Curriculum Vitae

Riccardo Focardi

(October 2019)

Personal information

First Name: Riccardo
Last name: Focardi

Qualifications

2/1999 Ph.D in computer science, University of Bologna
3/1993 Laurea (Master degree) *cum laude* in computer science, University of Bologna

Current and previous positions

9/2017-present Full Professor, University Ca' Foscari, Venezia, Italy
9/2013-present Chief Scientist, Cryptosense, Paris
12/2002-8/2017 Associate Professor, University Ca' Foscari, Venezia, Italy
10/1996-12/2002 Assistant Professor, University Ca' Foscari, Venezia, Italy

Bibliometrics

Google Scholar

- Citations: 3599
- h-index: 30
- i10-index: 74

Scopus

- Citations: 1763 by 943 documents
- h-index: 20
- Documents: 113

Research activity

Riccardo Focardi has published more than 100 research papers in international journals and conferences. His research interests include:

IT Security: System and network security, cryptography, Web security, security protocols, security APIs and trusted hardware;

Formal methods: Models and languages for the description and analysis of security properties.
Model-checking, static analysis and verification tools.

Riccardo Focardi has focussed his research activity to the investigation and development of formal methods for the analysis of IT Security. He is particularly interested in developing tools based on formal techniques for the verification of real systems. *Cryptosense Analyzer* summarizes well this approach: it is a software tool that interacts with cryptographic hardware devices and builds a formal model of their behaviour. It then applies a mixture of model-checking and static analysis techniques to look for attacks that are tested on the real device under inspection, to confirm their effectiveness. The analyzer has found numerous problems on commercial devices. The tool is also able to check for cryptographic attacks enabled by the specific device under inspection. For example, in a recent paper presented at Crypto'12 (also mentioned in the *New York Times* newspaper and blog it is shown how padding errors in ciphertexts enable to break RSA encryption is a few minutes on some commercial devices.

Coordination of research projects and fundraising

- **9/2008 - 9/2010** PRIN project *SOFT: Security Oriented Formal Techniques* (National coordinator)
- **11/2017-10/2020** POR FESR project *An integrated secure IoT home automation system for smart buildings*, European fund for regional development (Coordinator of the Venice unit)
- **1/2017-12/2019** CINI FilieraSicura, *Security of national infrastructures*, funded by CISCO and Leonardo (Coordinator of the Venice unit)
- **5/2016-5/2017** MIUR-DAAD mobility project with Saarbrücken University (Coordinator of the Venice unit)
- **2/2013 - 2/2016** PRIN project *Security Horizons* (Coordinator of the Venice unit)
- **5/2013 - 5/2014** European Social Fund of Veneto Region: "Sicurezza delle informazioni nel territorio veneto", in collaboration with Yarix srl. One research contract funded for one year
- **2/2010 - 2/2011** European Social Fund of Veneto Region: "Sicurezza delle infrastrutture di nuova generazione nel territorio veneto", in collaboration with Actv Spa. One research contract funded for one year
- **12/2001 - 12/2003** PRIN project *Formal methods for security* (Coordinator of the Venice unit)

Technological transfer

Cryptosense is an INRIA spin-off co-founded by Riccardo Focardi in September 2013 that produces software for security analysis of cryptographic systems. Cryptosense products are based on formal verification techniques but are usable by non-expert to check real cryptographic systems. Products include: the *Cryptosense Analyzer* described above; a compliance tester for PKCS#11, one of the standard APIs for cryptographic devices; an App tracer that detects if applications use crypto in a secure way; a monitor that periodically performs checks on live systems to detect possible security problems. Cryptosense has won a 37k € grant by OSEO and the French Ministry of Higher Education and Research and has recently closed a 700k € seed funding round led by Elaia Partners with the participation of IT-Translation.

Test of RFID cards for public transportation From September 2011 to January 2014, Riccardo Focardi has been responsible, on behalf of the department of Computer Science of Ca' Foscari University, of testing RFID cards used by public transportation in Venice, one of the first city in Italy adopting RFID technology for ticketing.

Responsibilities in the Scientific Community

Riccardo Focardi has been a member of many program and scientific committees of international conferences, schools and journals.

Program Committee Chair

- 16th IEEE Computer Security Foundations Workshop (CSFW16) 2003
- 17th IEEE Computer Security Foundations Workshop (CSFW17) 2004;
- 7th International Workshop on Issues in the Theory of Security (WITS07) 2007;
- 4th International Conference on Principles of Security and Trust (POST) 2015, one of ETAPS conferences;
- 8th International Workshop on Analysis of Security APIs (ASA8), satellite workshop of IEEE CSF 2015.
- 1st Italian Conference on Cybersecurity (ITASEC). Venice 17-20 January 2017

General Chair

- IEEE Computer Security Foundations Workshop (CSFW) 2006;
- IEEE Computer Security Foundations Symposium (CSF) 2007;
- 1st Italian Conference on Cybersecurity (ITASEC). Venice 17-20 January 2017

Program committees

- IEEE Symposium of Security & Privacy 2005;
- IEEE Computer Security Foundations Symposium (CSFW/CSF), 2001, 2002, 2006, 2008, 2012, 2013, 2014, 2019;
- IEEE International Conference on Software Engineering and Formal Methods (SEFM) 2003 and 2004;
- European Symposium on Research in Computer Security (ESORICS) 2012, 2013, 2016, 2017;
- ACM Conference on Computer and Communications Security (ACM CCS) 2012;
- International Conference on Information Systems and Industrial Management (CISIM) 2012 and 2013;
- International Conference on Principles of Security and Trust (POST) 2014, 2016, 2018.

