

# FLAVIO TOFFALINI

(+39) · 340 255 9962 ◊ flavio.toffalini@rub.de

My research interest covers many aspects of system security. My Ph.D. background focuses on software security for Trusted Execution Environment.

## CURRENT POSITION: ASSISTANT PROFESSOR

---

**Ruhr-Universität Bochum (RUB), Germany**  
Assistant Professor in Automated Security Analysis

*Sep 2024 to Now*

## FORMER POSITION

---

**École Polytechnique Fédérale de Lausanne (EPFL), Switzerland**  
PostDoc, supervised by Prof. Mathias Payer  
Topic: fuzzing, mitigation, software analysis

*Nov 2021 – Aug 2024*

## EDUCATION

---

**Singapore University of Technology and Design, Singapore**  
Ph.D., supervisor Prof. Jianying Zhou  
Topic: trusted computing, system security  
Thesis Title: Challenges, threats, and novel defenses for Trusted Execution Environments

*Jan 2017 - Sep 2021*

**University of Verona, Italy**  
M.S. in Computer Science and Engineering 108/110, GPA 3,9/4  
Supervisor Prof. Damiano Carra  
Master thesis topic: Google dorks, Web security

*Sep 2012 - Oct 2015*

**University of Pavia, Italy**  
B.S. in Computer Engineer 101/110, GPA 3,67/4  
Supervisor Prof. Paolo Gamba

*Sep 2006 - Dec 2009*

## ACADEMIC ACTIVITIES

---

**King's College London**  
*Visiting fellow, supervised by Prof. Lorenzo Cavallaro*  
Topic: trusted computing, system security

*Nov 2019 - Mar 2020  
London, UK*

**University of Padua**  
*Visiting fellow, supervised by Prof. Mauro Conti*  
Topic: trusted computing, system security

*Jan 2018 - Aug 2018  
Padua, Italy*

**University of Verona**  
*Research Assistant, supervised by Prof. Fausto Spoto*  
Topic: static analysis of Android applications

*Dec 2015 - July 2016  
Verona, Italy*

**Eurecom**  
*Visiting fellow, supervised by Prof. Davide Balzarotti*  
Topic: Google dorks, Web security

*April 2015 - July 2015  
Biot, France*

## TEACHING ACTIVITES

---

“Advanced Automatic Testing” (Master Course, Main Instructor) at Ruhr-Universität Bochum, 48 hours

“Seminar in Advanced Automatic Testing” (Master/Bachelor Seminar, Main Instructor) at Ruhr-Universität Bochum, 48 hours

## SUPERVISION

---

PhDs: Currently 1, 2 co-supervised during Post-Doctoral

MSc: Currently 3, 3 successfully completed

BSc: 3 successfully completed

Interns: Currently 1, 1 successfully completed

## RESEARCH GRANTS

---

“Advancing Cybersecurity Through Semantic Bugs in Interpreted Programming Languages” (PI) funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany’s Excellence Strategy - EXC 2092 CASA - 390781972 (approved from 2025 to 2028)

“Detecting Semantic Bugs in JavaScript Engines” unrestricted git from Google Research Scholar (\$60,000 USD)

## PUBLICATIONS

---

### Conference

- C17 Vanoverloop D., Sanchez A., **Toffalini F.**, Piessens F., Payer M., and Van Bulck J.  
“TLBlur: Compiler-assisted automated hardening against controlled channels on off-the-shelf Intel SGX platforms” Proceeding of the 34nd USENIX Security Symposium (Usenix SEC 2025)
- C16 Badoux N., **Toffalini F.**, and Payer M.  
“Sourcerer: channeling the void” Proceeding of the 22th International Conference of Detection of Intrusions, Malware, and Vulnerability Assessment (DIMVA 2025)
- C15 **Toffalini F.**, Badoux N., Tsinadze Z., and Payer M.  
“Liberating libraries through automated fuzz driver generation: Striking a Balance Without Consumer Code” Proceeding of the ACM International Conference on the Foundations of Software Engineering (FSE 2025)
- C14 Zheng H., **Toffalini F.**, Böhme M., and Payer M.  
“MendelFuzz: The Return of the Deterministic Stage” Proceeding of the ACM International Conference on the Foundations of Software Engineering (FSE 2025)
- C13 Wachter L., Gremminger J., Wressnegger C., Payer M., and **Toffalini F.**  
“DUMPLING: Fine-grained Differential JavaScript Engine Fuzzing” Proceeding of the 32th Network and Distributed System Security Symposium (NDSS 2025) - **Distinguished Paper**
- C12 Badoux N., **Toffalini F.**, Jeon Y., and Payer M.  
“type++: Prohibiting Type Confusion With Inline Type Information” Proceeding of the 32th Network and Distributed System Security Symposium (NDSS 2025) - **Distinguished Paper**

