# Marcel **Busch**

*Lehrstuhl für Informatik 1, Martensstraße 3, 91058 Erlangen, Germany*

(+49) 151-46626301  |  marcel.busch@cs.fau.de

## **Edu**cation

### **University of Erlangen-Nürnberg (FAU)**                                      *Erlangen, Germany*

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, Germany*

MASTER OF SCIENCE IN COMPUTER SCIENCE (WITH HONORS – GPA 1.0)                        *Spring 2013 - Spring 2016*

- Thesis: "Android Application Protection Reinforced by Off-Device Ahead of Time Compilation"

### **Technische Hochschule Ingolstadt**                                           *Ingolstadt, Germany*

BACHELOR OF SCIENCE IN INFORMATION SYSTEMS (GPA 1.4)                                 *Spring 2009 - Spring 2013*

## **Exp**erience

### **Friedrich-Alexander University Erlangen-Nürnberg**                           *Erlangen, Germany*

POSTDOCTORAL RESEARCHER                                                              *Winter 2020 - now*

- Research on rehosting of proprietary Trusted Execution Environments.
- Coordinator for seminar course on academic writing.
- Supervision and mentoring of bachelor's and master's theses.

### **Friedrich-Alexander University Erlangen-Nürnberg**                           *Erlangen, Germany*

PH.D. IN COMPUTER SCIENCE                                                            *Spring 2016 - Winter 2020*

- Integration of Trusted Execution Environments 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 Trusted Execution Environments as part of the *SoftwareCampus*.
- Supervision and mentoring of bachelor's and master's theses.

### **University of California in Santa Barbara**                                  *Santa Barbara, CA, USA*

VISITING RESEARCHER                                                                  *Winter 2018 - Spring 2018*

- Analysis of proprietary Trusted Execution Environments on Android.
- Black-box fuzzing of trusted applications.

### **Siemens AG**                                                                 *Erlangen, Germany*

WORKING STUDENT                                                                      *Spring 2013 - Spring 2016*

- Evaluation of hybrid app development frameworks as part of the *Center of Expertise for Mobile*.
- Development of native apps for Android and iOS.

### **Institute for Applied Research Ingolstadt**                                  *Ingolstadt, Germany*

STUDENT RESEARCH ASSISTANT                                                           *Summer 2011 - Winter 2012*

- Implementation of parallel sort algorithms in C.
- Automation of performance evaluations.

### **Technische Hochschule Ingolstadt**                                           *Ingolstadt, Germany*

TEACHING ASSISTANT                                                                   *Spring 2010 - Fall 2011*

- Provided weekly tutoring for undergraduates.
- Topics: linear algebra and programming in C.

### **Siemens AG**                                               *Erlangen, Germany & Orlando, FL, USA*

DUAL STUDY PROGRAMME                                                                 *Spring 2009 - Spring 2013*

- Interned with several departments during the practical semester and semester breaks of my bachelor's program.
- Various development tasks including technologies like Excel VBA, SAP ERP, MS IIS, MSSQL, Android, and iOS.

## **Hon**ors & Awards

ACADEMIC

| 2020 | **WOOT@USENIX Best Student Paper Award**, Paper title: "Unearthing the TrustedCore: A Critical Review on Huawei's Trusted Execution Environment". | *Virtual Conference* |
| 2020 | **EAI ICDF2C Best Paper Award**, Paper title: "Make Remote Forensic Investigations Forensic Again: Increasing the Evidential Value of Remote Forensic Investigations". | *Virtual Conference* |
| 2019 | **SysTEX@SOSP Best Paper Award**, Paper title: "TEEMo: Trusted Peripheral Monitoring for Optical Networks and Beyond". | *Huntsville, Ontario, Canada* |
| 2019 | **Software Campus Grant**, ~100k EUR grant for outstanding academic achievements and innovative entrepreneurial spirit. | *Berlin, Germany* |
| 2016 | **ASQF Förderpreis**, Master thesis award for outstanding academic performance. | *Erlangen, Germany* |
| 2014 | **Deutschlandstipendium**, Scholarship for outstanding academic performance. | *Erlangen, Germany* |
| 2013 | **Deutschlandstipendium**, Scholarship for outstanding academic performance. | *Erlangen, Germany* |

## HACKING COMPETITIONS

| 2019 | **Finalist**, DEFCON 27th CTF Hacking Competition World Final | *Las Vegas, U.S.A* |
| 2019 | **Finalist**, XIII Russian National Open Student Information Security Championship RUCTF 2019 | *Yekaterinburg, Russia* |
| 2018 | **Finalist**, DEFCON 26th CTF Hacking Competition World Final | *Las Vegas, U.S.A* |
| 2018 | **Finalist**, XII Russian National Open Student Information Security Championship RUCTF 2018 | *Yekaterinburg, Russia* |
| 2018 | **Finalist**, Tencent CTF 2018 | *Shenzhen, China* |

# **Ext**racurricular Activity

**FAUST (FAU Security Team)**                                                              *Erlangen, Germany*
CORE MEMBER                                                                                *Fall 2013 - PRESENT*
- Active participation in capture-the-flag competitions with a focus on reversing and pwning challenges.
- Hosted weekly capture-the-flag competition preparation sessions.
- Co-founded and co-organized the FAUST Attack-Defense CTF competition.

**FAUDroids**                                                                              *Erlangen, Germany*
DEVELOPER                                                                                   *Summer 2015 - Spring 2016*
- Challenge of designing, developing, and publishing one Android app per month for one year.
- The apps MyAdvent and Werewolf were commercialized and can be found on app stores.

# **Pub**lications

[1] Marcel Busch and Kalle Dirsch. "Finding 1-Day Vulnerabilities in Trusted Applications using Selective Symbolic Execution". In: Proceedings of the 3rd Workshop on Binary Analysis Research (BAR) co-located with the 27th Network and Distributed System Security Symposium (NDSS). 2020.

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

[3] 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.

[4] Fabian Fleischer, Marcel Busch, and Phillip Kuhrt. "Memory Corruption Attacks within Android TEEs: A Case Study Based on OP-TEE". In: Proceedings of the International Workshop on Security of Mobile Applications (IWSMA) co-located with the 15th International Conference on Availability, Reliability and Security (ARES). 2020.

[5] Chad Spensky, Aravind Machiry, Marcel Busch, Kevin Leach, Rick Housley, Christopher Kruegel, and Giovanni Vigna. "TRUST. IO: Protecting Physical Interfaces on Cyber-physical Systems". In: Proceedings of the 8th IEEE Conference on Communications and Network Security (IEEE CNS). 2020.

[6] 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.

[7] Marcel Busch, Mykolai Protsenko, and Tilo Müller. "A Cloud-Based Compilation and Hardening Platform for Android Apps". In: Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES). ACM, 2017.

[8] Markus Meyer, Helge Janicke, Peter Trapp, Christian Facchi, and Marcel Busch. "Performance Simulation of a System's Parallelization". In: Proceedings of the 6th International Conference on Software Engineering Advances (ICSEA). IARIA, 2011.