

TeleTrust-EBCA "PKI-Workshop" 2019

Bundesverband IT-Sicherheit e.V. (TeleTrust)

Berlin, 18.06.2019

Brauchen wir wirklich eine Backdoor? TLS 1.3 vs. eTLS

Sören Beiler / Net at Work GmbH

Was ist TLS 1.3, was gibt es neues?

- Zwingend Perfect Forward Secrecy durch Diffie-Hellman Schlüsselaustausch
- Höhere Performance dank moderner Cipher Suites
- Einsatz von AEAD gewährleistet Vertraulichkeit und Integrität der übermittelten Daten
- Unsichere Cipher Suites wie 3DES, MD5, AES-CBC, SHA-1 werden konsequent ausgeschlossen

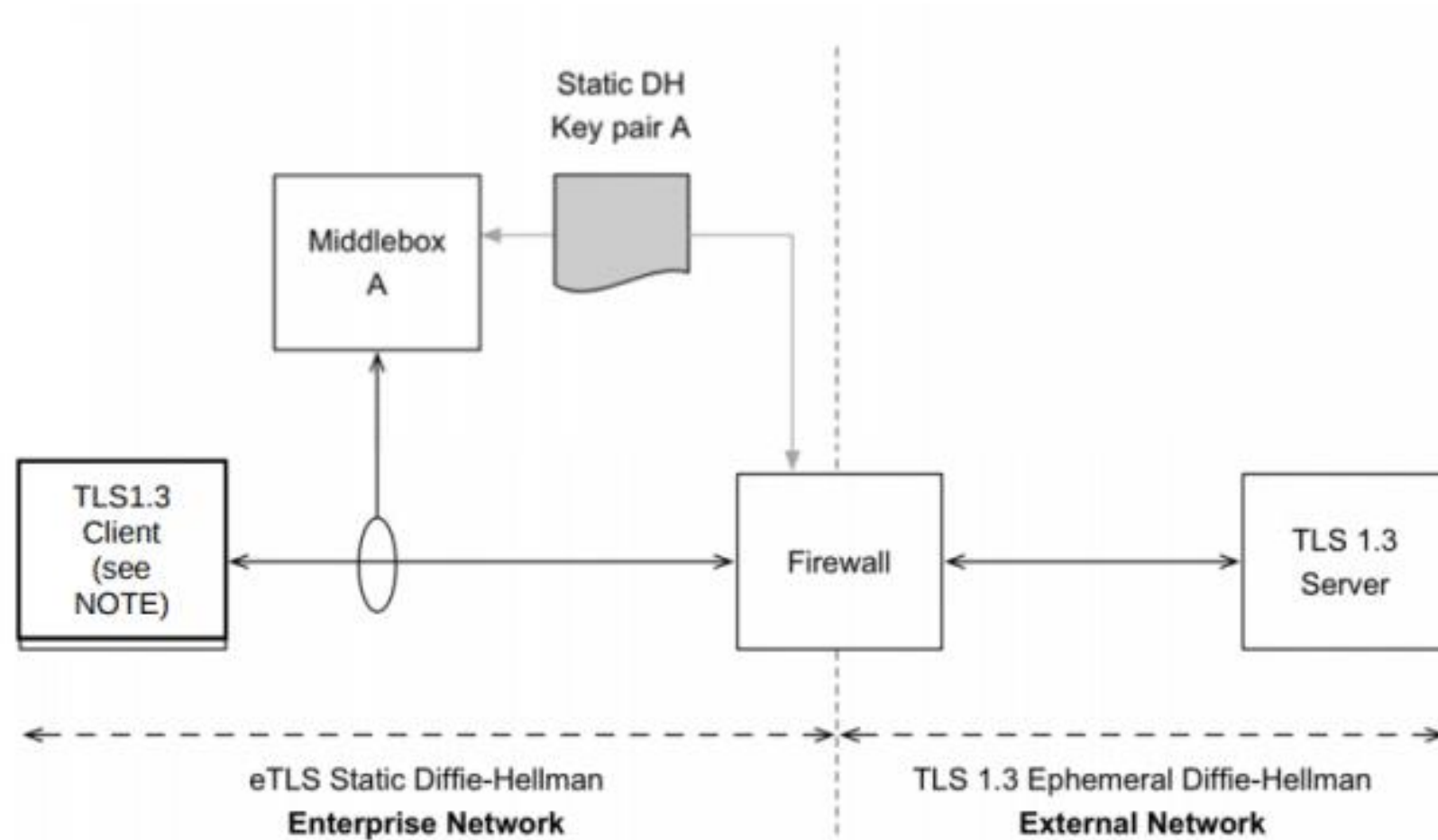
Welche Probleme sind trotz TLS 1.3 noch offen?

- Content Security Policys können umgangen werden
- Clickjacking, Code Injection kann nicht verhindert werden
- Keine Deep Paket Inspection mehr möglich
- Partielle Forward Secrecy: bestand bereits eine Verbindung, wird der PSK Key beim erst 0-RTT nicht neu ausgehandelt
- Weiterhin Side Channel Attacken auf RSA nach Bleichenbacher möglich
- Downgrade Attacken auf TLS 1.1 oder 1.2 weiterhin möglich

Was ist ETS, formerly known as eTLS

- Hat das Ziel trotz Transportverschlüsselung den Datenstrom der Clients inspizieren zu können
- Hebelt die erzwungene Perfect Forward Secrecy aus durch Einsatz statischer DH Schlüssel

Wie funktioniert eTLS (ETS)



Brauchen wir wirklich eine Backdoor in TLS?

