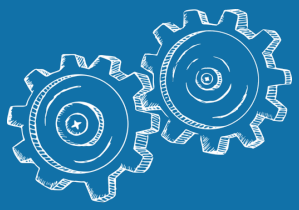

Fingerprinting Analysis

Advisor: **Simone Franza**

Motivation

Fingerprinting attacks enable an attacker to identify which websites (or videos) a victim is loading. Traditionally, these attacks rely on a MitM position to monitor the victim's network packets. However, recent attacks like SnailLoad, showed that fingerprinting is also possible from an unprivileged remote location and without code execution.

In this thesis, you will investigate properties of different fingerprinting attacks. This topic is rather broad and can go into multiple directions – just feel free to ask if you want to know more.

Goals and Tasks

- Get familiar with the SnailLoad attack and other website fingerprinting attacks
- Compare the performance of different fingerprinting attacks
- Implement existing fingerprinting attacks

Literature

- S. Gast et al.
  SnailLoad: Exploiting Remote Network Latency Measurements without JavaScript
  USENIX Security
  https://www.usenix.org/conference/usenixsecurity24/presentation/gast
- S. Bhat et al.
  Var-CNN: A Data-Efficient Website Fingerprinting Attack Based on Deep Learning
  PoPETS 2019

Courses & Deliverables

- ☑ **Introduction to Scientific Working**
  Short report on background
  Short presentation
- ☑ **Bachelor Project**
  Project code and documentation
- ☑ **Bachelor's Thesis**
  Project code
  Thesis
  Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- basic knowledge of TCP
- Programming (C, Python)

Advisor Contact

simone.franza@tugraz.at