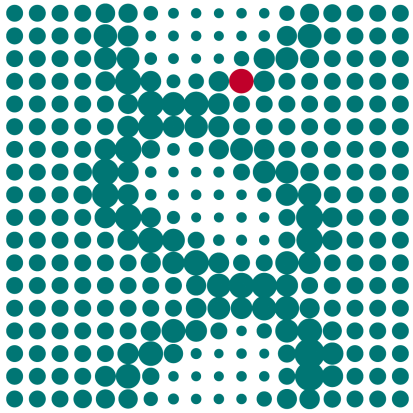
Sicherheit im Netz von SMTP- und HTTP-Servern

Paul Menzel (Max-Planck-Institut für molekulare Genetik)

9. November 2017

Wer bin ich?



- Systemarchitekt beim Max-Planck-Institut für molekulare Genetik
- Diplom-Wirtschaftsmathematiker an TU Berlin
- FLOSS-Befürworter

Problemstellung

Ziel

- Sichere Übertragung von Daten
- Geheim und authentifiziert

Angriffsmodell

- Annahme: Keine Übernahme der Server durch Angreifer
- Mittelsmannangriff

Realistisch?

- DFN-Netz separat vom „Internet“
- Netzwerkgeräte meist im Ausland produziert und enthält BLOBs
- Snowden-Veröffentlichungen zeigen, dass realistisch.

Lösungen

Angriffe

Verschiedene Angriffe.

1. Downgrade-Attacke (STARTTLS)

Verbreitung bei MPG

Werkzeuge

- Nmap
- SSLyze

Zeitraum

- 8.,November 2017

Ausblick

Sicherheit der Serverprogramme

- Problem: Dienste von überall erreichbar
- Beliebige Eingabe (Analyseprogramme (Spam, Virenschutz), Formulare)
- Untersuchung der Sicherheit der Server
  - SMTP: Postfix, Exim, ...
  - HTTP: Apache HTTP Server, Nginx, ...

Fragen