DEEPSEC

Lawful Interception in Theorie und Praxis

Linuxwochen Eisenstadt 2019, FH Burgenland, 27. April 2019

René Pfeiffer

Lawful Interception

DEEPSEC

- Lawful Interception
  - Verwendet im PSTN
  - Standardisiert für moderne Netzwerke (ETSI, 3GPP, CALEA, …)
- Militärische Überwachung
  - SIGINT / COMINT
  - CYBINT / DNINT
- Massenüberwachung

Geschichte: Briefgeheimnis

DEEPSEC

- Josephinischen Wahlkapitulation (1690)
- Allgemeinen preußischen Postordnung vom 10. August 1712
- Secret de la correspondance (Ludwig XV, 25. September 1742)
  - Für Briefe und Pakete
  - Todesstrafe für Zuwiderhandelnde (Postbeamte)
- Artikel 141 der Paulskirchenverfassung (1849)
- Briefgeheimnis im Grundgesetz (Weimarer Reichsverfassung)
- Übernommen in vielen modernen Verfassungen

Deutschland: Art. 10 GG

DEEPSEC

1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.

2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, daß sie dem Betroffenen nicht mitgeteilt wird und daß an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt.

Österreich: Art. 10 StGG

- Das Briefgeheimniß darf nicht verletzt und die Beschlagnahme von Briefen, außer dem Falle einer gesetzlichen Verhaftung oder Haussuchung, nur in Kriegsfällen oder auf Grund eines richterlichen Befehles in Gemäßheit bestehender Gesetze vorgenommen werden.

Europa: Art. 8 EMRK

DEEPSEC

- Europäische Menschenrechtskonvention 1998

  1) Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.

  2) Der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts ist nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die *nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer* notwendig ist.

Telekommunikationsgesetze

- Abhören von Telekommunikation ist strafbar
- Geregelt in TKG (Deutschland & Österreich)
- Ausnahmen betreffen
  - Strafverfolgung
  - Bedrohung für den Staat
  - Kriegsfall / Verteidigungsfall

USA: CALEA

DEEPSEC

- Communications Assistance for Law Enforcement Act (1994)
- Abhöreinrichtung für digitale Kommunikation
  - Voice Calls, Textnachrichten
  - Echtzeitfähigkeiten
  - Vorschrift für Telekommunikationsfirmen
  - VoIP und Breitband (ab 2004)
- Entschlüsselung vorgeschrieben (soweit möglich)
- Anmerkung: Skype war bis ca. 2009 nicht CALEA-konform

EU: ETSI Lawful Interception

DEEPSEC

- Europarat Resolution (17. Januar 1995)
- Modelliert nach CALEA
- Publizierte Standards
  - ES 201 671 Handover Interface for the Lawful Interception of Telecommunications Traffic
  - ES 201 158 Requirements for Network Functions
  - TS 102 234 Service-specific details for Internet access services
  - TS 102 233 Service-specific details for e-mail services
  - TS 102 232 Handover Specification for IP Delivery
  - TS 102 815 Service-specific details for Layer 2 Lawful Interception
  - TS 101 331 Requirements of Law Enforcement Agencies
  - TR 102 053 Notes on ISDN lawful interception functionality
  - TR 101 944 Issues on IP Interception
  - TR 101 943 Concepts of Interception in a Generic Network Architecture

Russland: SORM-3

DEEPSEC

- IPv4/IPv6 Adresse/Netzwerk
- User ID eines Telekommunikationsanbieters
- E-Mail mit POP3, IMAP, SMTP ohne SSL/TLS
- E-Mail ausgewählter Webmail-Anbieter
- Telefonnummer
- IMEI, IMSI
- MAC Adresse der verwendeten Hardware
- ICQ UIN

Transport Layer Security

DEEPSEC

- Secure Sockets Layer (SSL) / Transport Layer Security (TLS)
- SSL veraltet, TLS v1.0/v1.1 ebenso
- TLS v1.2 hat Brückenfunktion
  - Kompromiss zwischen v1.0/v1.1 und Sicherheit
  - Perfect Forward Secrecy (Session Keys)
- TLS v1.3 seit August 2018 (RFC8446)
  - Grundlegende Überarbeitung
  - Neue Algorithmen
  - End-to-End Encryption per Design

