September 27th, 2018
“Emilio Gatti”Conference Room
DEIB, Politecnico di Milano
2.00 - 6.00 pm

Hardware security in digital systems

Abstract

The security of digital architectures, at hardware (microelectronic circuital) level, that is, of processor, memory system and communication systems, is a topic of growing importance. More or less invasive technologies capable of simulating, physically probing and even perturbing (tampering with) or changing digital microelectronic chips, steadily become more sophisticated and accurate: behavioural and structural simulation at logical, electrical, thermal, radio and optical level; profiling of the power consumed or irradiated; physical inspection at radio or optical frequency; tampering by the injection of temporary malfunctions or permanent faults; to end with reverse engineering of the circuit, at various accuracy levels, or even editing of the circuit. Thus the attack methods proliferate, and more and more security functions need to be integrated into the modern digital micro-architectures. This seminar presents the state of the art in the topic, by illustrating concepts and models, technologies and solutions, and by discussing some examples in the main technological and applicative domains: processors, memory system and “Internet of Things” (IoT). The seminar is mainly targeted at professional engineers and at engineering students in information and communication technologies (ICT), thus it benefits of a basic knowledge of digital systems, yet it does not require any specialized competence.

Program

Chairs: Luca Breveglieri (Polimi - DEIB), Giuseppe Gattavari (AEIT - AMES), Mariagiovanna Sami (Accademia delle Scienze)

- 14.00-14.30: Domenico Squillace (Technical Relations Executive IBM Italia – Presidente UNINFO)

Information security: what do we need to defend us from and how? (Application reference framework and regulations with an eye on IoT)

Introductory talk to help the audience frame the security problems and solutions in the applications and regulations (with some attention to IoT).

- 14.30-15.00: Guido Bertoni (Security Patterns)

Hardware security in the modern integrated circuits: attacks and prevention

Most integrated circuits (microchips), and particularly processors and memories, exhibit security functions. One can find such functions both in the microcontrollers for industrial process automation and in the general purpose microprocessors (network servers, desktop computers and mobile devices). System integrators and final consumers steadily raise their request for security, and even low-end and cheap devices must have some security features (primitives). Such primitives are realized as basic hardware function blocks to design a secure system. In this tutorial, it will be shown which such blocks are, and what functions they have, in relation to the attacks they are intended to prevent or mitigate. In fact, on one side the offering of security increases, but on the other side the attack methods become more refined and powerful, thanks to the variety of technologies to simulate, probe and tamper with digital systems of all kinds. Finding the right balance between security need and cost sustainability strongly depends on the application and on the data types to be processed.

- 15.00-15.30: Francesco Regazzoni (Università della Svizzera Italiana - Alari)

Security functions in the microprocessor architectures

Dedicated machine instructions and mechanisms of various kinds for security are and will be increasingly integrated into modern microprocessors. The dedicated instructions mainly help a system speed-up the computation of cryptographic algorithms and protocols, when these computations are executed in software, while the security support mechanisms are intended to create and maintain secure “enclaves”, to encrypt and thus make confidential the memory contents, and to realize the so-called “root-of-trust”. This tutorial presents the security functions offered by most successful microprocessors, and illustrates some security problems that show up in the microprocessor architectures.

- 15.30-16.00: **Break**

- 16.00-16.30: Paolo Amato (Micron)

Security problems and solutions in the traditional and emerging microelectronic memories

Memories are becoming more and more a key element of secure systems. Today, as DRAM memories scale down to smaller technology nodes, new failure mechanisms emerge that threaten the correct operation of the memory and thus may induce some practical vulnerability in the system security. A prime example of this has been the DRAM “RowHammer” issue. When looking ahead, there are even more challenging and lasting security-privacy issues that may stem from the progressive adoption of emerging nonvolatile memories (NVMs), e.g., PCM and others. In fact, on one hand, NVMs can enrich the memory hierarchy by providing low-latency, high density and data persistency, all highly desirable features. On the other hand, having a persistent memory (or part thereof) means that data are exposed to attacks for a longer time than in a conventional memory. In this tutorial we will review these threats and the approaches under investigation to eliminate or at least mitigate them.

- 16.30-17.00: Marco Macchetti (Kudelski Group)

Hardware security problems and solutions in the Internet of Things (IoT)

By 2025 the installed base of devices connected to the Internet will amount to over 75 billions. The quick development of this “Internet of Things” (IoT) poses enormous challenges regarding data security and protection. Today, integrated circuits often contain hardware security primitives, ranging from Trusted Execution Environments, to secure boot, secure storage, etc. There is a clear consensus on the need of hardware security, yet at the same time the aggressive pricing policy practiced by many companies is pushing IC (Integrated Circuit) designers and manufacturers to find new ways for ensuring security at a lower cost. In this tutorial we will address some of the most advanced hardware security features found on the market, or about to appear. We will give an overview of the Physically Unclonable Function (PUF) technology, and we will talk about the integrated Secure Elements and integrated SIMs technology, e.g., iUICCs. Such advanced technologies, coupled with protocols and communication stacks specifically thought for low power devices, e.g., NB-IoT (NarrowBand Internet of Things), will hopefully allow or facilitate security functions to be omnipresent in the IoT world, at a reasonable price level and at a sustainable complexity.

- 17.00-18.00: case studies by AEIT