PhD in Information Technology and Electrical Engineering
Università degli Studi di Napoli Federico II

PhD Student: Daniele Lombardi

Cycle: XXXVII

Training and Research Activities Report

Year: Second

Daniele Lombardi

Tutor: prof.ssa Valentina Casola Valentina Casola

Co-Tutor: -

Date: December 13, 2023

Training and Research Activities Report

PhD in Information Technology and Electrical Engineering

Cycle: XXXVII **Author: Daniele Lombardi**

1. Information:

- **PhD student:** Daniele Lombardi
- **DR number:** DR996240
- **Date of birth:** 19/07/89
- **Master Science degree:** Computer Engineering
- **University:** University of Naples “Federico II”
- **Doctoral Cycle:** XXXVII
- **Scholarship type:** *(no scholarship)*
- **Tutor:** prof.ssa Valentina Casola
- **Co-tutor: -**

2. Study and training activities:

Activity	Type[1]	Hours	Credits	Dates	Organizer	Certificate[2]
“Research and experimentation activities on: testing techniques for safety critical systems, with different Safety Integrity Level; Security challenges in iot systems”	Research	-	6	28.02.2022	-	N
“Resilience is the cybersecurity of the xxi century: a blockchain example”	Seminar	2	0.4	05.04.2023	Sapienza, University of Rome	Y
“Research and experimentation activities on: Timing Behavior Characterization of Critical Real-Time Systems; Security challenges in IoT systems”	Research	-	6	30.04.2023	-	N
9th IEEE International Workshop on Advances in Sensors and Interfaces	Seminar	18	3.6	08/09.06.2023	Department of Electric and Computer Engineering Polytechnic of Bari	Y
“Design and formal	Research	-	6.4	30.06.2023	-	N

security analysis of protocols for point-to-point and group confidentiality.”						
“Research and experimentation activities on: Security challenges in IoT systems”	Research	-	7	31.08.2023	-	N
“Ricerca e formazione nella società della transizione digitale”	Seminar	5	1	22.09.2023	CINI - DIETI	N
“Come può tornarci utile la scienza”	Seminar	2	0.4	28.09.2023	UniNa	N
“Data spaces discovery day”	Seminar	5	1	16-17.10.2023	UniNa	Y
“Research on: Provide authentication, integrity and confidentiality properties as a service in the computing continuum.”	Research	-	7	30.10.2023	-	N
“The 14th Ieee International Conference On Cloud Computing Technology And Science”	Seminar	25	5	4-6.12.2023	-	Y
“CSAW 2023 – Puf-enabled Security Challenge”	Seminar	10	2	9-10.11.2023	Ecole d'ingénieur·es en systèmes intelligents cybersécurisés, Valence (France)	N
“Risk Assessment”	Course	-	6	30.11.2023	UniNa	Y
“Research on: Provide authentication, integrity and confidentiality properties as a service in the computing continuum.”	Research	-	8	13.12.2023	-	-

1) Courses, Seminar, Doctoral School, Research, Tutorship
2) Choose: Y or N

2.1. Study and training activities - credits earned

	Courses	Seminars	Research	Tutorship	Total
Bimonth 1	6	7	8	0	21
Bimonth 2	0	0	6	0	6
Bimonth 3	0	0,4	6	0	6,4
Bimonth 4	0	3,6	6,4	0	10
Bimonth 5	0	0	7	0	7
Bimonth 6	0	2,4	7	0	9,4
Total	6	13,4	40,4	0	59,8
Expected	10	10	40	0	60

3. Research activities:

Currently, my research activity focuses on two main themes: data security of IoT-based applications; the design, development and testing of safety-critical applications, with particular reference of railway domain. In the following, they will be discussed in detail.

