Federico Maggi, Ph.D

Cybersecurity Researcher

@ fede@maggi.cc Northern Italy https://maggi.cc https://twitter.com/@phretor

After more than 15 years, I concluded that I found my place in the cybersecurity field because it **challenges me** to solve new exciting problems every day. I especially enjoy creating tools to monitor, extract data, analyze, and explain unknown phenomena in any ICT system, at any scale.

Research Summary and Approach

I did **research** on web applications, network protocols and devices, embedded systems, radio-frequency control systems, industrial robots, cars, and mobile devices. I always strive to follow **data-driven** approaches, which I've successfully applied to analyze **botnet** traffic, mobile **ransomware** detection, banking **fraud** detection, malware **behavior** mining, large-scale **measurements**, and **anomaly** detection.

My work has been recognized by several **research groups**, with which I collaborated and keep good contacts, and some has been featured on **mainstream outlets** such as Wired, Reuters, Forbes, Hackread, ZDNet, and MIT Technology Review.

Professional Culture

During the past 17 years I have had both industrial and academic work experience, as an employee, professor, and consultant. As such, I have experience dealing with **various ecosystems**, from large corporate environments, to academic research laboratories, and small companies.

I have experience from **development** to pure research, including both technical and **dissemination** tasks, and assessing the quality of technical documents and other scientific artifacts. I've done vulnerability **assessment** and penetration-testing as a consultant, and I was hired multiple times as a subject-matter expert for courts in Italy.

Teamwork and Management Experience

In addition to team work as part of small groups of researchers in large corporate organizations, I have been **teaching** graduate-level courses in public schools (Politecnico di Milano is the leading engineering University in Italy), I **co-directed** a young security group, and **managed** hundreds of graduate students, including Ph.D students.

I coordinated the organization of computer-security challenges and international **competitions** (CTFs). During my research projects, I am keen to involve **people** actively and work closely with them. During my academic career, this resulted in more than 35 theses and hundreds of students that I supervised since 2009.

Toolbox & Technical Skills

R&D activities demand high **flexibility**, and I'm always keen to apply new ideas, tools, and technologies.

- **Data analysis and ML:** Pandas, NumPy, SciPy, Scikit-Learn, R.
- **Storage:** MongoDB, Elastic Search, Kibana, Splunk, Hadoop.
- **Development:** Python, Bash, C/C++, Arduino, x86, LaTeX.
- **Reverse engineering:** Apktool, GDB, IDA Pro, Smali, lots of scripting.
- **Web:** Flux, React, FastAPI, Flask, Django, Bootstrap.
- **Systems:** OS X, Linux, FreeBSD, Windows, Docker, AWS.
- **Hardware:** Universal Radio Hacker, GNU Radio, RFCat, KiCad.

Record of Employment

Senior Threat Researcher
Trend Micro, Inc.
07/2016–Present Italy

Adjunct Professor, Cybersecurity
Politecnico di Milano (POLIMI)
2016–2017 Italy

Visiting Professor
UC Santa Barbara (UCSB)
10/2015–03/2016 United States

Fixed-term Assistant Professor
Politecnico di Milano (POLIMI)
2014–2016 Italy

Post-doctorate Researcher
Politecnico di Milano (POLIMI)
2010–2014 Italy

Cybersecurity Consultant
Secure Network S.r.l.
2005–2016 Italy

ICT Consultant
B.M.S. S.r.l.
2002–2006 Italy

Formal Education

BSc in Psychological Science
Università degli Studi di Padova (UNIPD)
10/2020–Ongoing Italy

Visiting Research Scholar
UC Santa Barbara (UCSB)
2008–2009 United States

PhD in Computer Enginering
Politecnico di Milano (POLIMI)
2007–2010 Italy

MSc in Computer Enginering
Politecnico di Milano (POLIMI)
2001–2006 Italy

Highlighted Projects & Publications

Securing Industrial Robots

2017–2020

Since 2017 I've been working in close collaboration with Politecnico di Milano on analyzing the attack surface of modern industrial robots, and creating tools to automatically analyze the programming logic for vulnerabilities.

Publication: Marcello Pogliani et al. (Oct. 2020). "Detecting Insecure Code Patterns in Industrial Robot Programs". In: *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security (ASIA CCS '20)*. Taipei, TW

Large Scale Analysis of Defaced Web Pages

2017–2018

We automatically tracked modus operandi and motivation behind web defacement over the past 20 years, from script kiddies to modern actors taking strong positions on real-world conflicts. We open-sourced the tool-chain that we use to explore million of web-deface pages.

Publication: Federico Maggi et al. (June 4, 2018). "Investigating Web Defacement Campaigns at Large". In: *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*. AsiaCCS '18. Incheon, Republic of Korea: ACM, pp. 443–456. ISBN: 978-1-4503-5576-6. DOI: 10.1145/3196494.3196542

Automatic Signature Generation for WebInject-based Bankers

2017

We implemented a differential memory analysis tool to extract and generate a model of a banking trojan behavior, and used it to build detection signatures.

Publication: Andrea Continella et al. (May 2, 2017). "Prometheus: Analyzing WebInject-based information stealers". In: *Journal of Computer Security* Preprint, pp. 1–21

A Targeted Espionage Toolkit

2016

Based on a scanned copy of a court order leaked in Italy, I created Yara hunting rules. Together with my colleagues, we've drawn a big picture of the whole scheme and started to find confirmatory evidence.

Publication: https://github.com/eyepyramid/eyepyramid/

Android Malware Tracking and Intelligence

2016

A tracker similar to ZeusTracker, but for mobile bankers, based on static and dynamic analysis to extract relevant CC endpoints and monitor them over time. We discovered a malware campaign spreading against Chinese and Korean bank customers.

Publication: Alberto Coletta, Victor Van der Veen, and Federico Maggi (Feb. 2016). "DroydSeuss: A Mobile Banking Trojan Tracker - Short Paper". In: *Financial Cryptography and Data Security*. Lecture Notes in Computer Science (LNCS). Springer Berlin Heidelberg

Review Service

- 2020: Black Hat Europe, APWG eCrime
- 2019: EuroSec, DIMVA, APWG eCrime
- 2018: AsiaCCS, ACSAC
- 2017: ACSAC, DIMVA, AsiaCCS, AppSec EU, APWG eCrime, IMPS
- 2016: ACSAC, DIMVA
- 2015: DIMVA, TRUST, MALWARE, WISTP, EUC, AppSecEU, PPREW, ESSoS.
- 2014: PPREW, MCSoC, TRUST, DPMPC, WISTP, IJCNN.
- 2013: CyCon, ICISS,
- 2011: EC2ND, BADGERS
- 2010: COMPENG
- 2008: DIMVA

Publications (since 2007)

- 49 peer-reviewed conference papers
- 10 peer-reviewed journal papers
- 17 technical reports
- 36 public conference talks

Awards

- Dimitri N. Chorafas PhD Thesis Award (USD 4,000), 2010
- Best M.Sc. Thesis Nominee at Premio tesi ClusIT, 2007

Volunteering

- Blood donor.
- LeadTheFuture.tech mentor.
- Local community activities.

Languages

Italian ●●●●●

English ●●●●○

More Information

Open-source Contributions
https://github.com/phretor

Full CV
https://maggi.cc/cv

Personal Blog
https://maggi.cc/diary

Previous Work

- Full list of publications: `https://maggi.cc/publication`
- Full list of talks: `https://maggi.cc/talk`
- Vulnerability advisories: `https://maggi.cc/advisories`