Luca Wilke

Curriculum Vitae

✉ *work@luca-wilke.com*
🌐 *luca-wilke.com*

Personal Information

Date of Birth	**30.09.1995**
Nationality	**German**

Professional Experience

02.2025 – today **Researcher**, *Azure Research, Microsoft*, Cambridge, UK
Research Areas: *Systems Security* and *Trusted Execution Environments*

Education

02.2020 – 02.2025 **PhD in Computer Science**, *University of Lübeck*, Grade *1.0*
Research Areas: *Systems Security* and *Trusted Execution Environments*

10.2017 – 01.2020 **Master in Computer Science**, *University of Lübeck*, Grade *1.0*, top of class
Focus: Computer Security and Reliability

10.2014 – 10.2017 **Bachelor in Computer Science**, *University of Lübeck*, Grade: *1.4*
Focus: Computer Security and Reliability

Selected Publications

2025 **Fabian Rauscher, Luca Wilke, Hannes Weissteiner, Thomas Eisenbarth, Daniel Gruss** , *TDXploit: Novel Techniques for Single-Stepping and Cache Attacks on Intel TDX*, USENIX Security Symposium 2025

2024 **Meulemeester&Wilke (equal contribution), Oswald, Eisenbarth, Verbauwhede, Van Bulck**, *BadRAM: Practical Memory Aliasing Attacks on Trusted Execution Environments*, IEEE S&P 2025

2024 **Wilke&Sieck (equal contribution), Eisenbarth**, *TDXdown: Single-Stepping and Instruction Counting Attacks against Intel TDX*, ACM CCS 2024

2024 **Wilke, Scopelliti**, *SNPGuard: Remote Attestation of SEV-SNP VMs Using Open Source Tools*, SysTEX'24

2023 **Wilke, Wichelmann, Rabich, Eisenbarth**, *SEV-Step: A Single-Stepping Framework for AMD-SEV*, CHES 2024

2023 **Wichelmann, Pätschke, Wilke, Eisenbarth**, *Cipherfix: Mitigating Ciphertext Side-Channel Attacks in Software*, USENIX Security Symposium 2023

2022 **Li&Wilke (equal contribution), Wichelmann, Eisenbarth, Teodorescu, Zhang**, *A Systematic Look at Ciphertext Side Channels on AMD SEV-SNP*, IEEE S&P 2022

2021 **Wilke,Wichelmann,Sieck,Eisenbarth**, *undeSErVed trust*, WOOT 2021
Best Paper Award

2020 **Wilke,Wichelmann,Morbitzer,Eisenbarth**, *SEVurity*, IEEE S&P 2020

Skills/Experience

06.2024 – 08.2024 **Summer Intern Microsoft Research**, *Cambridge*, UK
Implementation of novel microarchitectural isolation features for hypervisors/TEEs

01.2024 – 04.2024 **Visiting Scholar**, *KU Leuven*, Belgium
Collaboration on novel TEE attack (embargoed S&P 2025 paper); single stepping countermeasures for CVMs

04.2016 – 02.2020 **Student Employee**, *University of Lübeck*
Conducting Tutoring Sessions, Grading Exercise Sheets

Languages, *German (native), English (fluent)*

Programming Languages, *C/C++, x86 Assembly, Go, Rust*

Trusted Execution Environments, *AMD SEV, Intel TDX, Keystone*

Linux Kernel Development

Invited Talks

2024 **Examining Control Flow Leakage Attacks on TEEs**, *Intel Product Assurance and Security - Tech Sharing*, Online

2024 **Single-Stepping Attacks and Defences for Confidential VMs**, *RISE Summer School & Annual Conference*, UK

2024 **SEV-Step: A Single-Stepping Framework for AMD-SEV**, *FOSDEM*, Belgium

2021 **The Role of Integrity in Attestation and Isolation**, *4rd Workshop on Attacks in Cryptography*, Online

2021 **Attestation and Isolation Mechanisms of AMD SEV**, *Microsoft Research Redmond Cryptography and Privacy Colloquium*, Online

Academic Service

2024 **Program Committee**, *34th USENIX Security*

2024 **Program&Artifact Committee**, *SysTEX'24*

2024 **External Reviewer**, *33rd USENIX Security*

2022 **External Reviewer**, *43rd IEEE S&P*

2020 **External Reviewer**, *30th USENIX Security*