Andreas Kogler - CV

Master of Science
andreaskogler.com

I am a security researcher at the Institute of Applied Information Processing and Communications at Graz University of Technology. I focus on software-based power analysis, software-based fault attacks & defenses, microarchitectural attacks & defenses, and trusted execution environments like Intel SGX or AMD SEV.

Education:

Graz University of Technology
2020 - 2024

Ph.D. *pass with distinction.*
- in *Computer Science.*

Publications: *see below*
Thesis: *Colliding Worlds: Exploiting Physical Properties from Software*

Graz University of Technology
2017 - 2020

Master of Science *pass with distinction.*
- in *Information and Computer Engineering.*

Major: *Measurement Signal Processing and Control Systems*
Minor: *Secure and Correct Systems*
Thesis: *Software-based Power Side-Channel Attacks*

Graz University of Technology
2013 - 2017

Bachelor of Science *pass with distinction.*
- in *Information and Computer Engineering.*

Work experience:

Apple
since 2024

Vulnerability Researcher and Security Engineering
- working as vulnerability researcher and security engineer.

KS Engineers
2014 - 2020

Software and Hardware Development
- for real-time operating systems, automotive measurement equipment, and high performance optimization on Intel CPUs.

Graz University of Technology
2020, 2 months

Project Assistant
- at the *Institute of Applied Information Processing and Communications.*

Skills:

Languages	German *native* | English *fluent*
Programming Languages	x86 Assembly | ARM Assembly *basics* | C | C++ | Rust | Python | VHDL | Verilog *basics*
Organization and Documentation	Git | Gitlab | Jira | AccuRev | LaTeX
Project Experience	Linux kernel | KVM | Intel SGX | AMD SEV | LLVM compiler infrastructure
Tooling Experience	Large Scale Data Analysis | Fuzzing *basics*
Fields of Expertise	SW Power Analysis | SW Fault Attacks | Microarchitectural Side Channels | TEEs

Selected Publications:

USENIX Security 2024

CacheWarp: Software-based Fault Injection using Selective State Reset

- AMD-SEV could be attacked by exploiting cache invalidation instructions to *forget* data within the caches.

Ruiyi Zhang, Lukas Gerlach, Daniel Weber, Lorenz Hetterich, Youheng Lü, **Andreas Kogler**, Michael Schwarz

USENIX Security 2023

Collide+Power: Leaking Inaccessible Data with Software-based Power Side Channels

- Software-based power side channels can leak arbitrary general-purpose data similar to Meltdown and MDS.

Andreas Kogler, Jonas Juffinger, Lukas Giner, Lukas Gerlach, Martin Schwarzl, Michael Schwarz, Daniel Gruss, Stefan Mangard

IEEE S&P 2023

CSI: Rowhammer - Cryptographic Security and Integrity against Rowhammer

- Replacing error-correcting codes allows for a hardware-software co-design with great flexibility for system security.

Jonas Juffinger, Lukas Lamster, **Andreas Kogler**, Maria Eichlseder, Moritz Lipp, Daniel Gruss

USENIX Securtiy 2022

ÆPIC Leak: Architecturally Leaking Uninitialized Data from the Microarchitecture

- The APIC MMIO range architecturally exposes data traveling over a microarchitectural decoupling buffer.

Pietro Borrello, **Andreas Kogler**, Martin Schwarzl, Moritz Lipp, Daniel Gruss, Michael Schwarz

USENIX Securtiy 2022

Half-Double: Hammering From the Next Row Over

- Rowhammer can be cascaded and extended beyond direct neighbors even if hardware mitigations are in place.

Andreas Kogler, Jonas Juffinger, Salman Qazi, Yoongu Kim, Moritz Lipp, Nicolas Boichat, Eric Shiu, Mattias Nissler, Daniel Gruss

IEEE S&P 2020

PLATYPUS: Software-based Power Side-Channel Attacks on x86

- Integrated power interfaces enable traditional power analysis from software to leak cryptographic keys.

Moritz Lipp, **Andreas Kogler**, David Oswald, Michael Schwarz, Catherine Easdon, Claudio Canella, Daniel Gruss

Additional Publications:

NDSS 2025

Power-Related Side-Channel Attacks using the Android Sensor Framework

- Sensors expose power-related signals due to physical coupling that can be exploited in power analysis attacks.

Mathias Oberhuber, Martin Unterguggenberger, Lukas Maar, **Andreas Kogler**, Stefan Mangard

NDSS 2025

A Systematic Evaluation of Novel and Existing Cache Side Channels

- The cldemote instruction can be used as replacement for clflush and enhance traditional attacks.

Fabian Rauscher, Carina Fiedler, **Andreas Kogler**, Daniel Gruss

Financial Crypto 2024

Remote Scheduler Contention Attacks

- Scheduler contention attacks are applicable from restricted environments like JavaScript.

Stefan Gast, Jonas Juffinger, Lukas Maar, Christoph Royer, **Andreas Kogler**, Daniel Gruss

NDSS 2024

IdleLeak: Exploiting Idle State Side Effects for Information Leakage

- CPU idle states get preempted due to certain systems activities and can be used for side-channel attacks.

Fabian Rauscher, **Andreas Kogler**, Jonas Juffinger, Daniel Gruss

IEEE/IFIP DSN 2023

PT-Guard: Integrity-Protected Page Tables to Defend Against Breakthrough Rowhammer Attacks

- Free bits within a page table entry can store integrity information to prevent bitflips and Rowhammer attacks.

