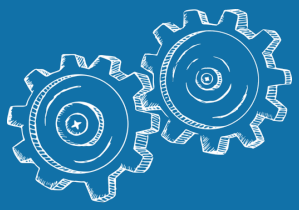

Introduction to Scientific Writing

Advisor: **Secure Systems area**

Motivation

Modern systems use many different building blocks and there are many interfaces between different components. In system security we look at systems in their entirety. This ranges from small **embedded** processors and **operating systems** to large **cloud** infrastructures with many connected servers. Our goal is to **analyze** the security of systems and discover potential **vulnerabilities** before they are exploited. At the same time, we **design defenses** to mitigate concrete attacks and to eliminate entire classes of vulnerabilities.We are an internationally recognized institution, not only constantly publishing **cutting-edge research** but our designs found their way into real-world products.

Example Topics: CoreSec

- Exotic **Cache Designs** – Compare and contrast several new or old cache designs that aim for enhanced security, performance or both.
  lukas.giner@iaik.tugraz.at
- Give an overview of **Rowhammer** attacks and mitigations, **AMD SEV** (Secure Encrypted Virtualization) or **DRAM** and its timing parameters.
  jonas.juffinger@iaik.tugraz.at

Example Topics: Secure Systems (SESYS)

- Exploitation techniques and countermeasures: Enhancing **Security in Kernel Softwares**
  lukas.maar@iaik.tugraz.at
- Give an overview of **Software-based Power Side-Channel Attacks** across different platforms and discuss different approaches using available interfaces.
  mathias.oberhuber@iaik.tugraz.at
- Analyzing and comparing the state of the art in **DRAM Encryption** & **Integrity Protection** as used in Trusted Execution Environments like Intel SGX or Intel TDX.
  lukas.lamster@iaik.tugraz.at
- The **CHERI Capability Architecture**: Analyze and extend CHERI for **memory safety** and **sandboxing**.
  moritz.waser@iaik.tugraz.at

Literature

- **CoreSec:** Stefan Gast, Jonas Juffinger, Lukas Giner
- **SESYS:** Lukas Lamster, Lukas Maar, Rishub Nagpal, Mathias Oberhuber, David Schrammel, Martin Unterguggenberger, Moritz Waser

Courses & Deliverables

☑ **Introduction to Scientific Working**
Short report on background
Short presentation

Note: You can select these topics *only* for the ISW course. If you are considering to combine ISW with a bachelor's thesis at IAIK (highly recommended), check the full list of topics:

https://www.iaik.tugraz.at/bachelor-thesis

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in **secure systems** or **implementation security**
- (Optional) *CON, SLP, OS, InfoSec*

Advisor Contact

your.supervisor@iaik.tugraz.at