well as the details on handwriting biometrics in Chapters 4 onwards. I would like to thank Klara for her support in the area of formalization, test methodology and also for her never-ending patience in correcting my English. I am very thankful to Ralf for opening the gate to the scientific alley for me and for his trust, patience and guidance over the years.

Writing in a foreign language gives an additional challenge to a scientific book project and the only way to avoid the worst blunders is to ask a native speaker for a linguistic review. Thank you Ryan Spring for helping me in this for Chapters 3 onwards.

Of course, I would like to thank all of the students that have worked with me over the past years. Without their creativity, hard work and patience, particularly during endless hours of programming, debugging and test runs, I

could not have completed this work. Especially Tobias Scheidat has helped me a great deal in implementing the test methodology and performing experiments over many days of test runs. These tests have been the basis for the experimental evaluations in the last three chapters of this book. My special thoughts are with Falko Ramann, who has devoted a lot of time to work with me and who contributed substantially to the user interface of the evaluation software. It is still very hard for his former colleagues and me to realize that Falko will not be able to share my joy about this book, as he was taken away from us far too early.

My thanks also go to all of my scientific colleagues at the Multimedia Communications Lab (KOM) in Darmstadt, Germany and at the Advanced Multimedia and Security Lab (AMSL) in Magdeburg, Germany, as well as to all my co-authors over the years. Our discussions were the basis of many inspirations and often influenced my scientific track.

Susan Lagerstrom-Fife and Sharon Palleschi from Springer Science and Business Media have provided terrific help in preparation and finalization of the book. I would like to thank both of them for their fulgurous responses, whenever I needed another hint to solve the many word processing problems.