Betriebssysteme und Middleware
Prof. Dr. rer. nat. habil. Andreas Polze
Masterprojekt Wintersemester 2011/2012

Secure Neighbor Discovery

Background

To protect local networks against address spoofing attacks, the SEcure Neighbor Discovery Protocol (SEND) was devised, but is currently unimplemented. A common threat in actual deployments of IPv6 is the spoofing of router advertisement (RA) messages, which is often the consequence of misconfiguration rather than mischief. To protect RA messages, the authorization delegation discovery subprotocol allows trusted signing of router advertisements. While this was mostly theoretical so far, a recent project of the regional registries to perform resource certification now allows, in principle, to implement and deploy this protocol.

Description

The objective of this project is to validate router advertisement messages against a trust chain, individually on each node of the network. This will allow to filter out rogue router advertisements sent from misconfigured machines, which currently cause denial of service to all hosts (by redirecting traffic to a rogue router), and harm privacy, as the routers become able to inspect all IPv6 traffic.

The project members first need to understand the existing specifications and resolve variations that the specifications may allow. Research should be performed on the status of implementations of SEND aspects so far. For the implementation, the project members will target both the server (i.e. the router), and different client systems (such as Windows, OS X, and Linux). A project report will summarize the findings; remaining open issues may become the topic of a master's thesis.

References

- RFC 4861: Neighbor Discovery for IP version 6 (IPv6)
- RFC 3971: SEcure Neighbor discovery (SEND)
- Geoff Huston: Resource Certification. The Internet Protocol Journal, Volume 12, No. 1

Contact

Fachgebiet

- Prof. Dr. Andreas Polze
- Dr. Martin v. Löwis