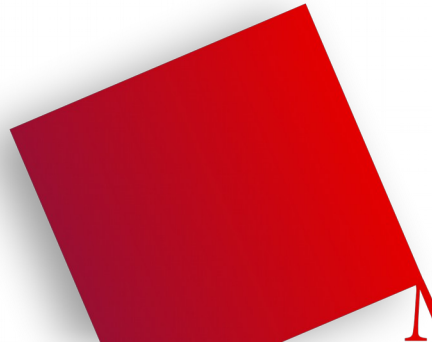


HOCHSCHULE
FÜR ANGEWANDTE
WISSENSCHAFTEN
MÜNCHEN

Sicherheitsanalyse der TLS-Konfiguration von SMTP-Installationen

Bachelorarbeit

Thomas Maier

Einführung

- Sicherheitsziele bei SMTP
- Entwicklung von TLS
- Frage:

  Wie sicher ist TLS
  bei Mailservern konfiguriert?
- Suche einer Antwort:

  Scan von vielen Mailservern
  + Auswertung!

Inhalt

- Problematiken von TLS
- Verwandte Arbeiten
- Datenerhebung
- Evaluierung
- Zusammenfassung
- Ausblick

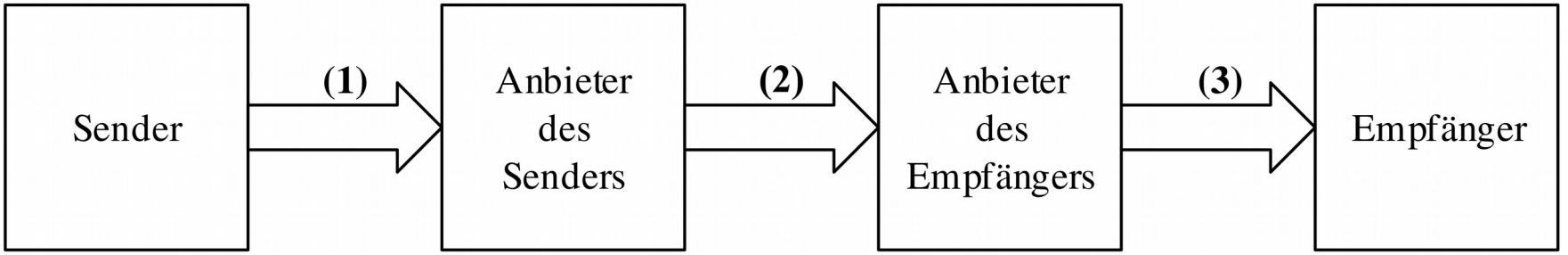
Problematiken von TLS

- Vertrauensverhältnis zu CAs
- Schwache Cipher Suites
  - NULL Cipher Suites

    `TLS_NULL_WITH_NULL`
    `TLS_RSA_WITH_NULL_MD5`
    `TLS_DH_anon_WITH_RC4_128_MD5`
  - Export Cipher Suites

    `TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5`
- Schwachstellen (z.B. Heartbleed)

Problematiken von TLS (bei SMTP)



- Kontrolle über Transportverschlüsselung
- TLS-Unterstützung
- Selbstsignierte Zertifikate / Unbekannte CAs
- Lösung
  - Inter Mail Provider Trust (IMPT)
  - DNS-based Authentication of Named Entities (DANE)

DANE

Records der Zone us.

```
us. 518400 IN DNSKEY 257 3 5 (AwEAAe+x...) ; KSK; alg = RSASHA1; key id = 7228
us. 518400 IN DNSKEY 256 3 5 (AwEAAdmM...) ; ZSK; alg = RSASHA1; key id = 6990
us. 518400 IN DNSKEY 256 3 5 (AwEAAbdi...) ; ZSK; alg = RSASHA1; key id = 64491
us. 518400 IN DNSKEY 257 3 5 (AwEAAcPL...) ; KSK; alg = RSASHA1; key id = 44323

us. 518400 IN RRSIG DNSKEY 5 1 518400 (20150329022117 20150227020000 44323 US. Oyw3r...)

DOUGBARTON.us. 7200 IN DS 12946 8 2 (417F297...)

DOUGBARTON.us. 7200 IN RRSIG DS 5 2 7200 (20150329220647 20150227214706 64491 us. LscYWEs...)
```

