Andrea Continella

Affiliation Postdoctoral Researcher, University of California Santa Barbara

Contact Information

University of California, Santa Barbara
Department of Computer Science
2104 Harold Frank Hall
Santa Barbara, CA 93106-5110
United States of America

acontinella@iseclab.org
https://conand.me
@_conand
conand

Biography

I am a Postdoctoral Researcher in the Computer Science Department at UC Santa Barbara working at the SecLab. I obtained a PhD cum laude in Computer Science and Engineering at Politecnico di Milano in Italy, where I worked at the NECST Laboratory. During my PhD, I took part in two research exchanges, working as a visiting researcher at UCSB and at the School of IT of the University of Sydney. I also love Capture The Flag (CTF) competitions, and I am a member of the mhackeroni and Shellphish hacking teams.

Research Interests

My research activity focuses on different aspects of system security, such as malware analysis, mobile security, vulnerability discovery, and large-scale measurement of security issues. I have worked on analysis and defense mechanisms against advanced threats including for example the current generation of trojan horses, or the infamous ransomware families. I also developed Agrigento, a tool for detecting obfuscated privacy leaks in Android apps, and contributed to Arancino and crAVe, respectively for analyzing evasive malware and testing Antivirus engines.

Positions & Education

Postdoctoral Researcher *July 2018-Current*
University of California, Santa Barbara, USA

Doctor in Philosophy (Ph.D.), Computer Science and Engineering *Nov 2014-Mar 2018*
Politecnico di Milano, Italy
Thesis: *Defending from Financially-Motivated Software Abuses*

Visiting Researcher *Nov 2017-Jan 2018*
University of Sydney, Australia
Activity: Research in understanding and setting the standard for consumer data sharing practices of health apps, with a focus on how mobile health apps handle users' sensitive data.

Research Consultant *Jan 2017-Mar 2017*
Trend Micro Inc., Italy
Activity: Research on ransomware detection with the Forward-Looking Threat Research (FTR) team.

Visiting Researcher *Mar 2016-Aug 2016*
University of California, Santa Barbara, USA
Activity: Research on analysis and detection of obfuscated privacy leaks in Android applications.

Master Degree in Computer Science Engineering *Oct 2012-Oct 2014*
Politecnico di Milano, 110/110 *cum laude*
Thesis: *Prometheus: A Web-based Platform for Analyzing Banking Trojans*

Bachelor Degree in Computer Science Engineering *Oct 2009-July 2012*
Università degli studi di Catania, 110/110 *cum laude*

Publications

[16] Riccardo Bortolameotti, Thijs van Ede, **Andrea Continella**, Maarten H. Everts, Willem Jonker, Pieter Hartel, Andreas Peter. *"Victim-Aware Adaptive Covert Channels"*. In Proceedings of the International Conference on Security and Privacy in Communication Networks (SecureComm), October, 2019.

[15] Quinn Grundy, Kellia Chiu, Fabian Held, **Andrea Continella**, Lisa Bero, Ralph Holz. *"Data sharing practices of medicines-related apps and the mobile ecosystem"*. BMJ, 2019.

Publications (Continued)

[14] Xiaolei Wang, **Andrea Continella**, Yuexiang Yang, Yongzhong He, Sencun Zhu. *"LeakDoctor: Toward Automatically Diagnosing Privacy Leaks in Mobile Applications"*. In Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT), March, 2019.

[13] **Andrea Continella**, Mario Polino, Marcello Pogliani, Stefano Zanero. *"There's a Hole in that Bucket! A Large-scale Analysis of Misconfigured S3 Buckets"*. In Proceedings of the Annual Computer Security Applications Conference (ACSAC), December, 2018.

[12] Gabriele Viglianisi, Michele Carminati, Mario Polino, **Andrea Continella**, Stefano Zanero. *"SysTaint: Assisting Reversing of Malicious Network Communications"* In Proceedings of the Software Security, Protection, and Reverse Engineering Workshop (SSPREW), December, 2018.

[11] Davide Quarta, Federico Salvioni, **Andrea Continella**, Stefano Zanero. *"Extended Abstract: Toward Systematically Exploring Antivirus Engines"*. In Proceedings of the Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), June, 2018.

