





Andrea Continella

| | | | |
|-----------------------|---|---|--|
| AFFILIATION | Associate Professor, University of Twente | | |
| CONTACT INFORMATION | University of Twente Faculty of Electrical Engineering, Mathematics and Computer Science Zilverling, P.O. Box 217 7500 AE Enschede, The Netherlands | acontinella@iseclab.org https://conand.me @_conand conand |     |
| BIOGRAPHY | <p>I am an Associate Professor at the Faculty of Electrical Engineering, Mathematics and Computer Science of the University of Twente, where I lead the cybersecurity team of the Semantics, Cybersecurity & Services group (SCS), and I am a member of the International Secure Systems Lab (iSecLab). Previously, I was a Postdoctoral Researcher in the Computer Science Department at UC Santa Barbara, and I obtained a Ph.D. <i>cum laude</i> in Computer Science and Engineering at Politecnico di Milano. During my Ph.D., 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 Shellphish hacking team.</p> | | |
| RESEARCH INTERESTS | <p>My research focuses on aspects of computer security traditionally known as <i>systems security</i>. In particular, my main research interests lie in the security of the software that people use in their daily tasks, and revolve around analyzing such software for multiple security purposes, such as malware detection, identification of privacy disclosures, and vulnerability discovery. For example, I have worked on analysis and defense mechanisms against advanced threats such as the infamous ransomware families, on the detection of obfuscated privacy leaks in Android apps, and on the design of novel program analysis techniques to identify and patch vulnerabilities in embedded firmware. I strongly believe in open, collaborative science, where researchers can easily and quickly access previous research outcomes to reproduce and analyze results obtained by others.</p> | | |
| POSITIONS & EDUCATION | Associate Professor Faculty of Electrical Engineering, Mathematics and Computer Science University of Twente, The Netherlands | June 2023-Current | |
| | Assistant Professor <i>Tenured since January 2022</i> Faculty of Electrical Engineering, Mathematics and Computer Science University of Twente, The Netherlands | May 2020-May 2023 | |
| | Postdoctoral Researcher University of California, Santa Barbara, USA | July 2018-Apr 2020 | |
| | Doctor in Philosophy (Ph.D.), Computer Science and Engineering Politecnico di Milano, Italy, <i>cum laude</i> Thesis: <i>Defending from Financially-Motivated Software Abuses</i> | Nov 2014-Mar 2018 | |
| | Visiting Researcher University of Sydney, Australia | Nov 2017-Jan 2018 | |
| | Research Consultant Trend Micro Inc., Italy | Jan 2017-Mar 2017 | |
| | Visiting Researcher University of California, Santa Barbara, USA | Mar 2016-Aug 2016 | |
| | Master Degree in Computer Science Engineering Politecnico di Milano, 110/110 <i>cum laude</i> Thesis: <i>Prometheus: A Web-based Platform for Analyzing Banking Trojans</i> | Oct 2012-Oct 2014 | |
| | Bachelor Degree in Computer Science Engineering Università degli studi di Catania, 110/110 <i>cum laude</i> | Oct 2009-July 2012 | |