Data security of IoT-based applications
In the ever-expanding realm of the Internet of Things (IoT), security concerns have become paramount. The interconnected nature of IoT devices exposes them to various vulnerabilities, making them susceptible to unauthorized access, data breaches, and other malicious activities.
One of the critical security issues in IoT lies in the management of cryptographic keys, which play a pivotal role in ensuring secure communication and data integrity. Traditional key management methods face challenges such as key distribution, storage, and vulnerability to attacks. In this context, Physical Unclonable Functions (PUFs) emerge as a promising solution to enhance the security posture of IoT applications. PUFs leverage inherent physical variations in electronic components to generate unique and unpredictable identifiers. These identifiers can be utilized as a basis for cryptographic key generation. Since PUF-based keys are intrinsically tied to the specific physical characteristics of the device, they are resistant to cloning and tampering, providing a robust foundation for secure key management. Implementing PUF-based key management schemes in IoT devices offers several advantages. Firstly, it mitigates the risk of key exposure during transmission or storage, as the keys are not explicitly stored but derived dynamically from the PUF. Secondly, PUF-based keys enhance device authentication, ensuring that only legitimate devices gain access to the IoT network. Moreover, PUFs contribute to the longevity of security measures since they are resistant to traditional attacks like side-channel attacks and key extraction methods. As a result, the overall security posture of IoT applications is fortified against evolving threats.

Design, development and testing of critical real-time systems

Critical systems, i.e., those systems for which the failures or malfunctions can cause serious injuries, or even the death, to people, environmental harm or severe economic losses, are increasingly common in many application fields, e.g., heavy industries, transportations, or the medicine field, just to mention. Depending on the actual application field, the development of such systems may have to comply with strict regulations, e.g., the IEC 61511 for the process industry, or the CENELEC 50128 for the railway domain. The latter aim at guaranteeing that systems exhibit a given Safety Integrity Level (SIL), that, albeit inconsistently defined among all the functional safety standards, is usually defined in terms of probability of dangerous failure per hour. Besides, such systems have to behave correctly both from the functional and timing perspective. There may be several causes that undermine the predictability of these kinds of systems (software, such as an operating system scheduler, interrupt management; but also hardware, MMU utilization, cache memory, and so on). For this reason, I set out to devise a methodology for the temporal characterization of these kinds of systems and to develop an analytical model for describing measurements of interrupts latency.

4. Research products:

Security in IoT applications

Title: Lightweight Secure Keys Management Based on Physical Unclonable Functions
Type: Workshop article
Authors: Mario Barbareschi, Valentina Casola, Daniele Lombardi
Status: published
Abstract: The concept behind Internet of Things (IoT) involves connecting physical objects to the internet and endowing them with the ability to identify one another and exchange data. This communication paradigm arises new security challenges. Mainly, authenticity of network nodes, to let ones with malicious intent not thrive in such a network; and confidentiality, when sensitive data have to be exchanged. Most classical security techniques are not suitable to address such issues, especially in Wireless Sensor Network (WSN) where network nodes are developed using resource-constrained devices. Consequently, the scientific literature has been starting to investigate how Physically Unclonable Functions (PUFs), a unique digital identifier obtained from physical variability induced by integrated circuit manufacturing process, could be exploited to provide security mechanisms. In this paper, we present ConPHEMAP, a new lightweight PUF-based key management-scheme for point-to-point communications. The proposed scheme extends the PHEMAP protocol and inherits same properties, including flexibility since can be adopted either in the case where both nodes are provided with PUFs or when only one of them includes it. We also conducted a security analysis to verify the protocol resilience against different kinds of attacks, which proves its suitability in a heterogeneous insecure context such as WSNs.
Workshop: 9th IEEE International Workshop on Advances in Sensors and Interfaces

Title: “Lightweight group key management: the GK-PHEMAP protocol”
Type: Master Thesis (as Co-rapporteur)
Status: Released

