Flavio Toffalini

flavio_toffalini@mymail.sutd.edu.sg
+65 8341 0549

Objective

Collaborating with professional teams for overcoming Information Security limitations with integrity and ingenuity. My current research aims to improve DL for malware detection borrowing fresh idea from program analysis' world. Previously, the core of my Ph.D. stretches the security properties of trusted execution environments, in particular SGX, by integrating multiple disciplines from program analysis, deep learning, network protocols, and cryptography. The goal of my work is to combine different perspectives in order to design strong trustworthy systems for daily tasks.

Education

2017 present — **Ph.D. student in Computer Science**
Singapore University of Technology and Design (SUTD)
Supervisor: Prof. Jianying Zhou; Co-Advisor: Prof. Lorenzo Cavallaro & Prof. Mauro Conti.
5th year PhD programme with ISTD pillar studying the limitations of modern trusted execution environments.

2015 — **M.S. in Computer Science and Engineering 108/110, GPA 3,9/4**
University of Verona, IT
Supervisor: Prof. Damiano Carra; Co-Advisor: Prof. Davide Balzarotti
I wrote my thesis under the supervision of Prof. Carra Damiano and co-advised by Prof. Davide Blazarotti. The topic of my thesis expands the Google Dork project started in Eurecom (FR). From the final thesis version, we extracted a research paper entitled "Google Dorks: Analysis, Creation, and new Defenses" and published in DIMVA 2016.

2009 — **B.S. in Computer Engineer 101/110, GPA 3,67/4**
University of Pavia, IT
Supervisor: Prof. Paolo Gamba
I wrote my thesis under the supervision of Prof. Paolo Gamba. In the project, I studied new data acquisition techniques for IoT networks.

Visiting Research Scholar

2021 present — **Research Collaboration**
King's College London, UK
I collaborate with Prof. Lorenzo Cavallaro's Systems Security Research Lab on a Multi-Task Learning project. I investigate the challenges of using MTL classifiers for malware analysis. The goal is to detect fine-grained malicious behaviors linked to the MITRE ATT&CK classification.

Fall 2019 — **Visiting Ph.D. Scholar**
King's College London, UK
I collaborated with Prof. Lorenzo Cavallaro's Systems Security Research Lab on a project about the runtime integrity limitations of SGX enclaves. We designed and deployed a runtime remote attestation able to measure and validate the enclave execution-flow. Part of our outcome has been included in the publication "Revisiting Program Analysis and Intrusion Detection for SGX" which is currently under submission at CCS 2021.

2018 — **Visiting Ph.D. Scholar**
University of Padua, IT
I collaborated with Prof. Mauro Conti's Security and Privacy Research Group (SPRITZ Group). I studied the limitations of runtime remote attestations in complex software. Part of the outcome has been included in the publication "ScaRR: Scalable Runtime Remote Attestation for Complex Systems" and published in RAID 2019.

2015 — **Visiting fellow**
Eurecom, FR
I collaborated with Prof. Davide Balzarotti's System Security team on a Web security project focused on Google Dorks. The objective was the proposal of novel mitigation strategies and study automatic techniques for creating new Google Dorks.

Employment

2016-2017 **Research Assistant**
Singapore University of Technology and Design, SG
I worked on an Insider Threat project under the supervision of Prof. Ochoa Martìn and co-funded by ST Electronics (SG). The project's purpose was to study novel ML methodologies for detecting insider threats and developing secure monitoring agents based on trusted computing technologies.

2015-2016 **Research Assistant**
University of Verona, IT
I studied the limitations of static analysis in detecting context memory leaks in Android applications. The project was supervised by Prof. Fausto Spoto and co-funded by Julia Soft.

Professional Development

2021 **Deep Learning Specialization**
Coursera at deeplearning.ai
A six months class that covers many theoretical and practical aspects of Deep Learning: CNN, Transfer Learning, Object Detection, NLP, GRU, LSTM, Attentions Models, and Multi-Head. Furthermore, the course provided deep knowledge of the Tensorflow framework.

Selected Publications

2021 **Following the evidence beyond the wall: memory forensic in SGX environments**
F. Toffalini, *A. Oliveri, M. Graziano, J. Zhou, D. Balzarotti*
• under submission
We study the impact of memory forensic techniques in SGX machines, what information can be extracted and how to use them for analyzing modern SGX malware.

Revisiting Program Analysis and Intrusion Detection for SGX
F. Toffalini, *J. Zhou, L. Cavallaro*
• under submission
We propose a runtime remote attestation that measures the execution flow of an SGX enclave and allows a remote Verifier to validate the enclave runtime integrity. We test our approach against modern enclave code-reuse attacks.

