PhD in Information Technology and Electrical Engineering

Università degli Studi di Napoli Federico II

PhD Student: Raffaele Martino

XXXII Cycle

Training and Research Activities Report – First Year

Tutor: prof. Alessandro Cilardo

Table of Contents

1. Information

Raffaele Martino

- Master’s Degree in Computer Engineering, magna cum laude, awarded by University of Naples Federico II in 2016
- Ph.D. student of the XXXII Cycle of the ITEE Course, at the University of Naples Federico II
- No Fellowship
- Tutor: prof. Alessandro Cilardo
- Collaboration from March to June 2017 with CINI[1] within the project “KONFIDO – Secure and Trusted Paradigm for Interoperable eHealth Services” funded by the European Commission under the Horizon 2020 Research and Innovation Programme; Grant Agreement nº727528

2. Study and Training Activities

Credits Summary

	Credits year 1							
		1	2	3	4	5	6	
	Estimated	bimonth	bimonth	bimonth	bimonth	bimonth	bimonth	Summary
Modules	30	0	10.6	0	6	13	0	29.6
Seminars	5	5	0	0	0	0	0	5
Research	25	3	0.4	10	2	0	10	25.4
	60	8	11	10	8	13	10	60

Courses

- “Le imprese e la ricerca”, **improvement research skills module** held by Dr. Marco Frizzarin, February – March 2017: 4.0 ECTS acquired on 02/05/2017.
- “Interoperability, Semantic Technologies and Applications”, **ad hoc module** held by Prof. Flora Amato, March 2017: 2.0 ECTS acquired on 03/05/2017.
- “Ethical, Legal and Social Aspects of ICT and Robotics”, **ad hoc module** held by Prof. Guglielmo Tamburrini, March – April 2017: 3.0 ECTS acquired on 09/05/2017.
- “Games on Graphs”, **ad hoc module** held by Dr. Sasha Rubin, April 2017: 1.6 ECTS acquired on 11/05/2017.

[1] Consorzio Interuniversitario Nazionale per l’Informatica

- “Sistemi Real-Time”, **M.Sc. module** held by Prof. Marcello Cinque, March – June 2017: 6 ECTS acquired on 29/09/2017.
- “Fondamenti di Analisi Funzionale”, **ad hoc module** held by Prof. Renato Fiorenza, April – June 2017: 7 ECTS acquired on 10/10/2017.
- “C1 Advanced”, **improvement research skills module**[2] held by Dr. Janet Parker, September – November 2017: 6 ECTS acquired on 28/11/2017.

Seminars

- “IBM Cognitive Computing: Challenges and Opportunities in Building an Artificial Intelligence Platform for Business”, **seminar** held by Dr. Pietro Leo on 17/02/2017: 0.4 ECTS.
- “Cognitive Computing and Da Vinci robot: Research Proposals and Discussion”, **seminar** held by Prof. Paolo Maresca on 17/02/2017: 0.2 ECTS.
- “FMAI 2017 – 1st Workshop on Formal Methods in Artificial Intelligence”, **international conference** organized by Prof. Aniello Murano on 22-24/02/2017: 2.5 ECTS.
- “How to Organize and Write a Scientific Rebuttal”, **seminar** held by Prof. Pasquale Arpaia on 10/03/2017: 0.4 ECTS.
- “Fuzzy Logic, Genetic Algorithms and their Application to Next Generation Networks”, **seminar** held by Prof. Leonard Barolli on 10/03/2017 (Part A) and 14/03/2017 (Part B): 0.8 ECTS.
- “Scaling Adaptive Streaming Systems with Network Support”, **seminar** held by Dr. Ali C. Begen on 13/03/2017: 0.3 ECTS.
- “Sound and music in Human Computer Interaction”, **seminar** held by Prof. Antonio Rodà on 28/03/2017: 0.4 ECTS.

Language Skills

- Cambridge Advanced English, passed with Grade A, awarded by University of Cambridge; Date of Examination: 01/12/2017; CEFR[3] Level: C2.

3. Research Activity

Design of a Secure Architecture for Cross – Border eHealth Data Exchange

Collaboration with CINI within the Horizon 2020 project “KONFIDO – Secure and Trusted Paradigm for Interoperable eHealth Services”

One of the most important achievements of the European Union (EU) is the establishment of an open border area between its Member States (MS), known as the Schengen Area, allowing citizens to freely travel across internal borders between MSs. A key enabling infrastructure for the freedom of movement of EU citizens is the one for the interchange of medical data across MS borders. This allows a Healthcare Professional (HP) in a MS to access relevant medical data of a person he takes care of, coming from another MS. It is clear that such an interchange must face not only technical issues, namely the interoperability between the National Infrastructures (NIs) of the Member States, but also legal issues, since medical

[2] Language course provided by CLA (Centro Linguistico di Ateneo) of University of Naples Federico II to prepare for the Certification in Advanced English awarded by University of Cambridge.

