Marcel **Busch**

marcel.busch@epfl.ch | @0ddcode

Education

University of Erlangen-Nürnberg (FAU) — *Erlangen, DE*

PhD in Computer Science (cum laude – GPA 1.0) — *Spring 2016 - Fall 2020*

- Thesis: "On the Security of ARM TrustZone-Based Trusted Execution Environments"

University of Erlangen-Nürnberg (FAU) — *Erlangen, DE*

Master of Science in Computer Science (with honors – GPA 1.0) — *Spring 2013 - Spring 2016*

Technische Hochschule Ingolstadt — *Ingolstadt, DE*

Bachelor of Science in Information Systems (GPA 1.4) — *Fall 2009 - Spring 2013*

Experience

HexHive, École Polytechnique Fédérale de Lausanne (EPFL) — *Lausanne, CH*

Postdoctoral Researcher — *Spring 2021 - now*

- Advisor: Mathias Payer
- Research on mobile device sofware and firmware security.
- Advanced automated testing and vulnerability discovery targeting embedded devices.
- Co-supervision and mentoring of PhD students.

IT Security Infrastructures Lab, Friedrich-Alexander University Erlangen-Nürnberg — *Erlangen, DE*

Postdoctoral Researcher — *Winter 2020 - Spring 2021*

- Advisor: Felix Freiling
- Research on rehosting of proprietary TrustZone-based Trusted Execution Environments (TEEs).
- Hosting of challenged-based and A/D CTFs on web security and kernel exploitation.
- Supervision and mentoring of bachelor's and master's theses.

IT Security Infrastructures Lab, Friedrich-Alexander University Erlangen-Nürnberg — *Erlangen, DE*

Ph.D. in Computer Science — *Spring 2016 - Winter 2020*

- Advisor: Felix Freiling
- Research on the security of TEEs on mobile devices.
- Integration of TEEs with optical network elements by Nokia as part of the *SENDATE-TANDEM* project.
- Acquisition and management of a ~100k EUR grant to investigate the security of TEEs as part of the *SoftwareCampus*.
- Supervision and mentoring of bachelor's and master's theses.

SecLab, University of California in Santa Barbara (UCSB) — *Santa Barbara, US*

Visiting Researcher — *Spring 2018 - Winter 2018*

- Advisors: Christopher Kruegel and Giovanni Vigna
- Analysis of proprietary TEEs on Android.
- Black-box fuzzing of propiretary Trusted Applications.
- Peripheral isolation on deeply embedded systems using TrustZone-M.

Siemens AG — *Erlangen, DE & Orlando, US*

Dual Study Programme — *Spring 2009 - Spring 2013*

- Internships with several departments during the practical semester and semester breaks of my bachelor's program.
- Evaluation of hybrid app development frameworks as part of the *Center of Expertise for Mobile*.
- Various development tasks including technologies like Excel VBA, SAP ERP, MS IIS, MSSQL, Android, and iOS.

Honors & Awards

Academic

2024	**WOOT@USENIX Best Paper**, "Exploiting Android's Hardened Memory Allocator".	*Philadelphia, US*
2024	**BAR@NDSS Best Paper**, "SURGEON: Performant, Flexible, and Accurate Re-Hosting via Transplantation".	*San Diego, US*
2020	**WOOT@USENIX Best Paper**, "Unearthing the TrustedCore: A Critical Review on Huawei's TEE".	*Virtual*
2020	**EAI ICDF2C Best Paper**, "Make Remote Forensic Investigations Forensic Again".	*Virtual*
2019	**SysTEX@SOSP Best Paper**, "TEEMo: Trusted Peripheral Monitoring for Optical Networks and Beyond".	*Huntsville, CA*
2019	**Software Campus Grant**, ~100k EUR for outstanding academic achievements and entrepreneurial spirit.	*Berlin, DE*
2016	**ASQF Förderpreis**, Master thesis award for outstanding academic performance.	*Erlangen, DE*
2014	**Deutschlandstipendium**, Scholarship for outstanding academic performance.	*Erlangen, DE*
2013	**Deutschlandstipendium**, Scholarship for outstanding academic performance.	*Erlangen, DE*

IT-Security Competitions

2018 '19 '22 '24	**Finalist**, DEFCON {26, 27, 30, 32}th CTF Hacking Competition World Finals	*Las Vegas, US*
2024	**2nd Place (Academic Teams)**, Insomni'Hack CTF	*Lausanne, CH*
2018 '19	**Finalist**, 12th and 13th Russian National Open Student Information Security Championship RUCTF	*Yekaterinburg, RU*
2018	**Finalist**, Tencent CTF 2018	*Shenzhen, CN*

