

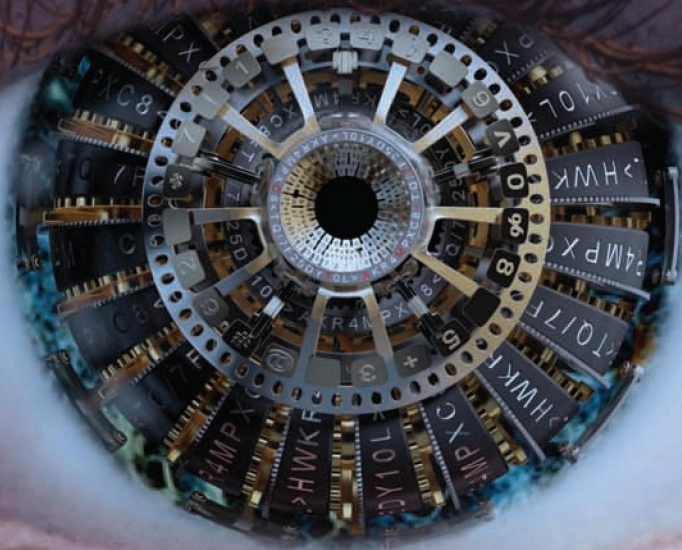
Hardware-Aided Security ■ Examining Cybersecurity Competitions' Effects ■ Law of the Horse

IEEE

# SECURITY & PRIVACY

BUILDING DEPENDABILITY, RELIABILITY, AND TRUST

REAL-WORLD



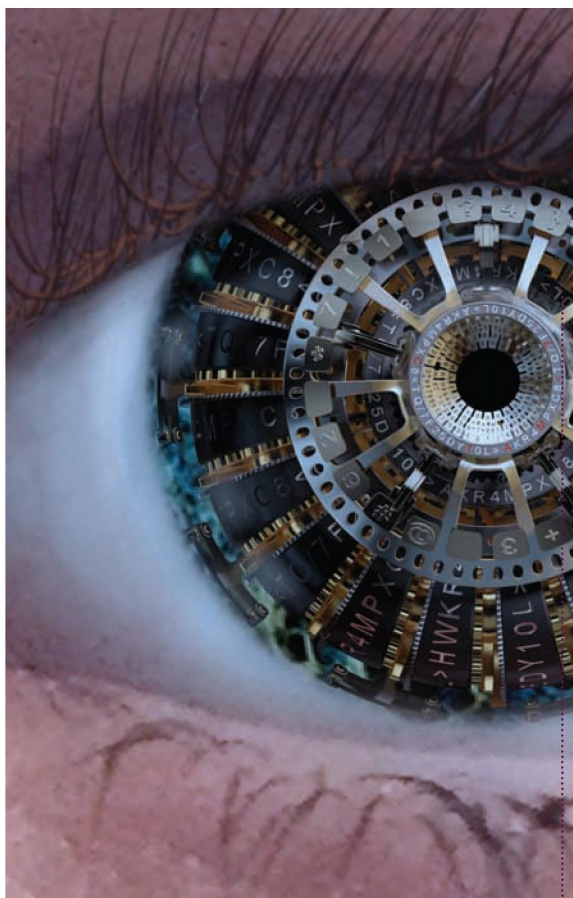
CRYPTO



November/December 2016  
Vol. 14, No. 6

IEEE  computer society  
CELEBRATING 70 YEARS





Cover art by Peter Bollinger, [www.shannonassociates.com](http://www.shannonassociates.com)

## Real-World Crypto

Great work is being done on the interface between cryptography practice and theory. The articles in this issue show that real-world cryptography isn't just focused on the traditional aspects of communications security but now ranges far and wide. They also demonstrate that practitioners are concerned about the societal impacts and the social constructs underlying our "science."

**7 Guest Editors' Introduction:  
Building a Community of Real-World Cryptographers**

Dan Boneh, Kenny Paterson, and Nigel P. Smart

**10 Practice-Oriented Provable Security and the Social  
Construction of Cryptography**

Phillip Rogaway

**18 miTLS: Verifying Protocol Implementations against  
Real-World Attacks**

Karthikeyan Bhargavan, Cédric Fournet, and Markulf Kohlweiss

**26 Automated Verification of Real-World  
Cryptographic Implementations**

Aaron Tomb

**34 A Riddle Wrapped in an Enigma**

Neal Koblitz and Alfred Menezes

**43 Network Traffic Obfuscation and Automated  
Internet Censorship**

Lucas Dixon, Thomas Ristenpart, and Thomas Shrimpton

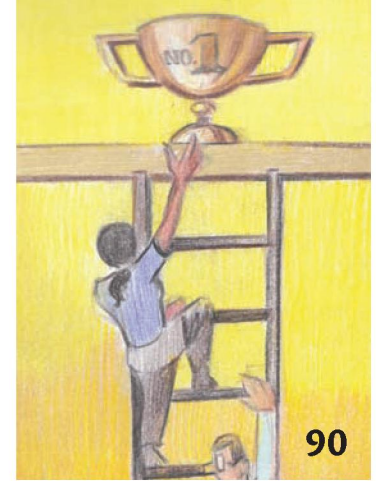
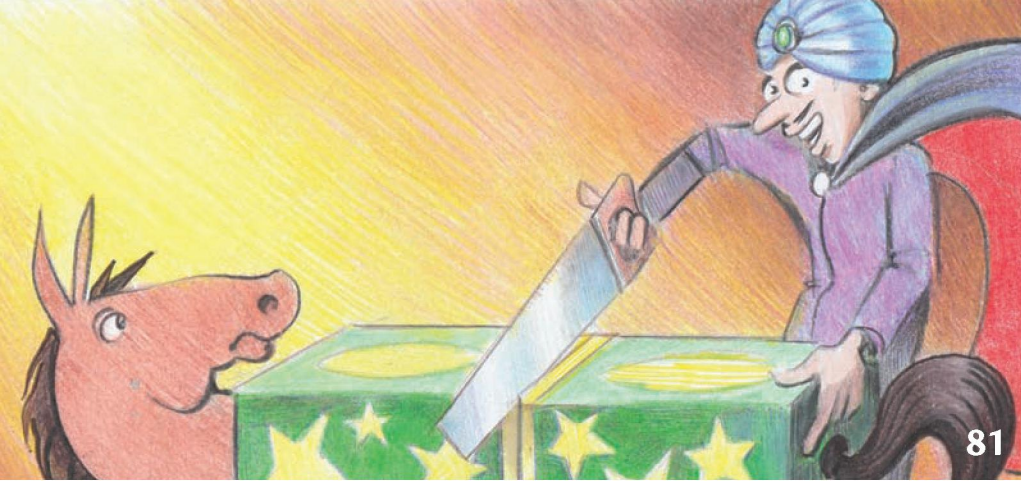
**54 Memory Encryption for General-Purpose Processors**

Shay Gueron

## Also in This Issue

**63 Secure Computing Using Registers and Caches: The  
Problem, Challenges, and Solutions**

Jingqiang Lin, Bo Luo, Le Guan, and Jiwu Jing



## Columns

### 96 Last Word

Easy Email Encryption  
Steven M. Bellovin

## Departments

### 3 Interview

Silver Bullet Talks with Jim Manico  
Gary McGraw

### 71 Spotlight

Security & Privacy Week Interviews, Part 2  
Ahmad-Reza Sadeghi and Ghada Dessouky

### 81 Privacy Interests

*Microsoft v. USA*: Location of Data and the Law of the Horse  
Omer Tene

### 86 It All Depends

Building Critical Applications Using Microservices  
Christof Fetzer

### 90 Education

The Outcomes of Cybersecurity Competitions and Implications for Underrepresented Populations  
Portia Pusey, Mark Gondree, and Zachary Peterson

## Also in This Issue

53 | IEEE Reliability Society Information

89 | IEEE Computer Society Information

95 | Advertiser Information



**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](http://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](http://www.computer.org/csdl).