PhD in Information Technology and Electrical Engineering

Università degli Studi di Napoli Federico II

PhD Student: Domenico Argenziano

XXX Cycle

Training and Research Activities Report – Second Year

Tutor: Alessandro Cilardo **Co-tutor: Clemente Galdi**

1. Information

Domenico Argenziano - Laurea Magistrale in Ingegneria Informatica - Università degli studi di Napoli "Federico II"

XXX Cycle- ITEE – Università di Napoli Federico II

External fellowship (WISCH Project)

Tutor: Alessandro Cilardo

2. Study and training

I attended the following MSc Courses:

- Advanced Computer Architectures and GPU programming
- Network Security
- Algoritmi e Strutture Dati II

and the following ad-hoc courses:

- Introduzione al Matlab
- Ottimizzazione – Mod.A and B
- Advanced Approximation Algorithms for Hard Combinatorial Optimization Problems

Seminars attended:

- Beyond the data: how to achieve actionable insights with machine learning (10/11/2015)
- Networks-on-chip: Introduction and advanced topics (16/11/2015, 18/11/2015)
- Security Operations in una Telco, esperienze e riflessioni dal campo (04/12/2015)
- Radar Adaptivity: Antenna Based Signal Processing Technique (12/02/2016)
- Gielis Transformations in the Natural Sciences and Technology (17/02/2016)
- Perception-based Surround Sound Recording and Reproduction (22/02/2016)
- Programmable Network Conjugations (26/02/2016)
- Microcontrollori di Misura: La Piattaforma ST Microelectronics Nucleo (21/03/2016)
- Half day EMC Design and Troubleshooting Course (29/09/2016)
- Automated generation of dynamic parking maps based on crowd-sensing (10/10/2016)
- Extracting WinAPI Call Graphs for Inferring Malicious Behaviours (10/10/2016)

Student: Domenico Argenziano — domenico.argenziano@unina.it
Tutor: Alessandro Cilardo — acilardo@unina.it
Cycle XXX

	Credits year 1								Credits year 2								Credits year 3									
	Estimated	1 bimonth	2 bimonth	3 bimonth	4 bimonth	5 bimonth	6 bimonth	Summary	Estimated	1 bimonth	2 bimonth	3 bimonth	4 bimonth	5 bimonth	6 bimonth	Summary	Estimated	1 bimonth	2 bimonth	3 bimonth	4 bimonth	5 bimonth	6 bimonth	Summary	Total	Check
Modules		0	0	0	0	6	18	24		0	6	3	6	0	8	23								0	47	30-70
Seminars		0	0	0,6	0,4	0	0,2	1,2		1,5	1,1	0,6	0	0	1,2	4,4								0	5,6	10-30
Research		0	0	0	10	10	15	35		6,6	6	6	4,6	3	6,4	33								0	68	80-140
	0	0	0	0,6	10	16	33	60	0	8,1	13	9,6	11	3	16	60	0	0	0	0	0	0	0	0	120	180

Year	Lecture/Activity	Type	Credits	Certification	Notes
1	Calcolabilità e complessità	MS Module	6	x	
1	Metodi algebrici per la crittografia	MS Module	6	x	
1	Sistemi Real-time	MS Module	6	x	
1	Elaborazione dei segnali numerici	MS Module	6	x	
1	Modelli matematici e calcolo scientifico nell'ingegneria e nell'innovazion	Seminar	0,6	x	
1	Memory technologies and tracing techniques in Android	Seminar	0,4	x	
1	Play with connectome – Challenges and opportunities from in-vivo imagi	Seminar	0,2	x	
2	Advanced Computer Architectures and GPU programming	MS Module	6	x	
2	Beyond the data: how to achieve actionable insights with machine learn	Seminar	0,3	x	
2	Networks-on-chip: Introduction and advanced topics	Seminar	0,8	x	
2	Security Operations in una Telco, esperienze e riflessioni dal campo	Seminar	0,4	x	
2	Introduzione al Matlab	PhD Module	3	x	
2	Radar Adaptivity: Antenna Based Signal Processing Technique	Seminar	0,4	x	
2	Gielis Transformations in the Natural Sciences and Technology	Seminar	0,2	x	
2	Perception-based Surround Sound Recording and Reproduction	Seminar	0,2	x	
2	Programmable Network Conjugations	Seminar	0,3	x	
2	Algoritmi e Strutture Dati II	MS Module	6	x	
2	Ottimizzazione – Mod.A and B	PhD Module	4+4	x	
2	Microcontrollori di Misura: La Piattaforma ST Microelectronics Nucleo	Seminar	0,6	x	
2	Half day EMC Design and Troubleshooting Course	Seminar	0,8	x	
2	Automated generation of dynamic parking maps based on crowd-sensin	Seminar	0,2	x	
2	Extracting WinAPI Call Graphs for Inferring Malicious Behaviours	Seminar	0,2	x	

3. Research activity

a. Secure Computing and Trusted Storage

b.

My research focused on two main branches in the field of information security. One branch, supported by the WISCH fellowship, led to the study of Trusted Computing and the related hardware facilities, in particular TrustZone and SecureBoot of ARM processors, and system virtualization standards, in particular GlobalPlatform standards, meant for embedded systems.

