Call for applications - PhD candidate

Secured access to IEEE 1687 test resources and lightweight crypto-processors in the IoT context

Location: TIMA Laboratory (AMfoRS team), Grenoble, France
Funding: 3-year PhD grant, ~1700€/month (brut) – HADES Penta (European) project
Starting date: September 2017
Key-words: hardware security, crypto-processors, authentication protocols, IEEE 1687, dynamic test access control

Context

The Internet-of-Things (IoT) is today in a phase of world-wide deployment with almost all sectors being impacted and billions of interconnected devices forecasted at short term. All those devices have not the same requirements, but an increasing part of them have strong dependability constraints. Safety and availability are some required attributes for many applications. Security (at hardware level, not just related to computer network threats) is also an increasing concern with all personal information stored and processed in those devices.

In order to ensure dependability, one of the first requirements is to be able to efficiently test the devices, after manufacturing (against manufacturing defects) but also throughout their operation lifetime (against e.g., ageing-related defects, but also for detecting malicious attacks). IEEE 1687 standard has provided a framework for hierarchical test of these devices, with inclusion of many types of instruments in order to monitor and optimize their behavior. However, the access to the monitored data must be restricted to authorized actors, so that this information cannot be used in a malicious way.

In this context the HADES project (Hierarchy-Aware and secure embedded test infrastructure for Dependability and performance Enhancement of integrated Systems), funded by the Penta European call, aims at providing ambitious solutions to the test challenges both in terms of efficiency and security throughout the system lifetime. The project purpose is to address the following markets: i) machine to machine and connected systems, ii) remote-controlled systems, iii) smart home and mobile phone, iv) safety-critical systems - typically found in the automotive and avionics domains, v) mission-critical systems -such as in space and security applications.

Historically, the first attacks demonstrated taking advantage of test mechanisms were based on a malicious control of scan-path chains and analysis of data in the chains during critical computations. The same kind of attacks can be performed using the boundary scan (or JTAG, or IEEE 1687) access if not protected. A simple protection is to disconnect the access to the test mechanisms after the end-of manufacturing test using e.g., an embedded fuse. However, such a protection is not efficient against skilled and properly equipped hackers and does not protect the circuit against potential threats due to untrusted manufacturers. In addition, such a protection is not compatible with the needs for in-situ testing during the product lifetime or with the use of JTAG for product updating. Using self-test (BIST) is one way to limit the leakage of data due to test infrastructure, but is neither affordable for all blocks in a circuit nor compatible with on-line continuous monitoring. It is therefore necessary to devise a robust authentication mechanism, in a view of collaborative Design-for-Security (DfS) and Design-for-Test (DfT). BIST remains an interesting part of the global solution, well-suited for

example to periodical test of crypto-processors. But authentication has also to be ensured to access the necessary remaining test infrastructures, with security, efficiency and flexibility constraints in mind.

Objectives

The proposed research is funded by the HADES project, and will be carried out in collaboration with many international industrial and academic actors. In the context previously mentioned, the main objectives are:

- to secure the (hierarchical) access to the embedded monitoring instruments, so that only a given set of authorized users can access each instrument. This implies a flexible authentication protocol that may be more or less complex depending on the criticality of each embedded instrument. An advanced authentication protocol aiming at robustness and light weight will be proposed, compliant with the definitive IEEE 1687 standard and supporting multiple access rights and/or policies. Security enhancement of test channels in unsecured environments must be achieved with no impact on test coverage and very small impact on test time.

- to implement a flexible set of optimized hardware security protection elements, including lightweight crypto-processors themselves protected against hardware attacks (fault attacks and side-channel attacks) and verified for self-testability in order to avoid additional backdoors. Efficient implementations will be based mainly on recent open cryptographic algorithms, but providing also support to industrial consortium requirements. Several trade-offs between hardware implementation costs, computation time for authentication and level of security will be analyzed, on the basis of several encryption algorithms. Validation will be carried out by simulation and/or emulation.

- to ensure scalability as another criterion, in order to propose a solution that can easily be adapted to the many types of IoT objects, with very different constraints and objectives. One aspect is the limited re-use of a secret access key when many similar objects are distributed, in order to reduce the risk in case a key is broken by a hacker. Also, dynamic communication between a test interface and the object will be enforced, on the basis of the MAST technology developed in the team and currently in industrialization phase.

Profile: Master degree or equivalent in the area of either Electronic Engineering or Computer Science.

Expected skills

Technical: Digital integrated electronics (digital design, VHDL, CAD tools), C/C++ and scripting. Knowledge about security and authentication is a plus.
Personal: Determination, perseverance, trustworthiness, autonomy, adaptability, initiative, good communication skills
Languages: English: at least B2 equivalent, excellent reading and writing level, good speaking level. Fluency in French is a plus but is not mandatory.

About TIMA

TIMA Laboratory is a public joint research laboratory located in Grenoble, France, and held jointly by Institut Polytechnique de Grenoble (Grenoble INP), University Grenoble-Alpes and French National Research Council (CNRS). TIMA is a multinational team of over 100 people, with members and interns from all over the world. The research topics of TIMA cover the specification, design, verification, test, CAD tools and design methods for integrated systems, from analog and digital

components on one end of the spectrum, to multiprocessor Systems-on-Chip together with their basic operating system on the other end.
This call is from the AMfoRS team, and targets people motivated by hardware security and test. More information about the team is available at http://tima.imag.fr/tima/en/AMfoRS/AMfoRSoverview.html

Advisors

Main advisors: Régis Leveugle, Professor, AMfoRS team leader and Paolo Maistri, CNRS Researcher. The work will be carried out in strong cooperation with the other members of the team contributing to the HADES project, in particular Lorena Anghel, Professor and Michele Portolan, Associate Professor.

To apply, send a mail to Regis.Leveugle@univ-grenoble-alpes.fr, with the following attachments (in English or French):
- Detailed curriculum vitae
- Application letter with clear motivations
- Academic transcripts for the last two years of study
- 2 or 3 recommendations (letters or reference persons with e-mail addresses)