Aktuelle Umsetzung von SMTP over TLS

Ein Realitätscheck

Thomas Maier[1] Thomas Schreck[2] Hans-Joachim Hof[1,3]

[1]Hochschule München

[2]FIRST.org

[3]Munich IT Security Research Group

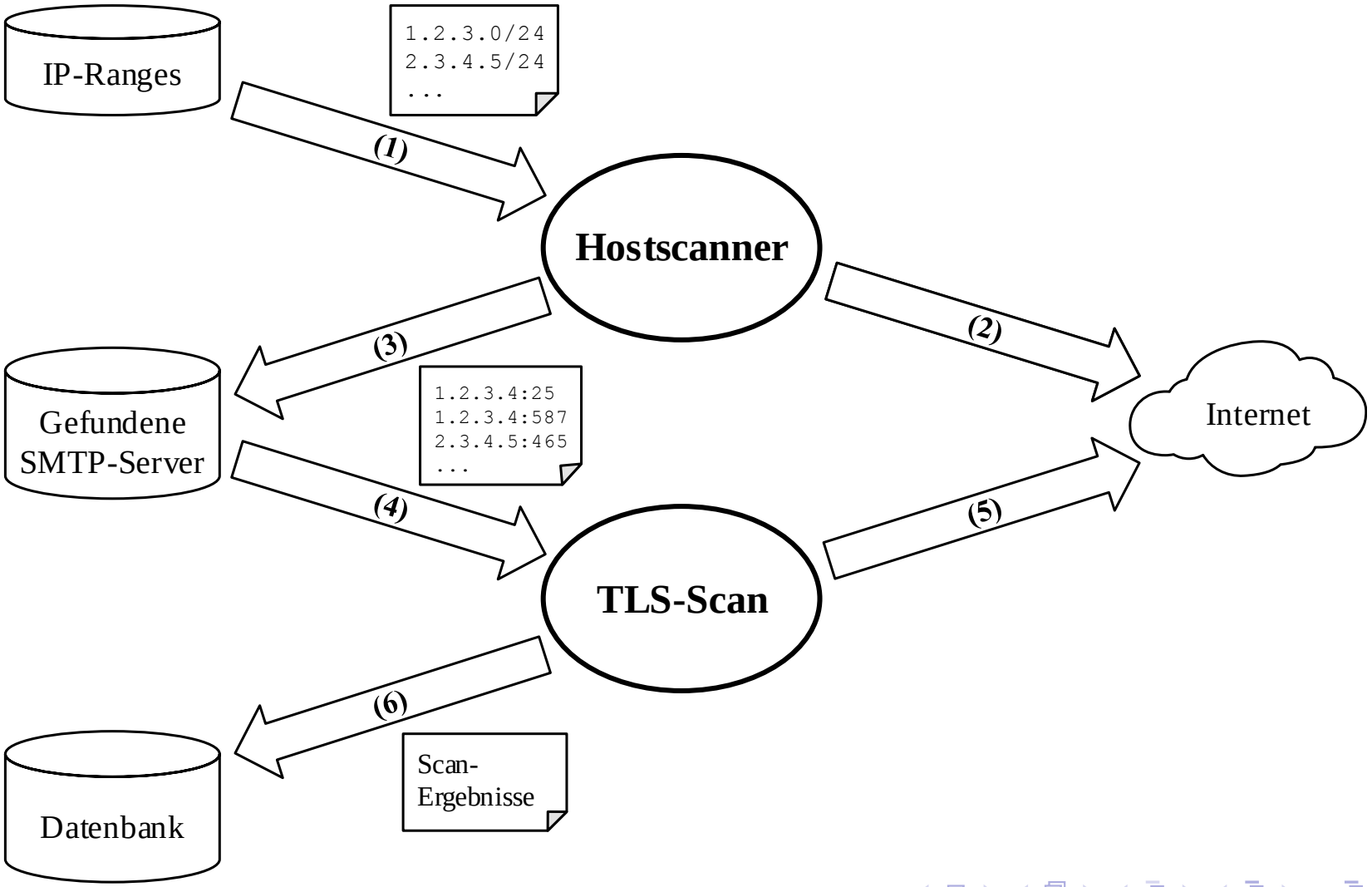
23. DFN-Konferenz "Sicherheit in vernetzten Systemen"

Motivation

- Sicherheit von SMTP-Servern beruht darauf, dass TLS richtig konfiguriert ist
- Wie wird TLS von SMTP-Betreibern in Deutschland umgesetzt?

