Features

Mohit Tiwari and Todd Austin

8  Newcache: Secure Cache Architecture Thwarting Cache Side-Channel Attacks  
Fangfei Liu, Hao Wu, Kenneth Mai, and Ruby B. Lee

17  Detecting Hardware Covert Timing Channels  
Guru Venkataramani, Jie Chen, and Milos Doroslovacki

28  Monitoring and Attestation of Virtual Machine Security Health in Cloud Computing  
Tianwei Zhang and Ruby B. Lee

38  Fast Protection-Domain Crossing in the CHERI Capability-System Architecture  

50  A Comparative Security Analysis of Current and Emerging Technologies  
Chandra K.H. Suresh, Bodhisatwa Mazumdar, Shik Subidh Ali, and Ozgur Sinanoglu

Departments

4  From the Editor in Chief  
Security and Our Reader Survey  
Lieven Eeckhout

62  Micro Economics  
No Rosetta Stone for Market Vitality  
Shane Greenstein

Computer Society Information, p. 3  
Advertising/Product Index, p. 27

Cover artwork by Giacomo Marchesi  
www.GiacomoMarchesi.com

On the Web

www.computer.org/micro

For more information on computing topics, visit the Computer Society Digital Library at www.computer.org/csdli.


Subscribe to IEEE Micro by visiting www.computer.org/micro.

Postmaster: Send address changes and undelivered copies to IEEE, Membership Processing Dept., 445 Hoes Ln., Piscataway, NJ 08855. Periodicals postage is paid at New York, NY, and at additional mailing offices. Canadian GST #125634188. Canada Post Corp. (Canadian distribution) Publications Mail Agreement #40013855. Return undeliverable Canadian addresses to 4960-2 Walker Road, Windsor, ON N9A 6J3. Printed in USA.

Reuse rights and reprint permissions: Educational or personal use of this material is permitted without fee, provided such use: 1) is not made for profit; 2) includes this notice and a full citation to the original work on the first page of the copy; and 3) does not imply IEEE endorsement of any third-party products or services. Authors and their companies are permitted to post the accepted version of IEEE-copyrighted material on their own web servers without permission, provided that the IEEE copyright notice and a full citation to the original work appear on the first screen of the posted copy. An accepted manuscript is a version which has been revised by the author to incorporate review suggestions, but not the published version with copy-editing, proofreading, and formatting added by IEEE. For more information, please go to www.ieee.org/publications_standards/publications/rights/paperversionpolicy.html.

Permission to reprint/republish this material for commercial, advertising, or promotional purposes or for creating new collective works for resale or redistribution must be obtained from IEEE by writing to the IEEE Intellectual Property Rights Office, 445 Hoes Lane, Piscataway, NJ 08854-4141 or pubs-permissions@ieee.org. Copyright © 2016 IEEE. All rights reserved.

Abstracting and library use: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy for private use of patrons, provided the per-copy fee indicated in the code at the bottom of the first page is paid through the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

Editorials: Unless otherwise stated, bylined articles, as well as product and service descriptions, reflect the author’s or firm’s opinion. Inclusion in IEEE Micro does not necessarily constitute an endorsement by IEEE or the Computer Society. All submissions are subject to editing for style, clarity, and space. IEEE prohibits discrimination, harassment, and bullying. For more information, visit www.ieee.org/web/aboutus/whatis/policies/p9-26.html.