(1) Signiert DNSKEY Set mit Key **44323**

(3) Signiert DS Set mit DNSKEY **64491**

(2) Verweist auf DNSKEY **12946** mit Hash

Records der Zone dougbarton.us.

```
dougbarton.us. 10765 IN DNSKEY 257 3 8 (AwEAAcQXw...) ; KSK; alg = RSASHA256; key id = 12946
dougbarton.us. 10765 IN DNSKEY 256 3 8 (AwEAAexPK...) ; ZSK; alg = RSASHA256; key id = 48078

dougbarton.us. 10765 IN RRSIG DNSKEY 8 2 10800 (20150331000000 20150228230000 12946 dougbarton.us. IuZ6F...)
dougbarton.us. 10765 IN RRSIG DNSKEY 8 2 10800 (20150331000000 20150228230000 48078 dougbarton.us. N8Fhz...)

_25._tcp.dougbarton.us. 10444 IN TLSA 1 0 2 (F994F42...)

_25._tcp.dougbarton.us. 10721 IN RRSIG TLSA 8 4 10800 (20150413103452 20150314094322 48078 ...)
```

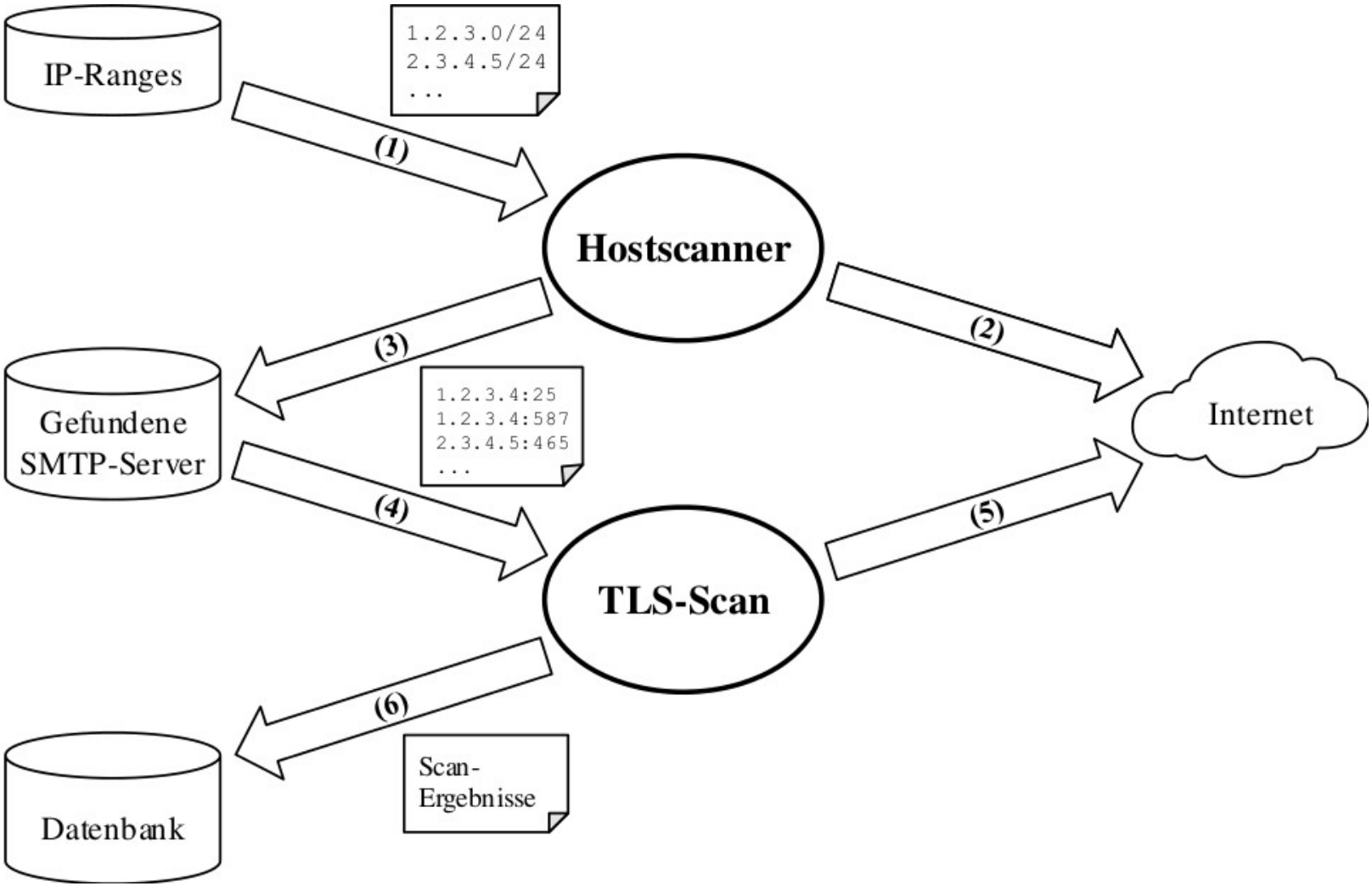
(4) Signieren DNSKEY Set mit Key **12946** und **48078**

