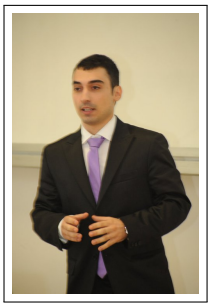
Gian Pietro Farina

Curriculum Vitae

4E Flickinger Court
14228, Buffalo, NY
(+1)7163354608
(+39)0758358190
farinagianpietro@gmail.com
Date Of Birth: 02/01/1988, Nationality: Italian



Description

I am a Computer Science PhD candidate at University at Buffalo. I am mostly interested in the intersection between Theory of Programming Languages and Information Security. I am now working in the area of verification of differentially private programs using type systems under the supervision of Prof. Marco Gaboardi.

Experience

Sep 2014 -> **PhD Candidate**, SUNY University at Buffalo, Buffalo, NY.
Research on Theory of Programming Languages, Differential Privacy, Verification of Probabilistic Programs.
Detailed Work:
- Differentially Private Bayesian Programming, (CSS 2016)
- PrivInver: A framework for differentially private Bayesian Programming, TPDP 2016 (**Poster**)
- Towards differentially private probabilistic programming, NIPS 2014, (**Poster**)
- Student at PPAML 2016 (Probabilistic Programming for Advanced Machine Learning Summer School)
- Student talk at Oregon Programming Languages Summer School, July '15: *Towards Differentially Private Bayesian Programming*
- Abstract submission at Phd Symposium 2015, Dundee University: *Towards Differentially Private Bayesian Programming*
- Teaching Assistant: *Machine Learning and Probabilistic Graphical Models*
- Attendance at Estonian Winter Schools in Computer Science March '15
- Attendance at Prosecco School in Paris, Nov. '14
- Managing of the University of Dundee Theory of Computing web site: http://tocai.computing.dundee.ac.uk/

Jan 2014-Aug 2014 **Penetration Tester**, Accenture Prague, Prague, Czech Republic.
Penetration Testing
Detailed Work:
- Web Application Penetration Testing
- Network/Infrastracture Penetration Testing
- Intense use of Burp Suite (Pro), Nessus Scanner, nmap.

Oct 2013-Dec 2013 **Internship as Information Security Analyst**, Lutech SpA, Information Security Group, Milan, Italy.
Intrusion Detection Systems:
Detailed work:
- Managing of Big Data logs with LogStash, Elasticsearch, Kibana.
- Use of SNORT to analize intrusions basing on signatures.
- Statistical Analisys of Big Data (logs) for Behavioural Anomaly Detection.
- Application of Machine Learning tools to Big Data (logs) for Behavioural Anomaly Detection.

Nov 2012–Oct 2013 **Research Assistant**, ETH, Computer Science Department, Zurich, Switzerland.
Research on Theoretical Cryptography
Detailed work:
- Application of the paradigm of Constructive Cryptography/Abstract Cryptography to Fully Black Box Reductions and Meta Reductions in the Random Oracle Model in the setting of digital signature schemes.
- Teaching Assistance:
  - Course: *Programming with MATLAB for Machine Learning*.
  - Production of the exam of Cryptography and the exercises for students and grading.
- Administration of a set of Laptops (hardware configuration, kernel updates, packages updates)
- Peer review of cryptography related research papers.

Jan **Exchange Student**, Aalto University, Computer Science Department, Helsinki, Finland.
2012–Aug Master Thesis: Distinguishing Distributions Using One-Bit Linear Trails in **PRESENT** cipher
2012 Detailed work:
- Implementation of the Block Ciphers **PRESENT** and **Maya**.
- Implementation of a test for the statistical saturation attack (SSA) on the Block Cipher **PRESENT**.
- Implementation of an algorithm to compute a lower bound on the data complexity of SSA on the Block Cipher **PRESENT**.

2004–2006 **Teaching Assistant**, Liceo Galeazzo Alessi, Perugia, Italy.
Teaching Assistant for the course on Java Programming
Detailed work:
- Introducing class mates to the concept of programming and Object Oriented programming in particular.

Education

2010-2012 **MSc**, *Computer Science (Security Curriculum)*, *110/110 cum laude*, Università Degli Studi Di Milano, Milan, Italy.
- Thesis: Distinguishing Distributions Using One-Bit Linear Trails In **PRESENT** Cipher.
- Supervisors: Prof. Kaisa Nyberg: kaisa.nyberg@aalto.fi; Prof. Stelvio Cimato: stelvio.cimato@unimi.it .

2011–2012 **Erasmus Exchange Student**, *Computer Science*, Aalto University, Helsinki, Finland.

2007-2010 **BSc**, *Computer Science*, *110/110 cum laude*, Alma Mater Studiorum, Bologna, Italy.
- Thesis: Automatic Proof of a Classic Result in Computational Cryptography.
- Supervisor: Prof. Ugo Dal Lago: dallago@cs.unibo.it .

Programming Languages and Provers Skills

- Programming Languages:
  - Very Good: C, Scheme, Java, Pascal, Latex, Assembly x86
  - Good: Haskell, Ocaml, Python, MATLAB/Octave, php, html, xml, bash scripting
  - Average: C++
- Theorem Provers
  - Good: CryptoVerif, ProVerif
  - Average: Agda, Coq

Background & Interests

- **Theoretical Computer Science**: Theory of Programming Languages, Types Systems, Randomized Algorithms, Computational Complexity Theory, Cryptography.
- **Applied Computer Science**: Programming, Networking, Information Security, Operating Systems.

Experience with *Security and Security* tools

These experiences have been earned in projects I decided to carry on individually:
- nmap, Metasploit, Kali Linux Distribution, Burp Suite.
- Traffic analysis with Wireshark.
- Intrusion detection and log analysis with SNORT (basic).
- Use of the forensic tool PTK Forensics.
- Use of standard Gnu/Linux networking tools: netcat, ping, tracerout, nslookup
- Web Application Penetration testing

Miscellaneous

Previous projects and experiences
- Experience in configuration of networks (Wifi, Ethernet).
- Experience in hardware configuration.
- Experience in compilation of the Linux kernel in order to support particular hardware settings.
- Experience with GTK libraries and Win32 API, and Swing Graphic Java library.
- Experience with automatic theorem provers: CryptoVerif, and ProVerif.
- Experience with Security in Web Services and SOAP/WS-Security.
- Experience with the symbolic model checker NuSMV.

- Development of a kernel for the virtual machine μMps (Assembly, C): https://sourceforge.net/projects/bohos/.
- Development of a simple video game (Java): http://www.the-root.org/airbum/.
- Development of a traffic load balancer for a device with two network interfaces (C/C++).
- Experience with TCP/IP, SSL/TLS, SSH.
- Experience with relational database MySQL
- Experience with Relational Algebras
- Development of a Sudoku solver (Java).
- Developing of a system which recognizes and categorizes pieces of metal basing on their form (Assembly): https://sourceforge.net/projects/optinsp8088/.
- Developing of a system for querying flights from an airport to another one with a booking system (Java, HTML, SQL).
- Improvement and Development of the Petri Net Security Checker for non-interference security notions (mostly in Java).
- Partial development of bootloader and a small kernel and a small shell (C, Assembly).

Languages

Italian **Mothertongue**
English **Proficient**
Spanish **Basic**
German **Basic**

Awards

- Winner of the *Borsa Di Studio Banca Valdichiana 2010*- for academic results
- Winner of the *Borsa Di Studio Banca Valdichiana 2012*- for academic results

Hobbies

- Reading: especially books on Philosophy of Science, Modern History and Fantasy
- Football
- Fussball
- Traveling
- Sudoku