SnakeGX: a sneaky attack against SGX Enclaves
F. Toffalini, *M. Graziano, M. Conti, J. Zhou*
ACNS • The 19th International Conference on Applied Cryptography and Network Security (ACNS)
We describe a data-only malware able to install a persistent backdoor in a running enclave. The backdoor leaves a privilege entrance for adversaries that can exfiltrate data in stealthy manner while leaving a limited footprint in memory. We compare the traces left with other state of the art attacks for SGX.

2019 **ScaRR: Scalable Runtime Remote Attestation for Complex Systems**
F. Toffalini, *E. Losiouk, Biondo A., J. Zhou, M. Conti*
RAID • The 22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID)
We describe a model for runtime remote attestation that can represent correct executions of complex software in a limited amount of memory. We compare our approach with state of the art runtime models and show our scalability properties.

Insight Into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures
I. Homoliak, **F. Toffalini**, *J. Guarnizo, Y. Elovici, M. Ochoa*
CSUR • ACM Computing Surveys (CSUR)
We study the state of the art of Insider Threats for IT. We identify common threats, propose a new taxonomy classification, and identify new challenges.

Careful-Packing: A Practical and Scalable Anti-Tampering Software Protection enforced by Trusted Computing
F. Toffalini, *M. Ochoa, J. Sun, and J. Zhou*
CODASPY · The 9th ACM Conference on Data and Application Security and Privacy (CODASPY)
We propose a combination of TEE and anti-tampering techniques to strengthen code integrity over untrusted memory regions while using a limited memory in the TEE modules. Our solution introduces a small overhead of around 5%.

2018 **Static Analysis of Context Leaks in Android Applications**
F. Toffalini, *M. Ochoa, J. Sun, and J. Zhou*
ICSE · The 40th International Conference on Software Engineering: Software Engineering in Practice (SEPA@ICSE)
We study the problem of context leak in Android application and propose a simple yet effective static analysis to find such errors.

Detection of Masqueraders Based on Graph Partitioning of File System Access Events
F. Toffalini, *I. Homoliak, A. Harilal, A. Binder, and M. Ochoa*
SPW · IEEE Security and Privacy Workshops (SPW)
We propose a novel detection, based on graph comparison, that spots anomaly activities in sequence of events. We apply our approach over two open source datasets, WUIL and TWOS, achieving an AUC over 0,94 and 0.85, respectively.

2017 **TWOS: A Dataset of Malicious Insider Threat Behavior Based on a Gamified Competition**
A. Harilal, **F. Toffalini**, *J. Castellanos, J. Guarnizo, I. Homoliak, and M. Ochoa*
MIST · The 9th ACM CCS International Workshop on Managing Insider Security Threats (MIST)
We present a dataset of insider threats obtained through a gamified competition that involved 6 teams of 4 students and that lasted for more than 300 hours. We designed the game in order to simulate realistic insider threats scenarios.

2016 **Google Dorks: Analysis, Creation, and new Defenses**
F. Toffalini, *M. Abba', D. Carra, and D. Balzarotti*
DIMVA · Detection of Intrusions and Malware, and Vulnerability Assessment The 13th International Conference, (DIMVA)
We study the impact of existing Google Dorks and proposed mitigation. In addition, we study new techniques to automatically generate new Google Dorks and propose relative mitigation.

References available upon request

- Prof. Janying Zhou (Ph.D. Supervisor) jianying_zhou@sutd.edu.sg
- Prof. Lorenzo Cavallaro (Ph.D co-advisor) lorenzo.cavallaro@kcl.ac.uk
- Prof. Mauro Conti (Ph.D. co-advisor) mauro.conti@unipd.it
- Prof. Davide Balzarotti (co-author) davide.balzarotti@eurecom.fr
- Mariano Graziano (co-author) magrazia@cisco.com

PC Member

- IEEE S&P (Shadow PC) 2021
- SecMT 2020, 2021

Reviewer

- EuroSec (subreviewer) 2021
- RAID (subreviewer) 2020
- USENIX Security (subreviewer) 2020
- ESORICS (subreviewer) 2018
- TIFS (subreviewer) 2018, 2019

Conference Volunteer

- ACM CCS 2019

Teaching Assistant

• Cyber Challenge Seminars	UNIPD	2020
• 50.039 Theory and Practice of Deep Learning	SUTD	2019
• 50.005 Computer System Engineering	SUTD	2019
• Informatics and Bioinformatics	UNIPD	2018

Other

- **MSc Co-supervision**: Mohamad Ridzuan Yusop, rebuilding ROP chains from Intel PT traces.
- **MSc Co-supervision**: Jon Kartago Lamida, comparing modern runtime remote attestations models.
- **MSc Co-supervision**: Alessandro Visintin, design novel remote attestation schemes for networks of IoT devices.