TeleTrusT-EBCA "PKI-Workshop" 2019

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Berlin, 18.06.2019

Brauchen wir wirklich eine Backdoor? TSL 1.3 vs. eTSL

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 Suiten
- 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?

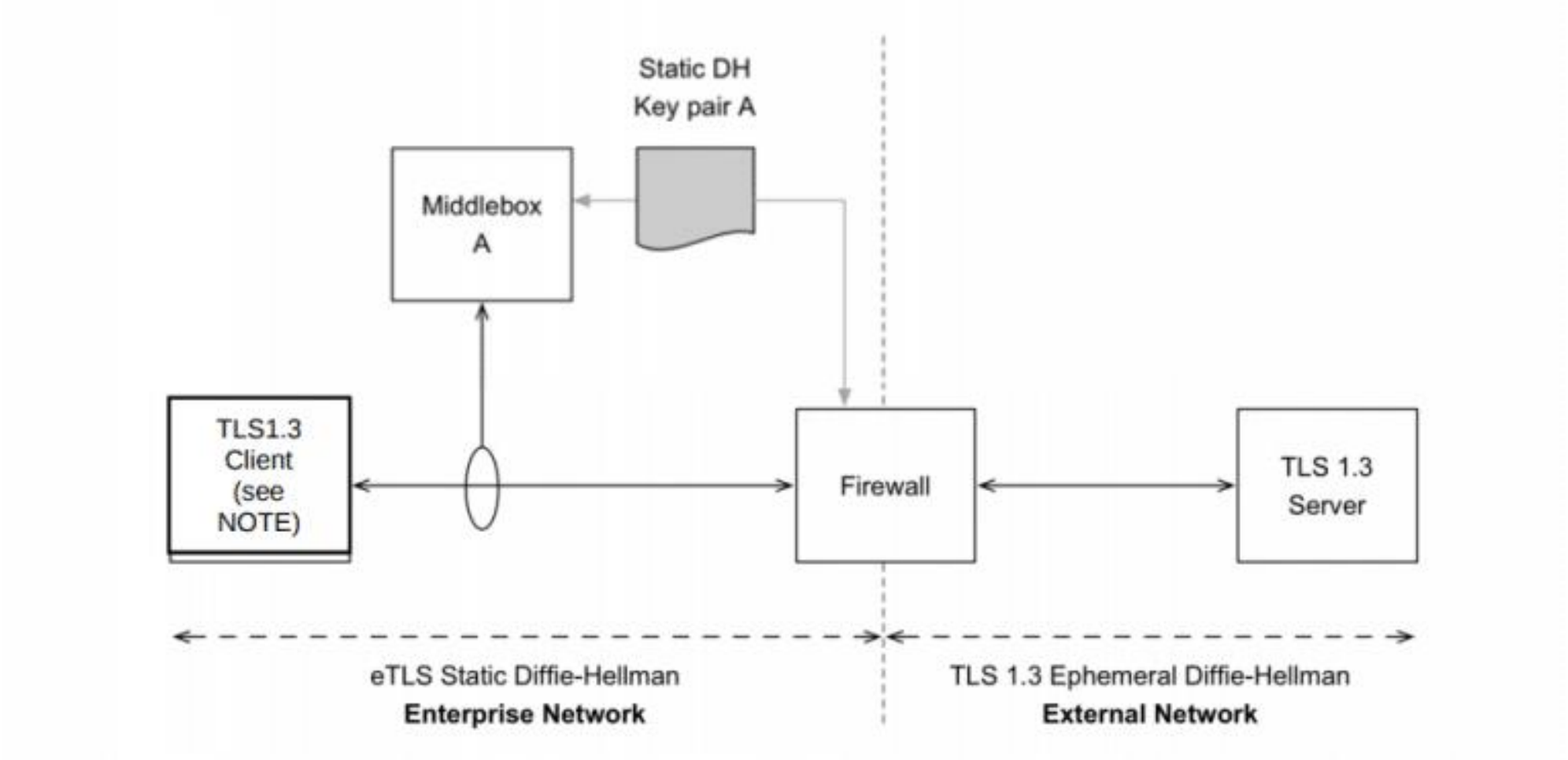
- Content Security Policys können umgangen werden
- Clickjacking, Code Injection kann nicht verhindert werden
- Keine Deep Paket Inspection mehr möglich
- Partielle Forward Secrecy: bestand bereits eine Verbindung, wird der PSK Key beim erst 0-RTT nicht neu ausgehandelt
- Weiterhin Side Channel Attacken 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
- Schädigt die Reputation der Transportverschlüsselung

Nein!

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: