



Introduction to Scientific Working (ISW)

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

- 💡 Network Side Channels and Traffic Analysis: Investigate network side channel attacks, including measurement methods, post-processing and attack scenarios
stefan.gast@tugraz.at
- 💡 Attacks on Endpoint Security Software: Research prior attacks on endpoint security software, like antivirus, endpoint/managed detection and response (EDR/MDR)...
stefan.gast@tugraz.at
- 💡 Side-channel Detection Tools: Research prior work on detecting side-channel vulnerabilities in software, and classify tools based on their approach, availability, usability, ...
hannes.weissteiner@tugraz.at

Example Topics: Secure Systems (SESYS)

- 💡 Security with/of AI: Investigate the weaknesses and strengths of **Language Models** in a specific use-case, e.g., with tools, RAG.
martin.wistauder@tugraz.at

Literature

- > **CoreSec:** Stefan Gast, Jonas Juffinger, Lukas Giner, Hannes Weissteiner, Simone Franza, Roland Czerny, Carina Fiedler, Sudheendra Raghav Neela
- > **SESYS:** Lukas Lamster, Lukas Maar, Rishub Nagpal, Mathias Oberhuber, David Schrammel, Martin Unterguggenberger, Moritz Waser, Martin Wistauder

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 ISEC (highly recommended), check the full list of topics:
<https://www.isec.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@tugraz.at