On the other side, the research line with my tutor focused on the devising of optimized hardware/software solutions for cryptographic primitives, both standard and advanced. In particular, my studies centered on vectorial computing, especially GPU-like architectures, and

on SIMD algorithms for known cryptographic operations, especially Montgomery multiplication (for RSA) and AES symmetric cipher. A more recent development focus on the study of more advanced cryptographic techniques, namely those for Secure Function Evaluation, which relates to my previous study of homomorphic encryption. In particular, I studied Garbled Circuits and their application to universal circuits.

c.

The research work on a Trusted Storage facility started with the definition of the requirements and desired features in relation with the expected security scenario. Our storage is intended for personal devices which host applications and data by multiple stakeholders (e.g., frontend applications for subscription services and related access credentials), besides device owner's data and personal information. Applications are usually isolated from each other, though they may share some general information such as user data or device location. Operating systems, in particular mobile and embedded, can ensure a certain level of isolation but managing and enforcing access control over shared data and services is, in general, not easy. Besides, such application will make frequently use of cryptography and the management of cryptographic keys is one of the most delicate matter in cryptography, especially in our context, where the device may store key for stakeholders' services, which must not be directly accessible by the device's owner.

In recent years, *Trusted Computing* has emerged as a paradigm to address the above and other problems. In particular, *Trusted Execution Environments* have emerged as the forthcoming standard for mobile and embedded trusted devices. It consists of a secure virtualization infrastructure which features strong isolation among workloads running on separate and protected operating systems and provide a Secure Storage facility to store sensitive data such as cryptographic keys.

Based on such technology, together with my co-tutor Clemente Galdi and researcher Luigi Catuogno, we worked on designing a cryptographic filesystem featuring data encryption and policy enforcement at file-level granularity. Starting with the security threat assessment, we outlined the filesystem requirements and designed a first system architecture. Throughout this doctoral year, I worked on the improvement of the architecture and its implementation, verification and debugging. I produced a full functional prototype which has been benchmarked. Two conference papers and a deliverable have been written about such filesystem.

It must be underlined that, given the difficulty in obtaining Trusted Environment software, which is mostly licensed or just internally developed by companies and not public, we designed our prototype on top of an emulation software for Trusted Environments, Open-TEE.

So I had to firstly setup such emulation environment on a desktop machine and understand its peculiar features and, occasionally, fixing its bugs.

A parallel research study involved the underlying physical facilities which allow the bringing up of a TEE and its management. Among the most important commercial solutions for embedded systems, there is TrustZone, present on the ARM processors. They support a mechanism of Secure Boot for bringing up a trusted system with guarantee of integrity and authenticity. I build a prototype system with a minimal Linux OS which is booted up using Secure Boot technology. Such system was prototyped on the Zynq SoC FPGA development board.

For the other main research line, I worked on devising accelerated hardware/software solutions for cryptographic operations. Firstly, I focused on basic operations for most common cryptographic standards, namely Montgomey multiplication for RSA and AES cipher basic blocks. Parallelization solutions for these algorithms have been studied, in particular those targeted for vectorial or SIMD (*Single Instruction Multiple Data*) architectures. I developed a simple prototype SIMD processor on which I experimented possible hardware and algorithmic optimizations. My particular work is part of the overall effort of my research group, under the guidance of my tutor Alessandro Cilardo, at designing a highly customizable GP-GPU processor for a wide range of target platforms, from HPC to embedded systems. Along with other group member, we also discussed and devised possible optimizations and customizations on the overall architecture.

More lately I dedicated to study more advanced security protocols, namely those for *Secure Function Evaluation*, which represent an interesting hot topic, since it allow to compute an arbitrary function on private data, without disclosing information on such private inputs. A specific technique under study is that devised by Yao, the *Garbled Circuits*. A particular research line involves using a general purpose processor to be “garbled” in order to execute an arbitrary program and at the same time keeping hidden the input data and, optionally, the program itself. I am studying if such technique is integrable in the above GPU project and which hardware and software (compiler, preprocessor, libraries) are needed.

4. Products

Published conference papers:

Alessandro Cilardo, Domenico Argenziano "Securing the Cloud with Reconfigurable Computing: An FPGA Accelerator for Homomorphic Encryption” *Design Automation and Test in Europe (DATE16),* publisher: IEEE

Conference papers (pending approval):

"A Fine-grained General Purpose Secure Storage Facility for Trusted Execution Environments", CODASPY 2017 (Scottsdale, Arizona, USA)

Deliverable:

"Progettazione di un File System cifrato su dispositivi mobili con supporto hardware crittografico" Progetto di Ricerca e Sviluppo, Interventi di potenziamento di Sistema e di Filiera della R&S di cui al D.D. n. 52 del 26/06/2014

(Filiera WISCH, Work Into Shaping Campanias Home) - CUP n. B68C14000270007

5. Conference and seminars

7. Tutorship

Support to the last part of the thesis work of MSc student Stefano Marano on an FPGA accelerator for Number Theoretic DFT and its FPGA-in-the-loop testbench (10 Hours).