PUBLICATIONS

- [46] Carlotta Tagliaro, Martina Komsic, **Andrea Continella**, Kevin Borgolte, Martina Lindorfer. *Large-Scale Security Analysis of Real-World Backend Deployments Speaking IoT-Focused Protocols*. In Proceedings of the International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2024.
- [45] Jorik van Nielen, Andreas Peter, **Andrea Continella**. *Framed: Toward Automated Identification of Embedded Frameworks in Firmware Images*. In Proceedings of the Workshop On The Security Of Industrial Control Systems & Of Cyber-Physical Systems (CyberICPS), 2024.
- [44] Zsolt Levente Kucsván, Marco Caselli, Andreas Peter, **Andrea Continella**. *Inferring Recovery Steps from Cyber Threat Intelligence Reports*. In Proceedings of the Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), 2024.
- [43] Tina Rezaei, Suzan Bayhan, **Andrea Continella**, Roland van Rijswijk-Deij. *ERAFL: Efficient Resource Allocation for Federated Learning Training in Smart Homes*. In Proceedings of the IEEE/IFIP Network Operations and Management Symposium (NOMS), 2024.
- [42] Asbat El Khairi, Marco Caselli, Andreas Peter, **Andrea Continella**. *ReplicaWatcher: Training-less Anomaly Detection in Containerized Microservices*. In Proceedings of the ISOC Network and Distributed System Security Symposium (NDSS), 2024.
- [41] Jerre Starink, Marieke Huisman, Andreas Peter, **Andrea Continella**. *Understanding and Measuring Inter-Process Code Injection in Windows Malware*. In Proceedings of the International Conference on Security and Privacy in Communication Networks (SecureComm), 2023.
- [40] Eric Gustafson, Paul Grosen, Nilo Redini, Saagar Jha, **Andrea Continella**, Ruoyu Wang, Kevin Fu, Sara Rampazzi, Christopher Kruegel, Giovanni Vigna. *Shimware: Toward Practical Security Retrofitting for Monolithic Firmware Images*. In Proceedings of the International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2023.
- [39] Jessica Pimienta, Jacco Brandt, Timme Bethe, Ralph Holz, **Andrea Continella**, Lindsay Jibb, Quinn Grundy. *Mobile apps and children's privacy: a traffic analysis of data sharing practices among children's mobile iOS apps*. Archives of Disease in Childhood (ADC), 2023.
- [38] Linus Hafkemeyer, Jerre Starink, **Andrea Continella**. *Divak: Non-invasive Characterization of Out-Of-Bounds Write Vulnerabilities*. In Proceedings of the Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), 2023.
- [37] Muhammad Ibrahim, **Andrea Continella**, Antonio Bianchi. *AoT - Attack on Things: A security analysis of IoT firmware updates*. In Proceedings of the IEEE European Symposium on Security and Privacy (EuroS&P), 2023.
- [36] Priyanka Bose, Dipanjan Das, Saastha Vasan, Sebastiano Mariani, Ilya Grishchenko, **Andrea Continella**, Antonio Bianchi, Christopher Kruegel, Giovanni Vigna. *COLUMBUS: Android App Testing Through Systematic Callback Exploration*. In Proceedings of the International Conference on Software Engineering (ICSE), 2023.
- [35] Chakshu Gupta, Thijs van Ede, **Andrea Continella**. *HoneyKube: Designing and Deploying a Microservices-based Web Honeypot*. In Proceedings of the SecWeb Workshop (SecWeb), 2023.
- [34] Dennis Reidsma, Jeroen van der Ham, **Andrea Continella**. *Operationalizing Cybersecurity Research Ethics Review: From Principles and Guidelines to Practice*. In Proceedings of the International Workshop on Ethics in Computer Security (EthiCS), 2023.
- [33] Luca Morgese Zangrandi, Thijs van Ede, Tim Booij, Savio Sciancalepore, Luca Allodi, **Andrea Continella**. *Stepping out of the MUD: Contextual threat information for IoT devices with manufacturer-provided behaviour profiles*. In Proceedings of the Annual Computer Security Applications Conference (ACSAC), December, 2022.
- [32] Thijs van Ede, Niek Khasuntsev, Bas Steen, **Andrea Continella**. *Detecting Anomalous Misconfigurations in AWS Identity and Access Management Policies*. In Proceedings of the ACM Cloud Computing Security Workshop (CCSW), November, 2022.
- [31] Asbat El Khairi, Marco Caselli, Christian Knierim, Andreas Peter, **Andrea Continella**. *Contextualizing System Calls in Containers for Anomaly-Based Intrusion Detection*. In Proceedings of the ACM Cloud Computing Security Workshop (CCSW), November, 2022.
- [30] Max Meijer, Giacomo Tommaso Petrucci, Matthijs Schotsman, Luca Morgese, Thijs van Ede, **Andrea Continella**, Ganduulga Gankhuyag, Luca Allodi, Savio Sciancalepore. *Federated Lab (FedLab): An Open-source Distributed Platform for Internet of Things (IoT) Research and Experimentation*. IEEE World Forum on IoT (WF-IoT), 2022.

PUBLICATIONS
(CONTINUED)

- [29] Thijs van Ede, Hojjat Aghakhani, Noah Spahn, Riccardo Bortolameotti, Marco Cova, **Andrea Continella**, Maarten van Steen, Andreas Peter, Christopher Kruegel, Giovanni Vigna. *"DeepCASE: Semi-Supervised Contextual Analysis of Security Events"*. In Proceedings of the IEEE Symposium on Security and Privacy (S&P), May, 2022.
- [28] Nicola Galloro, Mario Polino, Michele Carminati, **Andrea Continella**, Stefano Zanero. *"A Systematic and Longitudinal Study of Evasive Behaviors in Windows Malware"*. Computers & Security, February, 2022.
- [27] Damiano Melotti, Maxime Rossi-Bellom, **Andrea Continella**. *"Reversing and Fuzzing the Google Titan M Chip"*. In Proceedings of the Reversing and Offensive-oriented Trends Symposium (ROOTS), November, 2021.
- [26] Nicola Ruaro, Lukas Dresel, Kyle Zeng, Tiffany Bao, Mario Polino, **Andrea Continella**, Stefano Zanero, Christopher Kruegel, Giovanni Vigna. *"SyML: Guiding Symbolic Execution Toward Vulnerable States Through Pattern Learning"*. In Proceedings of the International Symposium on Research in Attacks, Intrusions and Defenses (RAID), October, 2021.
- [25] Chinmay Garg, Aravind Machiry, **Andrea Continella**, Christopher Kruegel, Giovanni Vigna. *"Toward a Secure Crowdsourced Location Tracking System"*. In Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), July, 2021.
- [24] Dongyu Meng, Michele Guerriero, Aravind Machiry, Hojjat Aghakhani, Priyanka Bose, **Andrea Continella**, Christopher Kruegel, Giovanni Vigna. *"Bran: Reduce Vulnerability Search Space in Large Open Source Repositories by Learning Bug Symptoms"*. In Proceedings of the ACM ASIA Conference on Computer and Communications Security (ASIACCS), June, 2021.
- [23] Nilo Redini, **Andrea Continella**, Dipanjan Das, Giulio De Pasquale, Noah Spahn, Aravind Machiry, Antonio Bianchi, Christopher Kruegel, Giovanni Vigna. *"DIANE: Identifying Fuzzing Triggers in Apps to Generate Under-constrained Inputs for IoT Devices"*. In Proceedings of the IEEE Symposium on Security & Privacy (S&P), May, 2021.
- [22] Ralph Holz, Diego Perino, Matteo Varvello, Johanna Amann, **Andrea Continella**, Nate Evans, Ilias Leontiadis, Christopher Natoli, Quirin Scheitle. *"A Retrospective Analysis of User Exposure to (Illicit) Cryptocurrency Mining on the Web"*. In Proceedings of the Network Traffic Measurement and Analysis Conference (TMA), June, 2020.
- [21] Fabio Gritti, Lorenzo Fontana, Eric Gustafson, Fabio Pagani, **Andrea Continella**, Christopher Kruegel, Giovanni Vigna. *"SYMBION: Interleaving Symbolic with Concrete Execution"*. In Proceedings of the IEEE Conference on Communications and Network Security (CNS), June, 2020.
- [20] Nilo Redini, Aravind Machiry, Ruoyu Wang, Chad Spensky, **Andrea Continella**, Yan Shoshitaishvili, Christopher Kruegel, Giovanni Vigna. *"KARONTE: Detecting Insecure Multi-binary Interactions in Embedded Firmware"*. In Proceedings of the IEEE Symposium on Security & Privacy (S&P), May, 2020.
- [19] Nilo Redini, Aravind Machiry, Ruoyu Wang, Chad Spensky, **Andrea Continella**, Yan Shoshitaishvili, Christopher Kruegel, Giovanni Vigna. *"Identifying Multi-Binary Vulnerabilities in Embedded Firmware at Scale"*. In Black Hat Asia, April, 2020.
- [18] Thijs van Ede, Riccardo Bortolameotti, **Andrea Continella**, Jingjing Ren, Daniel J. Dubois, Martina Lindorfer, David Choffnes, Maarten van Steen, Andreas Peter. *"FlowPrint: Semi-Supervised Mobile-App Fingerprinting on Encrypted Network Traffic"*. In Proceedings of the ISOC Network and Distributed System Security Symposium (NDSS), February, 2020.
- [17] Riccardo Bortolameotti, Thijs van Ede, **Andrea Continella**, Thomas Hupperich, Maarten H. Everts, Reza Rafati, Willem Jonker, Pieter Hartel, Andreas Peter. *"HeadPrint: Detecting Anomalous Communications through Header-based Application Fingerprinting"*. In Proceedings of the ACM Symposium on Applied Computing (SAC), March, 2020.
- [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.
- [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.

