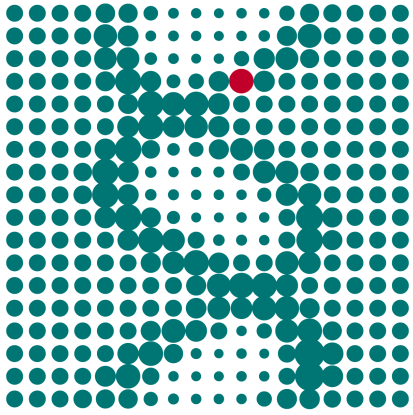
Sicherheit im Netz von SMTP- und HTTP-Servern

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

Problemstellung

Ziel

- Sichere Übertragung von Daten
- Geheim und authentifiziert

Betrachtung in Vortrag

- SMTP: Zwischen SMTP-Servern (MTA)

Angriffsmodell

- Annahme: Keine Übernahme der Server durch Angreifer
- Annahme (SMTP): Vertrauen in Betreiber der Server auf Sender- und (Ziel-)Empfängerseite
- Annahme (HTTP): Sicherer Browser, HTTP korrekt konfiguriert
- Mittelsmannangriff

Realistisch?

- Innerhalb der MPG: DFN-Netz separat vom „Internet“ (Florida, CBS, . . .)
- Netzwerkgeräte meist im Ausland produziert und enthalten BLOBs
- Snowden-Veröffentlichungen zeigen, dass realistisch

Lösungen (TLS)

- SMTP: `STARTTLS`
- HTTP: HTTPS (Port 443)
- 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

Angriffe

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 ...
```

MPG

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!

HTTP

Techniken

1. Weiterleitung von HTTP zu HTTPS (DNS-Angriff noch möglich)
2. HSTS (DNS-Angriff bei erstem Zugriff immer noch möglich)
3. HTTPS Everywhere (EFF)
4. HKPK
5. DNSSEC/DANE

DNSSEC/DANE

1. Abfrage von DANE nur mit Erweiterungen
2. Boykott von Browserherstellern (DNSSEC schwer zu handhaben), bevorzugen HKPK

Problem bei Umsetzung

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

Lösung

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

HTTP/2

1. Standardmäßig HTTPS
2. Vorteil für mobile Nutzer (besonders bei schlechtem System wie Fiona oder OHB)

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