Lukas **Giner**

Microarchitectural Security · Software Engineering

Dr.-Robert-Graf-Strasse 24/14, 8010 Graz, Austria

+43 680 1201335 | giner.lukas@hotmail.com | ginerlukas.com | redrabbyte | lginer | @redrabbyte | Lukas Giner

Education

Graz University of Technology — *Graz, Austria*

PhD. in Computer Science, advisor Daniel Gruss — *2020 - 2025*

- Thesis: Microarchitectural Attacks and Defenses for Isolated Domains

M.Sc. in Information and Computer Engineering — *2015 - 2020*

- Thesis: Robust High-Speed Cache Covert Channels in the Cloud

B.Sc. in Information and Computer Engineering — *2009 -2015*

Experience

Graz University of Technology, ISEC/IAIK, CoreSec — *Graz, Austria*

Postdoc / PhD Student — *Apr. 2020 - Sep. 2025*

- Vulnerability research in microarchitectural security and OS security
- Data analysis, black-box reverse-engineering of CPU functionality
- Writing and presenting of top tier conference papers, awarded with best paper award
- Supervision of bachelor's and master's theses
- Lecturing and exercise supervision for *Side-Channel Security* lecture, focusing on Meltdown and Spectre

Student Researcher — *Oct. 2018 - Mar. 2020*

- Development of proof-of-concept exploit code for microarchitectural attacks
- Contributions to multiple peer-reviewed publications (see Publications)

Speaking Engagements — *Worldwide*

- Black Hat USA 2025: Derandomizing the Location of Security-Critical Kernel Objects in the Linux Kernel
- RuhrSec 2022: Secure Cache Designs: The State of the Art and Beyond
- Black Hat Asia 2019: Store-to-Leak Forwarding
- USENIX 2022, S&P 2023, AsiaCCS 2024, DIMVA 2025, ARES 2025

Space Research Institute, Austrian Academy of Sciences — *Graz, Austria*

Software Engineer & Data Analyst — *Aug. 2010 - Sep. 2010*

- Development of data analysis software for the ESA/NASA *Cluster* & *MMS* Missions — *Sep. 2011 - Sep. 2011*
- Statistical analysis of magnetometer data — *Jul. 2012 - Sep. 2012*
- Design and development of *Spacewire* driver for embedded SPARC V8 platform — *Aug. 2013 - Sep. 2013*
- Performance evaluation of the platform and testing of real-time OS suitability — *Oct. 2014 - Oct. 2014*
- Development of custom tooling for the CDF file format used in the *MMS* Mission — *May 2015 - Apr. 2015*

Selected Publications

Scatter and Split Securely: Defeating Cache Contention and Occupancy Attacks — *S&P, 2023*

Lukas Giner, Stefan Steinegger, Antoon Purnal, Eichlseder Maria, Thomas Unterluggauer, Stefan Mangard, and Daniel Gruss

SassCache is a randomization-based L3 cache design that introduces a two-layered low-latency cipher into the mapping from addresses to cache ways. This breaks the linear association and partly partitions the cache, providing very strong security properties for moderate performance costs.

Generic and Automated Drive-by GPU Cache Attacks from the Browser — ***Best Paper Award**, AsiaCCS, 2024*

Lukas Giner, Roland Czerny, Christoph Gruber, Fabian Rauscher, Andreas Kogler, Daniel De Almeida Braga, and Daniel Gruss

We explore the new WebGPU standard for browsers and find that it enables cache attacks that work on a wide range of devices. This includes graphics cards by NVIDIA and AMD, as well as some Android devices and iPhones. We show that attacks can be executed in the background of a website, unbeknownst to the user.

Cohere+Reload: Re-enabling High-Resolution Cache Attacks on AMD SEV-SNP — *DIMVA, 2025*

Lukas Giner, Sudheendra Raghav Neela, and Daniel Gruss

This work demonstrates that AMD SEV-SNP is vulnerable to high-speed, high-accuracy cache attacks that can potentially leak cryptographic keys from a single encryption. This is enabled by the cache coherence mechanism between encrypted and decrypted cache lines of the same data.

Skills

Programming	C, C++, C#, Python, JS, WebGPU, x86 assembly, basic ARM, LaTeX, TikZ
Data Analysis	Matlab, IDL, NumPy
Technologies	Linux Kernel Modules, Intel SGX, AMD SEV, x86 Memory Subsystem, T-table AES, S&M RSA
Languages	native German, ~C2 English, ~B1 French, ~A1 Russian

All Publications

- **PhD Thesis 2025**
  Microarchitectural Attacks and Defenses for Isolated Domains
  My PhD Thesis, framing my first-author publications in the larger state of the art.
  Lukas Giner

- **USENIX Security 2025**
  When Good Kernel Defenses Go Bad: Reliable and Stable Kernel Exploits via Defense-Amplified TLB Side-Channel Leaks
  Some kernel defenses unintentionally amplify TLB side channels and enable reliable exploitation primitives.
  Lukas Maar, **Lukas Giner**, Daniel Gruss, and Stefan Mangard

- **ARES 2025**
  Fast and Efficient Secure L1 Caches for SMT
  A secure L1 cache design for SMT that mitigates cache side channels with minimal performance overhead.
  Lukas Giner, Roland Czerny, Simon Lammer, Aaron Giner, Paul Gollob, Jonas Juffiger, and Daniel Gruss

- **DIMVA 2025**
  Cohere+Reload: Re-enabling High-Resolution Cache Attacks on AMD SEV-SNP
  Demonstrates cache attacks against AMD SEV-SNP by exploiting the encryption coherence mechanism.
  Lukas Giner, Sudheendra Raghav Neela, and Daniel Gruss

