Virtualization and Security

Back to the Future

SAMUEL T. KING
University of Illinois

SEAN W. SMITH
Dartmouth College

In recent years, virtualization has experienced a resurgence of development that has enabled a slew of next-generation virtualization-based applications. However, we're just beginning to understand the security potential and implications resulting from the near ubiquity of today's virtualization technology. Our goal in this special issue of *IEEE Security & Privacy* is to help further our understanding of this complex, interesting, and important topic.

We received many articles—thank you to all the authors who submitted one. We're especially thankful to the diligent and thorough external reviewers for providing detailed reviews of the submitted work, which helped us identify the three articles that we chose for this special issue. These articles cover a broad range of topics, including I/O, hardware-based security, and virtual machine introspection.

Our first article comes from IBM—the company that invented the virtual machine monitor (VMM) in the '60s. In Paul Karger and David Safford's article, "I/O for Virtual Machine Monitors: Security and Performance Issues," the authors discuss the different trade-offs system designers can make when handling I/O operations in VMMs. They discuss different VMM architectures and the inherent trade-offs of I/O handling in each of these.

Ronald Perez and Reiner Sailer from IBM team up with Leendert Van Doorn of Advanced Micro Devices (formerly of IBM) to discuss the state of the art in hardware support for virtualization and for security in their article, "Virtualization and Hardware-Based Security." Among the key contributions of this article are the detailed discussions about integrating security hardware within VMMs and the security implications of these new mechanisms.

In our third article, Kara Nance and Brian Hay from the University of Alaska Fairbanks collaborate with Matt Bishop from the University of California, at Davis, to discuss virtual machine introspection—the act of understanding the semantic information of systems running within a virtual machine from outside of it—in particular, the authors' virtual machine introspection system called VIX.

These articles represent the state-of-the-art in security as it applies to virtualization. We anticipate that future research in virtualization will continue to further our understanding of the security potential and implications of virtualization technology as it continues to permeate throughout our everyday lives. □

__Samuel T. King__ is an assistant professor of computer science at the University of Illinois. His research interests include security, operating systems, and virtualization. King has a PhD in computer science and engineering from the University of Michigan. Contact him at kingst@uiuc.edu.

__Sean W. Smith__ is an associate professor of computer science at Dartmouth College. Previously, he was a research staff member at IBM Watson, working on secure coprocessor design and validation, and a staff member at Los Alamos National Laboratory, doing security reviews and designs for private and public-sector clients. Smith has a PhD in computer science from Carnegie Mellon University. Contact him at sws@cs.dartmouth.edu; www.cs.dartmouth.edu/~sws.