Christof Ferreira Torres

Contact Information

ETH Zurich, CAB F 74.1
Universitätstrasse 6
8092 Zurich
Switzerland

Cell: +41 44 632 09 67
Email: christof.torres@inf.ethz.ch
GitHub: github.com/christoftorres
Website: www.christoftorres.com

Research Interests

Smart contract security, distributed ledgers, browser fingerprinting, web privacy, fuzz testing, software and system security, static and dynamic analysis techniques

Education

Technical University of Munich, Munich, Germany

University of Luxembourg, Luxembourg, Luxembourg

Joint Ph.D. (Cotutelle), Computer Science **April 2018 – May 2022**

- Thesis: *From Smart to Secure Contracts: Automated Security Assessment and Improvement of Ethereum Smart Contracts*
- Graduation Date: *31.05.2022*
- Advisors: *Dr. Radu State* (University of Luxembourg) and *Dr. Claudia Eckert* (Technical University of Munich)

University of Luxembourg, Luxembourg, Luxembourg

M.Sc., Computer Science **September 2014 – September 2016**

- GPA: 4.0 (17.5/20.0)
- Thesis: *The Revival of Mining: Anonymised Micropayments via Mined Tickets*
- Advisors: *Dr. Alex Biryukov* and *Dr. Ivan Pustogarov* (Cornell University)

University of Luxembourg, Luxembourg, Luxembourg

B.Sc., Computer Science **September 2011 – July 2014**

- GPA: 3.7 (16.5/20.0)
- Thesis: *Fingerprint Privacy: A Fresh Perspective on Web Privacy*
- Advisors: *Dr. Sjouke Mauw* and *Dr. Hugo Jonker*

Professional Experience

ETH Zurich, Zurich, Switzerland **August 2022 – Present**
Postdoctoral Researcher, Secure & Trustworthy Systems Group (SECTRS)

- Group lead: Dr. Shweta Shinde
- Research on various topics related to trusted computing, system security, program analysis and formal verification.

University of Luxembourg, Luxembourg, Luxembourg **May 2022 – July 2022**
Postdoctoral Researcher, Services and Data Management Group (SEDAN)

- Group lead: Dr. Radu State
- Research on various topics related to distributed systems, blockchain and smart contracts.

Banque et Caisse d'Épargne de l'État, Luxembourg, Luxembourg **April 2018 – March 2022**
PhD Candidate, Software Development Department

- *Blockchain Development and Security Assessment:* Guidance and advice on blockchain security related topics including the security assessment and development of smart contracts.

Fraunhofer AISEC, Garching near Munich, Germany **October 2016 – March 2018**
Research Fellow, Service and Application Security Department

- *Mobile Payment Solution Security Assessment:* Security assessment and penetration testing of mobile payment applications (Android and iOS) with a focus on solutions implementing the Visa payment standards.

Selected Publications

Is Your Wallet Snitching On You? An Analysis on the Privacy Implications of Web3. **Christof Ferreira Torres**, Fiona Willi, Shweta Shinde. 32th USENIX Security Symposium, August 9-11, 2023 **(USENIX'23)**

A Flash(bot) in the Pan: Measuring Maximal Extractable Value in Private Pools Ben Weintraub, **Christof Ferreira Torres**, Cristina Nita-Rotaru, Radu State. 22nd ACM Internet Measurement Conference, October 25-27, 2022 **(IMC'22)**

Elysium: Context-Aware Bytecode-Level Patching to Automatically Heal Vulnerable Smart Contracts. **Christof Ferreira Torres**, Hugo Jonker, Radu State. 25th International Symposium on Research in Attacks, Intrusions and Defenses, October 26-28, 2022 **(RAID'22)**

Frontrunner Jones and the Raiders of the Dark Forest: An Empirical Study of Frontrunning on the Ethereum Blockchain. **Christof Ferreira Torres**, Ramiro Camino, Radu State. 30th USENIX Security Symposium, August 11-13, 2021 **(USENIX'21)**

ConFuzzius: A Data Dependency-Aware Hybrid Fuzzer for Smart Contracts. **Christof Ferreira Torres**, Antonio Ken Iannillo, Arthur Gervais, Radu State. 6th IEEE European Symposium on Security and Privacy, October 7–22, 2021 **(EuroS&P'21)**

The Eye of Horus: Spotting and Analyzing Attacks on Ethereum Smart Contracts. **Christof Ferreira Torres**, Antonio Ken Iannillo, Arthur Gervais, Radu State. 25th International Conference on Financial Cryptography and Data Security, March 1–5, 2021 **(FC'21)**

High-Frequency Trading on Decentralized On-Chain Exchanges. Liyi Zhou, Kaihua Qin, **Christof Ferreira Torres**, Duc V Le, Arthur Gervais. 42nd IEEE Symposium on Security and Privacy, May 23-27, 2021 **(S&P'21)**

