


Doctoral Dissertation
Doctoral Program in Computer and Control Engineering (32nd cycle)

Cyber-security for embedded systems: methodologies, techniques and tools

Sebastiano Fabrizio Finocchiaro

* * * * * *

Supervisor
Prof. Gianpiero Cabodi

Doctoral Examination Committee:
Prof. Aurelien Francillon, Referee, EURECOM
Prof. Joao Marques Silva, Referee, University of Toulouse
Prof. Pietro Laface, Politecnico di Torino
Prof. Luciano Lavagno, Politecnico di Torino
Prof. Silvio Ranise, Fondazione Bruno Kessler

Politecnico di Torino
2020

I hereby declare that, the contents and organisation of this dissertation constitute my own original work and does not compromise in any way the rights of third parties, including those relating to the security of personal data.

. . . . . .

Sebastiano Fabrizio Finocchiaro

Turin, 2020

Summary

The last two decades have produced an enormous change in technical systems that revolutionized the way how people live their lives, organizations conduct business and even the notion of society itself. This tendency is far from ending soon, rather the future will be ubiquitously connected by computing environments that pervade our whole life. These environments (not merely hardware/software systems, but they are inherently designed for the cyberspace, and perhaps in the future will be integrated also in the human body) are now termed as Cyber-Physical Systems (CPSs). CPSs are made up by a heterogeneous set of subsystems: embedded computers, actuators, distributed sensors, physical processes are integrated together over a communication network. It has been anticipated that CPSs are likely to take over traditional computing systems thanks to adaptability, safety, robustness, efficiency, and reliability. The level of predominant presence of such systems will dictate the development of intuitive and intelligent user interfaces, some of them manually operated and others autonomously controlled. The interfaces will provide service delivering and communication effectively and efficiently, thus enabling sophisticated ambient intelligence systems. Today, CPSs are typically deployed in manufacturing, medical devices, civil infrastructure, smart grids, transportation, industrial environments and so on. As society employs more and more ubiquitous computing technologies, individuals, organisations and companies are increasingly depending on them. It is already challenging and it will be even more to orient oneself among the extensive amounts of services and information. On one hand, this trend will lead to an increase of sensitive and critical operations. On the other hand, its very ubiquity (almost imperative presence in every aspect of society) will entice people to expect a comforting nature from it, making people forget about security requirements yet especially crucial.

Nowadays, the use of CPSs in some strategic areas of our society, where human life is directly affected, is of vital importance: from medicine to traffic control to stock exchange markets and international finance. We are progressively relying on such systems, even depending in some cases, yet a question raises concerns: *Do we trust enough these systems to let them manage our lives?*. This question hides the growing need for new and more effective security approaches in embedded systems and it is the motivation of this work.

Historically, security research and development were born in the IT area. Traditional IT security methods use the notions of confidentiality, integrity and availability. They, too, can be applied to CPSs security. However, they do not cover the full spectrum of CPSs security, hence new challenges are open to be solved.

In particular, the effort has been devoted to verification techniques and methodologies. The main focus of this work is on formal verification of security properties that guarantee confidentiality, integrity and availability. Starting from state-of-the-art formal verification techniques (model checking, equivalence checking, etc.) we developed new approaches for security-critical systems. We defined a portfolio of Taint properties and provided experimental results for hardware systems that employ root of trust support and remote attestation. From the experience of applying Taint properties on real architectures we realised that this class of properties is able to capture some specific behaviors of a system, neglecting others. We therefore proposed a new class of properties called Path properties that are able to capture information flow behaviors. A portfolio of this properties has been presented and experimental results have been provided to support our claim. Eventually we thought that a combined approach would be useful, so we presented a verification approach to verify both Taint properties and Path properties in a standard model checker. Ground breaking attacks such as Spectre and Meltdown made us wonder whether it would be possible to verify hardware designs against this kind of attacks. We then proposed a novel verification approach towards out-of-order speculative execution microprocessors that are prone to side channel attacks like Spectre and Meltdown. Our verification methods rely on widely known abstraction and reduction techniques for large designs, but they have been paired with the application of a information flow verification approach.

This Ph.D. thesis has been typeset by means of the TEX-system facilities. The typesetting engine was pdfLATEX. The document class was `toptesi`, by Claudio Beccari, with option `tipotesi=scudo`. This class is available in every up-to-date and complete TEX-system installation.