Robert Schilling

Summary

I am a security researcher focusing on secure code execution in the presence of physical attacks and currently obtaining my Ph.D. in the Secure Systems (SESYS) group under Prof. Stefan Mangard. My research aims to build general-purpose computing architectures with strong security capabilities by modifying and extending the processor. In particular, my research addresses the development of countermeasures against fault attacks and, when possible, easing the adoption of the developed techniques by providing compiler support, e.g., with LLVM integration.

Work experience

Apr. 2023 - present **Security Architecture**, *Rivos Inc.*, Graz, Austria

Apr. 2019 - April 2023 **University Assistant**, *Graz University of Technology*, Graz, Austria
- Research related to secure code execution in the presence of physical attacks
- Teaching of bachelor and master courses
  - Computer Organization and Networks
  - Digital System Design

Apr. 2016 - Mar. 2019 **Research Assistant**, *Know-Center GmbH*, Graz, Austria
Research related to secure code execution in the presence of physical attacks

Feb. 2015 - Jul. 2015 **Student Researcher**, *Graz University of Technology*, Graz, Austria
Hardware development of secure systems

May 2010 - Jan. 2015 **Software Developer**, *NXP Semiconductors Austria GmbH*, Gratkorn, Austria
Lead development for automated measurement systems used for NFC-IC verification

Sept. 2009 – Mar. 2010 **Austrian army service**, *Bundesministerium für Landesverteidigung und Sport*, Gratkorn, Austria

Jul. 2008 **Internship - Mechanical Department**, *Knapp AG*, Hart bei Graz, Austria

Jul. 2007 **Internship - Electrical Department**, *ThyssenKrupp Austria Gmbh*, Gratkorn, Austria

Aug. 2006 **Internship - Electrical Department**, *ThyssenKrupp Austria Gmbh*, Gratkorn, Austria

Education

Apr. 2016 - Sept. 2023 **PhD Programme**, *Graz University of Technology*, Graz, Austria
Hardware Extensions and Compiler Support for Protection Against Fault Attacks

Aug. 2015 - Feb. 2016 **Master Thesis**, *ETH Zurich*, Zurich, Switzerland
"Securing the Communication- and Memory-Interfaces of a Multi-Core Cluster"

schilling.ro@gmail.com • *www.rschilling.net*

Mar. 2014 - Apr. 2016 **Master of Science**, *Graz University of Technology*, Graz, Austria
Telematik (Information and computer engineering)
- Digital Signal Processing
- System-on-Chip Design

Oct. 2010 - Mar. 2014 **Bachelor of Science**, *Graz University of Technology*, Graz, Austria
Telematik (Information and computer engineering)
- Bachelor Thesis: "Automized NFC Compliance Testbench"

Sept. 2004 - July 2009 **Matura**, *Höhere technische Bundeslehranstalt Kaindorf*, Kaindorf, Austria, Department for mechanical engineering and automation

Scholarships and Grants

2015 **Scholarship of Excellence**, *Industriellenvereinigung Kärnten*

2015 **Scholarship Grant**, *Graz University of Technology*

2015 **Research Abroad Stipendium** , *Graz University of Technology*

2011, 2012, 2015 **Scholarship of Excellence**, *Graz University of Technology*

Personal skills

German mother tongue

English fluent, written and spoken

Languages
- C, C++
- Python
- Ruby
- (System)-Verilog, VHDL

Operating systems
- Linux (Ubuntu/Debian)
- Mac OS X
- Microsoft Windows

Tools
- LLVM
- GitLab (CI)
- GitHub
- git

Publications

Martin Unterguggenberger, David Schrammel, Pascal Nasahl, Robert Schilling, Lukas Lamster, and Stefan Mangard. Multi-tag: A hardware-software co-design for memory safety based on multi-granular memory tagging. In Joseph K. Liu, Yang Xiang, Surya Nepal, and Gene Tsudik, editors, *Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security, ASIA CCS 2023, Melbourne, VIC, Australia, July 10-14, 2023*, pages 177–189. ACM, 2023.

Pascal Nasahl, Martin Unterguggenberger, Rishub Nagpal, Robert Schilling, David Schrammel, and Stefan Mangard. SCFI: state machine control-flow hardening against fault attacks. In *Design, Automation & Test in Europe Conference & Exhibition, DATE 2023, Antwerp, Belgium, April 17-19, 2023*, pages 1–6. IEEE, 2023.

Robert Schilling, Pascal Nasahl, Martin Unterguggenberger, and Stefan Mangard. SFP: providing system call flow protection against software and fault attack. In

Jakub Szefer, editor, *Hardware and Architectural Support for Security and Privacy , HASP 2022, Chicago, USA*.

Robert Schilling, Pascal Nasahl, and Stefan Mangard. FIPAC: thwarting fault- and software-induced control-flow attacks with ARM pointer authentication. In Josep Balasch and Colin O'Flynn, editors, *Constructive Side-Channel Analysis and Secure Design - 13th International Workshop, COSADE 2022, Leuven, Belgium, April 11-12, 2022, Proceedings*, volume 13211 of *Lecture Notes in Computer Science*, pages 100–124. Springer, 2022.