- Einsatz von ETS kann nicht vom Client erkannt werden

- Kann auch zur Spionage ausgenutzt werden

Nein!

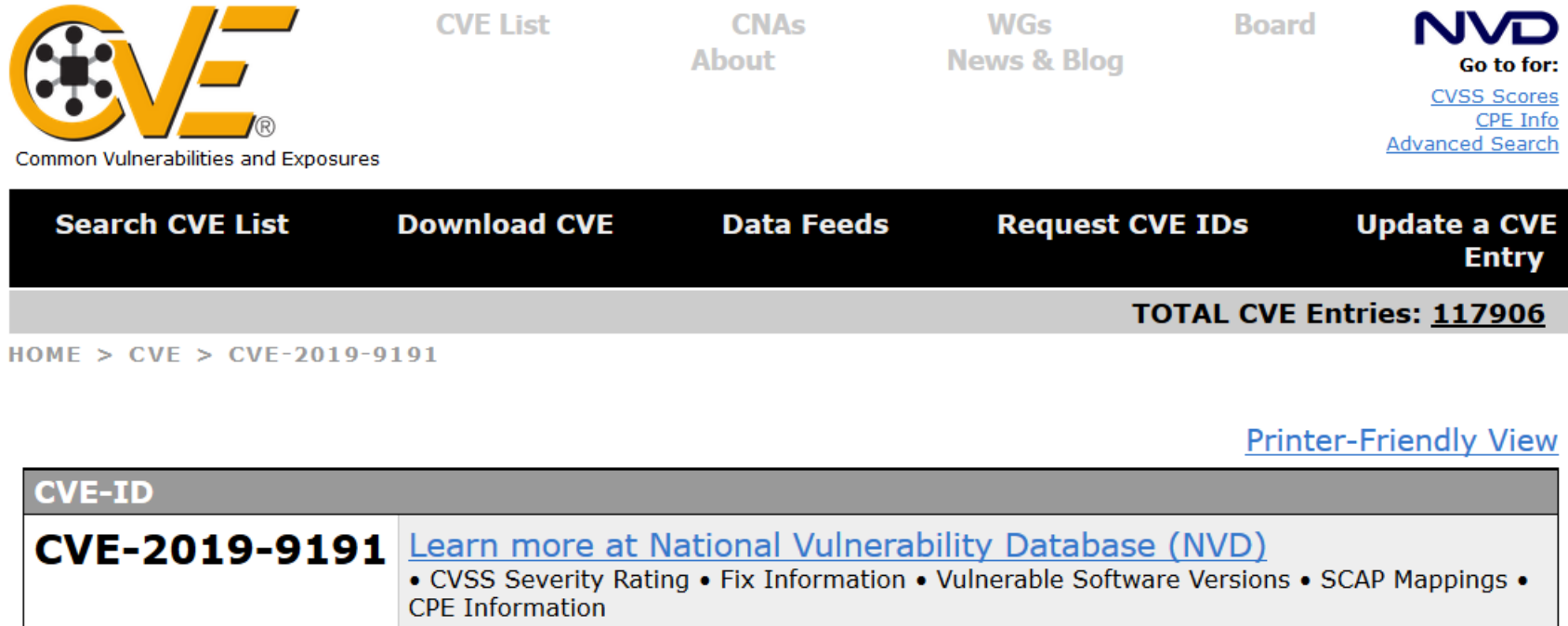
- Schädigt die Reputation der Transportverschlüsselung

Aktive Gegenmaßnahmen bei Einsatz von ETS

- Server (Web, Mail, usw.) können erkennen das ein statischer DH Key eingesetzt wird
- Können dann die Verbindung abrechen
- Webserver könnten einen Redirect machen und auf einer speziellen Seite anzeigen, dass die Verbindung nicht sicher ist

ETS als Fazit

- ETS (eTLS) als Fazit:



The screenshot shows the CVE website interface. At the top left is the CVE logo (Common Vulnerabilities and Exposures) with the text "Common Vulnerabilities and Exposures" below it. To the right of the logo are navigation links: "CVE List", "CNAs About", "WGs News & Blog", and "Board". Further right is the "NVD" logo with the text "Go to for:" and links for "CVSS Scores", "CPE Info", and "Advanced Search". Below these links is a black navigation bar with white text: "Search CVE List", "Download CVE", "Data Feeds", "Request CVE IDs", and "Update a CVE Entry". Below the navigation bar is a grey bar with the text "TOTAL CVE Entries: 117906". Below that is a breadcrumb trail: "HOME > CVE > CVE-2019-9191". To the right of the breadcrumb trail is a link for "Printer-Friendly View". Below the breadcrumb trail is a table with two columns: "CVE-ID" and a description. The first row of the table has the CVE-ID "CVE-2019-9191" and a description that includes a link to "Learn more at National Vulnerability Database (NVD)" and a list of items: "CVSS Severity Rating", "Fix Information", "Vulnerable Software Versions", "SCAP Mappings", and "CPE Information".

CVE
Common Vulnerabilities and Exposures

[CVE List](#) [CNAs About](#) [WGs News & Blog](#) [Board](#) **NVD**
Go to for:
[CVSS Scores](#)
[CPE Info](#)
[Advanced Search](#)

[Search CVE List](#) [Download CVE](#) [Data Feeds](#) [Request CVE IDs](#) [Update a CVE Entry](#)

TOTAL CVE Entries: **117906**

HOME > CVE > CVE-2019-9191

[Printer-Friendly View](#)

CVE-ID	
CVE-2019-9191	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information