Stefano Guarino   *Curriculum Vitae*

EDUCATION

PhD in Mathematics   "Roma Tre" University, 26 May 2014
Thesis: "Security and Privacy for Distributed and Resource-Constrained Systems"
Advisor: Prof. Roberto Di Pietro

MSc in Mathematics   "Roma Tre" University, 25 Feb 2010
Thesis: "Ciphertext-Only Reconstruction of LFSR-Based Stream Ciphers"
Advisor: Prof. Marco Pedicini
Final Mark: 110/110

BSc in Mathematics   "Roma Tre" University, 12 Jul 2007

POSTDOC RESEARCH AND PROFESSIONAL EXPERIENCE

Istituto per le Applicazioni del Calcolo "Mauro Picone" (IAC-CNR)   May 2017 - ongoing
Research Fellow   *PI: Prof. Massimo Bernaschi*

· Design and implementation of solutions for the cryptanalysis on GPU/CPU clusters

"La Sapienza" University of Rome (associate IAC-CNR)   May 2016 - April 2017
Research Fellow   *PI: Prof. Luigi Mancini, Prof. Massimo Bernaschi*

· Extraction and correlation of semantics and topological properties of the *Tor* Dark Web

Istituto per le Applicazioni del Calcolo "Mauro Picone" (IAC-CNR)   Nov 2014 - Apr 2016
Research Fellow   *PI: Prof. Massimo Bernaschi*

· Design and implementation of solutions for the cryptanalysis of Dark Web data, within the EU ISEC Project *IANCIS "Indexing of Anonymous Networks for Crime Information Search"*

"Roma Tre" University   Nov 2015 - Jan 2016
Independent Contractor   *TM: Prof. Roberto Di Pietro*

· Software design, implementation and testing, and user training, within the EU ISEC Project *EAFIT TOOLS "European Antitrust Forensic IT Tools"*

Nova Systems Roma (NSR)   Sep 2015 - Jan 2017
Independent Contractor

· Development of methodologies and techniques for the IT Forensics analysis of incidents in online payment systems, within the Project *"Protezione dei Servizi Digitali e di Pagamento Elettronico"* of the Italian *District Cyber Security*

"Roma Tre" University   Dec 2013 - Nov 2016
Independent Contractor

· Improvement of cyber-security-related knowledge, skills and policies within Montenegrin public and private organizations and companies, within the EU TEMPUS Projecy *ECESM "Enhancement of Cyber Educational System of Montenegro"*

SKILLS AND LANGUAGES

Programming Languages	C, Python, Java (basic)
Other IT	SVN, Vim, Latex
Languages	English (C1), French (A1)

PUBLICATIONS

Journal

J1 R. Di Pietro, **S. Guarino**, N. V. Verde, and J. Domingo-Ferrer, "Security in Wireless Ad-Hoc Networks - A Survey", Elsevier Computer Communications (ComCom), vol. 51, September 15, 2014, pp. 1-20, ISSN 0140-3664.

J2 **S. Guarino**, E. S. Canlar, M. Conti, R. Di Pietro, and A. Solanas, "Provable Storage Medium for Data Storage Outsourcing", IEEE Transactions on Services Computing (TSC), vol. PP, no.99, September 05, 2014, pp.1-14, ISSN 1939-1374

J3 G. Aliberti, R. Di Pietro, and **S. Guarino**, "Reliable and perfectly secret communication over the generalized Ozarow-Wyner's wire-tap channel", Elsevier Computer Networks (ComNet), vol. 109, part 1, November 09, 2016, pp.21-30, ISSN 1389-1286.

J4 M. Bernaschi, A. Celestini, **S. Guarino**, and F. Lombardi, "Exploring and Analyzing the Tor Hidden Services Graph", ACM Transactions on the Web, *in press*.

J5 G. Aliberti, R. Di Pietro, and **S. Guarino**, "Epidemic Data Survivability in Unattended Wireless Sensor Networks: New Models and Results", Elsevier Journal of Network and Computer Applications, *in press*.

Conference/Workshop

C1 R. Di Pietro, and **S. Guarino**, "Data Confidentiality and Availability via Secret Sharing and Node Mobility in UWSN", in Proceedings of the IEEE 32nd International Conference on Computer Communications (INFOCOM 2013), Turin-Italy, 2013, pp. 205-209.

