Curriculum Vitae

Name	Nicholas
Surname	Mainardi
Birth date	21/08/1991, Monza(MI), Italy

Education

High School	Liceo Scientifico Tecnologico P. Hensemberger, Monza. Diploma: 2010, grade 99/100
Bachelor	Computer Science Engineering at Politecnico di Milano. Starting in September 2010, degree in July 2013, grade:110L/110
Master	Computer science engineering at Politecnico di Milano, starting in September 2013, degree in April 2016. Grade: 110L/110
Erasmus+	Chalmers Tekniska Hogskola, Gothenburg, Sweden, from September 2014 to January 2015
PhD	HEAP Lab, Dipartimento Elettronica, Informatica e Bioingegneria, Politecnico di Milano. Starting November 2016 until now

Language Skills

Mothertongue	Italian
English	I daily read and write manuscripts in english. Absolutely comfortable with interactive conversation
Certifications	Toefl:105

Computer Skills

Operating Systems	Linux (daily usage), Windows
Programming Languages	C, C++, Java, PHP, HTML, Javascript, SQL, Python, R, AngularJS, Arduino, OpenCL
Editing and Office	Word,Excel,Power Point,Google doc,Latex

Professional Experiences:

Research Fellow

Where	HEAP Lab, Dipartimento di Elettronica, Informazione e Bioingegneria, Politecnico di Milano
Role	Research Fellow

When	From June 2016 to October 2016
Research Interests	Secure Multiparty Computation, Language Theoretic Security (LangSec)

Teaching Assistant Activities

Where	Politecnico di Milano
Role	Teaching assistant (40 hours)
When	a.y. 2016/17, 2017/18, 2018/19,
Course	Algoritmi e Principi dell'Informatica, Moduli 1 e 2, undergraduate level

Research Interests:

Language-Theoretic Security

This research line focuses on improving the security of a system by designing an accurate parser for the input data fed to the system, hinging upon concepts of formal language theory. In this context, I focused on X.509 digital certificates, which are widely employed to authenticate public keys in protocols for secure communication such as SSL/TLS; in particular, I provided the following contributions:

- Design of a grammar for the X.509 digital certificate format to the extent of automatically generating an accurate parser that turned out to be more accurate than existing TLS libraries [4]
- Proposal of a novel regular format for X.509 digital certificates, which allows an efficient and effective parsing [1]
- Analysis of the format of digital certificates in the OpenPGP protocol, a peer-to-peer alternative to the hierarchical approach of X.509 for public key authentication; the analysis identified several parsing hindrances and the syntactic flaws in the design of the format [2]

Homomorphic Encryption

Homomorphic encryption schemes allow to perform a computation over encrypted data, with neither involving the secret key nor decrypting the data. My research activity in this area focuses on two topics:

- Cryptanalysis of a particular kind of homomorphic encryption schemes, namely noise-free ones; specifically, I devised a plaintext-recovery attack that amplifies the effect of an existing vulnerability in the targeted schemes, subverting the confidentiality guarantees of the scheme at hand[5,8]
- Design and implementation of a protocol, based on homomorphic encryption schemes, that allows to retrieve the occurrences of a string over a set of documents outsourced on an untrusted server without revealing to the server any sensitive information about both the string and the content of the documents; the protocol exhibits a low bandwidth while retaining a reasonable computational effort on server side to execute a query [9]

Scientific Publications

Publications with authors in alphabetical order:

1. A. Barenghi, **N.Mainardi**, G. Pelosi. **A Novel Regular Format for X.509 Digital Certificates**. Published at ITNG 2017 International Conference, 10-12th April 2017, Las Vegas (US). DOI: 10.1007/978-3-319-54978-1_18 .
2. A. Barenghi, **N.Mainardi**, G. Pelosi. **A Security Audit of the OpenPGP Format**. Published at FCST 2017 International Conference, 21st-23rd June 2017, Exeter (UK). DOI: 10.1109/ISPAN-FCST-ISCC.2017.35.
3. A. Barenghi, M. Madaschi, **N.Mainardi**, G. Pelosi. **OpenCL HLS Based Design of FPGA Accelerators for Cryptographic Primitives.** Published at SHPCS 2018 International Workshop, 16th - 20th July 2018, Orléans (FR). DOI: 10.1109/HPCS.2018.00105.

4. A. Barenghi, **N. Mainardi,** G. Pelosi. **Systematic Parsing of X.509: Eradicating Security Issues with a Parse Tree.** Published in the International Journal of Computer Security (JCS), Volume 26, Issue 6. DOI: 10.3233/JCS-171110
5. A. Barenghi, **N. Mainardi**, G. Pelosi. **Comparison-Based Attack against Noise-Free Fully Homomorphic Encryption Schemes.** Published at ICICS 2018 International Conference, 29th - 31st October 2018, Lílle (FR). DOI: 10.1007/978-3-030-01950-1_11
6. G. Agosta, A. Barenghi, T. Ciesielczyk, R. Dutta, W. Fornaciari, T. Goubier, J. Hagemeyer, L. Kosmann, **N. Mainardi**, A. Oleksiak, G. Pelosi, W. Piatek, C. Pieper, M. Porrmann, D. Schlitt, M. Zanella. **The M2DC Approach towards Resource-efficient Computing.** Chapter of the book on OPPORTUNITIES AND CHALLENGES for European Projects - Volume 1 EPS Portugal. DOI: 10.5220/000886260150017

