Robert Schilling

Silicon Engineer · Hardware Security
12 Titch Street, CB5 8JN Cambridge, UK
(+44) 7356 019393 | (+43) 664 4496130 | schilling.ro@gmail.com | www.schilling.casa | Razer6 | HackerOne: xanbanx

Summary

Silicon engineer at Meta working on platform security for custom silicon.

Previously at Rivos Inc. (acquired by Meta), where I led the development of Darjeeling, the SoC-integrated variant of OpenTitan, an open-source silicon root of trust — from design through tapeout, silicon bringup, and full provisioning.

Ph.D. from Graz University of Technology — hardware extensions and compiler support for fault-attack countermeasures on RISC-V processors. Active bug bounty researcher with 42 CVEs discovered in GitLab. Passionate about automation and building reusable, scalable hardware-software co-designs that extend beyond security.

Work Experience

Meta — *Cambridge, UK*
Silicon Engineer, MTIA — *Feb. 2026 - Present*
- Platform security for Meta's custom silicon
- Working on Caliptra, an open-source hardware root of trust for data center SoCs

Rivos Inc. (acquired by Meta) — *Graz, Austria*
Security Architect — *Apr. 2023 - Feb. 2026*
- Led development of Darjeeling, the SoC-integrated OpenTitan Root of Trust
- FIPS 140-3 readiness for the security subsystem
- End-to-end silicon lifecycle: tapeout, bringup, and secure provisioning
- Upstreamed Darjeeling to the open-source OpenTitan project

Graz University of Technology — *Graz, Austria*
University Assistant — *Apr. 2019 - Apr. 2023*
- Research on secure code execution in the presence of physical attacks
- Teaching: Computer Organization and Networks, Digital System Design

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

Graz University of Technology — *Graz, Austria*
Student Researcher — *Feb. 2015 - Jul. 2015*
- Built an AXI encryption pipeline for authenticated encryption, FPGA prototype with Linux boot

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

Education

Graz University of Technology — *Graz, Austria*
Ph.D. in Computer Science, passed with distinction — *Apr. 2016 - Sept. 2023*
- Hardware Extensions and Compiler Support for Protection Against Fault Attacks

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

Graz University of Technology — *Graz, Austria*
Master of Science — Telematik (Information and Computer Engineering), passed with distinction — *Mar. 2014 - Apr. 2016*

Graz University of Technology — *Graz, Austria*
Bachelor of Science — Telematik (Information and Computer Engineering), passed with distinction — *Oct. 2010 - Mar. 2014*

Skills

Security	Secure boot, attestation, DICE, confidential compute, key management & provisioning, FIPS 140-3, threat modeling, post-quantum cryptography, side-channel & fault mitigations
Hardware	RISC-V, OpenTitan, Caliptra, SoC integration, post-silicon validation, CDC/RDC, RAS, ASIC design & verification, FPGA prototyping
Programming	C, C++, Rust, Python, Tcl, Bash, SystemVerilog, VHDL, Assembly (RISC-V, ARM)
Tools	VCS, Xcelium, Bazel, LLVM, Git, CI/CD automation
Languages	German (native), English (fluent)

Scholarships & Grants

2015 **Scholarship of Excellence,** Industriellenvereinigung Kärnten
2015 **Scholarship of Excellence,** Graz University of Technology
2015 **Research Abroad Stipendium,** Graz University of Technology
2012 **Scholarship of Excellence,** Graz University of Technology
2011 **Scholarship of Excellence,** Graz University of Technology

Industry Talks

[RWC'26] *Migrating a Silicon Root of Trust to Post-Quantum Crypto*
Amin Abdulrahman, Andrew Huang, **Robert Schilling**, et al.
Hardware-accelerated post-quantum crypto (ML-DSA, ML-KEM, SLH-DSA) on OpenTitan root of trust.

[RISC-V'25] *OpenTitan Integrated: A RISC-V Open-Source Silicon Root-of-Trust for Large SoCs*
Robert Schilling, Samuel Ortiz, Ravi Sahita, and Andreas Kurth
Open-source silicon root of trust designed for integration into large SoC security subsystems.

Selected Publications

[DIMVA'25] *FAULTLESS: Flexible and Transparent Fault Protection for Superscalar RISC-V Processors*
Moritz Waser, David Schrammel, **Robert Schilling**, and Stefan Mangard
3.5% LUT overhead on VeeR EH1; runtime-toggleable security/performance tradeoff; compatible with unmodified binaries.

[COSADE'22] *FIPAC: Thwarting Fault- and Software-Induced Control-Flow Attacks with ARM Pointer Authentication*
Robert Schilling, Pascal Nasahl, and Stefan Mangard
Basic-block granular CFI with full LLVM compiler support; reuses existing ARM PAC hardware.

[HASP'22] *SFP: Providing System Call Flow Protection against Software and Fault Attack*
Robert Schilling, Pascal Nasahl, Martin Unterguggenberger, and Stefan Mangard
OS-level protection ensuring syscall sequences can't be hijacked by fault or software attacks.

[HOST'21] *SecWalk: Protecting Page Table Walks Against Fault Attacks*
Robert Schilling, Pascal Nasahl, Stefan Weiglhofer, and Stefan Mangard
Protects virtual-to-physical address translation against faults; covers multi-level page tables on application-class CPUs.

