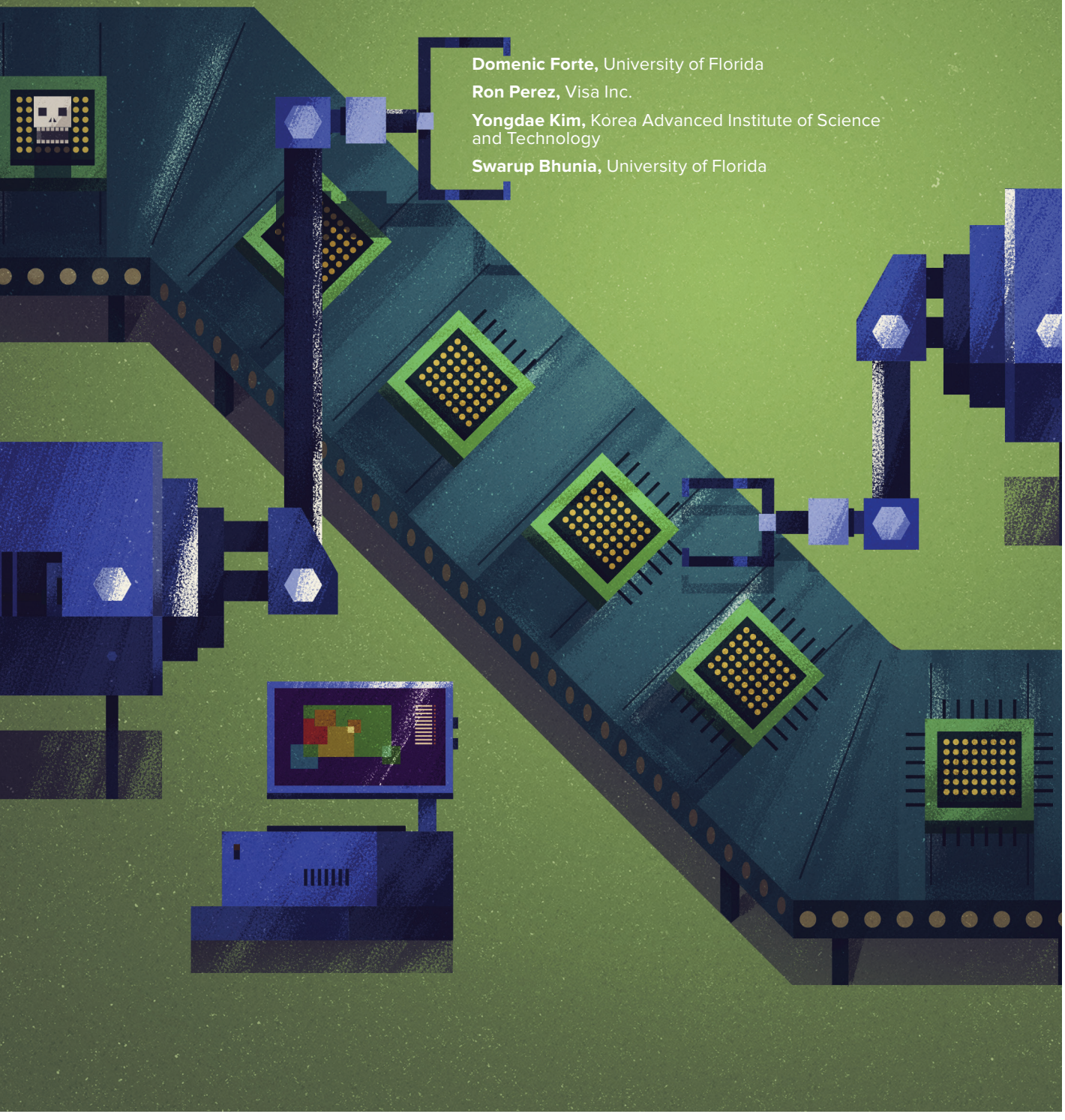
Supply-Chain Security for Cyberinfrastructure

Domenic Forte, University of Florida
Ron Perez, Visa Inc.
Yongdae Kim, Korea Advanced Institute of Science and Technology
Swarup Bhunia, University of Florida



0018-9162/16/$33.00 © 2016 IEEE

The globalization and complexity of modern supply chains introduce risks that jeopardize our cyberinfrastructure and demand bold, comprehensive solutions to ensure the integrity of hardware and software components across their life cycle of design, manufacturing, distribution, integration, and updating.

