SpringerBriefs in Computer Science

For further volumes:
http://www.springer.com/series/10028

Markus Jakobsson

Mobile Authentication

Problems and Solutions

Springer

Markus Jakobsson
PayPal
San Jose
CA, USA

ISSN 2191-5768 ISSN 2191-5776 (electronic)
ISBN 978-1-4614-4877-8 ISBN 978-1-4614-4878-5 (eBook)
DOI 10.1007/978-1-4614-4878-5
Springer New York Heidelberg Dordrecht London

Library of Congress Control Number: 2012942921

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

For A and Art.

Foreword

“Something you are; something you know; something you have.” – I first heard these words as a graduate student studying computer security technologies and authentication. These three factors are all we have at our disposal to try to correctly identify other human beings.

In face-to-face interaction, familiar people use ”something you are” to identify one another such as their facial structure or voices. When driving through an EZPass toll booth, one uses ”something you have” to identify one’s car, so that the appropriate account is billed. And when logging into most websites, users typically use ”something you know” as the password. Using multiple factors in combination is known to increase security.

While most facets of technology have advanced exponentially, authentication of people to machines has stagnated for quite some time. Most people still use conventional passwords to log into websites for shopping, banking, and other sensitive transactions. We are starting to see small advances in practice, typically in the form of two-factor authentication instead of one, but we have not had the kind of revolution that other areas of technology have enjoyed.

In his new book featuring “duets” with several of his co-authors, Markus Jakobsson gives a fascinating look at current and potential future authentication technologies. He explains why the problem of authenticating users to machines is so difficult and gives a peek under the hood of some of the more promising techniques. For example, while many consider biometrics to be the holy grail for authentication, this book highlights the real benefits as well as the limitations of these techniques.

This book offers a deep understanding of password and PIN schemes and also covers such topics as visual authentication and defeating spoofing. Whether you are a practitioner who needs to understand your options for authenticating users, or a computer scientist who wants to perform research on this important and interesting topic, this book has plenty to offer you.

As a security professional, I began reading this book thinking that it would be a review of concepts I was already familiar with, but I found that I learned a tremendous amount, and think that this book is a must have for anyone in the security field.

Baltimore, May 2012 *Avi Rubin*

Preface

As a society, we have used different forms of authentication since ancient times – of people, documents, materials of value, etc. With the emergence of networked computers in the latter part of the twentieth century, authentication research flourished and many new techniques were developed. Among the central concepts developed or improved upon, we find PINs, passwords, various forms of backup authentication, techniques for device identification, and cryptographic techniques for message authentication.

While consumer habits and the use of legacy systems have hampered changes to authentication systems, we argue that systems designed with these issues in mind can be successfully deployed, and help address global security issues of increasing importance. In this book, we support this argument by describing a collection of new authentication technologies to address unmet authentication needs in a way that minimizes friction, and experimental evaluations of the technologies to quantify the benefits of deployment.

A handset is not just a small computer – it is a small computer with a different user interface. People use it differently. Therefore, mobile authentication is not simply authentication on a mobile device – there are other constraints and enablers. This book focuses on mobile authentication.

While this book provides a view of frontiers in authentication research, we certainly do not make any claims of covering all angles. However, we hope to convince the reader of the value of departing from the status quo and adopting new authentication methods.

Mountain View, California,
May, 2012

Markus Jakobsson
Principal Scientist of Consumer Security, PayPal

Acknowledgements

This book would not have been possible without the contributions of my co-authors – Ruj Akavipat, Mayank Dhiman, Debin Liu, Saman Gerami Moghaddam, Mohsen Sharifi and Hossein Siadati. We have benefitted from insightful discussions with Dirk Balfanz, Jeff Edelen, Aaron Emigh, Nathan Good, William Leddy, Brett McDowell, Jim Palmer, Garry Scoville, and Diana Smetters. Many thanks to Dahn Tamir, who helped in the execution of experiments involving Amazon Mechanical Turk, and to Hampus Jakobsson for assistance with recruiting subjects. We also appreciate the helpful feedback we have received from participants in the user studies underlying many of the chapters. Also, we wish to thank Jeff Hodges, M. Mannan, Netanel Raisch, and Chris Schille for feedback on earlier drafts; Hossein Siadati for LaTex assistance; and Eric Park for editorial guidance. Last but not least, thanks to Michael Barrett for recognizing the benefits of both basic and applied research at Paypal, thereby enabling much of this work.

Contents