(5) Signiert TLSA Set mit DNSKEY **48078**

Verwandte Arbeiten

- TLS-Untersuchungen: Nur für HTTP vorhanden
- Qualys SSL Labs
  - SSL Server Test (Web-Interface)
  - SSL Server Rating Guide (Rating-System)
  - SSL Labs API
  - SSL Pulse
- SSLyze

Datenerhebung



Datenerhebung

- Empfehlungen ZMap-Paper
- Server (KVM, 16 GB RAM, 2,6 GHz x4)
- Organisatorisches
  - Munich IT Security Research Group (MuSe)
  - Fakultät für Informatik
  - Hochschule München
  - Leibniz-Rechenzentrum (LRZ)
  - Deutsches Forschungsnetz (DFN)

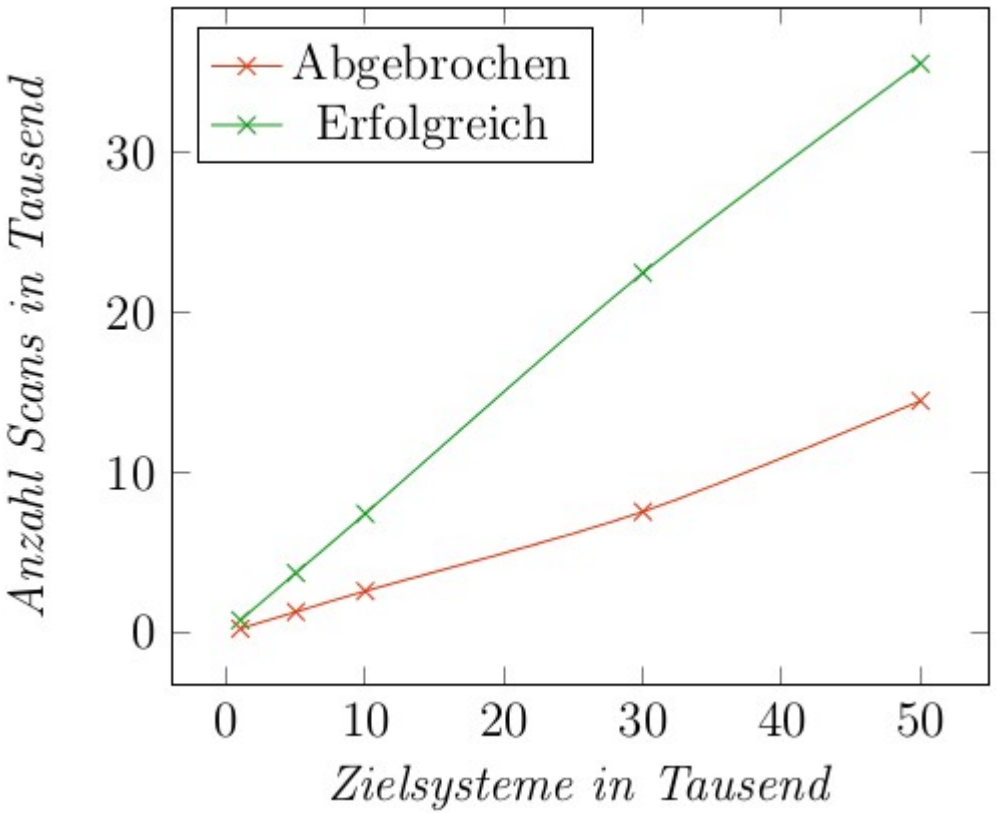
Datenerhebung

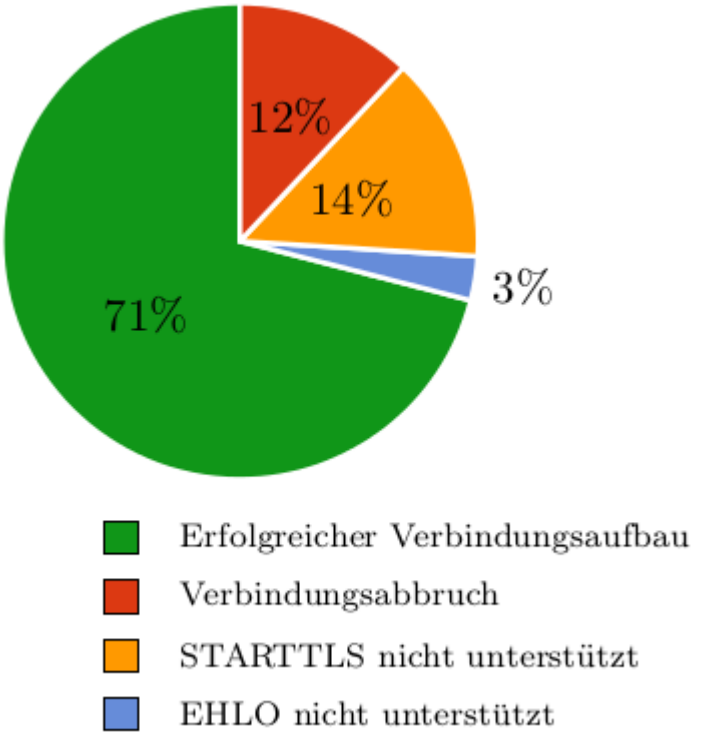
- Dauer
  - 30.000 Zielsysteme: ~ 14 Stunden
  - 18,7 Mio. Zielsysteme: ~ 23 Jahre
  - 50.000 Zielsysteme: ~ 23 Stunden
- Einschränkung auf Deutschland

