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

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

Rapping Their Knuckles: Monitoring X.509 Certificate Revocation

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. No-one seems exactly sure what to do about it.

In this work, you will build on research we have already conducted. 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 implement a scanner that downloads Certificate Revocation Lists. Certificate data will be extracted from them and stored in a data base for further analysis.

Second, you will use our OCSP scanner to monitor the availability of OCSP responders.

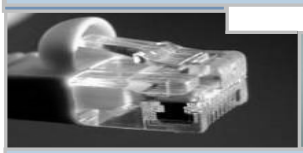
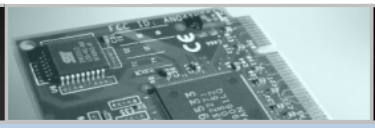
Once you have collected the data, you will analyse it to derive statistics about the current state of revocation and revocation infrastructure. You will apply statistical methods to obtain a good picture of the state of X.509 revocation, including changes over time.

Requirements

Knowledge in network security is expected. Do not wory 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 should also be OK with SQL. Above everything, however, we want someone who enjoys his work and is motivated to participate in our research.

Keywords

Network Security, X.509 certificates


Ralph Holz, Nils Kammenhuber, Lothar Braun,
holz@net.in.tum.de, hirvi@net.in.tum.de, braun@net.in.tum.de