Abstract

Information security is a critical concern in a wide range of embedded computing and communications systems. Embedded systems are being used in critical applications (medical electronics, automotive systems, and avionics), where the consequence of security attacks can be severe. Several business models (e.g., distribution of multimedia content, mobile e-commerce, etc.) require an adequate level of security in the associated electronic systems in order to be viable. On the other hand, the increasing complexity and networked nature of embedded systems has led to many vulnerabilities or weaknesses that can be easily targeted for security attacks. IBM’s Global Business Security Index Report (2005) projected “the aggressive spread of viruses and worms to handheld devices, cell phones, wireless networks, car and satellite systems, and other embedded computers”, as a major emerging trend.

If our past experience is any indication, conventional approaches to security or simple add-on security schemes are insufficient. Adequate security can be achieved in a system only if security is considered throughout the design process, including the design of the SoCs (HW and embedded SW). It is therefore imperative that SoC architects, HW designers, and embedded SW developers be aware of the security challenges and techniques to address them. This tutorial will introduce security challenges in embedded systems, identify the security requirements for SoCs that they contain, and present approaches to designing secure SoCs. Secure SoC design will be described as an attempt to bridge three “design gaps” – the assurance gap, performance gap, and battery gap. Examples from various state-of-the-art commercial SoCs will be used to illustrate the presented concepts. The tutorial will be organized into the following parts:

- **Part 1.** Security concerns in embedded systems and challenges in secure SoC design
- **Part 2.** Efficient security processing architectures - Bridging the performance/battery gaps
- **Part 3.** SW attacks and SW attack-resistant architectures - Bridging the assurance gap
- **Part 4.** Physical & side-channel attacks, and attack-resistant circuit design - Bridging the assurance gap

Target Audience:

SoC Architects, HW designers, and SW developers involved in designing and implementing SoCs for security-sensitive embedded systems (including, but not limited to mobile phones, smart cards, automotive systems, avionics, medical appliances). VLSI and Embedded System researchers and students interested in the area of secure SoC and embedded system design.

Presenter Biographies

**Dr. Anand Raghunathan** (Co-ordinating presenter) is a Senior Research Staff Member at NEC Laboratories America. He leads a team that is developing security solutions for NEC’s mobile platforms, which have been incorporated into three generations of NEC’s products (mobile processor chips). He has presented a plenary talk on secure embedded system design at the IEEE International Workshop on Logic and Synthesis (IWLS 2005), and invited talks on the same topic at the ACM/IEEE Design Automation Conference (DAC 2004) and VLSI Design 2003. He has co-authored several papers on security challenges and solutions for embedded systems. His paper titled “Security in Embedded Systems: Design Challenges” was the most downloaded publication from ACM’s digital library (across all conference and journal publications) twice in 2004 and twice in 2005. He has presented full-day tutorials at ASP-DAC 1998, VLSI Design 1999, DAC 2000, and VLSI Design 2001, and a half-day tutorial at DATE 2001. Anand received a B. Tech from IIT Chennai, and M.A and Ph.D degrees from Princeton University. For further information, please visit: http://www.princeton.edu/~anandr/

**Dr. Srinivaths Ravi** is a DFT Lead at Texas Instruments. He was previously a Research Staff Member at NEC Laboratories America, where he architected hardware components of NEC’s MOSES security processor for mobile SoCs, which has been implemented in NEC’s commercial products. He presented mini-keynotes on Secure SoC design at the International Forum on Application-Specific Multiprocessor SoCs (MPSoC 2005 and 2006). He also presented invited talks on mobile security at the International Symposium on System Synthesis (ISSS 2003), and the Design, Automation, and Test in Europe Conference (DATE 2003), and an embedded keynote on tamper-resistant design at VLSI Design 2004. His paper titled “Security in Embedded Systems: Design Challenges” was the most downloaded publication from ACM’s digital library (across all conference and journal publications) twice in 2004 and twice in 2005. He has presented a full-day tutorial at ASP-DAC 2005. Srinivaths received a B. Tech from IIT Chennai, and M.A and Ph.D degrees from Princeton University. For further information, please visit: http://www.princeton.edu/~sravi/

**Dr. Stefan Mangard** is a researcher at the VLSI & Security research group at the Institute for Applied Information Processing and Communications (IAIK), Graz University of Technology. His research interests are mainly side-channel attacks and countermeasures as well as on the design and the security of cryptographic devices in general. Stefan has contributed to several national and international research projects with partners from industry. He gave several invited talks at companies and at the IPICS summer school. In 2005, he received the best paper award at the workshop on cryptographic hardware and embedded systems. Together with his colleagues Elisabeth Oswald and Thomas Popp, he is currently writing the first book on power analysis attacks and countermeasures (see http://www.dpabook.org). Stefan received the MSc degree in computer engineering from Graz University of Technology, Austria, and the PhD degree from Graz University of Technology. For further information, please visit: http://www.iaik.tugraz.at/aboutus/people/mangard/.

Further information is available at http://www.princeton.edu/~anandr/vlsi07_tutorial.html