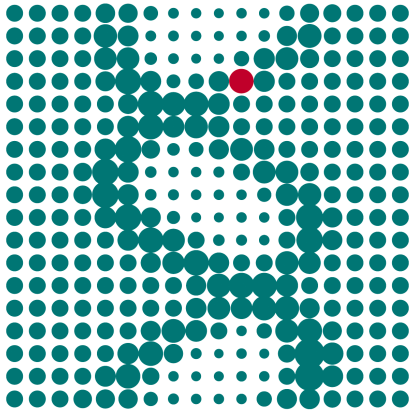
Sicherheit im Netz von SMTP- und HTTP-Servern

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.

TinyURL: https://tinyurl.com/smtphttp

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

Mittelsmannangriff

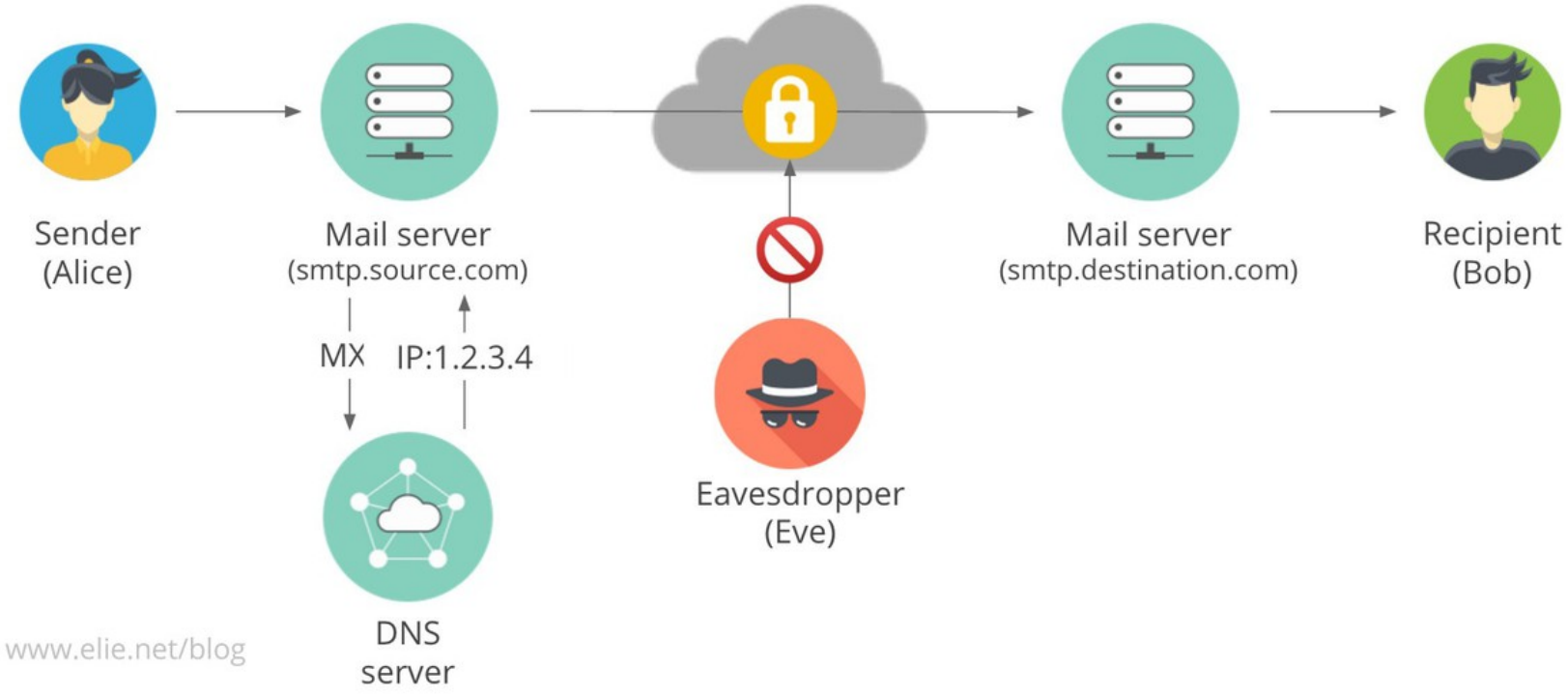


Figure 1: Mittelsmannangriff (https://www.elie.net/blog/understanding-how-tls-downgrade-attacks-prevent-email-encryption)

Realistisch?

