(Ne)bojím se IPv6

Z přednášky Matěje Grégra na LinuxAltu

Bc. Lumír Balhar

@lumirbalhar on Twitter
www.frenzy.cz

Situace u IPv4

- Jednoduchá konfigurace skrze DHCP
- Existující ochrana proti útokům
  - Krádež IP adresy
  - Kráděž MAC adresy
  - Falešný DHCP server
  - Falešný DNS server
- Ochrana pomocí DHCP snooping

Situace u IPv6

- Složitá (bez)stavová konfigurace
  - DHCP existuje teprve chvíli
  - Komunikace v síti mezi klienty
- Neexistující ochrana proti útokům
  - DAD útok
  - Router advertisement flood
  - Man in the Middle

Ochrana proti útokům

- Drahá zařízení
- SeND – podpisy NS/NA zpráv (certifikáty)
  - Složité na klientskou část
- RA-Guard – podobný DHCP snoopingu
  - Lze obejít díky rozšířeným hlavičkám
- ACL pravidla
  - Lze obejít díky omezeným zdrojům

Nejlepší ochrana je

Zakázat IPv6!

Nějaké dotazy?