C2 R. Di Pietro, and **S. Guarino**, "Confidentiality and Availability Issues in Mobile Unattended Wireless Sensor Networks", In Proceedings of the IEEE 14th International Symposium and Workshops on a World of Wireless, Mobile and Multimedia Networks (WoWMoM 2013), Madrid-Spain, 2013, pp. 1-6.

C3 M. Cianfriglia, **S. Guarino**, M. Bernaschi, F. Lombardi, and M. Pedicini, "A Novel GPU-Based Implementation of the Cube Attack", *To appear* in Proceedings of the 15th International Conference on Applied Cryptography and Network Security (ACNS 2017), Kanazawa-Japan, 2017.

C4 M. Cianfriglia, and **S. Guarino**, "Cryptanalysis on GPUs with the Cube Attack: Design, Optimization and Performances Gains", *To appear* in Proceedings of the 12th International Workshop on Security and High Performance Computing Systems (SHPCS 2017), Genova-Italy, 2017.

C5 G. Aliberti, R. Di Pietro, and **S. Guarino**, "SLAP: Secure Lightweight Authentication Protocol for Resource-Constrained Devices", *To appear* in Proceedings of the 14th International Conference on Security and Cryptography (SECRYPT 2017), Madrid-Spain, 2017.

C6 A. Celestini, and **S. Guarino**, "Design, Implementation and Test of a Flexible Tor-Oriented Web Mining Toolkit", *To appear* in Proceedings of the 7th ACM International Conference on Web Intelligence, Mining and Semantics (WIMS 2017), Amantea-Italy, 2017.

In Preparation

* R. Di Pietro, and **S. Guarino**, "Data Security in Distributed Sensor Networks - Fundamental Results".

* R. Di Pietro, and **S. Guarino**, "Privacy Preserving Computation Outsourcing for Embedded Systems".

TEACHING EXPERIENCE

Teacher/Lecturer

· John Cabot University of Rome
Calculus 2015, 2016
· Dept. of Statistical Science, "La Sapienza" University
Informatica (Computer Science, Python Programming Module) 2016
· Dept. of Mathematics, "Roma Tre" University
Error Correction for Security Applications (Mini-Cycle of 3 Lectures) 2012
· Centro Intelligence Interforze delle Forze Armate Italiane
Coding and Cryptoanalysis Systems Course 2009

Assistant/Tutor

· Dept. of Economics and Management, "LUISS Guido Carli" University
Informatica (Computer Science) 2017
· Dept. of Mathematics, "Roma Tre" University
IN110 (Introduction to Computer Science) 2013, 2014
CR1 (Introduction to Cryptography) 2009
· Dept. of Engineering, "Roma Tre" University
Analisi 1 (Calculus) 2014
Calcolo 2 (Advanced Calculus) 2013
· Dept. of Economics and Finance, "Tor Vergata" University
Matematica Generale (Calculus) 2014
· Dept. of Architecture, "Roma Tre" University
Istituzioni di Matematiche 1 (Calculus) 2014

OTHER INFORMATION

Selected Schools

6th PhD School on Security of WIreless NetworkinG (SWING 2011)
Bertinoro, Italy Fall 2011
Intensive Program on Information Communication Security (IPICS 2011)
Kerkyra (Corfu), Greece Summer 2011

Reviewer/TPC

Springer IJIS - International Journal of Information Security
Wiley ETT - Transactions on Emerging Telecommunications Technologies
Elsevier ComCom - Computer Communications
IEEE TPDS - Transactions on Parallel and Distributed Systems
IEEE TMC - Transactions on Mobile Computing
IEEE Communications Letters
ANT (2014,2016,2017) - International Conference on Ambient Systems, Networks and Technologies
SPIN (2015,2016) - International Conference on Signal Processing and Integrated Networks
SecAN (2014) - International Workshop on Security in Ad Hoc Networks
SECOTS (2014) - International Symposium on Security in Collaboration Technologies and Systems
EUSPN (2014) - International Conference on Emerging Ubiquitous Systems and Pervasive Networks
PriSec (2014) - International Symposium on Privacy and Security in Cloud and Big Data
SIoT (2014) - International Workshop on Secure Internet of Things