[3] Common European Framework of Reference

data are highly sensitive and hence their processing and dissemination are strictly regulated by the laws of each MS.

The research and development of an infrastructure to effectively perform a cross – border healthcare – related data interchange, achieving interoperability between NIs while complying with both national and European laws, had been a long – term objective for the European Commission. The objective was met with the epSOS project, when it was demonstrated that such an infrastructure is possible by the deployment of a Large Scale Pilot (LSP). After an initial implementation containing some proprietary software, the reference implementation developed under the epSOS project was released as open source software, called OpenNCP, which is now maintained by a community, hosted by the European Commission; while the deliverables of the epSOS project have been adopted by the European Commission as eHealth Digital Service Infrastructure (DSI) Interoperability Specifications (eHDSI).

Although OpenNCP implemented a number of security measures, its main concern was the demonstration of the technical feasibility of a cross – border interchange of eHealth – related data, hence a detailed security analysis and the deployment of advanced security techniques have been left as future work. The goal of the KONFIDO project is hence to improve security in cross – border healthcare – related data interchange. It builds over the federated approach of the eHDSI, adding a holistic approach to the issue of secure communication, processing and storage of medical data.

Freedom of movement is further enhanced by the development of Internet of Things (IoT) biomedical sensors, that allow the remote control of a chronic patient. However, when such a patient is abroad, currently the European infrastructure does not support the transfer of data from the sensors to the tele – monitoring centre. The KONFIDO project explicitly considers, as one of its use cases, the cross – border tele – monitoring scenario.

In the context of the KONFIDO project, the research contribution has been twofold. On one hand, a security analysis of the cross – border eHealth – related data interchange infrastructure has been performed. The analysis started from the data flow, in order to characterize the actors involved in the communication and the potential vulnerabilities of the flow. Moreover, a threat model has been developed, analysing the weaknesses of each participant so that proper security countermeasures can be designed. The most vulnerable actor has been found to be the HP's terminal, where poor or no security measures are in place, and the user is likely to be not especially trained in computer security.

On the other hand, a proposal for the overall security architecture has been outlined. The proposed solutions are built upon the security techniques already implemented in eHDSI, enhancing security by customizing general - purpose technology to the cross – border eHealth data interchange scenario. First, the Secure Enclave technology can be used by each participant to build a secure channel along the whole end – to – end path. The Secure Enclave can be particularly effective if employed by the gateway of the NI and the HP's terminal. In addition, audit data can also be employed to identify unexpected events, and this can lead to the early detection of a running attack. This requires intelligence to correlate different log entries to the same event and to infer a running attack from a pattern of log entries. To do so, a customization of a Security Information and Event Management (SIEM) to the specific eHealth data interchange scenario has been proposed. Lastly, to cope with the problem of communication with the biomedical sensors, a proper customization of the already existing OpenNCP operation has been proposed.

Advanced Hardware Implementations of SHA-2 for Emerging Innovative Applications

Hash algorithms are a fundamental building block of a number of secure applications. Traditionally, these algorithms are the basis for message integrity, which in turn constitutes the building block for Digital Signature Algorithms (DSAs) and Hash – based Message Authentication Codes (HMACs). But there are also more innovative applications which are gaining increasingly wide popularity. A paramount example is the **blockchain** technology, which at the very essence is an efficient way to maintain a distributed database growing with time within a peer – to – peer network. This technology was originally proposed as the enabling technology for cryptocurrencies, namely for the Bitcoin cryptocurrency, but it is clear that blockchains can be used for totally different applications; actually, to find applications of blockchain is currently a flourish research and development field.

The key idea of the blockchain is to split the database into subsequent blocks, then each block is hashed; the chain is built by including the hash value of the previous block in the hash of every block. The hash value is considered valid by the network only if it complies to a validity rule, which is characteristic of each blockchain technology. Once a new valid block is produced, it is announced to the network, so that every peer has a complete view of the whole chain. This makes impractical to alter the entries of the database without being detected, because such an operation would require to produce new valid hash values for all the subsequent blocks up to the last one, and announcing the forged chain to the network before the production of a new valid block on the original chain. Unless the majority of the nodes are compromised and agree to the forged chain, the network will agree with the original chain and the forged block will be rejected.

A fundamental part in ensuring the level of security of a blockchain is the validity rule of hash values. In the Bitcoin blockchain, the hash value of a block is valid if and only if it is lower than a specified value, called target and encoded in the block header. In order to obtain such a hash value, a nonce is included in the hash input, hence finding a valid hash value of a block implies finding a value of the nonce which makes the hash function to output a valid value. Finding a valid nonce requires the inversion of the underlying hash function, which is double SHA-256[4]; since hash functions are non – invertible by construction, the only way to find a valid nonce is brute – force. The first peer which find a valid nonce for the current block and announces it to the network is rewarded by the Bitcoin protocol with a predetermined amount of newly – minted coin: for this reason, the process of producing a new block in a blockchain is referred to as **mining**.

