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

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

Understanding Certificate Revocation: OCSP, CRLs, and data sets

Motivation

X.509 is the *de facto* standard for digital certificates on the Internet. X.509 certificates are widely used in setting up SSL/TLS connections, especially for HTTP on the WWW. X.509 establishes a certification hierarchy, with Certification Authorities at the top.

However, recent research – including our own – has shown that certification practices are not up to scratch. Mismatches of certified subjects and use of such certificates on WWW servers, invalid or expired certificates, etc. – all this seems to be the norm. Depending on your point of view, the global state of the X.509 landscape is either cause for tears or for hilarity.

In this work, we will not look at certificates themselves, but at the revocation mechanisms that Certification Authorities use. Certificates can either be revoked by being placed on so-called Certificate Revocation Lists (CRLs), which can be downloaded, or by making their status available via the Online Certificate Status Protocol (OCSP). Our aim is to monitor revocation practices over the course of several months.

Your Task

In your task, you will build on – and extend – software that we have already written.

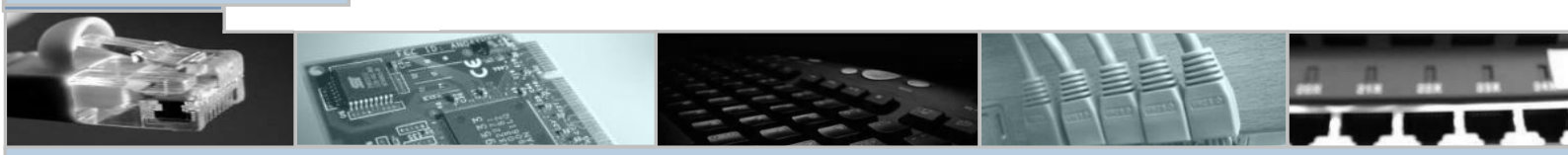
First, you will improve a scanner to monitor OCSP hosts continuously for availability and correctness.
Second, you will will implement a scanner that downloads Certificate Revocation Lists.
Certificate data will be extracted from them and stored in a data base for further analysis.
Third, you will have access to a large data set of already collected CRLs that we have obtained courtesy of our colleagues at University of Luxembourg. We also have data on the CRLs built into the Chrome browser. Once the data is collected, you will analyse it to derive statistics about the current state of revocation and revocation infrastructure.
The topic is for a Master's student, but can be adapted for a Bachelor's thesis.

Requirements

Knowledge in network security is expected. Enjoying working with large data sets while extracting useful information from them is a prerequisite. Do not worry about details of X.509, though – we can teach you everything you need to know. We will program in Python, so knowledge of that language will be useful. You need to be OK with SQL. Above everything, however, we want someone who enjoys his work and is motivated to carry out their own research.

Keywords

Network Security, X.509 certificates



Ralph Holz
holz@net.in.tum.de