[10] Michele Carminati, Mario Polino, **Andrea Continella**, Andrea Lanzi, Federico Maggi, Stefano Zanero. *"Security Evaluation of a Banking Fraud Analysis System"*. ACM Transactions on Privacy and Security (TOPS), February, 2018.

[9] Niccolò Marastoni, **Andrea Continella**, Davide Quarta, Stefano Zanero, Mila Dalla Preda. *"GroupDroid: Automatically Grouping Mobile Malware by Extracting Code Similarities"*. In Proceedings of the Software Security, Protection, and Reverse Engineering Workshop (SSPREW), Orlando, FL, December, 2017.

[8] Mario Polino, **Andrea Continella**, Sebastiano Mariani, Stefano D'Alessio, Lorenzo Fontana, Fabio Gritti, Stefano Zanero. *"Hiding Pin's Artifacts to Defeat Evasive Malware"*. In Black Hat Europe, 2017.

[7] **Andrea Continella**, Alessandro Guagnelli A, Giovanni Zingaro, Giulio De Pasquale, Alessandro Barenghi, Stefano Zanero, Federico Maggi. *"ShieldFS: The Last Word In Ransomware Resilient Filesystems"*. In Black Hat USA, 2017.

[6] Mario Polino, **Andrea Continella**, Sebastiano Mariani, Stefano D'Alessio, Lorenzo Fontana, Fabio Gritti, Stefano Zanero. *"Measuring and Defeating Anti-Instrumentation-Equipped Malware"*. In Proceedings of the Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), Bonn, Germany, July, 2017.

[5] Nicola Mariani, **Andrea Continella**, Marcello Pogliani, Michele Carminati, Federico Maggi, Stefano Zanero. *"Poster: Detecting WebInjects through Live Memory Inspection"*. IEEE Symposium on Security and Privacy (S&P), San Jose, CA, May, 2017.

[4] **Andrea Continella**, Yanick Fratantonio, Martina Lindorfer, Alessandro Puccetti, Ali Zand, Christopher Kruegel, Giovanni Vigna. *"Obfuscation-Resilient Privacy Leak Detection for Mobile Apps Through Differential Analysis"*. In Proceedings of the ISOC Network and Distributed System Security Symposium (NDSS), San Diego, CA, February, 2017.

[3] **Andrea Continella**, Michele Carminati, Mario Polino, Andrea Lanzi, Stefano Zanero, Federico Maggi. *"Prometheus: Analyzing WebInject-based information stealers"*. Journal of Computer Security, 2017.

[2] **Andrea Continella**, Alessandro Guagnelli A, Giovanni Zingaro, Giulio De Pasquale, Alessandro Barenghi, Stefano Zanero, Federico Maggi. *"ShieldFS: A Self-healing, Ransomware-aware Filesystem"*. In Proceedings of the Annual Computer Security Applications Conference (ACSAC), Los Angeles CA, December, 2016.

[1] Giovanni Micale, **Andrea Continella**, Alfredo Ferro, Rosalba Giugno, Alfredo Pulvirenti. *"GASOLINE: a Cytoscape app for multiple local alignment of PPI networks"*. F1000Research, 2014.

Patents

[P1] **Andrea Continella**, Alessandro Guagnelli A, Giovanni Zingaro, Giulio De Pasquale, Alessandro Barenghi, Stefano Zanero, Federico Maggi. *"Protection system and method for protecting a computer system against ransomware attacks"*. Patent US20180157834A1.

Invited Talks

- Facebook, Inc., Menlo Park, CA, USA — *June 2018*
- Pinterest Inc., San Francisco, CA, USA — *May 2018*
- University of New South Wales (UNSW), Sydney, NSW, Australia — *January 2018*
- Black Hat USA, Las Vegas, NV, USA — *July 2017*
- Samsung Research America (SRA), Mountain View, CA, USA — *June 2017*

Invited Talks (Continued)

- Microsoft Research, Mountain View, CA, USA — *June 2017*
- Black Hat Webcast — *July 2016*
- INFOSEK 2015, Nova Gorica, Slovenia — *Nov 2015*
- Microsoft Research, Mountain View, CA, USA — *June 2015*
- HackInBo, Bologna, Italy — *May 2015*
- Essos Doctoral Symposium, Milan, Italy — *March 2015*