- **AsiaCCS 2024, Best Paper Award**
  Generic and Automated Drive-by GPU Cache Attacks from the Browser
  Introduces portable browser-based GPU cache attacks using WebGPU across desktop and mobile devices.
  Lukas Giner, Roland Czerny, Christoph Gruber, Fabian Rauscher, Andreas Kogler, Daniel De Almeida Braga, and Daniel Gruss

- **IEEE S&P 2023**
  Scatter and Split Securely: Defeating Cache Contention and Occupancy Attacks
  SassCache is a randomized cache architecture that mitigates contention and occupancy side-channel attacks.
  Lukas Giner, Stefan Steinegger, Antoon Purnal, Eichlseder Maria, Thomas Unterluggauer, Stefan Mangard, and Daniel Gruss

- **USENIX Security 2023**
  Collide+Power: Leaking Inaccessible Data with Software-based Power Side Channels
  Software-based power side channels capable of leaking data across security boundaries. CVE-2023-20583
  Andreas Kogler, Jonas Juffinger, **Lukas Giner**, Lukas Gerlach, Martin Schwarzl, Michael Schwarz, Daniel Gruss, and Stefan Mangard

- **USENIX Security 2022**
  Repurposing Segmentation as a Practical LVI-NULL Mitigation in SGX
  Uses x86 segmentation to reduce the attack surface of LVI-NULL attacks against Intel SGX enclaves.
  Lukas Giner, Andreas Kogler, Claudio Canella, Michael Schwarz, and Daniel Gruss

- **IEEE S&P 2021**
  Systematic Analysis of Randomization-based Protected Cache Architectures
  Introduces a generic framework to evaluate and compare a class of randomized cache architectures.
  Antoon Purnal, **Lukas Giner**, Daniel Gruss, and Ingrid Verbauwhede

- **arXiv 2021**
  Domain Page-Table Isolation
  Introduces stronger page-table isolation techniques to reduce transient-execution attack surfaces during syscalls.
  Claudio Canella, Andreas Kogler, **Lukas Giner**, Daniel Gruss, and Michael Schwarz

- **Master's Thesis 2020**
  A Robust High-Speed Cache Covert Channel in the Cloud
  Develops and examines a reliable, high-bandwidth Prime+Probe cache covert channel for cloud environments.
  Lukas Giner

- **CCS 2019**
  Fallout: Leaking Data on Meltdown-resistant CPUs
  Meltdown-class transient-execution vulnerabilities affecting CPUs previously believed secure. CVE-2018-12126
  Claudio Canella, Daniel Genkin, **Lukas Giner**, Daniel Gruss, Moritz Lipp, Marina Minkin, Daniel Moghimi, Frank Piessens, Michael Schwarz, Berk Sunar, Jo

Van Bulck, and Yuval Yarom

- **arXiv 2019**
  Store-To-Leak Forwarding: Leaking Data on Meltdown-resistant CPUs
  Exploits speculative store-to-load forwarding mechanisms to leak protected data on post-Meltdown CPUs.
  Michael Schwarz, Claudio Canella, **Lukas Giner**, and Daniel Gruss
- **USENIX Security 2019**
  ScatterCache: Thwarting Cache Attacks via Cache Set Randomization
  Introduces cache-set randomization to significantly reduce the effectiveness of cache side-channel attacks.
  Mario Werner, Thomas Unterluggauer, **Lukas Giner**, Michael Schwarz, Daniel Gruss, and Stefan Mangard
- **NDSS 2017**
  Hello from the Other Side: SSH over Robust Cache Covert Channels in the Cloud
  Demonstrates practical Prime+Probe covert channels over shared cloud caches.
  Clémentine Maurice, Manuel Weber, Michael Schwarz, **Lukas Giner**, Daniel Gruss, Carlo Alberto Boano, Stefan Mangard, and Kay Römer
- **Geoscientific Instrumentation, Methods and Data Systems 2014**
  Interinstrument Calibration using Magnetic Field Data from the Flux-Gate Magnetometer (FGM) and Electron Drift Instrument (EDI) onboard Cluster
  Rumi Nakamura, Ferdinand Plaschke, Robert Teubenbacher, **Lukas Giner**, Wolfgang Baumjohann, Werner Magnes, Manfred Steller, Roy Torbert, H Vaith, M Chutter, et al.
- **EGU General Assembly 2014**
  Determination of Flux-Gate Magnetometer Spin Axis Offsets with the Electron Drift Instrument
  Ferdinand Plaschke, Rumi Nakamura, **Lukas Giner**, Robert Teubenbacher, Mark Chutter, Hannes K Leinweber, and Werner Magnes
- **Geoscientific Instrumentation Methods and Data Systems 2013**
  Inter-instrument Calibration using Magnetic Field Data from Flux Gate Magnetometer (FGM) and Electron Drift Instrument (EDI) onboard Cluster
  Rumi Nakamura, Ferdinand Plaschke, Robert Teubenbacher, **Lukas Giner**, Wolfgang Baumjohann, Werner Magnes, Manfred Steller, Roy Torbert, H Vaith, M Chutter, et al.
- **EGU General Assembly 2013**
  Magnetic Field Gradients Inferred from Multi-point Measurements of Cluster FGM and EDI
  Robert Teubenbacher, Rumi Nakamura, **Lukas Giner**, Ferdinand Plaschke, Wolfgang Baumjohann, Werner Magnes, Hans Eichelberger, Manfred Steller, and Roy Torbert