ÆGIS: Shielding Vulnerable Smart Contracts Against Attacks. **Christof Ferreira Torres**, Mathis Baden, Robert Norvill, Beltran Fiz Pontiveros, Hugo Jonker, Sjouke Mauw. 15th ACM Asia Conference on Computer and Communications Security, October 5–9, 2020 **(AsiaCCS'20)**

ÆGIS: Smart Shielding of Smart Contracts (Poster). **Christof Ferreira Torres**, Mathis Baden, Robert Norvill, Hugo Jonker. 26th ACM Conference on Computer and Communications Security, November 11-15, 2019 **(CCS'19)**

The Art of The Scam: Demystifying Honeypots in Ethereum Smart Contracts. **Christof Ferreira Torres**, Mathis Steichen, Radu State. 28th USENIX Security Symposium, August 14-16, 2019 **(USENIX'19)**

Osiris: Hunting for Integer Bugs in Ethereum Smart Contracts. **Christof Ferreira Torres**, Julian Schütte, Radu State. 34th Annual Computer Security Applications Conference, December 3-7, 2018 **(ACSAC'18)**

Investigating Fingerprinters and Fingerprinting-Alike Behaviour of Android Applications. **Christof Ferreira Torres**, Hugo Jonker. 23rd European Symposium on Research in Computer Security, September 3-7, 2018 **(ESORICS'18)**

FP-Block: Usable Web Privacy by Controlling Browser Fingerprinting. **Christof Ferreira Torres**, Hugo Jonker, Sjouke Mauw. 20th European Symposium on Research in Computer Security, September 21-25, 2015 **(ESORICS'15)**

Awards and Grants

2022 Excellent Doctoral Thesis (Award)
Awarded every year by the doctoral schools of the University of Luxembourg to the best 10% doctoral candidates to acknowledge their outstanding thesis projects.

2022 UBRI Impact (Award)
Awarded by a jury of internationally renowned professors (elected by the Ripple Foundation) as part of the Ripple University Blockchain Research Initiative (UBRI) for outstanding contributions in the field of blockchain research.

2019 Luxembourg's Most Promising Young Talent (Award)
Awarded by the Luxembourgish government for coaching the Luxembourgish national cybersecurity team during the European Cybersecurity Challenge (ECSC) in Bucharest, Romania.

2018 FNR Industrial Fellowship (Grant)
Obtained funding for the entire period of the PhD by the Luxembourgish National Research Fund (FNR) for carrying out research on secure blockchain technologies for the financial sector.

2016 Top Student (Award)
Awarded by the University of Luxembourg as one of the best students of the Faculty of Science, Technology and Communication.

Academic Services

Technical Program Committee (TPC) member
IEEE ICBC 2019, IEEE ICBC 2020, IEEE ICBC 2021, BLOCKCHAIN 2021, BLOCKCHAIN 2022,

IEEE ICBC 2022, IEEE ICBC 2023

External Reviewer
ESORICS 2019, ESORICS 2020, ACNS 2021, ISSRE 2021, IEEE EuroS&P 2022, IEEE EuroS&P 2023, IEEE S&P 2023

Artifact Evaluation Committee (AEC) member
ACSAC 2022, USENIX Security 2022, USENIX Security 2023

Teaching Experience

252-0833-00L Computer Science II
Teaching Assistant (TA), Spring Semester 2023

252-0217-00L Computer Systems
Teaching Assistant (TA), Autumn Semester 2022

Thesis Mentoring

Data Flow Analysis of EVM Smart Contracts
Master Thesis, Ece Kubilay, Technical University of Munich, 2018

Invited Talks

A Journey on Smart Contract Security: A Story of Glory and Greed
Secure & Trustworthy Systems Group, ETH Zurich, Switzerland, November 2021

The Art of The Scam: Demystifying Honeypots in Ethereum Smart Contracts
Ripple UBRI Connect 2019, University of Berkeley, Berkeley, CA, USA, October 2019
Digital Security Lunch Colloquium, Radboud University, Nijmegen, Netherlands, July 2019

Investigating Fingerprinters and Fingerprinting-alike Behaviour of Android Applications
Digital Security Lunch Colloquium, Radboud University, Nijmegen, Netherlands, August 2018

Relevant Skills

Programming Languages: Python, JavaScript, Java, C
Security Analysis: symbolic execution (Z3), taint analysis, logic-driven analysis (Datalog/Soufflé)

Languages

Portuguese: Native Speaker
French: Proficient (C1)
Luxembourgish: Fluent (C2)
English: Fluent (C2)
German: Fluent (C2)
Dutch: Beginner (A1)