[NDSS'20] *ConTExT: A Generic Approach for Mitigating Spectre*
Michael Schwarz, Moritz Lipp, Claudio Canella, **Robert Schilling**, Florian Kargl, and Daniel Gruss
Minimal ISA extension marking secrets so they can enter but not transiently leak from registers; 0% overhead for non-secret code.

[DATE'18] *High speed ASIC implementations of leakage-resilient cryptography*
Robert Schilling, Thomas Unterluggauer, Stefan Mangard, Frank K. Gürkaynak, Michael Muehlberghuber, and Luca Benini
Fresh re-keying as algorithmic DPA countermeasure; eliminates need for masking with minimal area overhead.

[DATE'18] *Securing conditional branches in the presence of fault attacks*
Robert Schilling, Mario Werner, and Stefan Mangard
Protected comparisons linked to CFI scheme; prevents single-instruction skips on password checks, secure boot, privilege escalation.

[ACSAC'18] *Pointing in the Right Direction - Securing Memory Accesses in a Faulty World*
Robert Schilling, Mario Werner, Pascal Nasahl, and Stefan Mangard
Compiler-generated pointer MACs detect fault-induced address corruption; protects loads and stores on embedded CPUs.

Additional Publications

[DATE'23] *SCFI: State Machine Control-Flow Hardening Against Fault Attacks*
Pascal Nasahl, Martin Unterguggenberger, Rishub Nagpal, **Robert Schilling**, David Schrammel, and Stefan Mangard
Protects hardware FSMs against fault injection; prevents adversaries from skipping security-critical states.

[CCS'23] *Multi-Tag: A Hardware-Software Co-Design for Memory Safety based on Multi-Granular Memory Tagging*
Martin Unterguggenberger, David Schrammel, Pascal Nasahl, **Robert Schilling**, Lukas Lamster, and Stefan Mangard
Overcomes small-tag collision limits of ARM MTE by combining object- and page-granular tags; gem5 + Linux + LLVM prototype.

[HOST'21] *Protecting Indirect Branches Against Fault Attacks Using ARM Pointer Authentication*
Pascal Nasahl, **Robert Schilling**, and Stefan Mangard
Extends PAC-based protection to indirect jumps and function pointers in safety-critical embedded/automotive systems.

[CCS'21] *CrypTag: Thwarting Physical and Logical Memory Vulnerabilities using Cryptographically Colored Memory*
Pascal Nasahl, **Robert Schilling**, Mario Werner, Jan Hoogerbrugge, Marcel Medwed, and Stefan Mangard
Encrypts memory with per-object keys; defeats both software exploits and physical probing without full memory safety overhead.

[CCS'21] *HECTOR-V: A Heterogeneous CPU Architecture for a Secure RISC-V Execution Environment*
Pascal Nasahl, **Robert Schilling**, Mario Werner, and Stefan Mangard
TEE via dedicated fault-protected security core alongside untrusted application core; protects even against malicious OS.

[VMCAI'19] *Small Faults Grow Up - Verification of Error Masking Robustness in Arithmetically Encoded Programs*
Anja F. Karl, **Robert Schilling**, Roderick Bloem, and Stefan Mangard
Shows that single-bit fault models underestimate real attacks; multi-bit faults can bypass arithmetic encoding.

[DATE'19] *Protecting RISC-V Processors against Physical Attacks*
Mario Werner, **Robert Schilling**, Thomas Unterluggauer, and Stefan Mangard
First systematic study of fault countermeasures for RISC-V; instruction encoding, CFI, and memory protection.

[TCAS'17] *An IoT Endpoint System-on-Chip for Secure and Energy-Efficient Near-Sensor Analytics*
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
PULP-based SoC (FULMINE) with HW crypto; taped out in 65nm UMC; targets battery-powered IoT endpoints.

[HiPEAC'17] *Multi-core data analytics SoC with a flexible 1.76 Gbit/s AES-XTS cryptographic accelerator in 65 nm CMOS*
Frank K. Gürkaynak, **Robert Schilling**, Michael Muehlberghuber, Francesco Conti, Stefan Mangard, and Luca Benini
Silicon-proven crypto accelerator for full-disk encryption integrated into PULP multi-core cluster.

[CARDIS'17] *Leakage Bounds for Gaussian Side Channels*
Thomas Unterluggauer, Thomas Korak, Stefan Mangard, **Robert Schilling**, Luca Benini, Frank K. Gürkaynak, and Michael Muehlberghuber
Bridges gap between leakage-resilient crypto theory and real-world side-channel noise models.

[FPL'17] *Transparent memory encryption and authentication*
Mario Werner, Thomas Unterluggauer, **Robert Schilling**, David Schaffenrath, and Stefan Mangard
Protects FPGA external memory against runtime probing and tampering; transparent to software.

[Austrochip'14] *A low-area ASIC implementation of AEGIS128—A fast authenticated encryption algorithm*
Robert Schilling, Manuel Jelinek, Markus Ortoff, and Thomas Unterluggauer
First ASIC of AEGIS-128 (CAESAR competition candidate); area-optimized for constrained devices.