Applications put higher and higher demands on the performance of hashing. In network applications such IPSec and SSL/TLS, the performance of the hash algorithm can become the bottleneck for the whole service. Innovative applications like Bitcoin mining are even more demanding, since every little improvement in performance can translate into a significant increase of revenues, due to the competitive nature of the mining process. These requirements make hardware solutions attractive for the research

[4] SHA-256 applied twice.

activity, due to higher performance achievable and the possibility to design power – efficient implementations. These two objectives can be simultaneously optimized; alternatively, one of them can be stressed more, paying a penalty on the other metric: the hardware design provides a wider design space in which different trade – offs can be found. Apart from the optimization potential, hardware solutions provide also more security than software implementations, since they cannot be affected by cyberattacks; on the contrary they can provide a form of physical protection. For all these reasons, some security bodies like the National Security Agency (NSA) allow only hardware implementations.

The research activity focuses on both algorithm optimizations and application – specific improvements. The application currently under study is the Bitcoin mining, hence algorithm optimizations are particularly focused on the underlying SHA-256 algorithm.

To design algorithm optimizations, the first step is to study the most effective design alternatives for the circuit implementing the hash algorithm, and to relate each design technique with its effects in terms of performance and power efficiency. To this end, a number of different designs proposed in the technical literature, hopefully the best ones, are currently under study and comparison.

The topic of Bitcoin – related improvements does not appear frequently in the technical literature. This is because Bitcoin has been developed by a community of enthusiast developers without any involvement of academic or industrial research. Nevertheless, the fact that there is room for improvement in the Bitcoin mining algorithm has been pointed out. A large share of the input of the algorithm is fixed, hence known a priori, or “slowly” variable; here the word “slowly” is referred to the hash rate. This means that some optimizations of the hashing algorithm can be performed, not valid in general but valid only for the Bitcoin mining. Namely, some values can be hard – coded into the circuit, while other values can be computed and stored to be used multiple times, until the part of the input upon which they depend will change.

Next steps

The goal of the comparison of design alternatives for SHA-256 implementation is to define an optimal design, by combining the best design techniques according to performance and/or power efficiency. It is worth noting that, due to the requirements of the applications, area occupation considerations are less relevant, hence a penalty in area occupation can be paid in order to achieve more performance (or, less likely, power efficiency), when compared with a generic hardware SHA-256 implementation.

Being impractical to work with Application – Specific Integrated Circuits (ASICs), the design space will be explored by using Field – Programmable Gate Arrays (FPGAs), but also innovative hardware design platforms composed by a System – on – Chip (SoC) provided with some Programmable Logic (PL).

The optimal design will also benefit from some study of the technological level. In fact, components can perform very differently when mapped to an FPGA rather than an ASIC, and differences can arise also between different FPGA technologies. For this reason, the different designs, especially their basic components, will be evaluated with respect to the specific FPGA to be employed, in order to find the one which fits best the given technology.

The subsequent step will be the design of the complete Bitcoin miner. Currently available Bitcoin FPGA miners employ standard design techniques for the hashing core, and even pipelining is not always used; hence the exploitation of an optimized version of the SHA-256 circuit is expected to produce a significant improvement. In addition, Bitcoin FPGA miners are usually developed as hashing accelerators with the need of a PC as controller. Conversely, the employment of a SoC board with availability of PL will allow for the implementation of a stand – alone Bitcoin miner.

Moreover, since the Bitcoin mining is basically a challenge about the inversion of the hash algorithm, the possibility of putting in place some collision attack will be studied. The SHA-2 family of algorithm has not yet been broken by collision attacks when all the rounds are executed, but there are some successful attacks to reduced – rounds SHA-256; such an attack could be put in place were it to be possible to reduce the hash computations thanks to the fixed values.

4. Products

International Conference papers

- **R. Martino**, S. D’Antonio, L. Coppolino, L. Romano, “Security in cross - border medical data interchange: a technical analysis and a discussion of possible improvements”, in *Proceedings of the 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, Turin, 2017, pp. 317-322.

5. Conferences and Seminars

SIS-SS 2017

1st IEEE International COMPSAC Workshop on Smart IoT Sensors and Social Systems for eHealth and Well-being Applications

- Venue: Politecnico di Torino, Turin, Italy.
- Date: 04/07/2017, in conjuction with COMPSAC 2017: 41st IEEE Computer Society Signature Conference on Computers, Software and Applications.
- Presented paper: “Security in cross - border medical data interchange: a technical analysis and a discussion of possible improvements”.