Biometrics

Identity Verification in a Networked World

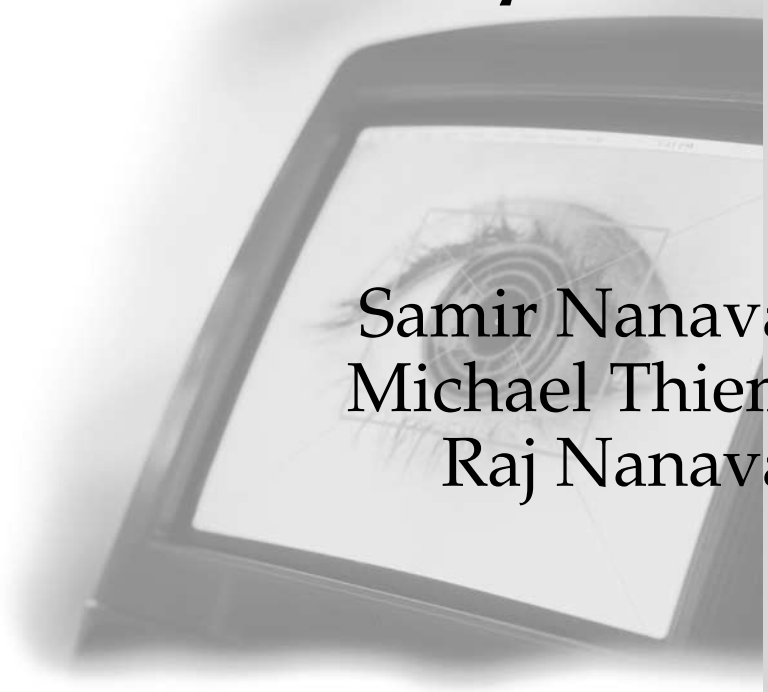
A Wiley Tech Brief

Samir Nanavati
Michael Thieme
Raj Nanavati

Biometrics

Identity Verification in a Networked World

A Wiley Tech Brief



Samir Nanavati
Michael Thieme
Raj Nanavati

Wiley Computer Publishing

John Wiley & Sons, Inc.

NEW YORK • CHICHESTER • WEINHEIM • BRISBANE • SINGAPORE • TORONTO

Publisher: Robert Ipsen
Editor: Margaret Eldridge
Editor: Adaobi Obi
Managing Editor: Micheline Frederick
Text Design & Composition: John Wiley Composition Services

Published by John Wiley & Sons, Inc.

Published simultaneously in Canada.

ISBN: 0471-09945-7

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Wiley Tech Brief Series

Other titles in this series:

Optical Networking, by Deborah Cameron, ISBN 0471443689

Service Providers, by Joseph R. Matthews and Mary Helen Gillespie, ISBN 0471418188

Internet Appliances, by Ray Rischpater, ISBN 0471441112

PKI, by Tom Austin, ISBN 0471353809

The Wireless Application Protocol (WAP), by Steve Mann and Scott Sbihli, ISBN: 047139992

Palm Enterprise Applications, by Ray Rischpater, ISBN: 0471393797

Wireless Internet Enterprise Applications, by Chetan Sharma, ISBN: 0471383827

Application Service Providers, by Traver Gruen-Kennedy, ISBN: 0471394912

Cryptography and E-Commerce, by Jon Graff, ISBN: 0471405744

Enterprise Application Integration, by William Ruh, Francis X. Maginnis, William Brown, ISBN: 0471376418

Contents

Introduction

Authentication is a fundamental component of human interaction with computers. Traditional means of authentication, primarily passwords and personal identification numbers (PINs), have until recently dominated computing, and are likely to remain essential for years to come. However, stronger authentication technologies, capable of providing higher degrees of certainty that a user is who he or she claims to be, are becoming commonplace. Biometrics are one such strong authentication technology.

Biometric technologies as we know them today have been made possible by explosive advances in computing power and have been made necessary by the near universal connectedness of computers around the world. The increased perception of data and information as near equivalents of currency, in conjunction with the opportunities for access provided by the Internet, is a paradigm shift with significant repercussions for authentication. If data is currency, then server-based or local hard drives are our new vaults, and information-rich companies will be held responsible for their security. Because of this, passwords and PINs are nearing the end of their life cycle for many applications.

Since early 1999, four factors (reduced cost, reduced size, increased accuracy, and increased ease of use) have combined to make biometrics an increasingly feasible solution for securing access to computers and networks. But biometrics are much more than a replacement for passwords. Millions of people around the world use biometric technology in applications as varied as time and attendance, voter registration, international travel, and benefits dispersal. Depending on the application, biometrics can be used for security, for convenience, for fraud reduction, even as an empowering technology.

This book teaches you the fundamentals of leading biometric technologies: how they work, their strengths and weaknesses, where they can be effectively

deployed. It helps you understand how biometrics are associated with technologies such as public key infrastructure (PKI) and smart cards. It defines how biometric deployments can be privacy enhancing or privacy invasive. It dispels various myths surrounding biometric technology. Finally, it provides guidelines for successful deployment of biometrics in today's enterprise environment.

How This Book Is Organized

There are many misconceptions about biometric technology that have taken hold in the general public. In order to provide you with a solid understanding of the technology, the industry, the applications, and the challenges that define biometrics, this book is divided into four parts.

Part One: Biometric Fundamentals

Part One provides you with a detailed understanding of the central concepts involved in biometrics, including reasons why the technology is deployed, how the technology operates, the key processes involved in biometric authentication, and how accuracy is defined in biometric systems.