  Insgesamt gefunden: ~ 900.000 Zielsysteme

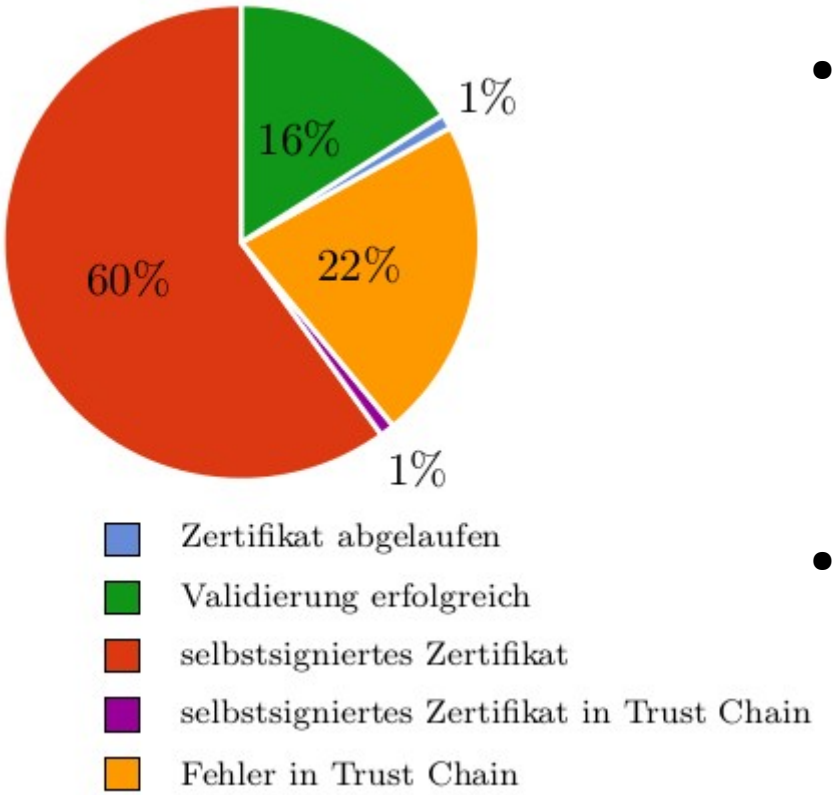
  Davon überprüft: 50.000 Zielsysteme

Evaluierung



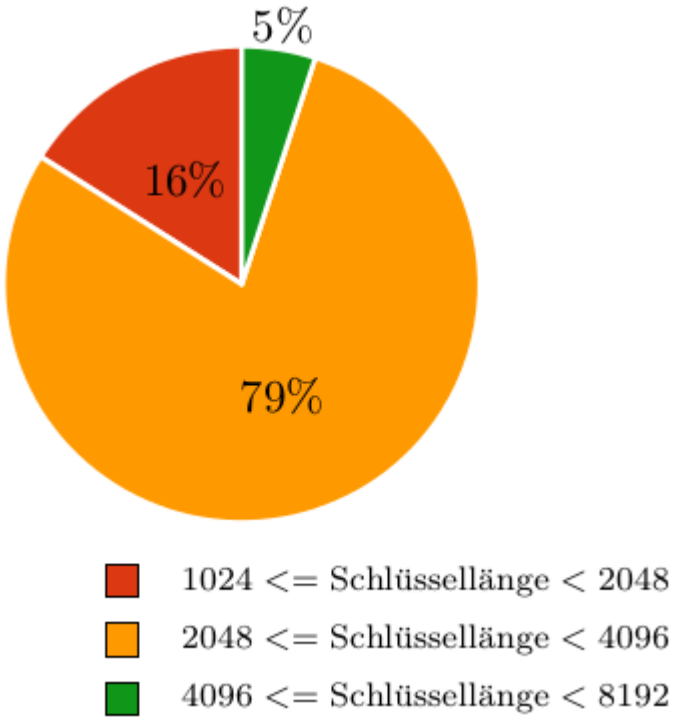


