FLAVIO TOFFALINI

(+41) · 77 239 72 25 ⋄ flavio.toffalini@epfl.ch

My research interest covers many aspects of system security. My Ph.D. background focuses on software security for Trusted Execution Environment. In my current position, I am intensively working on automatic testing and mitigation applied to many system levels, from user-space to virtual devices.

CURRENT POSITION: POSTDOC IN THE HEXHIVE LABORATORY AT EPFL

École Polytechnique Fédérale de Lausanne (EPFL), Switzerland *Nov 2021 to Now*
PostDoc, supervised by Prof. Mathias Payer
Topic: fuzzing, mitigation, software analysis

EDUCATION

Singapore University of Technology and Design, Singapore *Jan 2017 - Sep 2021*
Ph.D., supervisor Prof. Jianying Zhou
Topic: trusted computing, system security
Thesis Title: Challenges, threats, and novel defenses for Trusted Execution Environments

University of Verona, Italy *Sep 2012 - Oct 2015*
M.S. in Computer Science and Engineering 108/110, GPA 3,9/4
Supervisor Prof. Damiano Carra
Master thesis topic: Google dorks, Web security

University of Pavia, Italy *Sep 2007 - Dec 2009*
B.S. in Computer Engineer 101/110, GPA 3,67/4
Supervisor Prof. Paolo Gamba

ACADEMIC ACTIVITIES

King's College London Nov 2019 - Mar 2020
Visiting fellow, supervised by Prof. Lorenzo Cavallaro *London, UK*
Topic: trusted computing, system security

University of Padua Jan 2018 - Aug 2018
Visiting fellow, supervised by Prof. Mauro Conti *Padua, Italy*
Topic: trusted computing, system security

University of Verona Dec 2015 - July 2016
Research Assistant, supervised by Prof. Fausto Spoto *Verona, Italy*
Topic: static analysis of Android applications

Eurecom April 2015 - July 2015
Visiting fellow, supervised by Prof. Davide Balzarotti *Biot, France*
Topic: Google dorks, Web security

PUBLICATIONS

Conference

[C1] Srivastava P., **Toffalini F.**, Vorobyov K., Gauthier F., Bianchi A., 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)

[C2] Zheng H., Zhang J., Huang Y., Ren Z., Wang H., Cao C., Zhang Y., **Toffalini F.**, Payer M.
"FishFuzz: Throwing Larger Nets to Catch Deeper Bugs" Proceeding of the 32nd USENIX Security Symposium (Usenix SEC 2023)

[C3] Xu J., Di Bartolomeo L., **Toffalini F.**, Mao B., Payer M.
"WarpAttack: Bypassing CFI through Compiler-Introduced Double-Fetches" Proceeding of the 44th IEEE Symposium on Security and Privacy (S&P 2023)

[C4] Liu Q., **Toffalini F.**, Zhou Y., Payer M.
"ViDeZZO: Dependency-aware Virtual Device Fuzzing" Proceeding of the 44th IEEE Symposium on Security and Privacy (S&P 2023)

[C5] **Toffalini F.**, Payer M., Zhou J., 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., Payer M.
"Evocatio: Conjuring Bug Capabilities from a Single PoC" Proceeding of the ACM SIGSAC Conference on Computer and Communications Security (CCS 2022)

[C7] **Toffalini F.**, Graziano M., Conti M., Zhou J.
"SnakeGX: a sneaky attack against SGX Enclaves" Proceeding of the 19th International Conference on Applied Cryptography and Network Security (ACNS 2022)

[C8] **Toffalini F.**, Losiouk E., Biondo A., Zhou J., 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)

[C9] **Toffalini F.**, Ochoa M., Sun J., 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)

[C10] **Toffalini F.**, Sun J., 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)

[C11] **Toffalini F.**, Abba' M., Carra D., 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

[W1] Zheng H., **Toffalini F.**, Payer M.
"TuneFuzz: Adaptively Exploring Target Programs" Proceeding of the 17th Intl. Workshop on Search-Based and Fuzz Testing (SBFT 2024)

[W2] **Toffalini F.**, Homoliak I., Harilal A., Binder A., Ochoa M.
"Detection of Masqueraders Based on Graph Partitioning of File System Access Events" Proceeding of IEEE Security and Privacy Workshops (SPW)

[W3] Harilal A., **Toffalini F.**, John C., Guarnizo J., Homoliak I., 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)

[W4] De Stefani F., Gamba P., Goldoni E., Savioli A., Silvestri D., **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

[J1] **Toffalini F.**, Oliveri A., Graziano M., Zhou J., Balzarotti D.
"The evidence beyond the wall: Memory forensics in SGX environments" Forensic Science International: Digital Investigation, 2021

[J2] Homoliak I., **Toffalini F.**, Guarnizo J., Elovici Y., Ochoa M.
"Insight Into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures" ACM Computing Surveys (CSUR), 2019

[J3] **Toffalini F.**, Sun J., Ochoa M.
"Practical static analysis of context leaks in Android applications" Software: Practice and Experience, 2019

[J4] Harilal A., **Toffalini F.**, Homoliak I., John C., Guarnizo J., Mondal S., 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

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