TLS v1.3

DEEPSEC

- ~~Typ (RSA, DSA, ECDSA) & Mechanismus (DHE or ECHDE)~~
- ~~Session Renegotiation~~
- ~~Compression~~
- ~~CBC Mode~~
- ~~RC4, DES, 3DES, Export-Algorithmen~~
- ~~SHA1~~
- ~~MD5~~
- ~~Statischer RSA Handshake~~

TLS v1.3

- Kürzerer Handshake (Illustration)
- Downgrade Protection
- Perfect Forward Secrecy für alle Sessions
  - Ausschaltung von Human-In-The-Middle
  - Detektieren von gefälschten Zertifikaten

TLS v1.3 in OpenSSL 1.1.1

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_8_SHA256
- TLS_AES_128_CCM_SHA256

Middleboxen

DEEPSEC

- TLS – Inhalte können nicht inspiziert werden
- Firewalls / Application Layer Gateways
  - führen eigene (interne) Certificate Authority
  - Clients kennen eigene CA (durch Import)
  - Generierung von Zertifikaten in Echtzeit
- Entwurf für interne Netzwerke
- Öffentliche CAs bieten Sub-CAs für Filter an
  - stark kritisiert
  - exponiert durch Cert Pinning & CA Transparency

- Middle Box Problematik
- Studie The Security Impact of HTTPS Interception

Product	Grade	Validates Certificates	Modern Ciphers	Advertises RC4	TLS Version	Grading Notes
A10 vThunder SSL Insight	F	✓	✓	Yes	1.2	Advertises export ciphers
Blue Coat ProxySG 6642	A*	✓	✓	No	1.2	Mirrors client ciphers
Barracuda 610Vx Web Filter	C	✓	✗	Yes	1.0	Vulnerable to Logjam attack
Checkpoint Threat Prevention	F	✓	✗	Yes	1.0	Allows expired certificates
Cisco IronPort Web Security	F	✓	✓	Yes	1.2	Advertises export ciphers
Forcepoint TRITON AP-WEB Cloud	C	✓	✓	No	1.2	Accepts RC4 ciphers
Fortinet FortiGate 5.4.0	C	✓	✓	No	1.2	Vulnerable to Logjam attack
Juniper SRX Forward SSL Proxy	C	✓	✗	Yes	1.2	Advertises RC4 ciphers
Microsoft Threat Mgmt. Gateway	F	✗	✗	Yes	SSLv2	No certificate validation
Sophos SSL Inspection	C	✓	✓	Yes	1.2	Advertises RC4 ciphers
Untangle NG Firewall	C	✓	✗	Yes	1.2	Advertises RC4 ciphers
WebTitan Gateway	F	✗	✓	Yes	1.2	Broken certificate validation

Fig. 3: **Security of TLS Interception Middleboxes**—We evaluate popular network middleboxes that act as TLS interception proxies. We find that nearly all reduce connection security and five introduce severe vulnerabilities. *Mirrors browser ciphers.

- Einwand von BITS auf IETF Mailing Liste
- ETSI ETS = TLS v1.3 – PFS
- „Data Centre TLS“