Title: Ensuring End-to-End Security in Computing Continuum Exploiting Physical Unclonable Functions
Type: Workshop article
Authors: Mario Barbareschi, Valentina Casola, Daniele Lombardi
Status: published
Abstract: In recent years, there has been an increase in Cloud Continuum adoption to support Internet of Things applications. Inevitably, such a paradigm introduces novel security challenges, particularly concerning the security of communicating nodes to prevent malicious actors from tampering within the network, and ensuring the confidentiality of sensitive data during transmissions. Traditional security methods often fall short in addressing these issues, especially where network nodes are built upon resource-constrained devices. Consequently, the scientific community has begun exploring the potential of Physical Unclonable Functions (PUFs), which are unique digital identifiers derived

from the inherent variability in the manufacturing process of integrated circuits, as a means to enhance security mechanisms at minimal overhead cost. This paper introduces Secure-PHEMAP (S-PHEMAP), a novel and lightweight PUF-based key management scheme designed for end-to-end communications that guarantees authenticity, confidentiality and integrity for pair communications. The proposed scheme builds upon the PHEMAP protocols, inheriting its security properties. S-PHEMAP can be employed in scenarios where both communicating devices embeds a PUF or in situations where only one of them has a PUF. In addition, the paper includes a deployment strategy in a Cloud Continuum domain, by leveraging the Chef automation framework.
Workshop: SCC 2023 International Workshop on Secure Cloud Continuum @ IEEE CloudCom 2023 Conference

Title: A Lightweight PUF-based Protocol for Dynamic and Secure Group Key Management in the IoT
Type: Journal article
Authors: Mario Barbareschi, Valentina Casola, Antonio Emmanuele, Daniele Lombardi
Status: submitted
Abstract: In many Internet of Things (IoT) applications, resource-constrained devices often collaborate in groups for the acquisition, transmission, and management of sensitive information. To uphold the security of these operations, symmetric encryption algorithms are commonly employed due to their efficiency and speed. Nevertheless, establishing a key management mechanism, that accommodates the distinctive features of the IoT domain, remains an ongoing challenge. This paper introduces Group-Key PHEMAP, a novel Physically Unclonable Function (PUF)-based protocol for group key management in IoT applications. The proposed protocol relies solely on lightweight operations for group key management and supports dynamic membership without leveraging additional cryptographic keys. We present a formal demonstration for security properties and a comprehensive analysis, regarding both computational and communication costs, as well as scalability property concerning the growing number of devices within the group. Finally, we validate the suitability of our proposal by resorting to the ns-3 network simulator, and, by implementing the protocol on devices representing typical characteristics of those used in IoT applications.
Journal: IEEE Internet of Things Journal

Design and development of critical systems

Title: “Automatic Test Generation to Improve Scrum for Safety Agile Methodology”
Type: Workshop article
Authors: Mario Barbareschi, Salvatore Barone, Valentina Casola, Salvatore Della Torca, Daniele Lombardi
Status: published
Abstract: Continuous compliance and living traceability, i.e., assure the tech nical quality of the software during the incremental flow of the agile process and trace the requirements’ implementation at any time during the development cycle, are two of the most challenging aspects of adopting agile methodologies in the safety critical domain. This is even more true when either user requirements are unstable, the knowledge of the product to be delivered is not enough, or there is no clear interfaces between various hardware/software subsystems, as it may be in a research and development context. In order to reduce the overall cost of these activities, in this manuscript, we discuss benefits resulting from adopting a semi-automatic method to perform continuous compliance and living traceability. The method aims to finding inconsistency between artifacts produced at the end of each iteration by exploit automatic generation of unit tests and coverage metrics. We validated the applicability of the proposed methodology over a real case study from the railway domain, proving it can find inconsistency between several regulations-required artifacts, including the requirements specification, the architectural specification, test specifications and their implementation, and the software implementation.
Workshop: STAM EU SYMPOSIUM @ ARES 2023

Title: “Proposal of an agile product management for a Computer-Based Interlocking”
Type: Master Thesis (as Co-rapporteur)
Status: Released