Publications with authors in order of contribution:

7. **N. Mainardi**, M. Zanella, F. Reghenzani, N. Raspa, C. Brandolese. **An Unsupervised Approach for Automotive Driver Identification.** Published as a Poster Abstract at the International Workshop INTESA 2018. DOI: 10.1145/3285017.3285023
8. **N. Mainardi**, A. Barenghi, G. Pelosi. **Plaintext recovery attacks against linearly decryptable fully homomorphic encryption schemes.** Published in the International Journal of Computers & Security, Volume 87, November 2019. DOI: 10.1016/j.cose.2019.101587
9. **N. Mainardi**, A. Barenghi, G. Pelosi. **Privacy-Preserving Substring Search Protocol with Polylogarithmic Communication Cost.** Published at ACSAC 2019 International Conference, 9th - 13th December 2019, San Juan (PR). DOI: 10.1145/3359789.3359842. ACM Reusability badge assigned for reproducibility of results and quality of the code
10. G. Agosta, C. Brandolese, W. Fornaciari, **N. Mainardi**, G. Pelosi, F. Reghenzani, M. Zanella, G. Des Courchamps, V. Ducrot, K. Juilly, S. Monot, L. Ceva. **Accelerating Automotive Analytics: The M2DC Appliance Approach.** Published at SAMOS 2019 International Conference, 7th - 11th July 2019, Samos (GR). DOI:10.1007/978-3-030-27562-4_33

Academic Activities

Master Thesis

A Predicated Grammar for X.509 Digital Certificates: Analysis of X509 Certificate Structures, used in SSL, to identify parsing issues and write a grammar, amenable for automatic parser generators, for certificates (which have been manually written so far), solving the vulnerabilities which may arise from handcrafted parsers. Design of a grammar is the core part of the thesis, which can be placed in the emerging field of LANGSEC. Results show that automatically generated parser outperforms current implementations; leveraging parsing issues identified in the implementations, I identify a powerful impersonation attack against OpenSSL and BoringSSL

Involvement in European Research Projects

Since November 2017 to July 2019 I was involved in the activities of the Politecnico di Milano (POLIMI) in the **Modular Microserver Data Centre**[1] **(M2DC)** european research project, which aims at proposing a modular heterogeneous architecture, based on microservers, for data centres to achieve high performance and energy efficiency. I contributed to the following activities in the project:

- Design and development of an R data analytics application for an automotive use case provided by Vodafone, concerning the identification of the number of drivers usually driving a vehicle from data gathered by on-vehicle devices [6, 7, 10]
- Attending several plenary meetings with all the partners in the consortium and the final review of the project as the single representative of POLIMI

[1] https://m2dc.eu/en/

- Design and development of a demo for the final review of the project about the FPGA accelerator, based on OpenCL, for symmetric cryptographic primitives [3] developed in the M2DC project by POLIMI

Supervision of Master Thesis

- Co-advisor of the master thesis entitled “ObSQRE: efficient full-text index for oblivious substring search queries with Intel SGX” by Davide Sampietro

Projects Done

- Design of an FPGA accelerator with OpenCL and Vivado HLS for the Montgomery’s algorithm to perform modular multiplications
- Kaggle competition “Taxi Trip Time Prediction”, where the time length of a taxi ride had to be predict based on the route observed so far. Technology used: R, Python.
- Development of a cross-platform mobile application for an event during Expo 2015 in Milan, using Cordova and Angular JS frameworks.
- Adding a system call to the Linux kernel to change the PID of a process
- Building a robot, conceived as a toy for kids, driven by the colors of some sheets of paper put on the floor. Technology used: Arduino platform.
- Design and development in Matlab of an algorithm, based on Wiener filtering, to restore a blurred image because of rotation of the camera
- Design of a game theory model, based on the prisoner’s dilemma, to analyze age effects on reciprocal altruism, a biologic behavior frequently observed in nature
- Development of a game called Horse Fever with GUI using Java.
- Requirement analysis, design and development of a web application using Java2EE
- Design and realization of some web sites

Personal Interests

- ➔ Passion and interest in engines, I studied the physics of engines for a thesis at high school and I built an application in flash that simulates an engine
- ➔ I had played violin for 6 years and I attended a course offered by my high-school to make electronic music, where I learnt the basic concepts of music theory
- ➔ I participated to several Capture the Flag (CTF) competitions with the Politecnico di Milano’s team

Past Experiences

- ➔ Treasurer in the international students association Board of European Students of Technology in the local group of Milan. This role allowed to learn how to write financial reports and to be in the management of the association, hence improving my skills about leadership, bargaining with companies and public speaking
- ➔ I worked in a pizzeria as a delivery boy, managing cash flows and scheduling the customers' orders
- ➔ I attended InnovactionLab 2015 course on how to run a startup; my team focused on a project I did not found interesting and stimulating, thus I decided to quit the activity