Pascal Nasahl, Robert Schilling, Mario Werner, and Stefan Mangard. HECTOR-V: A heterogeneous CPU architecture for a secure RISC-V execution environment. In Jiannong Cao, Man Ho Au, Zhiqiang Lin, and Moti Yung, editors, *ASIA CCS '21: ACM Asia Conference on Computer and Communications Security, Virtual Event, Hong Kong, June 7-11, 2021*, pages 187–199. ACM, 2021.

Pascal Nasahl, Robert Schilling, Mario Werner, Jan Hoogerbrugge, Marcel Medwed, and Stefan Mangard. Cryptag: Thwarting physical and logical memory vulnerabilities using cryptographically colored memory. In Jiannong Cao, Man Ho Au, Zhiqiang Lin, and Moti Yung, editors, *ASIA CCS '21: ACM Asia Conference on Computer and Communications Security, Virtual Event, Hong Kong, June 7-11, 2021*, pages 200–212. ACM, 2021.

Robert Schilling, Pascal Nasahl, Stefan Weiglhofer, and Stefan Mangard. Secwalk: Protecting page table walks against fault attacks. In *IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2021, Tysons Corner, VA, USA, December 12-15, 2021*, pages 56–67. IEEE, 2021.

Pascal Nasahl, Robert Schilling, and Stefan Mangard. Protecting indirect branches against fault attacks using ARM pointer authentication. In *IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2021, Tysons Corner, VA, USA, December 12-15, 2021*, pages 68–79. IEEE, 2021.

Michael Schwarz, Moritz Lipp, Claudio Canella, Robert Schilling, Florian Kargl, and Daniel Gruss. Context: A generic approach for mitigating spectre. In *27th Annual Network and Distributed System Security Symposium, NDSS 2020, San Diego, California, USA, February 23-26, 2020*. The Internet Society, 2020.

Mario Werner, Robert Schilling, Thomas Unterluggauer, and Stefan Mangard. Protecting RISC-V processors against physical attacks. In Jürgen Teich and Franco Fummi, editors, *Design, Automation & Test in Europe Conference & Exhibition, DATE 2019, Florence, Italy, March 25-29, 2019*, pages 1136–1141. IEEE, 2019.

Anja F. Karl, Robert Schilling, Roderick Bloem, and Stefan Mangard. Small faults grow up - verification of error masking robustness in arithmetically encoded programs. In *Verification, Model Checking, and Abstract Interpretation - 20th International Conference, VMCAI 2019, Cascais, Portugal, January 13-15, 2019, Proceedings*, pages 183–204, 2019.

Robert Schilling, Mario Werner, Pascal Nasahl, and Stefan Mangard. Pointing in the right direction - securing memory accesses in a faulty world. In *Proceedings of the 34th Annual Computer Security Applications Conference, ACSAC 2018, San Juan, PR, USA, December 03-07, 2018*, pages 595–604, 2018.

Robert Schilling, Thomas Unterluggauer, Stefan Mangard, Frank K. Gürkaynak, Michael Muehlberghuber, and Luca Benini. High speed ASIC implementations of leakage-resilient cryptography. In *2018 Design, Automation & Test in Europe Conference & Exhibition, DATE 2018, Dresden, Germany, March 19-23, 2018*, pages 1259–1264, 2018.

Robert Schilling, Mario Werner, and Stefan Mangard. Securing conditional branches in the presence of fault attacks. In *2018 Design, Automation & Test in Europe Conference & Exhibition, DATE 2018, Dresden, Germany, March 19-23, 2018*, pages 1586–1591, 2018.

Francesco Conti, Robert Schilling, Pasquale Davide Schiavone, Antonio Pullini, Davide Rossi, Frank Kagan Gürkaynak, Michael Muehlberghuber, Michael Gautschi, Igor Loi, Germain Haugou, Stefan Mangard, and Luca Benini. An iot endpoint system-on-chip for secure and energy-efficient near-sensor analytics. *IEEE Trans. on Circuits and Systems*, 64-I(9):2481–2494, 2017.

Thomas Unterluggauer, Thomas Korak, Stefan Mangard, Robert Schilling, Luca Benini, Frank K. Gürkaynak, and Michael Muehlberghuber. Leakage bounds for gaussian side channels. In *Smart Card Research and Advanced Applications - 16th International Conference, CARDIS 2017, Lugano, Switzerland, November 13-15, 2017, Revised Selected Papers*, pages 88–104, 2017.

Mario Werner, Thomas Unterluggauer, Robert Schilling, David Schaffenrath, and Stefan Mangard. Transparent memory encryption and authentication. In *27th International Conference on Field Programmable Logic and Applications, FPL 2017, Ghent, Belgium, September 4-8, 2017*, pages 1–6, 2017.

Frank K. Gürkaynak, Robert Schilling, Michael Muehlberghuber, Francesco Conti, Stefan Mangard, and Luca Benini. Multi-core data analytics soc with a flexible 1.76 gbit/s AES-XTS cryptographic accelerator in 65 nm CMOS. In *Proceedings of the Fourth Workshop on Cryptography and Security in Computing Systems, CS2@HiPEAC 2017, Stockholm, Sweden, January 24, 2017*, pages 19–24, 2017.

Robert Schilling, Manuel Jelinek, Markus Ortoff, and Thomas Unterluggauer. A low-area asic implementation of aegis128—a fast authenticated encryption algorithm. In *22nd Austrian Workshop on Microelectronics (Austrochip)*, pages 1–5. IEEE, 2014.

Graz, September 8, 2023

schilling.ro@gmail.com • *www.rschilling.net*