
**Ich schreibe meinen
eigenen SSL/TLS-Checker.
Ist doch ganz einfach, oder ??**

Dirk Wetter

@drwetter



0. Wer bin ich?

■ Einzelunternehmer

- ▶ Sicherheit seit 1996
- ▶ Kunden aus allen Branchen
 - Bank, Versicherer, ISPs, E-Government (Bund, Land, Kommune), Versorger, Health, Produzierendes Gewerbe, E-Commerce, Soziale Netze, u.v.a.
- ▶ Kompetenz
 - [Vorträge](#) zum Thema (Web-)sicherheit auf Konferenzen
 - Zahlreiche [Veröffentlichungen](#),
- ▶ Ehrenamt
 - Engagiert in [GUUG](#) und [OWASP](#)
 - PKs Fachkonferenzen, Chair
 - Organisation OWASP [AppSecEU 2013](#) u.a.
- ▶ Open Source

0. Einleitung

■ testssl.sh

- ▶ Gestartet 2005 als Inhouse-Tool (Pentests)
- ▶ Open sourced: <= 2010
 - 2/2014: gleichnamige Domain
 - 4/2014: bitbucket
 - 10/2014: github
- ▶ In BackTrack, BlackArch Linux
 - Debian, Arch Linux: wishlist

0. Einleitung

■ testssl.sh

▶ Besonderheit:

- Kommandozeile!
- `/bin/bash`

▶ Kompatibel:

- Linux-Distributionen ≤ 4 Jahre
- Mac OS X
- (Free)BSD
- Windows: MSYS2, Cygwin

1. Idee

■ Anno 2005

- ▶ OpenSSL als Schweizer Messer
 - CN / expiration date
 - Zertifikate
 - Protokollversionen
 - Cipher

- ▶ Trust:
 - s.o. / -verify
 - Browser



1. Idee

■ Demo

1. Idee

■ Anno 2005

- ▶ Mehr?
- ▶ Brauchte es (fast) nicht!
 - Ok ok ...
 - es gab da ein paar Bugs ;-)
 - Debian weak keys (2006)
 - Sonst: NSE Plugin ggf.
 - Sonst: Version/Banner Fingerprinting

2. Heute

■ Anno 2015

- ▶ Tierisch gewachsen
 - Knapp 5000 Zeilen Code
 - Relativ „reif“
 - Viele Features

- ▶ **Demo**

2. Heute, etwas zurück gespult

■ Wie macht der das mit

▶ Heartbleed

- TLS Extension
- Was ist eine TLS Extension?



(Einschub: TLS Extension)

■ RFC 3546 (2003)

- ▶ Erweiterung des ursprünglichen Handshakes
 - **Server Name Indication**
 - **Status Request (OCSP)**

```

√ Secure Sockets Layer
  √ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    - Content Type: Handshake (22)
    - Version: TLS 1.0 (0x0301)
    - Length: 403
    √ Handshake Protocol: Client Hello
      - Handshake Type: Client Hello (1)
      - Length: 399
      - Version: TLS 1.2 (0x0303)
      > Random
      - Session ID Length: 0
      - Cipher Suites Length: 238
      > Cipher Suites (119 suites)
      - Compression Methods Length: 2
      > Compression Methods (2 methods)
      - Extensions Length: 119
      > Extension: server_name
      > Extension: ec_point_formats
      > Extension: elliptic_curves
      > Extension: SessionTicket TLS
      > Extension: signature_algorithms
      > Extension: status_request
      > Extension: Heartbeat
      > Extension: next_protocol_negotiation

```

Request



Secure Sockets Layer

▼ TLSv1.2 Record Layer: Handshake Protocol: **Server Hello**

Content Type: Handshake **(22)**

Version: TLS 1.2 (0x0303)

Length: 87

▼ Handshake Protocol: Server Hello

Handshake Type: Server Hello (2)

Length: 83

Version: **TLS 1.2 (0x0303)**

▶ Random

Session ID Length: 0

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)

Compression Method: null (0)

Extensions Length: 43

▶ Extension: server_name

▶ Extension: renegotiation_info

▶ Extension: ec_point_formats

▶ Extension: SessionTicket TLS

▶ Extension: status_request

▼ Extension: Heartbeat

Type: Heartbeat (0x000f)

Length: 1

Mode: Peer allowed to send requests (1)

▶ Extension: next_protocol_negotiation

Response
openssl s_client

3. Sockets vs. OpenSSL

■ Anno 2014

▶ Heartbleed



TLS Extension



Was ist eine TLS Extension?