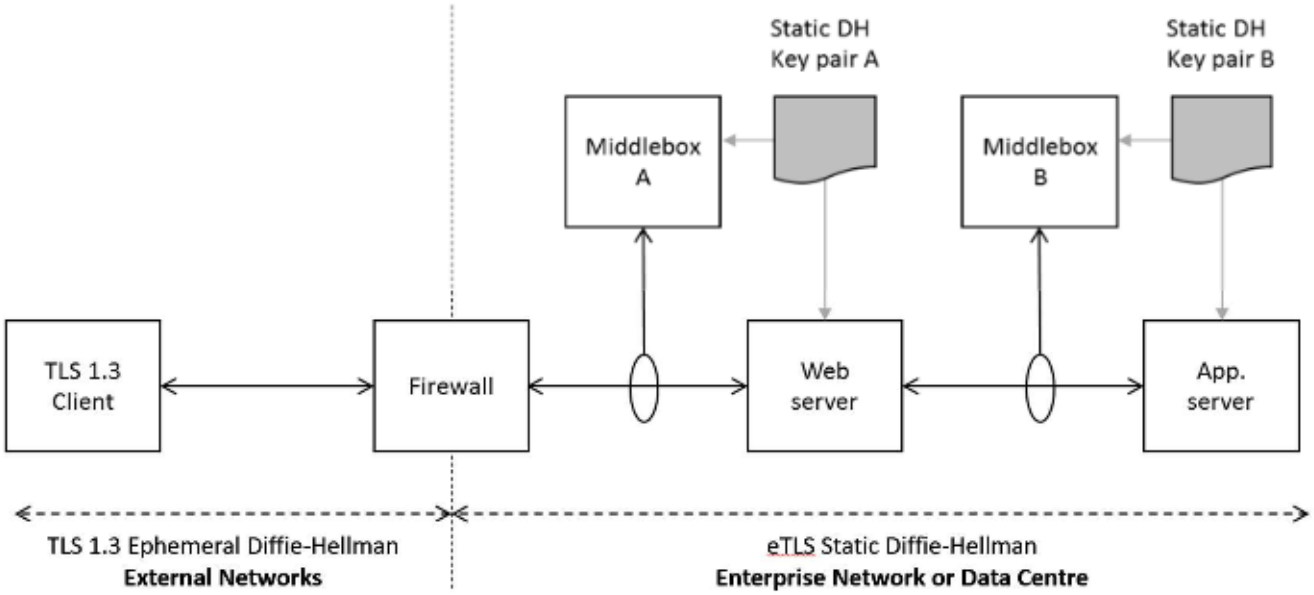


Figure 4.1: eTLS architecture with enterprise servers

USA: NIST Empfehlungen

DEEPSEC

October 15, 2018

Transport Layer Security (TLS) provides mechanisms for protecting data during electronic dissemination across the Internet. **Draft NIST Special Publication (SP) 800-52 Rev.2, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations***, provides guidance for selecting and configuring TLS protocol implementations using NIST-recommended cryptographic algorithms and Federal Information Processing Standards (FIPS). The document requires that government TLS servers and clients support TLS 1.2 configured with FIPS-based cipher suites.

This second draft extends the deadline by which agencies are urged to support TLS 1.3 to January 1, 2024. Moreover, it clarifies that TLS 1.3 is intended to coexist with TLS 1.2 rather than replace it. An appendix has also been added to discuss key exchange using RSA key transport and includes a list of cipher suites that may be used if a transition period is needed. The extensions guidance now clarifies which versions of TLS each extension applies to and provides guidance on the raw public keys extension.

A public comment period for this document **is open until November 16, 2018**.

Quelle: Second Draft of NIST's Transport Layer Security (TLS) Guidance

ETSI Warnungen

DEEPSEC

- Europäische Standards-Organisation warnt USA vor TLS 1.3
- CVE-2019-9191 – fehlende PFS in ETSI ETS
  - CVSS v3.0 Medium (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)
  - CVSS v2.0 Medium (AV:N/AC:M/Au:N/C:P/I:N/A:N)
- PCI 3.1 empfiehlt TLS v1.2 oder besser

TLS „Forensik“

DEEPSEC

- Verwendung von TLS bei Schadsoftware
  - Infizierung
  - C&C
  - Nachladen von Code
- TLS leicht erkennbar
- sehr viele Betriebsmodi und -parameter