Acknowledged Vulnerabilities as Common Vulnerabilities and Exposures (CVEs)

Intel	CVE-2022-38787, CVE-2023-49614, CVE-2023-22327, CVE-2024-22390
MediaTek	CVE-2023-32834, CVE-2023-32835, CVE-2023-32848, CVE-2024-20078
Others	CVE-2019-10561 (Qualcomm), CVE-2023-31339 (AMD), CVE-2023-49100 (ARM TFA), CVE-2024-20881 (Samsung)

Technical Program Committees

2025	**Reviewer**, USENIX Security Symposium (SEC)
2024	**Reviewer**, Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)
2024	**Reviewer**, Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)
2023	**Reviewer**, Conference on Computer and Communications Security (CCS)
2023	**Reviewer**, Network and Distributed System Security Symposium (NDSS)
2022	**Reviewer**, International Symposium on Research and Attacks (RAID)
2022	**Reviewer**, Digital Forensics Research Workshop (DFRWS) EU
2021	**Reviewer**, International Symposium on Research and Attacks (RAID)

Extracurricular Activity

2024	**Speaker**, BlackAlps, Talk: "GlobalConfusion: TrustZone Trusted Application 0-Days by Design".	*Yverdon, CH*
2024	**Speaker**, Hardwear.io NL, Talk: "EL3XIR: Fuzzing COTS Secure Monitors".	*Amsterdam, NL*
2024	**Speaker**, 3rd Huawei Paris Workshop on Building Open Trust Systems, Talk: "Spill the TeA: An Empirical Study of Trusted Application Rollback Prevention on Android Smartphones".	*Paris, FR*
2023	**Speaker**, Hardwear.io NL, Talk: "TEEzz: Fuzzing Trusted Applications on COTS Android Devices".	*Den Haag, NL*
2016-2021	**Co-Founder**, FAUST CTF, Co-founded and co-organized the FAUST Attack-Defense CTF competition.	*Erlangen, DE*

Selected Publications

[1] Marcel Busch, Philipp Mao, and Mathias Payer. "GlobalConfusion: TrustZone Trusted Application 0-Days by Design". In: 33th USENIX Security Symposium (USENIX Security). 2024.

[2] Marcel Busch, Philipp Mao, and Mathias Payer. "Spill the TeA: An Empirical Study of Trusted Application Rollback Prevention on Android Smartphones". In: 33th USENIX Security Symposium (USENIX Security). 2024.

[3] Florian Hofhammer, Marcel Busch, Qinying Wang, Manuel Egele, and Mathias Payer. "SURGEON: Performant, Flexible, and Accurate Re-Hosting via Transplantation". In: Workshop on Binary Analysis Research (BAR'24). 2024.

[4] Christian Lindenmeier, Mathias Payer, and Marcel Busch. "EL3XIR: Fuzzing COTS Secure Monitors". In: 33th USENIX Security Symposium (USENIX Security). 2024.

[5] Philipp Mao, Elias Valentin Boschung, Marcel Busch, and Mathias Payer. "Exploiting Android's Hardened Memory Allocator". In: 18th USENIX WOOT Conference on Offensive Technologies (WOOT) co-located with the 33rd USENIX Security Symposium (USENIX Security). 2024.

[6] Marcel Busch, Aravind Machiry, Chad Spensky, Giovanni Vigna, Christopher Kruegel, and Mathias Payer. "TEEzz: Fuzzing Trusted Applications on COTS Android Devices". In: 44th IEEE Symposium on Security and Privacy (S&P). 2023.

[7] Marcel Busch, Johannes Westphal, and Tilo Müller. "Unearthing the TrustedCore: A Critical Review on Huawei's Trusted Execution Environment". In: 14th USENIX Workshop on Offensive Technologies (WOOT) co-located with the 29th USENIX Security Symposium (USENIX Security). 2020.

[8] Marcel Busch, Florian Nicolai, Fabian Fleischer, Christsian Rückert, Christoph Safferling, and Felix Freiling. "Make Remote Forensic Investigations Forensic Again: Increasing the Evidential Value of Remote Forensic Investigations". In: International Conference on Digital Forensics and Cyber Crime (EAI ICDF2C). 2020.

[9] Marcel Busch, Ralph Schlenk, and Hans Heckel. "TEEMo: Trusted Peripheral Monitoring for Optical Networks and Beyond". In: Proceedings of the 4th Workshop on System Software for Trusted Execution (SysTEX) co-located with the 27th ACM Symposium on Operating Systems Principles (SOSP). 2019.