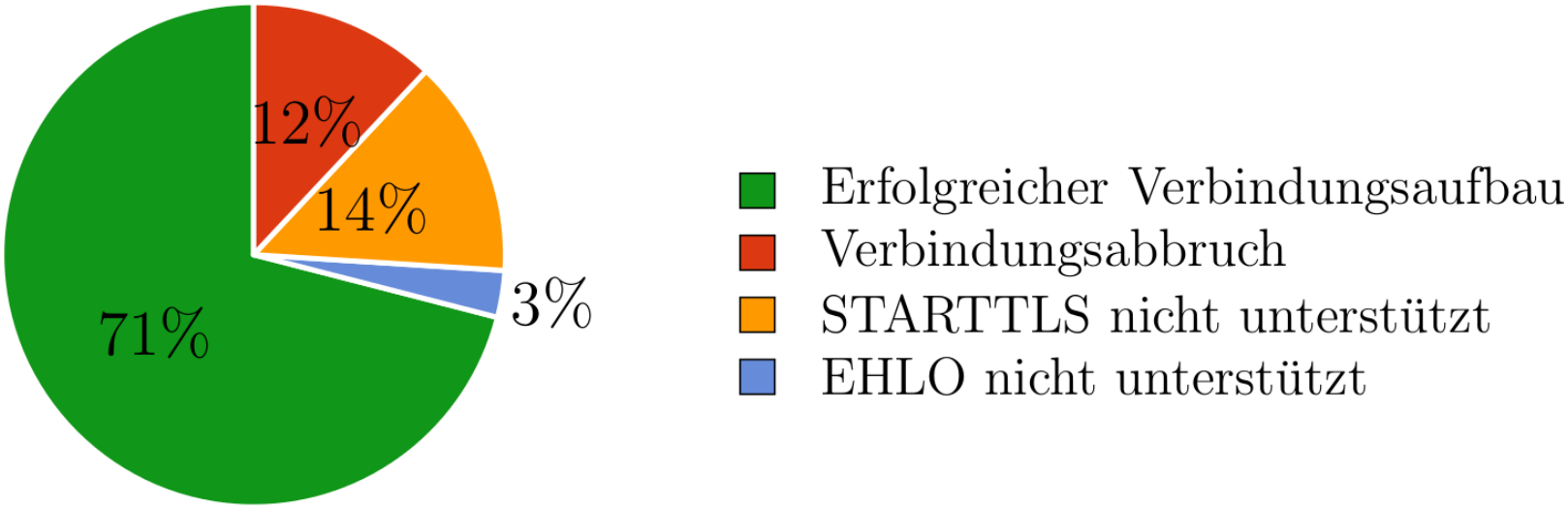
Datenerhebung

50.000 IP-Port-Kombinationen in 24 Std. (Auswahl randomisiert)



Evaluierung

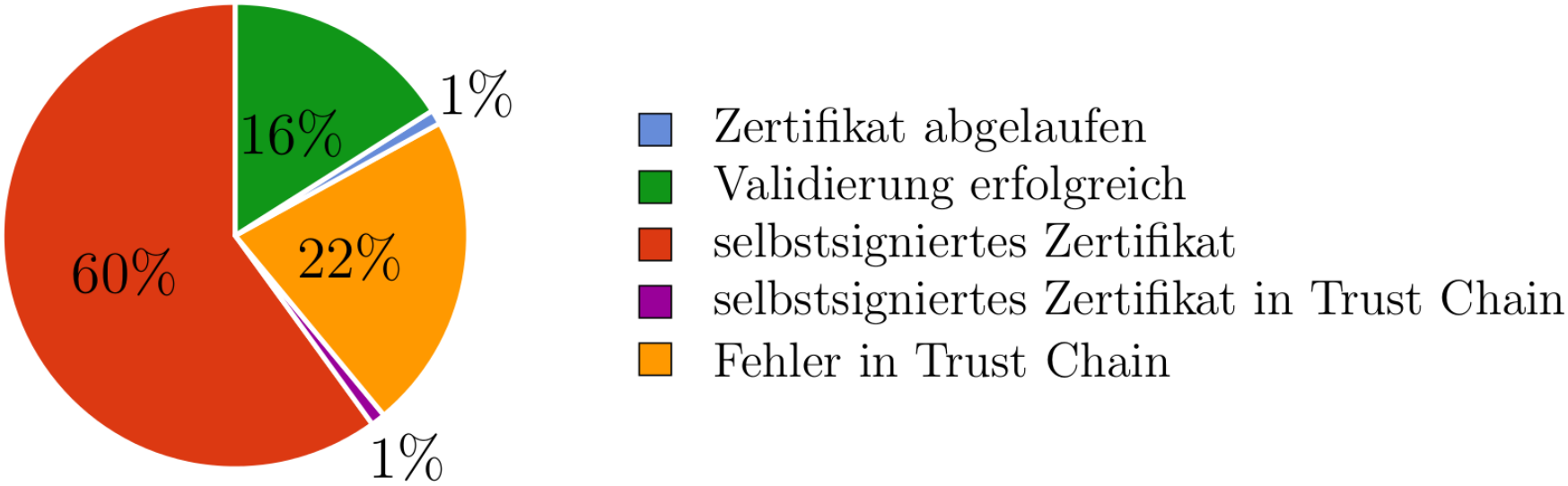
