ANDREA **CONTINELLA**

Personal Data

Place and Date of Birth:	Catania (CT), Italy | 20 May 1991
Residency:	Milan, Italy
Email:	andreacontinella@gmail.com
Home Page:	`https://conand.me`

Positions and Education

Nov 2014-Current	**PhD Student in Computer Science and Engineering** at Politecnico di Milano
Research Activity:	My research interests are mainly focused on computer security and in particular on threat analysis. I have been working on analysis and defense mechanisms against advanced malware, including for example the current generation of trojan horses, or the infamous ransomware families.
Nov 2017-Current	**Visiting Researcher** at the University of Sydney
Research Activity:	I'm involved in a research project that aims at 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.
Jan 2017-Mar 2017	**Temporary Contractor** at Trend Micro Inc.
Activity:	Research on ransomware analysis and detection with the Forward-Looking Threat Research (FTR) team.
Mar 2016-Aug 2016	**Visiting Researcher** at University of California Santa Barbara
Research Activity:	Research on analysis and detection of obfuscated privacy leaks in Android applications.
Oct 2012-Oct 2014	**Master Degree in Computer Science Engineering** at Politecnico di Milano, 110/110 cum laude
Thesis title:	*"Prometheus: A Web-based Platform for Analyzing Banking Trojans"*
Thesis link:	`https://goo.gl/ykadsu`
Oct 2009-July 2012	**Bachelor Degree in Computer Science Engineering** at Università degli studi di Catania, 110/110 cum laude
Thesis title:	*"Politiche e strumenti di gestione dell'Advance Reservation all'interno di scenari Cloud e Multicore"* (Policies and Tools to Manage Advance Reservations in Cloud and Multicore environments)
Thesis link:	`https://goo.gl/csRg9s`

Awards

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

Technical Skills

Operating Systems:	Linux, Windows, OS X
Programming Languages:	Python, C, Java, PHP, C#
Other:	Sysadmin and Networking skills

Publications

[7] *"GroupDroid: Automatically Grouping Mobile Malware by Extracting Code Similarities"*
Marastoni N, **Continella A**, Quarta D, Zanero S, Dalla Preda M.
In Proceedings of the Software Security, Protection, and Reverse Engineering Workshop (SSPREW), Orlando, FL, December, 2017

[6] *"Measuring and Defeating Anti-Instrumentation-Equipped Malware"*
Polino M, **Continella A**, D'Alessio S, Fontana L, Gritti F, Mariani S, Zanero S.
In Proceedings of the Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), Bonn, Germany, July, 2017

[5] *"Poster: Detecting WebInjects through Live Memory Inspection"*
Mariani N, **Continella A**, Pogliani M, Carminati M, Maggi F, Zanero S.
IEEE Symposium on Security and Privacy (S&P), San Jose, CA, May, 2017

[4] *"Obfuscation-Resilient Privacy Leak Detection for Mobile Apps Through Differential Analysis"*
Continella A, Fratantonio Y, Lindorfer M, Puccetti A, Zand A, Kruegel C, Vigna G.
In Proceedings of the ISOC Network and Distributed System Security Symposium (NDSS), San Diego, CA, February, 2017

[3] *"Prometheus: Analyzing WebInject-based information stealers"*
Continella A, Carminati M, Polino M, Lanzi A, Zanero S, Maggi F.
Journal of Computer Security, 2017

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

[1] *"GASOLINE: a Cytoscape app for multiple local alignment of PPI networks"*
Micale G, **Continella A**, Ferro A, Giugno R, Pulvirenti A.
F1000Research, 2014

Selected Projects

Jan 2017 **Arancino**
Arancino is a dynamic protection framework that defends Intel Pin against anti-instrumentation attacks.
`https://github.com/necst/arancino`

Sep 2016 **Agrigento**
Agrigento is a tool that identifies privacy leaks in Android apps by performing black-box differential analysis on the network traffic.
`https://github.com/ucsb-seclab/agrigento`

Feb 2016 **ShieldFS**
ShieldFS is an add-on driver that makes the Windows native filesystem immune to ransomware attacks by detecting malicious activities and transparently reverting the effects of such attacks.
`http://shieldfs.necst.it`

Oct 2014 **Prometheus**
Prometheus is a platform to analyze banking trojans exploiting the visible DOM modifications that they cause in the HTML pages. Prometheus, independently from the trojan's family, detects the injections performed by the malware and extracts the WebInject targets.

Languages

Italian:	Mother tongue
English:	First Certificate in English (FCE), C - June 2012
	TOEIC Listening and Reading Test, 895/990 - Sept 2014

Other Activities

- Member of "Tower of Hanoi" (**http://toh.necst.it**) and "Shellphish" (**http://shellphish.net**), the Politecnico di Milano and UCSB hacking teams.
- Teaching Assistant for the following courses at Politecnico di Milano: Computer Security (2015 & 2017), Privacy and Security (2016), Elements of Computer Science (2015 & 2016).
- Black Hat Speaker.
  "In Your PC & In Your Pocket: Desktop And Mobile Ransomware Threat Landscape Overview", July 2016, **https://goo.gl/fYAxrP**.
  "ShieldFS: The Last Word In Ransomware Resilient Filesystems", July 2017, **https://goo.gl/ME3tcF**.

Interests

Computer Security, Cryptography, Distributed Systems, Machine Learning, Game Theory, Bioinformatics, Music, Soccer, Hiking.