- C11 Srivastava P., **Toffalini F.**, Vorobyov K., Gauthier F., Bianchi A., and Payer M.  
 “Crystallizer: A Hybrid Path Analysis Framework To Aid in Uncovering Deserialization Vulnerabilities” Proceeding of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE 2023)
- C10 Zheng H., Zhang J., Huang Y., Ren Z., Wang H., Cao C., Zhang Y., **Toffalini F.**, and Payer M.  
 “FishFuzz: Throwing Larger Nets to Catch Deeper Bugs” Proceeding of the 32nd USENIX Security Symposium (Usenix SEC 2023)
- C9 Xu J., Di Bartolomeo L., **Toffalini F.**, Mao B., and Payer M.  
 “WarpAttack: Bypassing CFI through Compiler-Introduced Double-Fetches” Proceeding of the 44th IEEE Symposium on Security and Privacy (S&P 2023)
- C8 Liu Q., **Toffalini F.**, Zhou Y., and Payer M.  
 “ViDeZZO: Dependency-aware Virtual Device Fuzzing” Proceeding of the 44th IEEE Symposium on Security and Privacy (S&P 2023)
- C7 **Toffalini F.**, Payer M., Zhou J., and Cavallaro L.  
 “Designing a Provenance Analysis for SGX Enclaves” Proceeding of the 38th Annual Computer Security Applications Conference (ACSAC 2022)
- C6 Jiang Z., Gan S., Herrera A., **Toffalini F.**, Romerio L., Tang C., Egele M., Zhang C., and Payer M.  
 “Evocatio: Conjuring Bug Capabilities from a Single PoC” Proceeding of the ACM SIGSAC Conference on Computer and Communications Security (CCS 2022)
- C5 **Toffalini F.**, Graziano M., Conti M., and Zhou J.  
 “SnakeGX: a sneaky attack against SGX Enclaves” Proceeding of the 19th International Conference on Applied Cryptography and Network Security (ACNS 2022)
- C4 **Toffalini F.**, Losiouk E., Biondo A., Zhou J., and Conti M.  
 “ScaRR: Scalable Runtime Remote Attestation for Complex Systems” Proceeding of the 22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2019)
- C3 **Toffalini F.**, Ochoa M., Sun J., and Zhou J.  
 “Careful-Packing: A Practical and Scalable Anti-Tampering Software Protection enforced by Trusted Computing” Proceeding of the 9th ACM Conference on Data and Application Security and Privacy (CODASPY 2019)
- C2 **Toffalini F.**, Sun J., and Ochoa M.  
 “Static Analysis of Context Leaks in Android Applications” Proceeding of the 40th International Conference on Software Engineering: Software Engineering in Practice (SEPA@ICSE)
- C1 **Toffalini F.**, Abba’ M., Carra D., and Balzarotti D.  
 “Google Dorks: Analysis, Creation, and new Defenses” Proceeding of the 13th International Conference of Detection of Intrusions, Malware, and Vulnerability Assessment, (DIMVA 2016)

## Workshop

- W6 Rusconi D., Zoia M., Buccioli L., Pierazzi F., Bruschi D., Cavallaro L., **Toffalini F.**, and Lanzi A.  
 “EmbedWatch: Fat Pointer Solution for Detecting Spatial Memory Errors in Embedded Systems” Proceeding of the 6th Workshop on CPS and IoT Security (CPSIoTSec)
- W5 Zheng H., **Toffalini F.**, and Payer M.  
 “TuneFuzz: Adaptively Exploring Target Programs” Proceeding of the 17th Intl. Workshop on Search-Based and Fuzz Testing (SBFT 2024)
- W4 Visintin A., **Toffalini F.**, Losiouk E., Conti M., and Zhou J.  
 “HolA: Holistic and autonomous attestation for IoT networks” Proceeding of the Applied Cryptography and Network Security Workshops (ACNS 2022) - **Best Paper**

- W3 **Toffalini F.**, Homoliak I., Harilal A., Binder A., and Ochoa M.  
“Detection of Masqueraders Based on Graph Partitioning of File System Access Events” Proceeding of IEEE Security and Privacy Workshops (SPW)
- W2 Harilal A., **Toffalini F.**, John C., Guarnizo J., Homoliak I., and Ochoa M.  
“TWOS: A Dataset of Malicious Insider Threat Behavior Based on Gamified Competition” Proceeding of the 9th ACM CCS International Workshop on Managing Insider Security Threats (MIST)
- W1 De Stefani F., Gamba P., Goldoni E., Savioli A., Silvestri D., and **Toffalini F.**  
“REnvDB, a RESTful Database for Pervasive Environmental Wireless Sensor Networks” Proceeding of the 30th IEEE International Conference on Distributed Computing Systems Workshops

### Journal

- J4 **Toffalini F.**, Oliveri A., Graziano M., Zhou J., and Balzarotti D.  
“The evidence beyond the wall: Memory forensics in SGX environments” Forensic Science International: Digital Investigation, 2021
- J3 Homoliak I., **Toffalini F.**, Guarnizo J., Elovici Y., and Ochoa M.  
“Insight Into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures” ACM Computing Surveys (CSUR), 2019
- J2 **Toffalini F.**, Sun J., and Ochoa M.  
“Practical static analysis of context leaks in Android applications” Software: Practice and Experience, 2019
- J1 Harilal A., **Toffalini F.**, Homoliak I., John C., Guarnizo J., Mondal S., and Ochoa M.  
“The Wolf Of SUTD (TWOS): A Dataset of Malicious Insider Threat Behavior Based on a Gamified Competition” Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 2018

### ACADEMIC SERVICE

---

NDSS reviewer 2022/23/24/25/26  
Usenix SEC 2025/26  
DIMVA reviewer 2022/23/24/25  
DIMVA poster chair 2024/25  
ACSAC reviewer 2024/25  
ISSTA reviewer 2024/25  
TOSEM reviewer 2024  
Usenix SEC AE reviewer 2022  
EuroSP shadow-reviewer 2020  
TIFS reviewer 2018/19

### OTHER ACTIVITES

---

Employee in IT Companies: 2009-2011  
Part-time Student during Master: 2012-2014