Title: “Timing Behavior Characterization of Critical Real-Time Systems through Hybrid Timing Analysis”
Type: Conference article
Authors: Salvatore Barone, Valentina Casola, Salvatore Della Torca, Daniele Lombardi
Status: published
Abstract: The spread of computing-systems, especially the real-time embedded ones, is rapidly growing in the last years, since they find usage in numerous fields of application, including, but not limited to, industry process, critical infrastructures, transportation systems, as so forth. Indeed, in these fields, precise time-constraints hold; hence, tasks need to be correct from both the functional and temporal perspectives. As for the latter, timing behavior has to be characterized, that is usually done by exploiting either static or dynamic analysis techniques, which leverage estimations based on either a model or the actual system.
In this paper, we foster an automated hybrid approach that allows characterizing the timing behavior of systems while introducing any alteration, i.e., relying on instruction-level tracing rather than code instrumentation for profiling purposes. Our approach is sensitive to the execution-context, – e.g., cache misses – and it allows re-using results from the

development processes – e.g., unit tests. We considered a complex real-time application from the railway domain as a case study to evaluate our approach, empirically proving that it can provide a faithful characterization of systems in terms of worst-case execution time.

Conference: 7th International Conference on System Reliability and Safety

Title: Interrupts-latency measurement: an evaluation model
Type: Journal article
Type: M. Barbareschi, S. Barone, V. Casola, D. Lombardi
Status: Still writing
Abstract: In the last few decades, the increasing adoption of computer systems for monitoring and control applications has fostered growing attention to real-time behavior, i.e. the property that ensures predictable reaction times to react on external events. In this perspective, performance of the interrupt management mechanisms are among the most relevant aspects to be considered. Therefore, the service-latency of interrupts is one of the metrics considered while assessing the predictability of such systems. To this purpose, there are different techniques to estimate it, including the use of on-board timers, oscilloscopes and logic analyzers, or even real-time tracers. Each of these techniques, however, is affected by some degrees of inaccuracy, and choosing one over the other have pros and cons. In this paper, we review methodologies for measuring interrupt-latency from the scientific literature and, for the first time, we define an analytical model that we exploit to figure out measurement errors committed. Finally, we present a case study whose purpose is to validate the proposed model.

Title: Testing di RFIOS
Type: Software tests
Status: Released
Description: This work is part of a joint project between the Dipartimento di Ingegneria Elettrica e delle Tecnologie dell'Informazione (DIETI) and the Rete Ferroviaria Italiana - Gruppo delle Ferrovie dello Stato S.p.a (RFI). which aims to test an ERTMS/ETCS propotype system on hybrid ARM/FPGA technology. The object in question is a hard-real time operating system used in the context of railway control and signalling systems. Its purpose is to provide a set of real-time functionalities to railway logic applications. The software has been designed to be distributed on the various and different systems in the railway context.

Title: MngSCC
Type: Project deliverables
Status: Released
Description: This work is part of a joint project between the Dipartimento di Ingegneria Elettrica e delle Tecnologie dell'Informazione (DIETI) and the Rete Ferroviaria Italiana - Gruppo delle Ferrovie dello Stato S.p.a (RFI). which aims to design and develop a software system called, MngSCC, to serve as an interface between ACC/ACC-M systems and SCC systems for rail traffic control. The project consisted in the production of all artifacts required by the industry standard EN50128, namely Software Requirements Specification; Software Architecture Specification; Software Design Components Specification; Software Test Specification; source code; tests reports.

Title: Mechanisms of redundancy in 2x2oo2 systems

Type: Project deliverables
Status: Still going
Description: This work is part of a joint project between the Dipartimento di Ingegneria Elettrica e delle Tecnologie dell'Informazione (DIETI) and the Rete Ferroviaria Italiana - Gruppo delle Ferrovie dello Stato S.p.a (RFI). which aims to develop and design switch-over capabilities to ensure 2x2oo2 redundancy in railway systems using the MASK software system as middleware for interfacing between railway logic applications and generic SIL4 platforms. The project consisted in the update of all artifacts required by the industry standard EN50128, namely Software Requirements Specification; Software Architecture Specification; Software Design Components Specification; Software Test Specification; source code; tests reports.

5. Conferences and seminars attended

- *9th IEEE International Workshop on Advances in Sensors and Interfaces, Monopoli (BA) - Italy*
- *14th IEEE International Conference on Cloud Computing Technology and Science, Naples - Italy*
- *CSAW'23 – PUF-enabled Security Challenge, Valence (France)*

6. Activity abroad:

Not yet.

7. Tutorship

Not yet.