PUBLICATIONS
(CONTINUED)

- [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), 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, Giovanni Zingaro, Giulio De Pasquale, Alessandro Barengi, 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, Giovanni Zingaro, Giulio De Pasquale, Alessandro Barengi, Stefano Zanero, Federico Maggi. *“ShieldFS: A Self-healing, Ransomware-aware Filesystem”*. In Proceedings of the Annual Computer Security Applications Conference (ACSAC), December, 2016.
- [1] Giovanni Micale, **Andrea Continella**, Alfredo Ferro, Rosalba Giugno, Alfredo Pulvirenti. *“GASO-LINE: a Cytoscape app for multiple local alignment of PPI networks”*. F1000Research, 2014.

PATENTS

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

FUNDING

P6: Prioritization for Prompt Patching of Programs with Pernicious Problems

Main PI: **Andrea Continella** (University of Twente)

Co-PIs: Erik van der Kouwe (Vrije Universiteit Amsterdam), Cristiano Giuffrida (Vrije Universiteit Amsterdam), Herbert Bos (Vrije Universiteit Amsterdam), Jeroen van der Ham (University of Twente), Giancarlo Guizzardi (University of Twente)

Funding: NWO Open Technology Programme, 812,322 EUR (6 years, expected starting April 2024)

Automated Patching for Embedded Firmware Images

PIs: **Andrea Continella** (University of Twente)

Funding: Ministry of Economic Affairs and Climate Policy (Dutch: Ministerie van Economische Zaken en Klimaat; EZK), 250,000 EUR (4 years starting March 2023)

| | | |
|------------------------|--|--------------------------------------|
| FUNDING (CONTINUED) | Designing and Building an IoT Cyber Lab | |
| | PIs: Andrea Continella (University of Twente), Roland van Rijswijk-Deij (University of Twente) | |
| | Funding: “Impuls Financiering”, Faculty of Electrical Engineering, Mathematics and Computer Science, 200,000 EUR (3 years starting January 2022) | |
| | Children’s privacy and mobile health applications: an analysis of data sharing practices and impact | |
| | PIs: Lindsay Jibb (Hospital for Sick Children), Quinn Grundy (University of Toronto) | |
| | Co-PIs: Andrea Continella (University of Twente), Ralph Holz (University of Twente) | |
| | Funding: New Frontiers in Research Fund, Exploration Grant, \$248,753 CAD (3 years starting May 2020) | |
| INVITED TALKS | • Keynote, DIMVA Conference, Lausanne, Switzerland | <i>July 2024</i> |
| | • Automated Vulnerability Research Challenge, The Hague, Netherlands | <i>June 2024</i> |
| | • Università degli Studi di Catania, NAS Research Group, Catania, Italy | <i>April 2024</i> |
| | • Keynote, Cyber Security Next Generation Workshop (CSng), Apeldoorn, Netherlands | <i>Nov 2023</i> |
| | • No Hat Security Conference, Bergamo, Italy | <i>Oct 2023</i> |
| | • University of Luxembourg, IRiSC Research Group, Luxembourg | <i>Oct 2023</i> |
| | • ONE Conference, The Hauge, Netherlands | <i>Oct 2023</i> |
| | • DIMVA’23 Panel, Hamburg, Germany | <i>July 2023</i> |
| | • Hack In The Box Security Conference, Amsterdam, Netherlands | <i>April 2023</i> |
| | • TU Wien, Security and Privacy Research Unit, Vienna, Austria | <i>Mar 2023</i> |
| | • Huawei Research Munich, AI4Sec Research Team, Online | <i>July 2022</i> |
| | • VUsec, Vrije Universiteit Amsterdam, Netherlands | <i>April 2022</i> |
| | • SI Seminar, Università della Svizzera italiana, Online | <i>Mar 2022</i> |
| | • No Hat Security Conference, Bergamo, Italy Online | <i>Nov 2020</i> |
| | • Black Hat Asia, Singapore Online | <i>Oct 2020</i> |
| | • Facebook, Inc., Menlo Park, CA, USA | <i>June 2018</i> |
| | • Pinterest Inc., San Francisco, CA, USA | <i>May 2018</i> |
| | • University of New South Wales (UNSW), Sydney, NSW, Australia | <i>January 2018</i> |
| | • Black Hat USA, Las Vegas, NV, USA | <i>July 2017</i> |
| | • Samsung Research America (SRA), Mountain View, CA, USA | <i>June 2017</i> |
| | • Microsoft Research, Mountain View, CA, USA | <i>June 2017</i> |
| | • Black Hat Webcast, Online | <i>July 2016</i> |
| | • INFOSEK 2015, Nova Gorica, Slovenia | <i>Nov 2015</i> |
| | • HackInBo, Bologna, Italy | <i>May 2015</i> |
| TEACHING | University of Twente | |
| | • “Software Testing and Reversing” (MSc course) | <i>2022 - Current</i> |
| | • “System Security” (MSc course) | <i>2021 - Current</i> |
| | • “Empirical Security Analysis & Engineering” (MSc course) — with Ralph Holz | <i>2021 - Current</i> |
| | • “AI & Cybersecurity” (BSc course) | <i>2020 - 2022</i> |
| | Politecnico di Milano | |
| | • Teaching Assistant for the “Computer Security” course | <i>2015 & 2017</i> |
| | • Teaching Assistant for the “Elements of Computer Science” course | <i>2015 & 2016</i> |
| SUPERVISING | PhD candidates | |
| | • Thijs van Ede — ML-based Intrusion Detection | <i>Graduated cum laude, Nov 2023</i> |
| | • Asbat El Khairi — Container & Cloud Security | <i>Starting date: Feb 2021</i> |
| | • Chakshu Gupta — IoT Security | <i>Starting date: Oct 2021</i> |
| | • Jerre Starink — Malware Analysis & Reversing | <i>Starting date: Nov 2021</i> |
| | • Zsolt Kucsavàn — Threat Detection & Response | <i>Starting date: Nov 2021</i> |