Society increasingly relies on cyberinfrastructure to manage a growing list of critical systems: the power grid, transportation networks, emergency response, potable water distribution and wastewater treatment, and so on. Electronic hardware, and the software stack that runs over it, form the foundation of the information systems comprising such cyberinfrastructure, and their susceptibility to bugs, faults, or vulnerabilities, could have disastrous economic and even life-threating consequences.

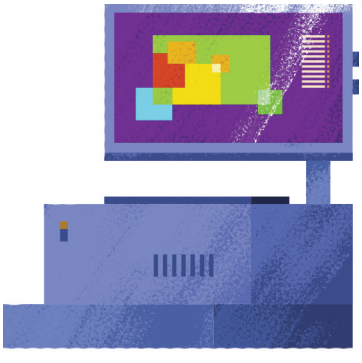
Unfortunately, the global nature of supply chains coupled with the complexity of today's hardware and software have increased the likelihood that design-related flaws could be introduced—whether maliciously or unintentionally. Modern electronic components go through a complex life cycle of design, fabrication, assembly, distribution, system integration, reuse, and resignation (end-of-life). These stages involve many independent and possibly untrustworthy parties; and evidence suggests that this trend will continue to grow, thereby bringing more and more unverified components into the global technology supply chain.

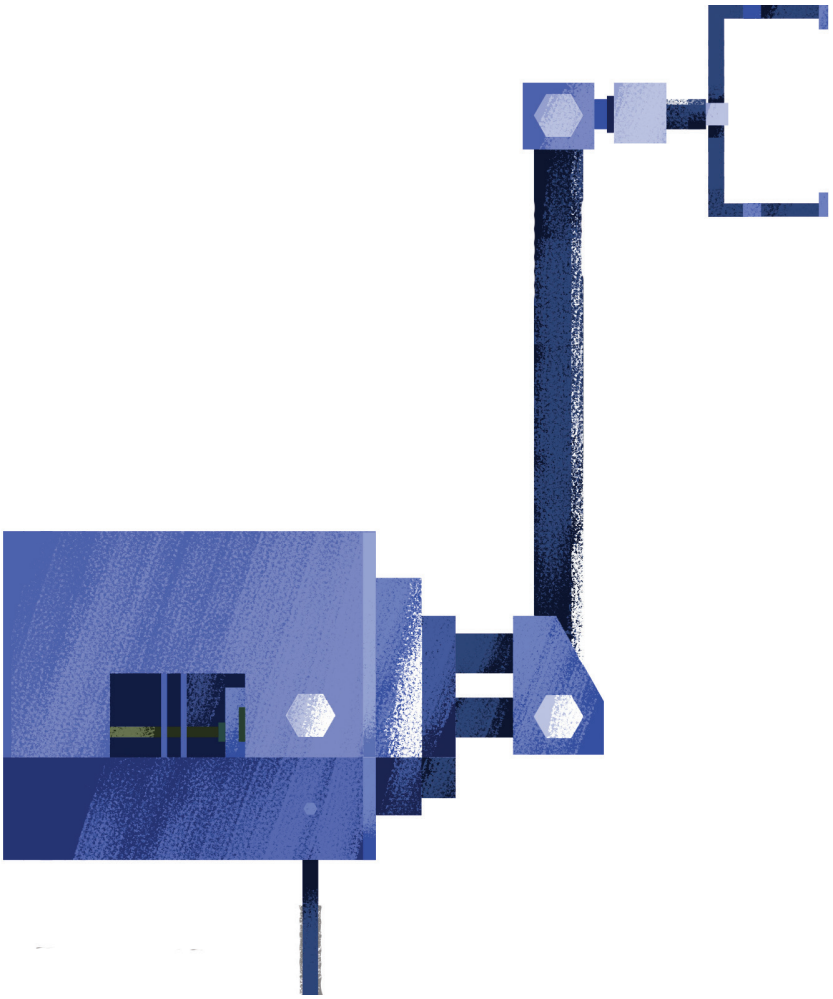
HARDWARE SUPPLY CHAIN

Similar to the well-known rule-of-10 principle in integrated circuit (IC) test—that is, the cost of detecting a fault increases by a factor of 10 at every step in the life cycle (from IC to board to system)—security flaws identified at a later stage in the system life cycle could also substantially impact the hardware intellectual property (IP) owner's profit and reputation. In the context of hardware, IP refers to a circuit design or subsystem that is abstracted into on-chip components for reusability. Although security vulnerabilities in the design are typically unintentional, they can be exploited through malicious attacks attributable to many different sources.

