Lorenz Hetterich

Saarbrücker Straße 280, 66125 Saarbrücken

lorenz.hetterich@web.de

Ausbildung

2023 – Heute

Promotionsstudium (IT-Sicherheit)
CISPA Helmholtz-Zentrum für Informationssicherheit & Saarbrücken Graduate School of Computer Science
Forschung zu mikroarchitekturellen Angriffen auf Prozessoren
Supervision: Dr. Michael Schwarz

- Mitwirkung an der Entdeckung & Analyse der Hardware-Schwachstellen **CVE-2023-20592** (CacheWarp) und **CVE-2024-44067** (GhostWrite)
- Internationale Präsentationen akademischer Ergebnisse (USA, Singapur, Taiwan, Italien, Niederlande)
- Bisher 3 Erstautor-Veröffentlichungen in A* Konferenzen

2021 – 2023

Vorbereitungsphase zur Promotion
CISPA Helmholtz-Zentrum für Informationssicherheit & Saarbrücken Graduate School of Computer Science
Finanziert durch Anstellung als wissenschaftliche Hilfskraft
Erfolgreiches „Qualifying Exam“ für den Übergang in die Promotionsphase

2018 – 2021

Bachelor of Science in Cybersicherheit
Universität des Saarlandes
Abschlussnote: 1,3
Titel der Bachelorarbeit: *„Exploiting Spectre on iOS“*

2010 – 2018

Allgemeine Hochschulreife
Celtis-Gymnasium, Schweinfurt
Abschlussnote: 1,8

Auszeichnungen & Preise

2023

FdSI-Bachelor-Preis
Auszeichnung für herausragende Bachelor-Abschlüsse

2022

CAST Förderpreis für IT-Sicherheit
2. Platz in der Kategorie Bachelorarbeiten

2019

Bachelor Förderprogramm Informatik
Aufnahme in das Förderprogramm (Top 5% der Studierenden)

Praktische Erfahrung & Engagement

2026

Hardware-Entwicklung: RISC-V CPU
RISC-V Community Challenge with HaDes-V
Programmierung einer voll-funktionstüchtigen RISC-V CPU in System Verilog sowie Präsentation beim HaDes-V Workshop auf dem „RISC-V Summit Europe 2026“ (Implementierung auf FPGA Board als Pong Arcade)

2024 – Heute

Betreuung von Abschlussarbeiten
CISPA Helmholtz-Zentrum für Informationssicherheit
Mentoring und wissenschaftliche Fachbetreuung von Studierenden:
- Aktuell in Betreuung: 1 Masterarbeit, 1 Bachelorarbeit
- Erfolgreich abgeschlossen: 2 Bachelorarbeiten

2024 – Heute

Mitwirkung in der Lehre
CISPA Helmholtz-Zentrum für Informationssicherheit & Universität des Saarlandes
Projektbetreuung, Feedback und Benotung im Rahmen des Promotionsstudiums:
- Computer Architecture Seminar (SoSe 2026)
- Side-Channel Attacks and Defenses (WiSe 2024/25, WiSe 2025/26)

2020 – Heute

Capture the Flag (CTF) IT-Security
Teams „saarsec“ und „DieterOverflow“
Teilnahme an zahlreichen internationalen CTF-Events, unter anderem dreifache Qualifikation für die Deutsche Hacking Meisterschaft (2024, 2025, 2027)

2020 – 2021

Studentische Hilfskraft
Universität des Saarlandes (Gruppe Prof. Hermanns)
Hardwarenahe Entwicklung einer Mikrocontroller-basierten Lösung zur Simulation und Wiedergabe von OBD2-Traces (Fahrzeug-Diagnosesysteme)

2019 – 2021

Tutor
Universität des Saarlandes
Tutorentätigkeit für „Programmierung 1“ (WiSe 2019/20), „Security“ (WiSe 2020/21) und „Programmierung 2“ (SoSe 2021)

Kenntnisse & Fähigkeiten

Programmiersprachen	C, Python, Java, Assembly (x86, ARM, RISC-V, LoongArch)
Tools & Technologien	Ghidra, GDB, Linux, Git
Sprachen	Deutsch (Muttersprache), Englisch (fließend in Wort und Schrift)

Publikationen

2026

LoongLeak: Architectural Cross-Privilege-Boundary Data Leakage on LoongArch CPUs
Lorenz Hetterich, Tristan Hornetz, Fabian Thomas, Michael Schwarz
35th USENIX Security Symposium (USENIX Security)

2026

InstrSem: Automatically and Generically Inferring Semantics of (Undocumented) CPU Instructions
Lorenz Hetterich, Fabian Thomas, Tristan Hornetz, Michael Schwarz
35th USENIX Security Symposium (USENIX Security)

2025

RISCover: Automatic Discovery of User-exploitable Architectural Security Vulnerabilities in Closed-Source RISC-V CPUs
Fabian Thomas, Eric García Arribas, **Lorenz Hetterich**, Daniel Weber, Lukas Gerlach, Ruiyi Zhang, Michael Schwarz
ACM SIGSAC Conference on Computer and Communications Security (CCS)

2025 **Rapid Reversing of Non-Linear CPU Cache Slice Functions: Unlocking Physical Address Leakage**
Mikka Rainer, **Lorenz Hetterich**, Fabian Thomas, Tristan Hornetz, Leon Trampert, Lukas Gerlach, Michael Schwarz
IEEE Symposium on Security and Privacy (IEEE S&P)

2025 **Peripheral Instinct: How External Devices Breach Browser Sandboxes**
Leon Trampert, **Lorenz Hetterich**, Lukas Gerlach, Mona Schappert, Christian Rossow, Michael Schwarz
Proceedings of the ACM on Web Conference (WWW)

2025 **ShadowLoad: Injecting State into Hardware Prefetchers**
Lorenz Hetterich, Fabian Thomas, Lukas Gerlach, Ruiyi Zhang, Nils Bernsdorf, Eduard Ebert, Michael Schwarz
Proceedings of the 30th ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)

2024 **CacheWarp: Software-based Fault Injection Using Selective State Reset**
Lukas Gerlach, Daniel Weber, **Lorenz Hetterich**, Ruiyi Zhang, Youheng Lü, Andreas Kogler, Michael Schwarz
33rd USENIX Security Symposium (USENIX Security)

2024 **Switchpoline: A Software Mitigation for Spectre-BTB and Spectre-BHB on ARMv8**
Markus Bauer, **Lorenz Hetterich**, Christian Rossow, Michael Schwarz
19th ACM ASIA Conference on Computer and Communications Security (AsiaCCS)

2024 **To Auth or Not To Auth? A Comparative Analysis of the Pre- and Post-Login Security Landscape**
Jannis Rautenstrauch, Metodi Mitkov, Thomas Helbrecht, **Lorenz Hetterich**, Ben Stock
IEEE Symposium on Security and Privacy (IEEE S&P)

2023 **FetchBench: Systematic Identification and Characterization of Proprietary Prefetchers**
Till Schlüter, Amit Choudhari, **Lorenz Hetterich**, Leon Trampert, Hamed Nemati, Ahmad Ibrahim, Michael Schwarz, Christian Rossow, Nils Ole Tippenhauer
ACM SIGSAC Conference on Computer and Communications Security (CCS)

2022 **Branch Different: Spectre Attacks on Apple Silicon**
Lorenz Hetterich, Michael Schwarz
19th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)

Saarbrücken, den 28. September 2026

Lorenz Hetterich