Lukas **Gerlach**

lukas.gerlach@cispa.de | www.lukasgerlach.me | s8lvg | lukas-g-00095a204 | Lukas Gerlach

Summary

Third-year Ph.D. candidate at CISPA specializing in microarchitectural security, hardware vulnerabilities, and applied cryptography (expected graduation: February 2027). Published 21 papers (193 citations), including 5 first-author publications at A and A* security venues, and contributed to 9 A* papers, collaborating with 36 researchers across 9 institutions. Award-winning researcher with Best Paper Award at USENIX Security (2025), Distinguished Artifact Award at NDSS (2025), two-time finalist at CSAW Applied Research Competition (2024, 2025). Discovered critical security vulnerabilities in hardware and software systems with 4+ assigned CVEs affecting RISC-V CPUs, Intel/AMD processors, and widely-used software implementations. 4+ years of hands-on experience in practical security research, spanning microarchitectural attacks, side-channel analysis, and formal verification methods. Ability to communicate complex security research through invited talks at Black Hat Europe and academic conferences, combined with teaching experience supervising 5 theses.

Experience

CISPA Helmholtz Center for Information Security — *Saarbrücken, Germany*
Doctoral Researcher — *02/2023 - Present*

- Conducted practical research with a focus on Microarchitectural Security, Side-Channel Attacks, RISC-V Security, and Applied Cryptography
- Published 5 first-author papers (2 IEEE S&P, 1 ESORICS, 1 FC, 1 uASC) and contributed to 16 additional publications at top-tier security conferences (USENIX Security, NDSS, CCS, ACM CCS, ESORICS, FC, etc.)
- Discovered critical security vulnerabilities in hardware and software systems, including RISC-V CPUs, Intel/AMD processors, and various software implementations (CVE-2023-20583,CVE-2023-20592,CVE-2024-44067)
- Performed scientific outreach by presenting research at industry conferences including Black Hat Europe and hardear.io
- Supervised 5 theses (1 Master's, 4 Bachelor's) out of which 3 resulted in publications

KU Leuven — *Leuven, Belgium*
Visiting Researcher — *2024*

Research on RISC-V transient execution attacks and artifact reproducibility

TU Graz — *Graz, Austria*
Visiting Researcher — *2024*

Research on software-based power side channels (Collide+Power publication)

CISPA Helmholtz Center for Information Security — *Saarbrücken, Germany*
Teaching and Research Assistant — *2021 - 2023*

Research on compression-based side channels

Real-Time and Embedded Systems Lab — *Saarbrücken, Germany*
Research Assistant — *2020 - 2021*

Research on formal methods against Spectre attacks

Honors & Awards

2025 **Finalist**, CSAW Applied Research Competition
Cascading Spy Sheets: Exploiting the Complexity of Modern CSS for Email and Browser Fingerprinting

2025 **Best Paper Award**, USENIX Security Symposium
Confusing Value with Enumeration: Studying the Use of CVEs in Academia

2025 **Distinguished Artifact Award**, NDSS
Cascading Spy Sheets: Exploiting the Complexity of Modern CSS for Email and Browser Fingerprinting

2024 **Distinguished Artifact Reviewer**, USENIX Security Symposium

2024 **Finalist**, CSAW Applied Research Competition
A Security RISC: Microarchitectural Attacks on Hardware RISC-V CPUs

2022 **Individual Bracket Winner**, Facebook BountyConEDU

Skills

Research Interests Microarchitectural Security, Side-Channel Attacks, RISC-V Security, Applied Cryptography
Programming Languages C/C++, Python, Assembly (x86, ARM, RISC-V)
Languages German (Native), English (Fluent)

Publications

21 publications, 9A* (3 IEEE S&P, 1 CCS, 1 NDSS, 4 USENIX Security)

First-Author Publications

Zero-Store Elimination and its Implications on the SIKE Cryptosystem — *uASC 2026*
Lukas Gerlach, Niklas Flentje, Michael Schwarz

Do Compilers Break Constant-time Guarantees? — *FC 2025*
Lukas Gerlach, Robert Pietsch, Michael Schwarz

Efficient and generic microarchitectural hash-function recovery — *IEEE S&P 2024*
Lukas Gerlach, Simon Schwarz, Nicolas Faroß, Michael Schwarz

