

NOVEMBER/DECEMBER 2009
VOLUME 7, NUMBER 6

IEEE SECURITY&PRIVACY

BUILDING DEPENDABILITY, RELIABILITY, AND TRUST

Features

Insider Threats

- 10** Guest Editors' Introduction
SHARI LAWRENCE PFLEEGER AND SALVATORE J. STOLFO
- 14** Detecting Insider Theft of Trade Secrets
DEANNA D. CAPUTO, MARCUS A. MALOOF, AND GREGORY D. STEPHENS
MITRE researchers designed a prototype system for identifying insider threats, which prompted a team of engineers and social scientists to study how malicious insiders use information differently from a benign baseline group.
- 22** Designing Host and Network Sensors to Mitigate the Insider Threat
BRIAN M. BOWEN, MALEK BEN SALEM, SHLOMO HERSHKOP, ANGELOS D. KEROMYTIS, AND SALVATORE J. STOLFO
To address the insider attack threat, the authors have designed an architecture for detection that combines an array of complementary monitoring and auditing techniques.
- 30** Building a System for Insider Security
FELICIA A. DURÁN, STEPHEN H. CONRAD, GREGORY N. CONRAD, DAVID P. DUGGAN, AND E. BRUCE HELD
Current protection strategies against insider adversaries are expensive, intrusive, not systematically implemented, and operated independently. The authors provide a systems-based framework and model for understanding important elements, their interactions, interdependencies, and gaps for insider security.



COVER ARTWORK BY GIACOMO MARCHESI. WWW.GIACOMOMARCHESI.COM

Tamper-Proofing

- 39** Failures of Tamper-Proofing in PIN Entry Devices
SAAR DRIMER, STEVEN J. MURDOCH, AND ROSS ANDERSON
The authors examined two market-leading PIN entry devices and found them easy to compromise because of both their design and the processes used to certify them as secure.

Access Control

- 46** The Rules of Redaction: Identify, Protect, Review (and Repeat)
ERIC BIER, RICHARD CHOW, PHILIPPE GOLLE, TRACY HOLLOWAY KING, AND JESSICA STADDON
Identifying and protecting sensitive content is difficult. Redaction is particularly challenging because it seeks to protect a document by selectively removing only the sensitive parts.

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, PO Box 3014, Los Alamitos, CA 90720-1314, phone +1 714 821 8380; IEEE Computer Society Headquarters, 2001 L St., Ste. 700, Washington, D.C. 20036. **Subscription rates:** IEEE Computer Society members get the lowest rates and choice of media option—\$29/37/725 US print + online/sister society/nonmember institutional. Go to www.computer.org/subscribe to order and for more information on other subscription prices. Back issues: \$20 for members and \$120 for nonmembers.

Departments

From the Editors

- 3 Labeling-in Security
FRED B. SCHNEIDER

Interview

- 5 Silver Bullet Talks with Fred Schneider
GARY MCGRAW

News

- 8 News Briefs
JAMES FIGUEROA

It All Depends

- 54 High Time for Trusted Computing
BRUCE POTTER

Education

- 57 The Dartmouth Cyber Security Initiative:
Faculty, Staff, and Students Work Together
ADAM GOLDSTEIN AND DAVID BUCCIERO

On the Horizon

- 60 A Tale of Three Cyber-Defense Workshops
O. SAMI SAYDJARI AND CYNTHIA E. IRVINE

Crypto Corner

- 65 Side-Channel Attacks
on Cryptographic Software
NATE LAWSON



SECURE SYSTEMS, P. 77

Basic Training

- 69 Malware Shall Greatly Increase ...
RICHARD FORD AND WILLIAM H. ALLEN

Attack Trends

- 72 Frightened by Links
FRANCO CALLEGATI AND MARCO RAMILLI

Secure Systems

- 77 Bickering In-Depth:
Rethinking the Composition
of Competing Security Systems
MICHAEL E. LOCASTO, SERGEY BRATUS,
AND BRIAN SCHULTE

Security & Privacy Economics

- 82 Nudging Privacy: The Behavioral
Economics of Personal Information
ALESSANDRO ACQUISTI

- 37 IEEE Reliability Society Information
81 Advertiser Index
85 IEEE Computer Society Information

Columns

For Good Measure

- 86 Patch Grief with Proverbs
DANIEL E. GEER JR. AND DANIEL G. CONWAY

Clear Text

- 88 Deskillng Digital Security
DANIEL E. GEER JR.

Printed in the USA with soy-based ink
on ANSI/NISO standard Z39.48-1992 recycled paper.



IEEE Security & Privacy is copublished by the IEEE Computer and Reliability Societies.
For more information on computing topics, visit the Computer Society Digital Library at www.computer.org/csdl.