Steering committees

- IEEE Computer Security Foundations Symposium (CSFW/CSF), until February 2019
- Italian Conference on Cybersecurity (ITASEC).

Schools and seminars

- Scientific director of the second and third International Schools on Foundations of Security Analysis and Design (FOSAD 2001 and 2002). Bertinoro, Italy.
- Organizer of Dagstuhl Seminar 12482 - Analysis of Security APIs (November 2012)

Editorial boards

- Member of the editorial board of the Journal of Computer Security (IOS Press), since 2005.

Activity as reviewer and supervisor

Riccardo Focardi has served as reviewer for both national and European projects and for various international journals, among which:

- ACM Transactions on Computer Systems
- ACM Computing Surveys
- IEEE journal on selected areas in communications
- IEEE Transactions on Software Engineering
- Information & Computation
- Journal of the ACM
- Journal of Computer Security
- Theoretical Computer Science

He has been PhD supervisor of

- Dr. Matteo Maffei
- Dr. Matteo Centenaro
- Dr. Marco Squarcina
- Mauro Tempesta and Francesco Palmarini (PhD candidates)
- Matúš Nemec (3rd year PhD student, co-supervision with Vashek Matyas, Masaryk University)
- Vladimír Sedláček (2nd year PhD student, co-supervision with Vashek Matyas, Masaryk University)

He has been thesis reviewer and member of the PhD defense committees of

- Dr. Buchholtz, Mikael (DTU, Technical University of Denmark)
- Dr. Andrea Turrini (Università di Verona)
- Dr. Gavin Keighren (University of Edinburgh)
- Dr. Hossein Fereidooni (Università di Padova)

Direction of working groups

Chair of IFIP Working Group 1.7 "Theoretical Foundations of Security Analysis and Design", since 2016.

Participation in projects and working groups

Apart from the coordinated projects (listed above) Riccardo Focardi has participated into numerous research projects, among which:

- MyThS: Models and Types for Security in Mobile Distributed Systems. FET-Global Computing, IST-2001-32617, 2002-2004 (key personnel);
- TESLA: Techniques for Enforcing Security in Languages and Applications (Region of Sardinia, grant L.R.7/2007-CRP2_120);
- National project AIDA - Abstract Interpretation: Design and Applications, 2005-2006;
- National project - Interpretazione astratta, sistemi di tipo e analisi Control-Flow. National coordinator Prof. Giorgio Levi, 2000;
- National project - Certificazione automatica di programmi mediante interpretazione astratta. National coordinator Prof. Roberto Giacobazzi, 1999-2000;

- National project Tecniche formali per la specifica, l'analisi, la verifica, la sintesi e la trasformazione di sistemi software. National coordinator Prof. Giorgio Levi;
- National project Modelli della Computazione e dei Linguaggi di Programmazione. National coordinator Prof. Andrea Maggiolo-Schettini;

Institutional responsibilities

- **10/2012 - 9/2019**: Coordinator of the PhD program in Computer Science of Ca' Foscari University;
- **8/2019 - now**: Deputy director of the Department of Environmental Sciences, Informatics and Statistics (DAIS) of Ca' Foscari University.

Teaching activity

His teaching activity is summarized below:

- **9/2016-now** PhD course "Advances in Autonomous, Distributed and Pervasive Systems", University Ca' Foscari, Venice.
- **September 2010** PhD course "Analysis of Security APIs" at the *10th International School on Foundations of Security Analysis and Design* (FOSAD 2010). Bertinoro University Residential Center, Italy.
- **September 2004** PhD course "Static Analysis of Authentication" at the *4th International School on Foundations of Security Analysis and Design* (FOSAD 2004). Bertinoro University Residential Center, Italy.
- **September 2001** PhD course "Non-Interference for security protocols" at the *Second International School On Foundations Of Security Analysis And Design* (FOSAD 2001), 17-29 September 2001, Bertinoro, Italy
- **September 2000** PhD course "Classification of Security Properties" at the *First International School On Foundations Of Security Analysis And Design* (FOSAD 2000), 18-30 September 2000, Bertinoro, Italy
- **9/1999-now** Security of Computer Systems, Master degree in computer science at Ca' Foscari University, Venice.
- **9/2001-now** Operating Systems, in Italian, undergraduate degree in computer science at Ca' Foscari University, Venice.
- **9/1999-9/2002** Software Engineering Lab, in Italian for undergraduate degree in computer science at Ca' Foscari University, Venice.
- **9/1997-9/1999** Teaching assistant for Computer Architecture, undergraduate degree in computer science at Ca' Foscari University, Venice.
- **9/1996-9/1997** Teaching assistant for Computer Networks, undergraduate degree in computer science at Ca' Foscari University, Venice.

Venice 17/10/2019 Signature