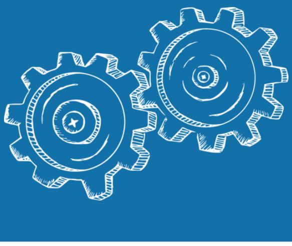
ISEC | Institute of Information Security



Instant Messenger Side-Channel Attacks

Advisor: **Roland Czerny**

Motivation

Instant messengers such as Signal, WhatsApp, or Telegram are widely used for private communication. They often use end-to-end encryption to protect message content from eavesdroppers. However, even if the content is secure, side-channel information such as message timing, size, or frequency may still leak sensitive information. The question is: can an attacker infer private information simply by observing instant messenger traffic patterns?

In this project, you will explore different instant messenger applications and their side-channel characteristics, and investigate potential attacks based on this information.

Goals and Tasks

- Explore the characteristics of several instant messenger applications.
- Develop potential side-channel attacks that could exploit these characteristics.
- Write small test programs to measure and analyze possible leaks.

Literature

- G. K. Gegenhuber et al.
  Careless Whisper: Exploiting Silent Delivery Receipts to Monitor Users on Mobile Instant Messengers
  RAID 2025
- S. Gast et al.
  Zero-Click SnailLoad: From Minimal to No User Interaction
  ESORICS

Courses & Deliverables

☑ **Master Project**
Project code
Report
Presentation

– OR –

☑ **Master's Thesis**
Initial presentation
Project code
Thesis (60+ pages)
Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in side-channel security
- Programming experience (Python and/or Go)
- Nice to have: statistics/machine learning knowledge

Advisor Contact

roland.czerny@tugraz.at