Awards

- CyCon Best Student Thesis Award at "International Conference on Cyber Conflict 2015" — *May 2015*
- Best M.Sc. Thesis Nominee at "Premio tesi ClusIT", 2nd place — *Mar 2015*
- Winner of a two-year scholarship at Politecnico di Milano — *Dec 2012*

Teaching

Politecnico di Milano

- Teaching Assistant for the "Comuter Security" course. — *2015 & 2017*
- Teaching Assistant for the "Privacy and Security" course. — *2016*
- Teaching Assistant for the "Elements of Computer Science" course. — *2015 & 2016*
- Member of the organization team of "Hacking Workshops". — *2015-2017*

Advising

Co-advised six master students in their M.Sc. theses at Politecnico di Milano

- RansomScan : extracting intelligence from ransomware families — *2018*
- SysTaint : assisting reversing of malicious network communications — *2018*
- Toward live memory forensics for malware identification — *2018*
- CrAVe : a comprehensive black-box approach to analyze antiviruses' emulators — *2017*
- RADAR: A Ransomware Detection And Remediation System — *2016*
- Apollo: Eliciting and Analyzing Advanced Web-Inject based Malware — *2016*

Academic Service

Program Committee

- ACM Internet Measurement Conference (IMC) (Poster Session) — *2019*

External Reviewer

- IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) — *2019*
- Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA) — *2018*
- Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA) — *2015*
- International Conference on Information Security Theory and Practice (WISTP) — *2015*

Journal Reviewer

- ACM Transactions on Privacy and Security (TOPS) — *2019*
- IEEE Transactions on Mobile Computing — *2018*
- Computers & Security (Elsevier) — *2018*
- IEEE Communications Surveys and Tutorials (COMST) — *2017*
- IEEE Communications Surveys and Tutorials (COMST) — *2015*

Media Coverage

Online (excerpt)

- BBC: Health apps pose 'unprecedented' privacy risks — *Mar 2019*
- VICE: Health Apps Can Share Your Data Everywhere, New Study Shows — *Mar 2019*
- Consumer Reports: Are Health Apps Putting Your Privacy at Risk? — *Mar 2019*
- Il Giorno (ITA): Hacker sì, ma con un'etica: ecco i "Mhackeroni" — *May 2018*
- WIRED: A Clever New Tool Shots Down Ransomware Before It's Too Late — *July 2017*

Media Coverage (Continued)

- Tom's guide: ShieldFS Promises to Stop Ransomware Dead in Its Tracks *July 2017*
- DarkReading: ShieldFS Hits 'Rewind' on Ransomware *July 2017*
- eSecurityPlanet: Black Hat: Building a Ransomware Resilient File System with ShieldFS *July 2017*
- Fossbytes: ShieldFS Stops Ransomware Attacks With 97% Success And [...] *July 2017*

Hacking

- Member of the Shellphish hacking team.
- Member of Tower of Hanoi & mhackeroni hacking teams.
- Qualified for several CTF finals, such as DEFCON and ruCTF.
- Member of the organization team of PoliCTF 2015 & 2017.

Open Source Research Tools

- **angr - Java engine.** Symbolic execution engine used by `angr` for Java/Dalvik bytecode.
- **truster.** Chrome extension that prevents the rendered web-pages from loading resources hosted in untrusted, writable S3 buckets.
- **crAVe.** Framework to automatically test and explore the capabilities of generic Antivirus engines.
- **Arancino.** Dynamic protection framework that defends Intel Pin against anti-instrumentation attacks.
- **Agrigento.** Tool that identifies privacy leaks in Android apps by performing black-box differential analysis on the network traffic.

References

Giovanni Vigna
Professor at University of California, Santa Barbara
vigna@cs.ucsb.edu

Christopher Kruegel
Professor at University of California, Santa Barbara
chris@cs.ucsb.edu

Stefano Zanero
Professor at Politecnico di Milano
stefano.zanero@polimi.it

Federico Maggi
Senior Researcher at Trend Micro
federico_maggi@trendmicro.com

Ralph Holz
Lecturer at University of Sydney
ralph.holz@sydney.edu.au