Evaluierung - Zertifikate



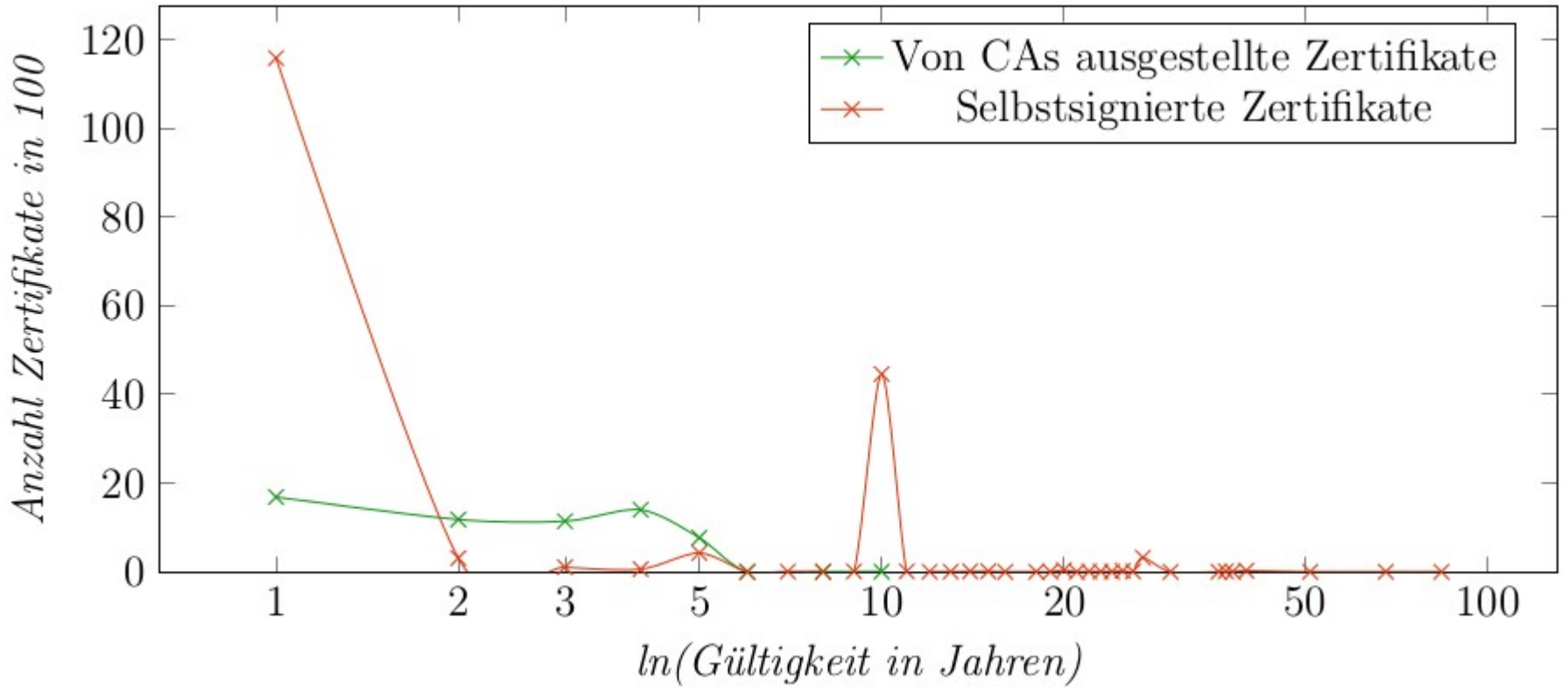
- X.509-Validierung
  - Hier:
    84% nicht validierbar
  - SSL Pulse:
    5,2% nicht validierbar
- DANE: 3 / 35.535 erfolgreich!