A Rowhammer Reproduction Study Using the Blacksmith Fuzzer — *ESORICS 2023*
Lukas Gerlach, Fabian Thomas, Robert Pietsch, Michael Schwarz

A Security RISC: Microarchitectural Attacks on Hardware RISC-V CPUs — *IEEE S&P 2023*
Lukas Gerlach, Daniel Weber, Ruiyi Zhang, Michael Schwarz

Selected Co-Authored Publications

Confusing Value with Enumeration: Studying the Use of CVEs in Academia — *USENIX Security 2025*
Moritz Schloegel, Daniel Klischies, Simon Koch, David Klein, **Lukas Gerlach** et al.

RISCover: Automatic Discovery of User-exploitable Architectural Security Vulnerabilities in Closed-Source RISC-V CPUs — *CCS 2025*
Fabian Thomas, Eric García Arribas, Lorenz Hetterich, Daniel Weber, **Lukas Gerlach** et al.
CVE-2024-44067

SCASE: Automated Secret Recovery via Side-Channel-Assisted Symbolic Execution — *USENIX Security 2025*
Daniel Weber, **Lukas Gerlach**, Leon Trampert, Youheng Lue, Jo Van Bulck, Michael Schwarz

Rapid Reversing of Non-Linear CPU Cache Slice Functions: Unlocking Physical Address Leakage — *IEEE S&P 2025*
Mikka Rainer, Lorenz Hetterich, Fabian Thomas, Tristan Hornetz, Leon Trampert, **Lukas Gerlach** et al.

ShadowLoad: Injecting State into Hardware Prefetchers — *ASPLOS 2025*
Lorenz Hetterich, Fabian Thomas, **Lukas Gerlach**, Ruiyi Zhang, Nils Bernsdorf, Eduard Ebert, Michael Schwarz

Cascading Spy Sheets: Exploiting the Complexity of Modern CSS for Email and Browser Fingerprinting — *NDSS 2025*
Leon Trampert, Daniel Weber, **Lukas Gerlach**, Christian Rossow, Michael Schwarz
CVE-2024-24510

CacheWarp: Software-based Fault Injection using Selective State Reset — *USENIX Security 2024*
Ruiyi Zhang, **Lukas Gerlach**, Daniel Weber, Lorenz Hetterich, Youheng Lü, Andreas Kogler, Michael Schwarz
CVE-2023-20592

Collide+Power: Leaking Inaccessible Data with Software-based Power Side Channels — *USENIX Security 2023*
Andreas Kogler, Jonas Juffinger, Lukas Giner, **Lukas Gerlach**, Martin Schwarzl, Michael Schwarz, et. al.
CVE-2023-20583

Talks

hardear.io — *The Hague, The Netherlands, Oct. 2024*
Presenter for "From Rowhammer to GhostWrite: Advanced Exploitation and Discovery of Hardware Bugs"

BlackHat Europe — *London, United Kingdom, Dec. 2023*
Presenter for "A Security RISC? The State of Microarchitectural Attacks on RISC-V"

m0leCon — *Torino, Italy, Dec. 2023*
Presenter for "Rowhammer Revisited: From Exploration to Exploitation and Mitigation"

Community Service

Reviewer USENIX Security AEC (2024), CCS AEC (2024)
Sub-Reviewer USENIX Security (2025), NDSS (2024, 2025), DIMVA (2024)
Doctoral Representative Helmholtz Juniors (CISPA representative across 19 Helmholtz centers)

Teaching & Supervision

Teaching Assistant Side-Channel Attacks and Defenses
Student Assistant Math Prep., Programming II Prep., Programming I, Programming II, Theory of Computation, Cryptography

2024 **Master's Thesis,** Tristan Hornetz, Execute-Only Memory as a Security Hardening Feature on x86-64
2024 **Bachelor's Thesis,** Luis Felger: Detecting Data-Obliviousness Violations in Multi-Stage Translation Environments
2024 **Bachelor's Thesis,** Maximilian Löffler: PowerDrop Fuzzing for Faulty Instruction Gadgets
2023 **Bachelor's Thesis,** Mika Rainer, Reversing the Microarchitecture with Unikernels
2023 **Bachelor's Thesis,** Robert Pietsch, Automated Checking of C Compiler Optimization Effects on Data Obliviousness