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

Thesis B.Sc.

Thesis M.Sc.

Certificate Monitoring

Motivation

Certificates are used for many purposes of authentication on the Internet. Web servers are commonly authenticated via X.509 certificates. Client authentication via certificates is more prevalent in email, e.g. in S/MIME. Problems with the security of certificates and the overall design of X.509 led to new developments to secure web communication. The most prominent one is Certificate Transparency which is currently promoted by Google. On a smaller scale, what is missing in current systems is a feedback channel from the one who verified the certificate to the one who was identified via the certificate. It is unknown to a server if clients might see a rogue certificate instead of a legitimate one. The server can only hope that a successful establishment of the secure channel indicates that the client has seen the correct certificate. Now, outside the area of web browsing, adding all the heuristics from the web may not exactly match the requirements. Our idea is to provide a feedback channel in the opposite direction of the certificate authentication and a general monitoring of what is seen when trying to connect. Since this involves addition activities by entities on the Internet, a design of such monitoring needs to consider Denial-of-Service attack defenses as attackers might be able to misuse such activities.

Your Task

- Study related work about certificate protection and monitoring, e.g. notary servers
- Conceptual design, use case in combination with sKnock for client auth and some service using a server for server auth
- API design for a certificate manager and a monitoring software component
- Implementation
- Evaluation

Contact

Dr. Heiko Niedermayer niedermayer@net.in.tum.de
Sree Harsha Totakura totakura@net.in.tum.de