SnailLoad Python Implementation

Advisor: **Stefan Gast**

Motivation

SnailLoad enables website and video fingerprinting attacks from just a TCP connection, without an attacker-in-the-middle or attacker controlled code on the victim machine. The original implementation of the attack relies on the TCP/IP stack of the Linux kernel on the attacker's server. While this approach makes it easy to demonstrate the basic attack, it does not provide full control over the packets sent. Bypassing the TCP/IP stack of the kernel and working with raw ethernet frames provides more flexibility for future experiments.

In this project, you will implement SnailLoad in Python, including a custom packet generator using the Scapy library. This project can also be upgraded to a bachelor thesis by evaluating possible attack variants or mitigations.

Goals and Tasks

- Get familiar with SnailLoad and scapy

- Implement basic TCP/IP functionality using Scapy

- Implement SnailLoad latency measurements

- Evaluate possible attack variants or mitigations (optional, for thesis)
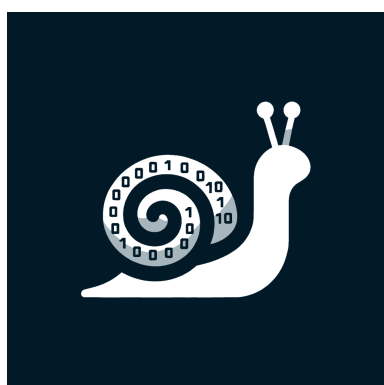
Literature

> S. Gast et al.
> SnailLoad: Exploiting Remote Network Latency Measurements without JavaScript
> USENIX Security
> https://www.usenix.org/conference/usenixsecurity24/presentation/gast

> Scapy community
> Scapy
> https://scapy.net/

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

> Python (good knowledge)

> TCP/IP (basic knowledge)

Advisor Contact

stefan.gast@tugraz.at