Evaluierung - Zertifikate

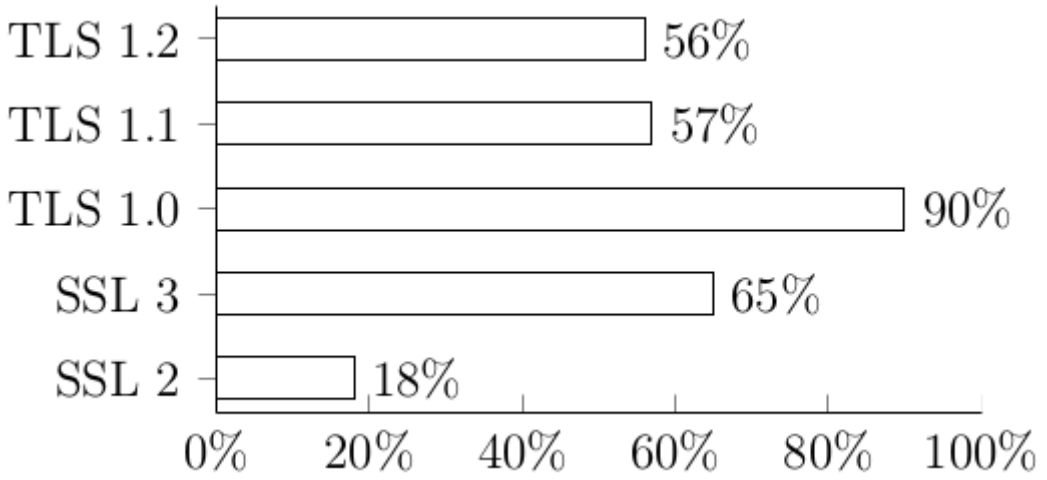


- NIST-Empfehlung: 2048 Bit
- Zu einem Großteil eingehalten
- Mittelwert hier: 1985 Bit

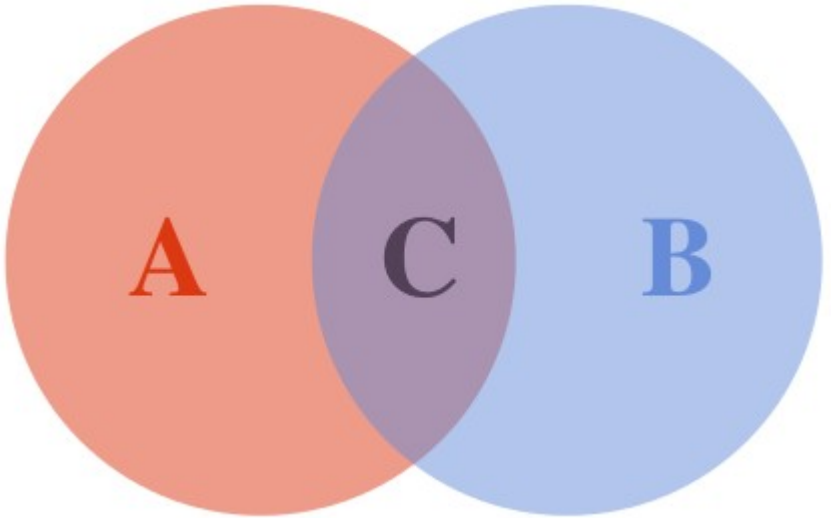
Evaluierung – Zertifikate



Evaluierung – TLS-Versionen



Evaluierung – Cipher Suites



- A: Mindestens eine BSI-CS
- B: Mindestens eine Nicht-BSI-CS
- A \ B: Nur BSI-CS (0,34%)
- B \ A: Nur Nicht-BSI-CS (90,73%)
- C = A ∩ B: BSI-CS und Nicht-BSI-CS (8,93%)
- B: 99,66% halten sich **nicht** komplett an BSI!

