Tutorial T4

Security and Dependability of Embedded Systems: A Computer Architects’ Perspective

Jörg Henkel, University of Karlsruhe, Karlsruhe, Germany, henkel@informatik.uni-karlsruhe.de
Vijaykrishnan Narayanan, Pennsylvania State University, USA, vijay@cse.psu.edu
Sri Parameswaran, University of New South Wales, Australia, sridevan@cse.unsw.edu.au
Roshan Ragel, University of Peradeniya, Sri Lanka, roshanr@ce.pdn.ac.lk

Abstract

Designers of embedded systems have traditionally optimized circuits for speed, size, power and time to market. Recently however, the dependability of the system is emerging as a great concern to the modern designer with the decrease in feature size and the increase in the demand for functionality. Yet another crucial concern is the security of systems used for storage of personal details and for financial transactions. A significant number of techniques that are used to overcome security and dependability are the same or have similar origins. Thus this tutorial will examine the overlapping concerns of security and dependability and the design methods used to overcome the problems and threats. This tutorial is divided into four parts: the first will examine dependability issues due to technology effects; the second will look at reliability aware designs; the third, will describe the security threats; and, the fourth part will illustrate the countermeasures to security and reliability issues.

Part I: Dependability Issues due to Technology Effects and Architectural Countermeasures

Moore’s law has been in place for more than four decades. Each new technology node provided advantages in basically all major design constraints (performance, power, area, etc.). When migrating to upcoming technology nodes it will become obvious that this win-win situation soon will be at an end. Or, in other words, in future it becomes far more difficult and expensive to migrate to new technology nodes. One major point is an inherent undependability which will become a challenging problem. Undependability addressed within this part of the tutorial is related to a) Fabrication and Design-Time Effects like “Yield and Process Variations” and “Complexity” as well as b) run-time effects as “Aging Effects”, “Thermal Effects” and “Soft Errors”. The first part of this tutorial will give the details of these effects and a prospect of how these effects might influence future architectures for embedded systems. An overview of selected state-of-the-art paradigms and approaches is given including a focus on organic computing principles as well as run-time adaptive embedded processor architectures that can deal with dependability issues.

Part II: Reliability Aware Design for Embedded Systems

Design of robust embedded systems meeting stringent quality, reliability, and availability requirements is becoming increasingly difficult in advanced technologies. The current design paradigm which assumes that no gate or interconnect will ever operate incorrectly within the lifetime of a product must change to cope with such failures. New architectural features are required for robust system design with built-in mechanisms for failure tolerance, detection and recovery during normal system operation. This part of the tutorial will focus on new design techniques required for building robust systems: concurrent error detection, recovery, and self-repair. A broad spectrum of circuit-level, logic-level, micro-architectural, hardware subsystem, and software techniques will be covered; the associated trade-offs among techniques will be presented. Implemented protection mechanisms are determined by a complex evaluation of power...
and performance requirements and constraints, in addition to the vulnerability of specific circuits or structures to failures.

Part III: Security Attacks in Embedded Systems
Security of embedded computing systems is becoming a paramount concern as these devices become more ubiquitous, contain personal information and are increasingly used for financial transactions. Security attacks targeting embedded systems illegally gain access to the information on these devices or destroy information. Security threats in embedded systems could be classified by the means used to launch attacks. Typical launch methods are: physical, logical/software-based and side-channel/lateral attacks. Physical attacks refer to unauthorized physical access to the embedded system itself and are feasible only when the attacker has direct access to the system. Logical attacks exploit weaknesses in logical systems such as software or a cryptographic protocol to gain access to unauthorized information. Logical attacks are deployed easily against systems which are able to download and execute software and have vulnerabilities in their design. Side-channel attacks are performed by observing properties of the system (such as power consumption, electromagnetic emission, etc.) while the system performs cryptographic operations. This part of the tutorial highlights the most popular attacks on embedded computing systems.

