Dr. Andreas Weichslgartner

Tulpenstr. 15
90439 Nürnberg
Germany
☎ +49-176-64059039
✉ weichslgartner@gmail.com

Resume

Experience

5.2017-now **Senior Technical Security Engineer**, *CARIAD SE(2020-now)/Audi AG(2017-2020)*, Ingolstadt, Germany.
Designed and implemented an embedded machine-learning-based intrusion detection system (IDS) prototype in **C/C++/Tensorflow/Scikit-Learn/Numpy** for detecting anomalies in POSIX systems and automotive networks (**CAN, Ethernet**). Performed data analysis of network data, Linux audit files, security risk analysis, vulnerability management research in **Python/Pandas/Polars**. Was the lead developer/architect in an **agile team (SCRUM)** to design and implement the **series automotive software** of infotainment IDS in **C++** in for the upcoming Premium Platform Electric of the VW Group. Pushed continous fuzz testing and security testing inside Cariad as technical expert. Worked on research projects like ML-based **fuzzing**, **adversarial attacks on LiDAR**, or **embedded post quantum cryptography**. Was involved in several penetration-test activities and held internal workshops (e.g., secure coding, fuzzing, ML in security), gave talks (e.g., FuzzCon 22, ELIV 19), and participated in panel discussions (e.g., Cariad Security Summit). Supervised PhD/Master students and interns.

9.2010-4.2017 **Researcher at the Department of Hardware/Software Co-Design**, *Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)*, Erlangen, Germany.
Conducted research on optimization, real-time/embedded systems, security, software (**Java, Python, C**) and hardware (**VHDL**) development. Collaborated in a transregional research center with 60 international researchers on future many-core architectures. (Co)authored various peer-reviewed research papers at international conferences (23 papers, e.g., CODES+ISSS, DATE, DAC), leading journals (9 articles, e.g., ACM TECS, IEEE TCAD), and a book. Acted as a member of a program committee (ReConFig) and reviewer for several conferences/journals. Supervised students' theses and was involved in teaching (e.g., foundations of technical computer science, design of interactive embedded systems).

9.2009-1.2010 **Internship: Embedded Linux and Waver Testing**, *Infineon Technologies AG*, Regensburg, Germany.
Developed an embedded Linux solution for intrinsic data monitoring of wafer testing machines. Included a C program for real-time logging/filtering of raw machine data and a web interface/dashboard.

2003-2004 **Civil Service (Zivildienst)**, *Kreiskrankenhaus Kelheim*, Kelheim, Germany.

Education

2010-2017 **PhD (Dr.-Ing.) in Computer Science at the Department of Hardware/Software Co-Design**, *Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)*, Erlangen, Germany.

Thesis Application Mapping Methodologies for Invasive NoC-Based Architectures (Grade 1.1)

2004-2010 **Diploma (Dipl.-Ing.) in Information and Communication Technology**, *Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)*, Erlangen, Germany (Grade 1.3).

Software Skills

Languages ○ Python (experienced), C++ (experienced), C (experienced), Java (intermediate), Rust (intermediate)
Technology ○ Git (experienced), CI/CD: GH Actions, Gitlab, Jfrog (experienced), Docker (intermediate),

Selected Publications

- J. Urfei, F. Smirnov, A. Weichslgartner, S. Wildermann: Gradient-free Adversarial Attacks on 3D Point Clouds from LiDAR Sensors. Machine Learning and Optimization Techniques for Automotive Cyber-Physical Systems, 1st ed., Springer, 2023.
- A. Weichslgartner: Embedded Intrusion Detection based on AI. In Proceedings of Electronics In Vehicles (ELIV), pp. 1-10. VDI. 2019.
- A. Weichslgartner, et al.: Invasive Computing for Mapping Parallel Programs to Many-Core Architectures. Pages 1-185. Springer Singapore. 2018.
- A. Weichslgartner, et al.: Design-Time/Run-Time Mapping of Security-Critical Applications in Heterogeneous MPSoCs. In Proceedings of SCOPES, pp. 153-162. 2016.

Languages

German (native), English (full professional proficiency), Portuguese (limited working proficiency)

Links

Google Scholar, Blog, Github, Linkedin,