Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Thesis M.Sc.

IDP, HiWi, Guided Research

Understanding the State of SSL/TLS Interception

Motivation

The deployment of encryption mechanisms on the Internet is becoming widespread and rising, therefore observers in the network are increasingly losing access to the transmitted information other than metadata. However, especially companies often want to inspect their network traffic for network-based malware scanning and attack detection. This has lead to the emergence of numerous solutions for SSL/TLS interception proxies both commercial (e.g. by Bluecoat, Dell or Cisco) and free software (mitmproxy.org).

Previous studies have looked into TLS interception and found evidence of TLS interception in the network [1] as well as on the client device itself [2]. We aim to perform a crowdsourced study of TLS interception that closely analyses the deployment, triggers and properties of TLS interception in the wild. Our measurement setup is based on the network troubleshooting tool Netalyzr [3] developed at ICSI in Berkeley, CA.

[1] Huang et. al., “Analyzing Forged SSL Certificates in the Wild”, SoSP14
[2] de Carné et al., “Killed by Proxy: Analyzing Client-end TLS Interception Software”, NDSS16
[3] http://netalyzr.icsi.berkeley.edu

Your Task

- Understand the benefits and problems of crowdsourced measurements
- Refine the existing test setup (client and server), prepare for public release
- Work in an international team, communicate in English

Prerequisites

- Interest in network security and the SSL/TLS protocol
- Java, Python, basic understanding of Linux/Android networking
- Problem-solving thinking and ability to work on your own

Contact

Florian Wohlfart wohlfart@in.tum.de

https://net.in.tum.de/~wohlfart