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

Thesis B.Sc.

Thesis M.Sc.

Enhanced Certificate Protection

Motivation

The security of HTTPS / TLS connections over the Internet has been discussed a lot in recent years. One main issue is the X.509 Public Key Infrastructure that is based on a meanwhile too large root store of trusted certification authorities that all can generate certificates for all websites. Browser vendors provided two main answers to the problem. One is Certificate Pinning where browsers expect certain certificates and do not accept other certificates for a website anymore. The other is Certificate Transparency where all certificates are stored in a public log to make the issuing of certificates transparent and find rough certificates after an attack.
In the project SafeCloud we want to provide security in a multiple lines of multiples defenses approach. On the lower layer of communication (between users and cloud, between cloud data centers, . . .). This includes to better protect TLS certificates than purely trusting a root store and X.509. Here, TLS does not operate in a browser and due to many layers on top, user interaction does not seem desirable. One has to consider this to be more a machine-2-machine case on the one hand. And on the other hand it is a case where not all computers on the Internet have to be considered for authentication, but only a restricted subset of machines of cloud providers and users.
Candidate technologies: Pinning, Notary Server, . . . note that it might be of interest to detect on which paths rough certificates are seen as the overall solution would allow to use alternative paths.

Your Task

- Study related work
- Analyse usage scenario in SafeCloud and in a partner scenario in particular
- Conceptual design
- Implementation in combination with a TLS library like OpenSSL
- Evaluation

Contact

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