Anish Saxena, Gururaj Saileshwar, Jonas Juffinger, **Andreas Kogler**, Daniel Gruss, Moinuddin Qureshi

USENIX Securtiy 2023

Side-Channel Attacks on Optane Persistent Memory

- The Optane memory technology deploys multiple optimizations and buffers that expose side channels.

Sihang Liu, Suraaj Kanniwadi, Martin Schwarzl, **Andreas Kogler**, Daniel Gruss, Samira Khan

IEEE S&P 2023

SQUIP: Exploiting the Scheduler Queue Contention Side Channel

- The queues used to distribute instructions within AMD CPUs expose side channels.

Stefan Gast, Jonas Juffinger, Martin Schwarzl, Gururaj Saileshwar, **Andreas Kogler**, Simone Franza, Markus Köstl, Daniel Gruss

IEEE S&P 2022

Finding and Exploiting CPU Features using MSR Templating

- Undocumented interfaces change the behavior of certain instructions, enabling potential attacks and defenses.

Andreas Kogler, Daniel Weber, Martin Haubenwallner, Moritz Lipp, Daniel Gruss, Michael Schwarz

USENIX Securtiy 2022

Minefield: A Software-only Protection for SGX Enclaves against DVFS Attacks

- SGX can be probabilistically shielded against software-based undervolting attacks by adding trap instructions.

Andreas Kogler, Daniel Gruss, Michael Schwarz

USENIX Securtiy 2022

Repurposing Segmentation as a Practical LVI-NULL Mitigation in SGX

- Segmentation registers limit the attack surface of LVI-NULL in SGX and can be used with our compiler extensions.

Lukas Giner, **Andreas Kogler**, Claudio Canella, Michael Schwarz, Daniel Gruss

arXiv 2021

Domain Page-Table Isolation

- Additional memory segregation during syscall invocation drastically limits the attack surface of an attacker.

Claudio Canella, **Andreas Kogler**, Lukas Giner, Daniel Gruss, Michael Schwarz

ESORICS 2021

Robust and Scalable Process Isolation Against Spectre in the Cloud

- Spectre attacks can be probabilistically detected and isolated in distinct processes to prevent data leakage.

Martin Schwarzl, Pietro Borrello, **Andreas Kogler**, Kenton Varda, Thomas Schuster, Daniel

Program Committees:

PC Member 2024

USENIX Security 2025

- USENIX Security Symposium

PC Member 2024

AsiaCCS 2025

- ACM Asia Conference on Computer and Communications Security

PC Member 2024

SECURWARE 2024

- International Conference on Emerging Security Information, Systems and Technologies

PC Member 2023

AsiaCCS 2024

- ACM Asia Conference on Computer and Communications Security

PC Member 2023

SECURWARE 2023

- International Conference on Emerging Security Information, Systems and Technologies

PC Member 2022

DIMVA 2023

- Detection of Intrusions and Malware & Vulnerability Assessment

PC Member 2022

SECURWARE 2022

- International Conference on Emerging Security Information, Systems and Technologies

Awards:

CVE 2023

CVE-2023-20592

- CacheWarp: Software-based Fault Injection using Selective State Reset

CVE 2023

CVE-2023-20583

- Collide+Power: Leaking Inaccessible Data with Software-based Power Side Channels

Finalist — **CSAW Applied Research Competition**
2022
- ÆPIC Leak and Half-Double

Award — **Pwnie Award for Best Desktop Bug**
2022
- ÆPIC Leak: Architecturally Leaking Uninitialized Data from the Microarchitecture

CVE — **CVE-2022-21233**
2022
- ÆPIC Leak: Architecturally Leaking Uninitialized Data from the Microarchitecture

CVE — **CVE-2021-46778**
2022
- SQUIP: Exploiting the Scheduler Queue Contention Side Channel

Award — **IAIK Student Research Excellence Award**
2022
- PLATYPUS: Software-based Power Side-Channel Attacks on x86

Award — **Förderpreis des Forum Technik und Gesellschaft (3rd place)**
2021
- Master's Thesis: Software-based Power Side-Channel Attacks

CVE — **CVE-2020-8694**
2020
- PLATYPUS: Software-based Power Side-Channel Attacks on x86

CVE — **CVE-2020-8695**
2020
- PLATYPUS: Software-based Power Side-Channel Attacks on x86

Presentations:

Talk — **Hardwear.io Netherlands**
2024
- Looking Back at 10 Years of Rowhammer Exploits

Talk — **Blackhat Europe**
2023
- Collide+Power: The Evolution of Software-based Power Side-Channels Attacks

Talk — **Blackhat Europe**
2022
- CSI:Rowhammer: Closing the Case of Half-Double and Beyond

Talk — **Blackhat USA**
2022
- AEPIC Leak: Architecturally Leaking Uninitialized Data from the Microarchitecture

Talk — **Blackhat Asia**
2022
- Dynamic Process Isolation

Lecture — **Invited Lecture @ Ben-Gurion University of the Negev**
2021
- PLATYPUS: Software-based Power Side-Channel Attacks on x86

Talk — **Remote Chaos Experience (CCC)**
2020
- Attacking CPUs with Power Side Channels from Software: Warum leaked hier Strom?