TLS-Unterstützung



Heartbleed: 3,72% anfällig

Evaluierung

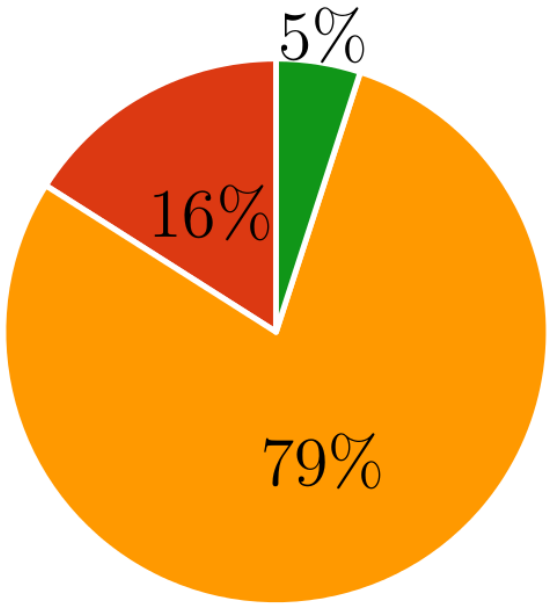
X.509-Validierung



DANE: 3/35.535 validierbar

Evaluierung

X.509-Schlüssellängen