SUPERVISING
(CONTINUED)

PhD candidates (continued)

- Tina Rezaei — Edge Computing Security & Privacy Starting date: April 2022
- Jorik van Nielen — Firmware Security Starting date: July 2023
- Matteo Grella — Cloud Security Starting date: Sept 2023
- Mattia Napoli — Software Security Starting date: Nov 2024

Master students supervised at the University of Twente

- N. Khasuntsev — Automatic Detection of Misconfigurations of AWS Identity and Access [...] 2021
- T. Leemreize — Analyzing fileless malware for the .NET Framework through CLR profiling 2021
- C. Scholten — Automatic detection of zero-day attacks in high-interaction IoT honeypots [...] 2021
- C. Gupta — HoneyKube: Designing a honeypot using microservices-based architecture 2021
- J. Starink — Analysis and automated detection of host-based code injection techniques [...] 2021
 - Runner-up Best Cybersecurity Master Thesis Award (BCMT) in the Netherlands
- C. Raghuraman — Detecting anomalies in programmable logic controllers through [...] 2021
- D. Melotti — Reversing and Fuzzing the Google Titan M Chip 2021
 - Winner of the Best Cybersecurity Thesis Clusit Award (Italian: Premio Tesi Clusit)
- L. Morgese — Stepping out of the MUD: Contextual network threat information for IoT [...] 2021
- L. Hafkemeyer — Non-invasive Characterization of Out-Of-Bounds Write Vulnerabilities 2022
 - Awarded as the 2022 Best Graduate of the EEMCS Faculty at TU Delft
- U. Nisslmuehler — LOLBin detection through unsupervised learning 2022
- M. Liberato — SecBERT : Analyzing reports using BERT-like models 2022
- M. de Redelijkheid — Monitoring network traffic and responding to malicious traffic [...] 2023
- J. van Nielen — Dynamic Detection and Classification of Persistence Techniques in Malware 2023
- M. Macarie — Fuzzing Android Automotive’s CAN interface 2023
- C. Xu — Automatically Generating User-specific Recovery Procedures after Malware Infections 2023
- W. van Beijnum — Haly: Automated evaluation of hardening techniques in Android & iOS apps 2023
- T. Bethe — Fallaway : High Throughput Stateful Fuzzing by making AFL* State-Aware 2024

Master students co-supervised at Politecnico di Milano

- G. Bucci — RansomScan : extracting intelligence from ransomware families 2018
- G. Viglianisi — SysTaint : assisting reversing of malicious network communications 2018
- G. Mazzotta — Toward live memory forensics for malware identification 2018
- F. Salvioni — CrAVE : a comprehensive black-box approach to analyze antiviruses’ emulators 2017
- A. Guagnelli & G. Zingaro — RADAR: A Ransomware Detection And Remediation System 2016
- S. Rodi — Apollo: Eliciting and Analyzing Advanced Web-Inject based Malware 2016

AWARDS &
CERTIFICATES

- USENIX Security Symposium — Distinguished Reviewer 2024
- Dutch Cyber Security Best Research Paper Award - Runner-up 2023, 2024
- University Teaching Qualification (UTQ) — “Basis Kwalificatie Onderwijs, BKO” 2022
- ESAE awarded the best MSc course in Computer Science Q1 by UTWente students 2021
- Google Cloud Research Credits Award (\$5,000) 2020
- CyCon Best Student Thesis Award at “International Conference on Cyber Conflict 2015” 2015
- Best M.Sc. Thesis Nominee at “Premio tesi ClusIT”, 2nd place 2015
- Richard Newton Young Fellow Award 2015

ACADEMIC
SERVICE

Chairing and Organization

- Poster Co-Chair for the USENIX Security Symposium 2024

ACADEMIC
SERVICE
(CONTINUED)

Program Committee

- USENIX Security Symposium 2021, 2022, 2023, 2024
- Annual Computer Security Applications Conference (ACSAC) 2022, 2023, 2024
- Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA) 2023, 2024
- IEEE European Symposium on Security and Privacy (EuroS&P) 2023
- IEEE Workshop on Offensive Technologies (WOOT) 2023
- Workshop on Binary Analysis Research (BAR) 2020, 2022
- ACM Conference on Computer and Communications Security (CCS) 2020, 2021
- USENIX Security Artifact Evaluation Committee 2020
- Privacy Enhancing Technologies Symposium (PETS) Artifact Review Committee 2020

External Reviewer

- IEEE European Symposium on Security and Privacy (EuroS&P) 2021
- IEEE Conference on Trust, Security and Privacy in Computing (TrustCom) 2019
- Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA) 2015, 2018

Journal Reviewer

- ACM Digital Threats: Research and Practice (DTRAP) 2023
- Computers & Security Elsevier (COSE) 2018, 2020, 2021, 2023
- ACM Transactions on Privacy and Security (TOPS) 2019, 2021
- IEEE Transactions on Dependable and Secure Computing (TDSC) 2021
- ACM Transactions on Autonomous and Adaptive Systems (TAAS) 2020
- IEEE Transactions on Mobile Computing (TMC) 2018, 2019
- ACM Computing Surveys (CSUR) 2018
- IEEE Communications Surveys and Tutorials (COMST) 2015, 2017

Other Committees

- Ethics Committee Computer & Information Science, University of Twente 2021 - Current
- IPN Cyber Security Special Interest Group (SIG SEC) 2023 - Current

MEDIA
COVERAGE

Online (excerpt)

- [MobiHealthNews: When fitness data becomes research data, your privacy may be at risk](#) Feb 2021
- [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 Giornò \(ITA\): 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
- [BleepingComputer: ShieldFS Can Stop and Revert the Effects of Ransomware Infections](#) July 2017
- [DarkReading: ShieldFS Hits 'Rewind' on Ransomware](#) July 2017

HACKING

- Mentor of the [Twente Hacking Squad \(THS\)](#)
- Member of the [Shellphish](#) hacking team. Previous member of [Tower of Hanoi](#) & [mhackeroni](#)
- Qualified for several CTF finals, such as DEFCON, ruCTF, and DragonSectorCTF
- Member of the organization team of the PoliCTF (2015 & 2017) and iCTF (2019 & 2020)

OPEN SOURCE
RESEARCH TOOLS

- [Diane](#). Black-box fuzzer for IoT devices
- [Karonte](#). Static analysis tool to detect multi-binary vulnerabilities in embedded firmware
- [anqr - Java engine](#). Symbolic execution engine used by anqr for Java/Dalvik bytecode
- [truster](#). Chrome extension that prevents 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 obfuscated privacy leaks in Android apps