- Innerhalb der MPG: DFN-Netz separat vom „Internet“
- Dienste außerhalb

```
$ host -t mx maxplanckflorida.org
maxplanckflorida.org mail is handled by \
0 maxplanckflorida-org.mail.protection.outlook.com.
$ host -t mx cbs.mpg.de
cbs.mpg.de mail is handled by \
10 mx0-cbs-mpg.heinlein-support.de.
cbs.mpg.de mail is handled by 20 \
mx1-cbs-mpg.heinlein-support.de.
```

- 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
- DNSSEC/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

Test

WWW

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

Kommandozeile

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

SMTP

Ideal für SMTP

Mehrere Komponenten: DNS, Zertifikate

TLS

- MX-Eintrag stimmt mit Servernamen überein

DNSSEC/DANE

- TLSA-DNS-Einträge

Beispiel zu posttls-finger

```
$ /usr/sbin/posttls-finger -c -l secure \
-P /etc/ssl/certs mpifr-bonn.mpg.de
posttls-finger: mail2.mpifr-bonn.mpg.de[134.104.18.60]:25:
Matched subjectAltName: mail2.mpifr-bonn.mpg.de
posttls-finger: mail2.mpifr-bonn.mpg.de[134.104.18.60]:25 \
CommonName mail2.mpifr-bonn.mpg.de
posttls-finger: mail2.mpifr-bonn.mpg.de[134.104.18.60]:25:
subject_CN=mail2.mpifr-bonn.mpg.de, issuer_CN=MPG CA, \
fingerprint=CA:5D:E7:7C:8A:6B:C5:4B:CC:7E:DB:F1:0C:43:C1:76
pkey_fingerprint=FD:27:CA:F2:DD:0B:AD:91:9C:6E:83:90:5E:A4
posttls-finger: Verified TLS connection established to \
mail2.mpifr-bonn.mpg.de[134.104.18.60]:25: \
TLSv1.2 with cipher \
ECDHE-RSA-AES256-GCM-SHA384 \(256/256 bits)
```

MPG

Zeitraum

- 8. November 2017

Inkorrekte MX-Einträge

Beispiel GV

```
$ host -t mx mpg.de
mpg.de mail is handled by 5 mx1.mpg.de.
mpg.de mail is handled by 5 mx2.mpg.de.
$ host mx1.mpg.de
mx1.mpg.de has address 194.95.232.60
mx1.mpg.de has address 194.95.238.60
mx1.mpg.de has address 194.95.234.60
$ host 194.95.232.60
60.232.95.194.in-addr.arpa domain name pointer \
mfilter-123-1-1.mx.srv.dfn.de.
```

Keine Antwort von postmaster@mpg.de auf Nachricht.

Problem Verwaltungsadressen

```
$ host vw.molgen.mpg.de
vw.molgen.mpg.de mail is handled by 5 mx2.mpg.de.
vw.molgen.mpg.de mail is handled by 5 mx1.mpg.de.
```

```
$ host vw.molgen.mpg.de
vw.molgen.mpg.de mail is handled by \
5 mfilter-123-1-2.mx.srv.dfn.de.
vw.molgen.mpg.de mail is handled by \
5 mfilter-123-1-1.mx.srv.dfn.de.
vw.molgen.mpg.de mail is handled by \
5 mfilter-123-1-3.mx.srv.dfn.de.
```

Bitte überprüfen!

GWDG und DFN sollten aktiv werden.

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, ...
- Finanzierung von Audits und Umsetzung von neuen Methoden

Fazit

1. MPG-Netz auch Vorbildwirkung
2. Mehr Gewissenhaftigkeit
3. Mehr Bewusstsein (DNSSEC, DFN)
4. Ohne DANE keine automatische Konfiguration möglich, manuelle Konfiguration erforderlich
5. Finanzierung von Verbesserung der Browser und Weiterentwicklung der Erweiterungen

Fragen