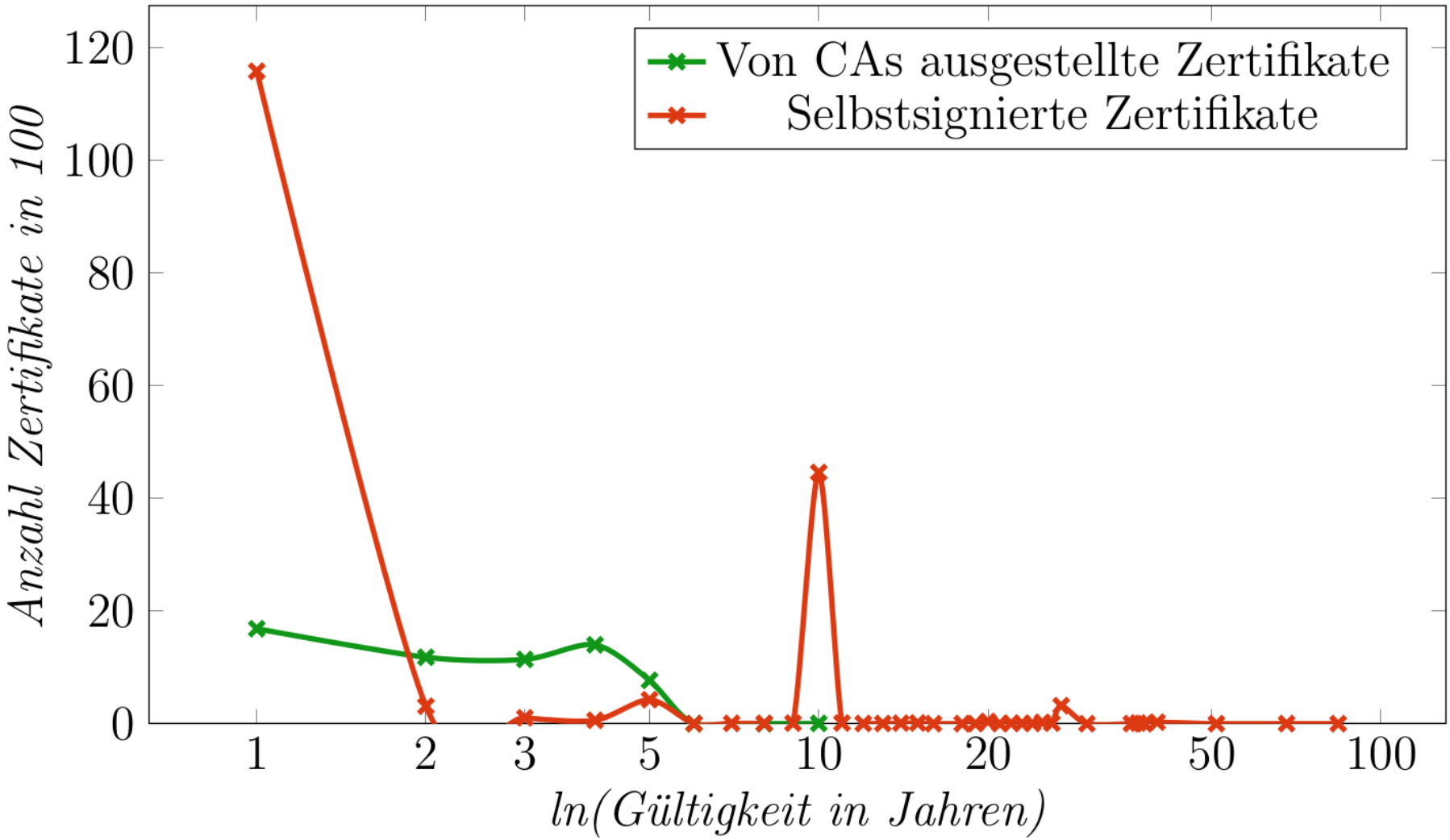


- $1024 <= \text{Schlüssellänge} < 2048$
- $2048 <= \text{Schlüssellänge} < 4096$
- $4096 <= \text{Schlüssellänge} < 8192$