Although today's IC designers typically have many years of design and test experience, they are often ill equipped to deal with security issues. For example, they might be unaware of the latest types of attacks, as well as the critical assets that must be protected in an IC, and thus inadvertently leave important components unprotected. Similarly, although adding new circuitries to a chip's design might improve manufacturing yield, testability, or debugging, it could negatively impact its overall security. For instance, a secret access key was extracted from Actel's ProASIC3 field-programmable gate array (FPGA) chip—using features presumably intended to aid in debugging and maintenance functionality—that ultimately activated backdoor control on the actual silicon. Commonly accepted procedures used to optimize a design for area, power, timing, and other parameters can also conflict with security principles. Hence, existing CAD and electronic design automation (EDA) tools that do not consider security during the design optimization process might unintentionally introduce vulnerabilities during hardware optimization.

Malicious modifications (referred to as "hardware Trojans") occurring during hardware design, fabrication, and testing are also a growing concern. Owning and maintaining a state-of-the-art foundry has become so prohibitively expensive that all but a few semiconductor companies have gone "fab-less." In this fab-less model, hardware designs are shared





with third-party foundries that are typically offshore. An attacker gaining access to a design can maliciously alter it before or during fabrication. Hardware Trojans can reduce the reliability of fabricated ICs, disrupt their functionality, or leak private/sensitive assets such as secret keys. On the other hand, today's complex system-on-chip (SoC) design increasingly employs reusable hardware IP blocks developed by third-party IP vendors located across the globe. Verifying that third-party IP is Trojan-free is an extremely challenging task because there is no golden reference model to determine which operations should occur during which clock cycle, and so on. Finally, rogue employees at any design stage could potentially compromise security by creating hidden back doors that give access to on-chip assets in the field.

IP piracy, reverse engineering, and cloning—leading to counterfeit electronics—are all serious by-products of third-party involvement in IP integration, fabrication, and testing and have become more pervasive. IP piracy can occur at virtually any stage of the supply chain. Additionally, out-of-spec/defective parts marked with ink dots by original component manufacturers are supposed to be properly disposed of, and yet somehow continue to appear in the supply chain. Even at end-of-life, previously used parts reclaimed from scrapped systems are misrepresented in terms of their age or grade and then reinserted into the supply chain. As with Trojans, the issues associated with counterfeit electronic components include security and reliability risks to critical systems and loss in profit and reputation for the IP owner, as well as socioeconomic effects stemming from negative forces on the innovation and expansion of computing technologies.

SOFTWARE SUPPLY CHAIN

Many parallel issues exist in the software supply chain, resulting from outsourced development, code reuse, failure to adequately test and patch codes, and so on. In addition, as with the hardware supply chain, open source libraries and other third-party software could contain malicious or unsafe code that renders the systems that use them susceptible to data loss, data leakage, and software IP loss. The Heartbleed and GHOST bugs in OpenSSL and glibc, respectively—which affected millions of users and websites—were recent examples of such incidents. The extent to which these types of flaws were used as zero-day exploits is still unknown. In addition, rogue employees engaged in the software development and system integration processes can insert malware and Trojans to initiate intentional "time bombs," leading to private data leakage and more. Finally, anyone with access to unprotected software can potentially reverse-engineer code, insert malware, and then redistribute pirated versions. In the 2016 BSA Global Software Survey (http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf), 60 percent of consumers and workers surveyed cited security threats as the primary reason to avoid using unlicensed applications. This problem is exacerbated by the large percentage of unlicensed PC software in use globally—75 percent or greater in 37 markets according to the BSA survey.

