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 (TU Berlin)
- ► FLOSS-Befürworter

Präsentation

Folien in Markdown mit Pandoc nach LaTeX-Beamer umgewandelt, verfügbar auf GitHub.

 $https://github.com/paulmenzel/sicherheit_im_netz_von_smtp-_und_http-servern$



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)

- Zertifizierungsstellen (DFN, Let's Encrypt)
- Monkeysphere Project
- DANE

Nur bei SMTP

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

Zielumsetzung

SMTP

- Authentifizierung: Zustellung an korrekten Server
- Schutz der Metadaten
- geheime Übertragung auch bei nicht Ende-zu-Ende-Verschlüsselung

HTTP

- Authentifizierung: Kommunikation mit korrektem Server (Interaktion)
- Datenschutz (Metadaten wie URL geschützt)
- Verschlüsselung



Poodle, DROWN, ...

Verschiedene Angriffe.

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

Sichere Konfiguration

<postmaster@....mpg.de> nach RFC 822 Pflicht!

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

Ideal für SMTP

Mehrere Komponenten: DNS, Zertifikate

TLS

▶ MX-Eintrag stimmt mit Servernamen überein

DANE

TLSA-DNS-Einträge

Test

WWW

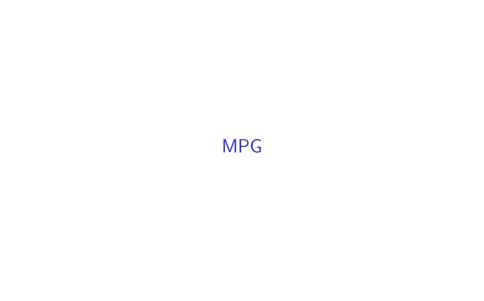
- 1. Hardenize
- 2. SSL-Tools
- 3. SSL Server Test von Qualys SSL Labs

Kommandozeile

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

Beispiel zu posttls-finger

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



Zeitraum

▶ 8. November 2017

Inkorrekte MX-Einträge

Beispiel GV

```
$ host mpg.de
[...]
$ host mx1.mpg.de
[...]
```

Keine Antwort von postmaster@mpg.de auf Nachricht.

Problem Verwaltungsadressen

```
$ host vw.molgen.mpg.de
[...]
```

Bitte überprüfen!



Problem

- 1. Viele alte Dienste ohne HTTPS-Zertifikat, ohne ACME oder Wildcard-Zertifikate schwer zu handhaben
- 2. Never-touch-a-running System

Lösung

- 1. SSL-Terminierung (HAProxy)
- Wechsel zu Let's Encrypt und Skript, dass Zertifikate in Echtzeit erstellt

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, ...

Fazit

- 1. MPG-Netz auch Vorbildwirkung
- 2. Mehr Gewissenhaftigkeit
- 3. Mehr Bewusstsein (DNSSEC, DFN)
- 4. Ohne DANE keine automatische Konfiguration möglich, manuelle Konfiguration erforderlich

Fragen