Technische Universität München
Lehrstuhl für Netzarchitekturen und Netzdienste
Prof. Dr. Georg Carle

# Thesis (B.Sc./M.Sc.)

# Turning the Tables: Hunting the SSL/TLS Men-in-the-Middle

## Motivation

The protocols **Secure Socket Layer (SSL) and Transport Layer Security (TLS)** are commonly used to secure HTTP connections to Web servers. Together with an X.509 Public Key Infrastructure (PKI), which relies on more-or-less-trusted Certification Authorities to issue certificates, SSL and TLS are meant to provide authentication, encryption and data integrity.

However, in recent months serious doubt has been cast how successfully these protocols and the corresponding PKI can really be used. In particular, what happens if an oppressive government decides to spy on its citizens? Several security activists have reported attacks that effectively represent **Man-in-the-middle scenarios (MitM)**. There are ready-to-buy SSL/TLS proxies which can **swap certificates on-the-fly**; but there have also been reports about **Man-in-the-middle attacks using hot spots in hotels**, and even using **nodes of the Tor anonymisation network**. What's worse, studies have shown that users are conditioned to click away security warnings readily and without much thought. This makes such attacks frighteningly simple.

In this work, we will implement an **add-on for the Firefox browser** that allows researchers and the security-conscious to **detect and report MitM attacks on SSL/TLS**. What's more, the tool will **collect information** including traceroutes **that other researchers can use to trace and possibly identify the attacker**.

## Your Task

Your task consists of the following steps.

First, you **write an add-on to detect the MitM** - either by detecting "weird" certificates after a Firefox security warning or by comparison with established certificate databases. The add-on will also **collect additional information** like IP traceroutes and send this to a central server.

Second, you set up an infrastructure to **store and process the collected data**.

Third, we release the add-on to the Firefox community under the GPL. With any luck, we can also process some real reports.

## Requirements

We will program in **Javascript** using the **Firefox extension API**, so some background here is appreciated but not required. The central server will likely be implemented in **Python or Java** and use **Postgresql**. You should definitely be comfortable with programming! Above everything, however, we appreciate **passion**: we can teach you what you don't know, but we do want someone who's keen to participate in this work.

## Keywords

**SSL/TLS, Man-in-the-middle, Network Security**





Ralph Holz, Heiko Niedermayer, Phillip Fehre
holz@net.in.tum.de, niedermayer@net.in.tum.de, fehre@net.in.tum.de