- Heartbeat: **sinnlose** Extension

- Für die meisten

▶ Buffer Overflow, mem access

- Trivialer Zugriff
- Geht nicht mit OpenSSL!
- PoC in bash sockets
 - Demo



3. Sockets vs. OpenSSL

■ Anno 2014

- ▶ Heartbleed
 - TLS Extension
- ▶ CCS Injection
 - Ähnlich, brauchte Sockets

→ **Demo**

3. Sockets vs. OpenSSL

■ OpenSSL

- ▶ Neue Distributionen/Mac OSX: „Fixes“
 - Null, Anonymous Ciphers
 - SSLv2
 - Wg. SSL-Poodle: SSLv3 maybe coming?
 - export ciphers (FREAK)
 - weak DH ciphers (Logjam)
- ▶ OTOH
 - Advanced features missing
 - 3x Chacha20/Poly1305 cipher
 - -proxy, -curves, -xmpphost host, ...

3. Sockets vs. OpenSSL

■ Sockets vs. OpenSSL

▶ Beides!

→ Sockets, ggf. wo nötig

- Protokoll check SSLv2 - TLS 1.1
- TLS time
- s.o. HB+CCS
 - Auch: Proxy
 - Auch: STARTTLS

→ Verteilung von Binaries

- Basierend auf [Peter Mosmans fork](#)
- Linux, BSD, Darwin, ARM

4. Bugs a.k.a. Features (sometimes)

■ Open LiteSpeed

- ▶ SSLv2: gar nicht erst supported
- ▶ Antwortet trotzdem

→ **Demo**

- Problem1: Plaintext
- Problem2: Es gibt keinen echten Handshake in SSLv2

■ IIS 6.0

- ▶ Support ist ausgelaufen

→ **Demo**

- (Für einige wohl egal)
- OpenSSL 1.0.2: Handshake failure
 - handshake-size limit, OpenSSL 1.0.2 hat mehr Cipher

4. Bugs a.k.a. Features (sometimes)

■ „Lustiger“ Debian/Ubuntu Bug

```
dirks@laptop:~|0% export OPENSSL_CONF=gost.conf
dirks@laptop:~|0% nslookup -query=a testssl.sh
GOST engine already loaded
08-Sep-2015 20:12:43.648 ENGINE_by_id failed (crypto failure)
08-Sep-2015 20:12:43.649 error:2606A074:engine routines:ENGINE_by_id:no such engine:eng_list.c
st
(null): dst_lib_init: crypto failure
dirks@laptop:~|10% host testssl.sh
GOST engine already loaded
08-Sep-2015 20:12:56.324 ENGINE_by_id failed (crypto failure)
08-Sep-2015 20:12:56.325 error:2606A074:engine routines:ENGINE_by_id:no such engine:eng_list.c
st
host: dst_lib_init: crypto failure
dirks@laptop:~|1% dig +short testssl.sh
GOST engine already loaded
08-Sep-2015 20:13:06.326 ENGINE_by_id failed (crypto failure)
08-Sep-2015 20:13:06.327 error:2606A074:engine routines:ENGINE_by_id:no such engine:eng_list.c
st
dig: dst_lib_init: crypto failure
dirks@laptop:~|10% grep PRETTY_NAME /etc/os-release
PRETTY_NAME="Ubuntu 14.04.3 LTS"
dirks@laptop:~|0% █
```

► Sonst: Debian Wheezy, Ubuntu 15.04

4. Zusammenfassung

- **Projekt ist „alive and kicking“**
 - ▶ Letztes Release: Contributions++
 - ▶ Herausforderungen
 - Verwundbarkeiten: Am Ball bleiben
 - Erwartungen: wird weniger
 - Kaputte Handshakes
 - Plattform-Kompatibilität

4. Zusammenfassung

■ Zukunft

▶ Missing Features (

[github.com/drwetter/testssl.sh/milestones/2.7dev%20\(2.8\)%20](https://github.com/drwetter/testssl.sh/milestones/2.7dev%20(2.8)%20))

- Sockets
 - TLS 1.2: extensions
 - Statt checks mit unsicheren Ciphers, disabled
- Trust stores
- Zertifikatskette
- EC Kurven
- JSON Output
 - HTML über „aha“
- Rating!

4. Zusammenfassung

■ Zukunft, cont'd

- ▶ Interne Verbesserungen
 - Codequalität ;-)
 - Dokumentation

5. Und immer dran denken...

- **Bestellung auf Webseite:**
 - ▶ **Beste Verschlüsselung**



5. Und immer dran denken...

► **Bestätigungsmail**

- Mit allen zuvor eingegebenen Daten



- **Danke!**

- > `https://testssl.sh/`

- > `dirk aet testssl.sh`

- > `https://drwetter.eu/`

- > `mail aet drwetter.eu`



@drwetter