Despite parallels with hardware supply chains, software supply chains also present unique challenges. Most notably, in recent years the

distribution model has shifted from a relatively sheltered physical model to a distributed, Internet-based digital model, creating even more opportunities for hackers to manipulate code. Rather than hacking into users' systems individually, opportunistic hackers can break into a software package's development and distribution site and wait until unsuspecting users install it. The wide reach of the Internet and social networks further facilitates the spread of malicious software. This digital distribution model has also increased the number of independent developers and the use of open source code and tools, which both present risks. Furthermore, software maintenance in the form of updates and patches present opportunities for both defenders to correct vulnerabilities and attackers to insert malware. One very sophisticated example, Stuxnet, used runtime patching of software as part of a multiphase attack, reportedly ruining almost one-fifth of Iran's nuclear centrifuges. Also, the relative ease with which bugs can be corrected might give software developers a false sense of security when time-to-market pressure leads to laxer testing, at the cost of security. Note that, in general, such update capabilities are limited in hardware, but they do exist for some systems containing FPGAs.

IN THIS ISSUE

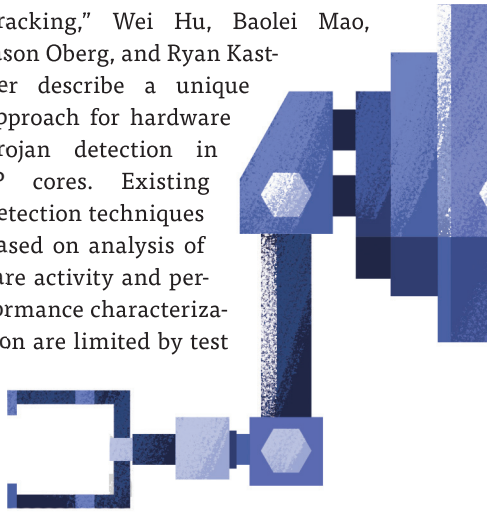
This exciting special issue is intended to raise awareness of diverse supply-chain security issues, highlight new vulnerabilities and attacks, point out the limitations of existing solutions, and present fresh approaches. We received 15 high-quality manuscripts from around the world, and chose 6 based on feedback from nearly 50 expert reviewers in academia, industry, and government. Thus, this special issue includes a stimulating mix of vision and practice, with four articles from academia and two from industry, as well as a global perspective with articles from the United States, Norway, and the United Arab Emirates.

In "Defeating Counterfeiters with Microscopic Dielets Embedded in Electronic Components," Parrish Ralston, David Fry, Scott Suko, Bryce Winters, Matthew King, and Robert Kober discuss their work on the DARPA Supply Chain Hardware Integrity for Electronics Defense (SHIELD) program. The proposed concept of operation places a "dielet" (small die) in the package of a component to be tracked, and uses an inexpensive inductive RF near-field reader (NFR) such that it can power the dielet long enough to retrieve its identifying information and passive environmental sensor readings. The dielets' design and implementation minimizes cost to electronics manufacturers and maximizes security.

In "A Platform Solution for Secure Supply-Chain and Chip Life-Cycle Management," Joseph P. Skudlarek, Tom Katsioulas, and Michael Chen propose an innovative platform to enable IC suppliers to minimize counterfeit devices (aiding and complementing approaches proposed in the first article), while also offering new value-added services during the life cycle of SoCs. A single security controller is embedded on-chip and works with appliances (including outsourced assembly and test [OSAT] companies, original equipment manufacturers [OEMs], and electronic manufacturing suppliers [EMSs]) and agents (such as the Joint Test Action Group [JTAG]) to communicate with a secure server for enrolling chips, collecting field information, chip tracking, IC/IP metering, and in-field chip provisioning. Representative protocols that ensure message integrity and authenticate the chip and the server are also discussed.

In "Supply-Chain Security of Digital Microfluidic Biochips," Sk Subidh Ali, Mohamed Ibrahim, Jeyavijayan Rajendran, Ozgur Sinanoglu, and Krishnendu Chakrabarty discuss supply-chain threats to an emerging technology—digital microfluidic biochips (DMFBs)—that primarily targets healthcare applications and toxic substance detection. The authors analyze prior techniques for protecting CMOS devices and determine that they cannot directly be used to protect DMFBs because CMOS devices are only in the electrical domain. DMFBs, on the other hand, span electrical, biochemical, and optical domains.