TLS Fingerprinting

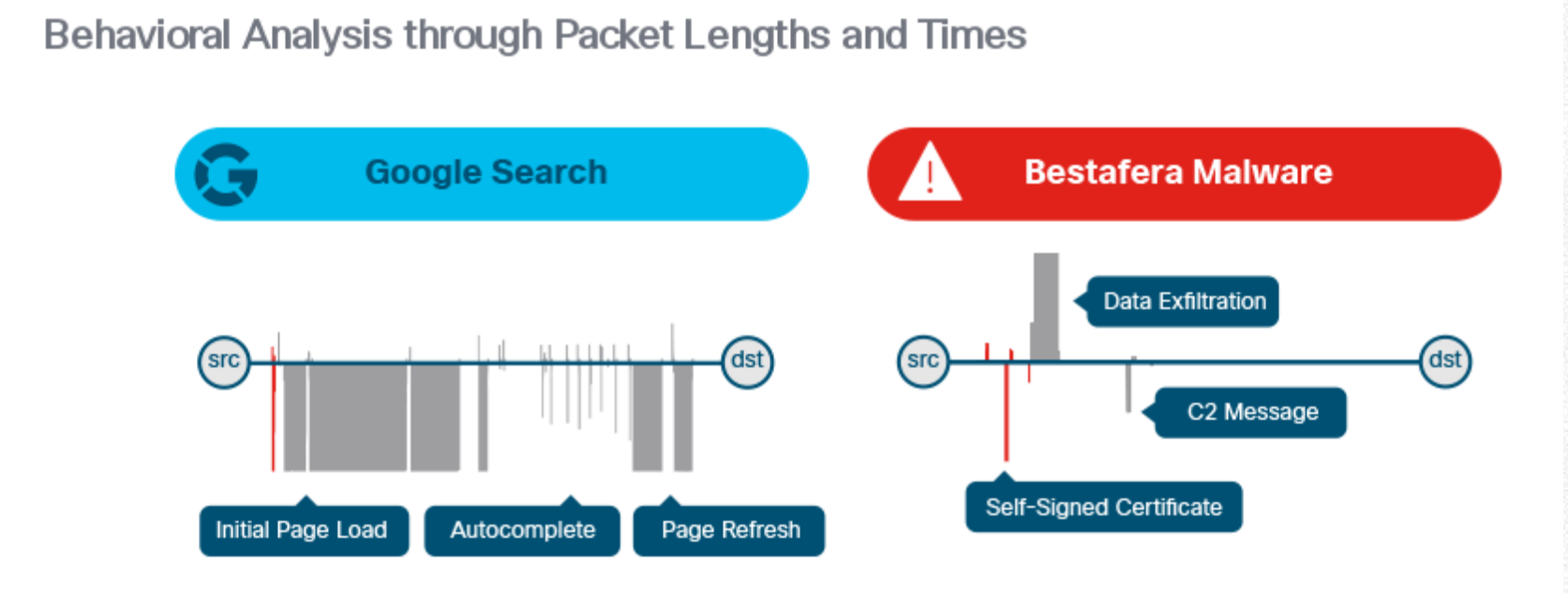
DEEPSEC

- SSL fingerprinting for p0f
- HTTP Client Fingerprinting Using SSL Handshake Analysis
  - Apache Modul
- TLS Fingerprinting with JA3 and JA3S
  - Client und Server
  - Tests im Tor Netzwerk
  - Funktioniert mit TLS v1.3
- FingerPrinTLS Collection

TLS Fingerprinting Daten

DEEPSEC

- TLS Handshake
- Paketlängen
- Intervalle zwischen Paketen
- TLS Metadaten
  - Cipher Suites mit Reihenfolge
  - TLS Extensions
  - Default Settings



