Guest Editors' Introduction: Security and Trust in Embedded-Systems Design

Patrick Schaumont
Virginia Tech

Anand Raghunathan
NEC Laboratories America

SECURITY AND TRUST have become important considerations in the design of virtually all modern embedded systems, such as mobile phones, multimedia players, game consoles, automotive electronics, medical electronics, sensors, and RFID tags. Multiple trends are at the basis of this evolution. First, various security-sensitive functions have moved from general-purpose computers to networked embedded devices. Such devices often contain our sensitive personal data, including information that can be used to impersonate us or exercise our purchasing power—clearly, they need to operate in a trusted and secure manner. Second, piracy and IP theft have become important risk factors in the current global media and communications landscape. Many businesses that sell multimedia services and content critically depend on the trustworthiness of the platforms that carry their products. Finally, the increase in software content and network connectivity of embedded systems makes them vulnerable to fast-spreading software-based attacks such as viruses and worms, which were hitherto primarily the concern of PCs, servers, and the Internet.

Conventional computing and communication systems address information security through functional security measures such as secure communication protocols, anti-virus software, firewalls, and network intrusion detection. These measures have traditionally been added to the target system without significant consideration regarding their embodiment in hardware or software. Simply adopting functional security measures is not enough to ensure the trustworthiness of an embedded system. Although useful, these techniques are unlikely to sufficiently address the wide range of attacks that embedded systems could face. For example, the discovery of side-channel attacks a decade ago has sparked a large body of research, highlighting a wide range of critical security issues in embedded systems that cannot be addressed through functional security measures alone. Therefore, security cannot be effectively addressed as an afterthought. Rather, it must be built into the embedded system when it is designed, and it must be considered at all stages of the design process.

The requirements of secure and trusted design are unique: Secure design emphasizes information leakage (or prevention thereof) and dependable behavior. A secure design is only as strong as the weakest link. Even strong cryptographic algorithms are of little use if the underlying processor can be tricked into releasing cryptographic keys. This leads to unique design techniques such as design and implementation of boundaries for logical and physical protection, design of protected storage and secure-computing primitives, runtime measurement and reporting of security properties, and implementation of side-channel-resistant hardware and software. Eventually, the embedded-system designer must cope with security as yet another requirement in addition to existing functional requirements, performance, power, and cost.

This special issue presents six articles that address various critical aspects of secure embedded-systems design. Three articles discuss issues related to secure hardware design; two articles discuss secure instruction-set processor design; and a final article discusses secure embedded-systems architecture and software design.

The first article, ''A Survey of Lightweight-Cryptography Implementations,'' by Thomas Eisenbarth et al., describes efficient implementation of cryptography in hardware and software. Many modern applications that use embedded cryptography have severe

0740-7475/07/$25.00 © 2007 IEEE Copublished by the IEEE CS and the IEEE CASS

restrictions on power consumption, area, and cost. The authors survey both symmetric- and asymmetric-key lightweight cryptography, and demonstrate the trade-offs that designers must make between performance, security, and cost.

''Power Analysis Attacks and Countermeasures,'' by Thomas Popp, Stefan Mangard, and Elisabeth Oswald, reviews the area of side-channel attacks and countermeasures. These attacks break cryptographic hardware implementations by using physically observable properties such as power consumption. The authors show how a decade of research in side-channel attacks has resulted in a fascinating cat-and-mouse game between attackers and countermeasure builders, with no obvious winner in sight.

The third article, ''Secured CAD Back-End Flow for Power-Analysis-Resistant Cryptoprocessors,'' by Sylvain Guilley et al., discusses a systematic design flow for creating hardware implementations that can resist side-channel attacks. With such a design flow, a designer who is not an expert in advanced secure circuit design can still develop a secure hardware implementation. The authors describe the SecLib cell library, which provides circuit- and layout-level support for side-channel-resistant implementations.

In ''Security-Performance Trade-offs in Embedded Systems Using Flexible ECC Hardware,'' Hamad Alrimeih and Daler Rakhmatov present a coprocessor design for elliptic-curve cryptography. They highlight the trade-offs between performance and security at the level of instruction-set architectures. Using a flexible microcoded architecture, they propose a coprocessor that can switch on and off several different countermeasures. These countermeasures provide resistance against timing- and power-based side-channel attacks, at the cost of performance.

The fifth article is ''Aegis: A Single-Chip Secure Processor,'' by G. Edward Suh, Charles O'Donnell, and Srinivas Devadas. The Aegis processor defines an architecture model for secure computing, in which only the processor chip is trusted. The processor then uses a specialized microarchitecture to support private and authenticated program execution, including physical unclonable functions (PUFs) and a runtime memory-integrity-checking protocol.

The last article, ''Implementing Embedded Security on Dual-Virtual-CPU Systems,'' by Peter Wilson et al., presents the software and hardware architecture of ARM's TrustZone technology. TrustZone enables secure processing in embedded systems by creating two strictly partitioned, virtual CPUs atop a single physical ARM processor core. The authors show how this approach lets a secure software world coexist with traditional embedded software.

Besides these six articles, there are four sidebars, especially written for this special issue by Atmel's Kevin Schutz, Chong Hee Kim and Jean-Jacques Quisquater of Université Catholique de Louvain, Steve Trimberger of Xilinx Research Labs, and Motorola's Tom Mihm.

One common theme that radiates from this special issue is that security introduces unique design requirements and a new set of challenges at all abstraction levels of IC design. Several important challenges remain. For example, how can we quantify the risk and security level of a given implementation such that a designer who works with quantities such as cycle counts and area can make trade-offs? Similarly, how can we provide trustworthy operation in ICs intended for systems that are unlike traditional computing systems (not always on, not always online) and which have severe implementation constraints? The solutions to these challenging research problems will lead to novel applications and a vastly improved integration of information technology in everyday life.

We hope you enjoy this special issue, and we welcome your comments and questions. We thank all the authors of the articles and sidebars in this issue for their contributions, as well as the authors of other submitted manuscripts. A special thanks goes out to the referees for their careful reading and useful comments. Finally, we thank EIC Tim Cheng for his support, as well as the editors of *IEEE Design & Test* for their help with this special issue. ■

Patrick Schaumont is an assistant professor of computer engineering at Virginia Tech. His research interests include design methods and architectures for embedded systems, with an emphasis on demonstrating new methodologies in practical applications. Schaumont has a BS in electronic engineering from Hogeschool Gent, Belgium, an MS in computer science from Rijksuniversiteit Ghent, Belgium, and a PhD in electrical engineering from the University of California, Los Angeles. He is a senior member of the IEEE.

Anand Raghunathan is a senior researcher at NEC Laboratories America in Princeton, New Jersey. His research interests include advanced SoC architectures and design methodologies, and secure embedded-systems design. Raghunathan has a BTech from the Indian Institute of Technology, Chennai, and an MA and a PhD from Princeton University, all in electrical engineering. He is a Golden Core member of the IEEE Computer Society and a senior member of the IEEE. He is on the editorial boards of *IEEE Design & Test* and *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*.

■ Direct questions and comments about this article to Patrick Schaumont, 302 Whittemore Hall (0111), Virginia Tech, Blacksburg, VA 24061, schaum@vt.edu; and Anand Raghunathan, 4 Independence Way, Suite 200, Princeton, NJ 08540; anand@nec-labs.com.