Zusammenfassung

- Nur wenige vorhandene Projekte
- Lange Laufzeiten
- Frage:
  Wie sicher ist TLS bei (deutschen) Mailservern konfiguriert?
- Antwort:
  Beim Abgleich mit Empfehlungen und im Vergleich zu HTTP: Nein!

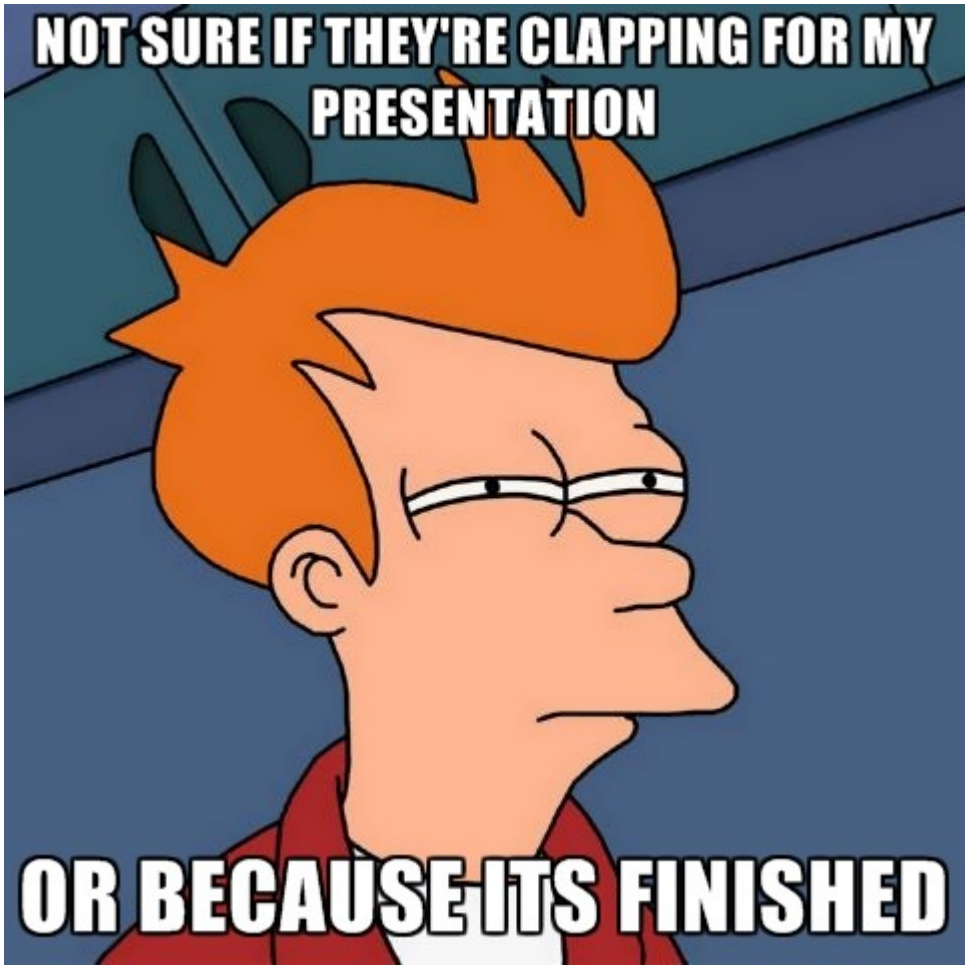
Ausblick

- Globale Datenerhebungen
- Regelmäßige Ausführung
- Weitere Überprüfungen
  - TLS-Versionen, z.B.
    Wie oft unterstützt ein Zielsystem nur SSL 2 und 3?
  - Cipher Suites
  - Zertifikate

Ende

- Vielen Dank für Ihre Aufmerksamkeit
- Zeit für Fragen :-)

Ende


NOT SURE IF THEY'RE CLAPPING FOR MY PRESENTATION
OR BECAUSE ITS FINISHED