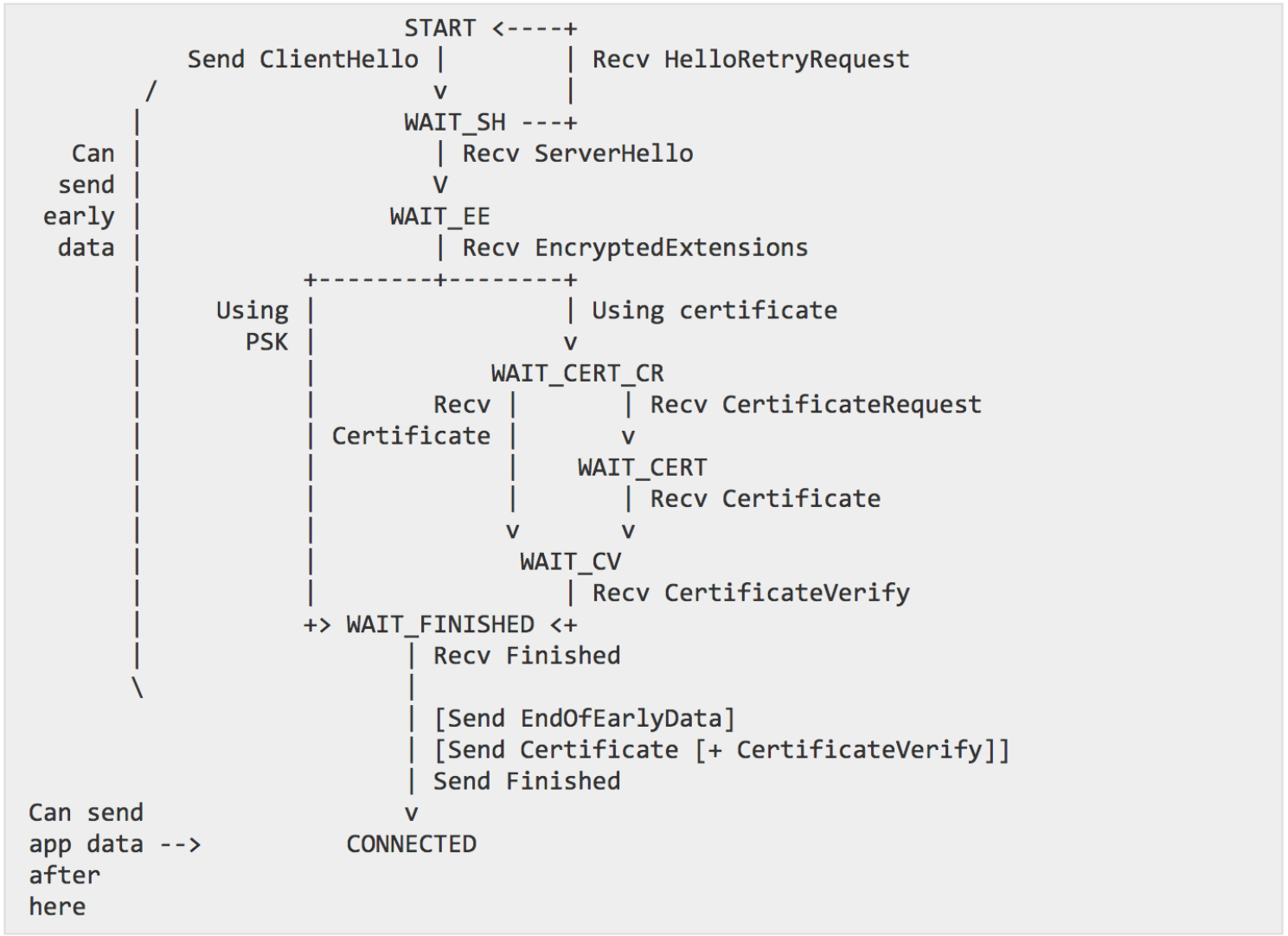
Quelle: Detecting Encrypted Malware Traffic (Without Decryption)

Zusammenfassung

DEEPSEC

- Standards für LI vorhanden
- TLS ist wesentlicher Transport in Netzwerken
- TLS v1.3 hat starken Fokus auf Ende-zu-Ende Verschlüsselung
- ETSI ETS ↔ NIST Empfehlung für TLS v1.3
  - Gefahr für Implementation (z.B. Software Entwicklung)
  - Motivation für gegenteilige Empfehlung unklar
- Middleboxes einzige Hürde für TLS v1.3 Einführung
  - TLS Version Intolerance (Implementationsfehler)
  - GREASE (Generate Random Extensions And Sustain Extensibility)

Fragen?


START <----+
Send ClientHello | | Recv HelloRetryRequest
v |
WAIT_SH ---+
Can | | Recv ServerHello
send | V
early | WAIT_EE
data | | Recv EncryptedExtensions
+--------+--------+
Using | | Using certificate
PSK | v
WAIT_CERT_CR
Recv | | Recv CertificateRequest
Certificate | v
| WAIT_CERT
| | Recv Certificate
v v
WAIT_CV
| Recv CertificateVerify
+> WAIT_FINISHED <+
| Recv Finished
|
| [Send EndOfEarlyData]
| [Send Certificate [+ CertificateVerify]]
| Send Finished
Can send v
app data --> CONNECTED
after
here


DEEPSEC

Kontaktmöglichkeiten

DEEPSEC

- ✉ rpfeiffer@deepsec.net
- 🔐 0x518A0576C3A9FF76 (PGP/GnuPG)
- FP: AE26 3866 FB54 4A5E 0BE5 AD90 8531 093E 6E40 37AF
- 📞 +43.676.5626390 (Signal verfügbar/empfohlen)
- 📞 +807 949 050 59 (GSMK Cryptophone™)
- 🖝 9EKKN34F (Threema)

Quellen

DEEPSEC

- Titelbild aus Artikel

  What the President Could Do If He Declares a State of Emergency

  von Elizabeth Goitein