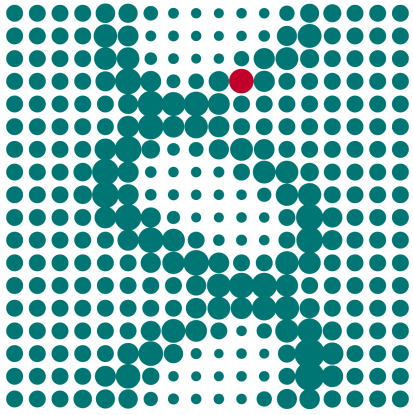
Sicherheit im Netz von SMTP- und HTTP-Servern

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

- TLS
- Zertifikatsstellen
- Monkeysphere Project
- DANE

Nur bei SMTP

- Ende-zu-Ende-Verschlüsselung (PGP/GPG, S/MIME)

Angriffe

Poodle, DROWN, ...

Verschiedene Angriffe.

1. Downgrade-Attacke (STARTTLS)
2. Poodle, DROWN
3. Unsichere Chiffren

Sichere Konfiguration

1. BetterCrypto.org
2. Mozilla Wiki: Security/Server Side TLS
3. Cipherli.st

Test

WWW

1. Hardenize
2. SSL-Tools
3. SSL Server Test von Qualys SSL Labs

Kommandozeile

1. OpenSSL, GnuTLS
2. Nmap
3. SSLyze
4. `posttls-finger`

Beispiel zu posttls-finger

```
$ posttls-finger ...
```

MPG

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