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

Thesis B.Sc.

Thesis M.Sc.

Protection of Secure Communication with DNS

Motivation

The identification of the server in SSH is not very secure. Since server keys can change, a change in key does usually not raise enough of an alarm to counter potential attacks. This can allow for a variety of attacks, in particular man-in-the-middle attacks where the attacker tells the client his own key and the client accepts this. This is a problem we also face in our infrastructure and where we consider to find improvements.
There are currently a variety of ideas to improve protection for DNS and with DNS. DNSSec (protect DNS) and DANE (Authenticate with help of DNS) are two examples. The idea of the thesis is to combine both for the protection of SSH. If DNSSec is too complicated, other forms of secure communication could be used to transport this information securely with DNS (to a local DNS resolver that speeks the secure communication protocol).

Your Task

- Evaluate state-of-art with respect to concepts, tools, linux support, productive software
- Concept Development
- Write Scripts and Software
- Experimental Evaluation

Contact

Heiko Niedermayer niedermayer@net.in.tum.de
tbd