In "Detecting Hardware Trojans with Gate-Level Information-Flow Tracking," Wei Hu, Baolei Mao, Jason Oberg, and Ryan Kastner describe a unique approach for hardware Trojan detection in IP cores. Existing detection techniques based on analysis of rare activity and performance characterization are limited by test



time constraints, process variations, and lack of golden (that is, known, authentic) designs. The proposed approach is a formal method that leverages gate-level information-flow

ABOUT THE AUTHORS

DOMENIC FORTE is an assistant professor in the Department of Electrical and Computer Engineering at the University of Florida. His research interests include hardware security and the investigation of hardware security primitives, hardware Trojan detection and prevention, electronics supply-chain security, and anti–reverse engineering. Forte received a PhD in electrical engineering from the University of Maryland. He coauthored the book *Counterfeit Integrated Circuits: Detection and Avoidance* (Springer, 2015). He is a member of IEEE. Contact him at dforte@ece.ufl.edu.

RON PEREZ is vice president and head of security research at Visa Inc., where he leads a team focused on fundamental and applied security research for the global digital commerce ecosystem. He previously held the positions of CTO and Fellow at the Cryptography Research Division of Rambus, Senior Fellow and senior director at AMD, and senior manager and senior technical staff member at IBM's T.J. Watson Research Center. Perez received a BA in computer science from the University of Texas at Austin. He is a member of the IEEE Computer Society and a Senior Member of ACM. Contact him at ronperez@visa.com.

YONGDAE KIM is a professor in the Department of Engineering and an affiliate professor in the Graduate School of Information Security at the Korea Advanced Institute of Science and Technology. His research interests include security issues in cyber-physical systems, mobile/ad hoc/sensor/cellular networks, social networks, storage systems, and anonymous communication systems. Kim received a PhD in computer science from the University of Southern California. He is a Senior Member of IEEE and a member of ACM. Contact him at yongdaek@kaist.ac.kr.

SWARUP BHUNIA is a professor of electrical and computer engineering at the University of Florida. His research interests include hardware and system security, implantable systems, adaptive nanocomputing, and energy-efficient electronics. Bhunia received an MTech degree in computer science from the Indian Institute of Technology (IIT), Kharagpur, and a PhD in electrical engineering from Purdue University. He is a Senior Member of IEEE and a member of ACM. Contact him at swarup@ece.ufl.edu.

tracking (GLIFT) to identify Trojans that violate the confidentiality and integrity properties of these hardware components, thereby avoiding the above limitations.

In "Security Rule Checking in IC Design," Kan Xiao, Adib Nahiyan, and Mark Tehranipoor investigate the role of CAD/EDA software for secure hardware design. Hardware vulnerabilities can be introduced by CAD/EDA tools, test and debug structures, and design errors. The authors propose a new framework that enhances the chip CAD/EDA flow at all levels of abstraction (from register transfer level [RTL] to physical layout) by providing quantitative feedback on IC vulnerabilities. This strategy can address security-related design and fabrication problems to both improve security and reduce design costs. The authors also outline the challenges associated with achieving the proposed vision.

In the last article, "Vendor Malware: Detection Limits and Mitigation," Olav Lysne, Kjell J. Hole, Christian Otterstad, Øyvind Ytrehus, Raymond Aarseth, and Jørgen Tellnes discuss methods for detecting and mitigating malware activity introduced by software vendors or other insiders. Propagating through compilers, assemblers, loaders, and software updates, vendor malware can be nearly impossible to detect with known methods. To limit the negative impact of such activity, the authors explore microservice solutions to help keep the malware's attack surface small and prevent its spread to other physical machines. The approach shows great promise, and the authors describe areas for further development and exploration.

We sincerely hope that you enjoy this special issue, and we would like to thank all authors and reviewers for their tremendous efforts in producing these high-quality articles. We also take this opportunity to thank *Computer* editor in chief Sumi Helal, the editorial board, and the entire editorial staff for their encouragement and assistance in delivering this special issue.

Selected CS articles and columns are also available for free at **http://ComputingNow.computer.org**.