Bystander-Centered Design ▪ Secure Computing ▪ Trusting Certificate Authorities

IEEE
SECURITY & PRIVACY
Building Dependability, Reliability, and Trust

THE SECURITY–USABILITY TRADEOFF MYTH

IEEE

IEEE computer society
CELEBRATING 70 YEARS

IEEE Reliability Society

September/October 2016
Vol. 14, No. 5

September/October 2016
Vol. 14, No. 5

Contents

Cover art by Peter Bollinger, www.shannonassociates.com

The Security–Usability Tradeoff Myth

This special issue of *IEEE Security & Privacy* features three articles and a roundtable discussion that examine the relationship between security and usability in detail to identify the perceptions, processes, and practices that underlie these continuing challenges and to identify what needs to change to advance the usable security field.

11 Guest Editors' Introduction: The Security–Usability Tradeoff Myth
M. Angela Sasse and Matthew Smith

14 Secure and Usable Enterprise Authentication: Lessons from the Field
Mary Theofanos, Simson Garfinkel, and Yee-Yin Choong

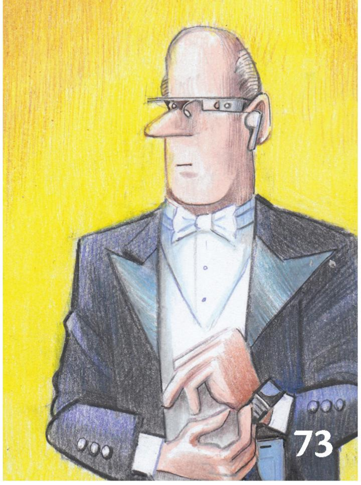
22 Barriers to Usable Security? Three Organizational Case Studies
Deanna D. Caputo, Shari Lawrence Pfleeger, M. Angela Sasse, Paul Ammann, Jeff Offutt, and Lin Deng

33 Debunking Security–Usability Tradeoff Myths
M. Angela Sasse, Matthew Smith, Cormac Herley, Heather Lipford, and Kami Vaniea

40 Developers Are Not the Enemy! The Need for Usable Security APIs
Matthew Green and Matthew Smith

Also in This Issue

48 Maturity and Performance of Programmable Secure Computation
David W. Archer, Dan Bogdanov, Benny Pinkas, and Pille Pullonen



Columns

3 From the Editors
Is It Legal? Is It Right? The Can and Should of Use
Susan Landau

96 Last Word
Stop Trying to Fix the User
Bruce Schneier

Also in This Issue

13 | IEEE Reliability Society Information
67 | Advertiser Information
92 | IEEE Computer Society Information

Departments

7 Interview
Silver Bullet Talks with Gary McGraw
Marcus Ranum

58 Spotlight
Security & Privacy Week Interviews, Part 1
Ahmad-Reza Sadeghi and Ghada Dessouky

68 Privacy Interests
Global InfoSec and Breach Standards
Rita Heimes

73 In Our Orbit
Genteel Wearables: Bystander-Centered Design
Ivo Flammer

80 It All Depends
Assessing the Security Properties of Software Obfuscation
Hui Xu and Michael R. Lyu

84 Education
GenCyber: Inspiring the Next Generation of Cyber Stars
Tina Ladabouche and Steve LaFountain

88 Crypto Corner
White-Box Cryptography: Security in an Insecure Environment
Marc Beunardeau, Aisling Connolly, Rémi Géraud, and David Naccache

93 Building Security In
That Certificate You Bought Could Get You Hacked
Jonathan Margulies and Michael Berg

Printed with inks containing soy and/or vegetable oils

SUSTAINABLE FORESTRY INITIATIVE Certified Chain of Custody At Least 25% Certified Forest Content www.sfiprogram.org SFI-01042

Postmaster: Send undelivered copies and address changes to *IEEE Security & Privacy*, Membership Processing Dept., IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854-4141. Periodicals postage rate paid at New York, NY, and at additional mailing offices. Canadian GST #125634188. Canada Post Publications Mail Agreement Number 40013885. Return undeliverable Canadian addresses to PO Box 122, Niagara Falls, ON L2E 6S8. Printed in the USA. **Circulation:** *IEEE Security & Privacy* (ISSN 1540-7993) is published bimonthly by the IEEE Computer Society. IEEE Headquarters, Three Park Ave., 17th Floor, New York, NY 10016-5997; IEEE Computer Society Publications Office, 10662 Los Vaqueros Circle, Los Alamitos, CA 90720, phone +1 714 821 8380; IEEE Computer Society Headquarters, 2001 L St., Ste. 700, Washington, D.C. 20036. Subscribe to *IEEE Security & Privacy* by visiting www.computer.org/security. *IEEE Security & Privacy* is copublished by the IEEE Computer and Reliability Societies. For more information on computing topics, visit the IEEE Computer Society Digital Library at www.computer.org/csdl.