Chapter 1, "Why Biometrics?," discusses why biometrics are of such interest to institutions looking to authenticate employees, customers, and citizens. This chapter also details the benefits that biometric technologies can provide when deployed correctly. Chapter 2, "Key Biometric Terms and Processes," digs deeper into biometric functionality, defining and explaining the variety of terms, both technical and nontechnical, used in the biometric industry. This chapter also discusses the biometric concepts essential to understanding how and why biometrics are deployed today. Chapter 3, "Accuracy in Biometric Systems," defines the categories used to determine how well biometric systems work and examines why most discussions of biometric accuracy are highly misleading.

Part Two: Leading Biometric Technologies

Part Two provides detailed discussions of leading biometric technologies. The information in Part Two is based on real-world experience in deploying and testing systems in operational environments. For each biometric discipline, Part Two addresses in full topics such as system components, data acquisition, template generation and matching, deployments, and strengths and weaknesses. Technologies discussed include finger-scan, facial-scan, iris-scan, retina-scan, signature-scan, keystroke-scan, hand-scan, AFIS, and biometric middleware.

Part Three: Biometric Applications and Markets

Part Three discusses the applications in which biometrics are used and the markets and industries in which they are most effectively deployed. Biometric solutions have emerged in a range of applications, including Citizen ID, Network/PC Access, Surveillance, and e-Commerce/Telephony. These applications can differ substantially in terms of technology selection, privacy impact, and performance requirements. Furthermore, biometrics have emerged as viable solutions in a handful of vertical markets, including government and financial sectors.

Part Four: Privacy and Standards In Biometric System Design

Part Four discusses critical factors related to standards and privacy that institutions must consider when designing, deploying, and maintaining biometric systems for customers, employees, or citizens. Privacy has long been a major issue in biometrics; the emergence of a framework for evaluating the privacy impact of biometric technologies and deployments should help address this central problem. In addition, the emergence of biometric standards has reduced the levels of risk involved in deploying biometric systems.

Who Should Read This Book

This book provides public- and private-sector professionals with a real-world understanding of biometric technologies and applications, helping them make informed decisions on the role that biometrics can play in their organization. No background in biometrics is required, but those with biometrics experience will benefit from the detailed discussion of concepts not often presented from a deployer's perspective, such as accuracy, privacy, and technology strengths and weaknesses. Although some of the discussions may go into detail about biometric processes or functions, the book is not intended to be highly technical.

Those new to biometrics are strongly encouraged to read from the beginning, as an understanding of biometrics requires familiarity with the reasons why biometrics are deployed and the key terms involved in biometrics. Those more experienced with biometrics can begin with the technologies of interest to them and move into privacy and system design. However, even those with biometrics experience are encouraged to read the entire book(many basic concepts in the biometrics industry have often been poorly defined or overlooked, a problem that this book addresses.

Looking Forward

Biometric technology has emerged as a viable solution for a range of applications where a person's identity must be verified or determined. No longer a science-fiction solution, biometrics are being deployed to solve security problems, to help companies generate revenues, and to protect personal information. The challenge is to ensure that biometrics are used intelligently and responsibly as the technology moves into the mainstream; the repercussions of unintelligent and irresponsible use could be severe.

Acknowledgments

The authors would like to express their appreciation to those whose diligent efforts have been instrumental to the growth of the biometric industry, and to those who have helped foster a greater understanding of the potential impact of biometrics on today's world:

Cathy Tilton, William Saito, Geoff Slagle, Barry Steinhardt, Peter Hope-Tindall, Colleen Madigan, Joseph Atick, Bill Voltmer, Jeff Stapleton, Paul Reid, Scott Moody, John Ticer, Karl Ware, Vance Bjorn, Erik Bowman, Mitch Tarr, Fernando Podio, Jeff Dunn, Dr. Ann Cavoukian, John Woodward, Dr. Jim Wayman, Dr. Doug McGovern, Peter Higgins, Bill Rogers, Bill Spence, John Harris, Rick Pratt, Dave Troy, Dr. Anil Jain, Oz Pieper, Ron Beyner, Walter Hamilton, Tom Hopper, Mike Garris, Ed German, Colin Soutar, Naeem Zafar, Dr. Bridgette Wirtz, Dave Mintie, Astrid Albrecht, Tony Mansfield, Dr. John Daugman, Denny Carlton, Tim Ruggles, Norm Hughes, Sid Lieberman, Gary Roethenbaugh, Steve Borza, Dr. Larry O'Gorman, Tom Colatosti, Dr. John Schneider, Dennis Quiggle, Jeff Poulson, Allen Ganz, David Hertz, Dae Won Im, Christer Bergman, Fabio Righi, Dr. Jonathan Phillips, Duane Blackburn, P.J. Bulger, and Jean-Marc Suchier.

Special thanks go to: J. Shoor, L. Corbett, J. Goodman, C. Russo, A. Carr, L. Wall, A. Garay, C. Connors, G. Gruber, B. Chen, J. Granato, R. Rasmussen, J. Goding, B. Hyslop, B. Aucoin, J. Homme, C. Thompson, R. Pollard, D. Fuchs, R. Hoyte, E. Olsen, J. Gee, A. Backenroth, M. Hanselman, T. Dorren, J. Medicus, K. Nessman, P. Anther, S. Walsh, M. Nazar, D. Ziemke, C. Nagy, M. Goldberg, I. Beyah, and M. Spivey.

The authors would like to recognize the research, consulting, integration and support professionals of International Biometric Group for their hard work and dedication. Without their creativity, integrity, and commitment,