NIST-Empfehlung: 2048 Bit

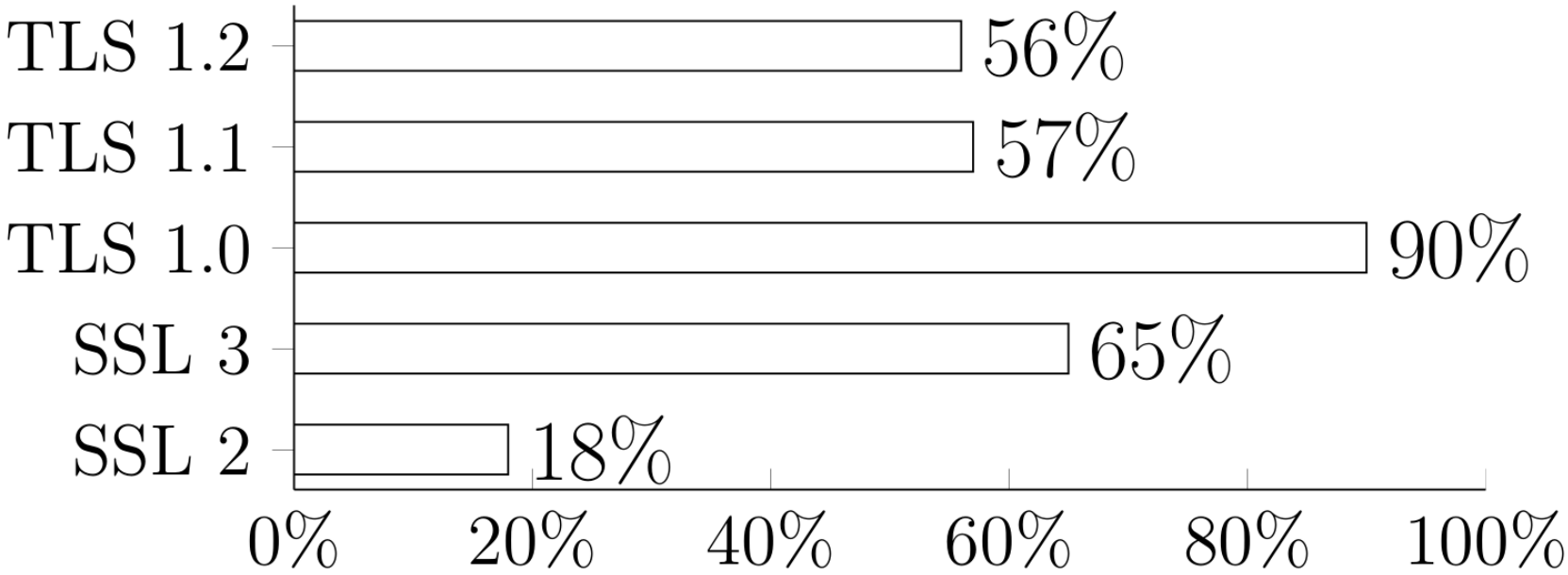
Evaluierung

X.509-Gültigkeit



Evaluierung

TLS-Versionen



Evaluierung

Cipher Suites nach BSI

- BSI empfiehlt Liste von Cipher Suites (CS)
- Nur BSI-CS: 0,34%
- Nur Nicht-BSI-CS: 90,73%
- Sowohl BSI-CS, als auch Nicht-BSI-CS: 8,93%
- 99,66% halten sich nicht komplett an BSI

Zusammenfassung

- Schlechterer Stand als bei HTTP (siehe SSL Pulse)
- Häufiger Einsatz schwacher Cipher Suites/gebrochener TLS-Versionen
- Häufiger Einsatz von zu lange gültigen selbstsignierten Zertifikaten
- Spätere Arbeiten bestätigen Ergebnisse
  - Wilfried Mayer et al., "No Need for Black Chambers: Testing TLS in the E-mail Ecosystem at Large" (Oct 2015)
  - Ralph Holz et al., "TLS in the wild: an Internet-wide analysis of TLS-based protocols for electronic communication" (Nov 2015)
- Empfehlungen: BetterCrypto.org

Kontakt

Fragen?

Bachelorarbeit: PDF

Kontakt

Mail: tmaier@fs.cs.hm.edu

Jabber: tamier@jabber.de

GnuPG key ID: 0x57824B8B