Part IV: Countermeasures Against Security Attacks
A wide range of techniques have been proposed in the past to detect and counter security attacks in embedded devices. They could broadly be categorised into software based techniques and hardware assisted techniques. Software based techniques use software tools such as code analyzers and methods such as proof-carrying-code to overcome these attacks without changing the architecture of the processor. Hardware assisted techniques use additional hardware blocks or microarchitectural support to detect and protect against these security attacks. The talk gives an overview of countermeasures against logical and side-channel attacks. The most prominent up-to-date countermeasures are discussed in detail.

Speaker Biographies

Jörg Henkel is currently with Karlsruhe University (TH), Germany, where he is directing the Chair for Embedded Systems CES. Before, he was with NEC Laboratories in Princeton, NJ. His current research is focused on design and architectures for embedded systems with focus on low power and reliability. Dr. Henkel has organized various embedded systems and low power ACM/IEEE conferences/symposia as General Chair and Program Chair and was a Guest Editor on these topics in various Journals like the IEEE Computer Magazine. He is/is has been a steering committee member of major conferences in the embedded systems field like at ICCAD and is also an editorial board member of various journals like the IEEE TVLSI. He has given full/half-day tutorials at leading conferences like DAC, ICCAD, DATE etc. Dr. Henkel is the Editor-in-Chief of the ACM Transactions on Embedded Computing Systems (ACM TECS) and holds nine US patents.

Vijaykrishnan Narayanan is currently at the Computer Science and Engineering and Electrical Engineering Departments at Penn State. He is a member of the Embedded and Mobile Computing Design Center and his research/teaching interests are in the areas of energy-aware reliable systems, embedded systems, on-chip networks, system design using emerging technologies (3D and Nano) and computer architecture. His research is supported by grants from National Science Foundation, The Technology Collaborative, and DARPA. He leads an interdisciplinary project funded by NSF that has set up a one-of-a-kind accelerated soft-error testing facility at the Penn State Nuclear reactor. Dr. Narayanan is actively involved with various technical service activities. He served as general co-chair, ISVLSI 2002; general-chair, ISVLSI 2003; vice-general chair, Nanonets 2007, and as program co-chair for GLSVLSI 2006, Nanonets 2006, and ISLPED 2007.
He serves on the steering committees of ISVLSI and GLSVLSI conferences. He is currently the editor-in-chief of the *ACM Journal on Emerging Technologies in Computing Systems*. He also serves on editorial boards of *IEEE Transactions on CAD* and the *Journal of Low Power Electronics*. He has offered full-day tutorials at major architectural conferences including ASPLOS, ISCA and PACT on reliability and low-power.

**Sri Parameswaran** is a Professor in the School of Computer Science and Engineering, University of New South Wales. His research interests are in Systems Security of SoCs and MPSoCs, System Level Synthesis, Low power systems, High Level Systems and Network on Chips. He has served on the Program Committees of numerous International Conferences, such as the Design Automation Conference (DAC), Design and Test in Europe (DATE), the International Conference on Computer Aided Design ( ICCAD), the International Conference on Hardware/Software Codesign and System Synthesis (CODES-ISSS, as TPC chair), and the International Conference on Compilers, Architectures and Synthesis for Embedded Systems (CASES). He is also an associate editor of the *ACM Transactions on Embedded Computing Systems*, and the *EURASIP Journal on Embedded Systems*.

**Roshan Ragel** is a Lecturer at the Department of Computer Engineering, University of Peradeniya since December 2002. He completed his B.Sc. Engineering (Honours I) degree in November 2001 (Peradeniya) and his PhD in June 2007 (University of New South Wales - Embedded Systems Lab). His research interests include secure embedded processors, rapid embedded hardware/software co-design, and micro-architectural support for secure and reliable computing. Mostly, he works on secure embedded systems, mainly countermeasures against code-injection attacks. Amongst his published works is the book *Microarchitectural Support for Security and Reliability: an Embedded Systems Perspective*. 

32