Grundlagen Informationsicherheit und Datensicherheit, Blatt 6

Lukas Baur, 3131138
Felix Bühler, 2973410
Marco Hildenbrand, 3137242

29. Januar 2018

Problem 1: Protocol for Mutual Authentication

Reflection attack:
Eine Person, die N_B korrekt entschlüsselt hat, ist jemand, der den KEY kennt (Alice). Allerdings kennt Bob selbst den KEY auch! Der Angreifer kann also die gesendeten Nachrichten auzeichnen und später nochmal senden und sich damit als Alice ausgeben.

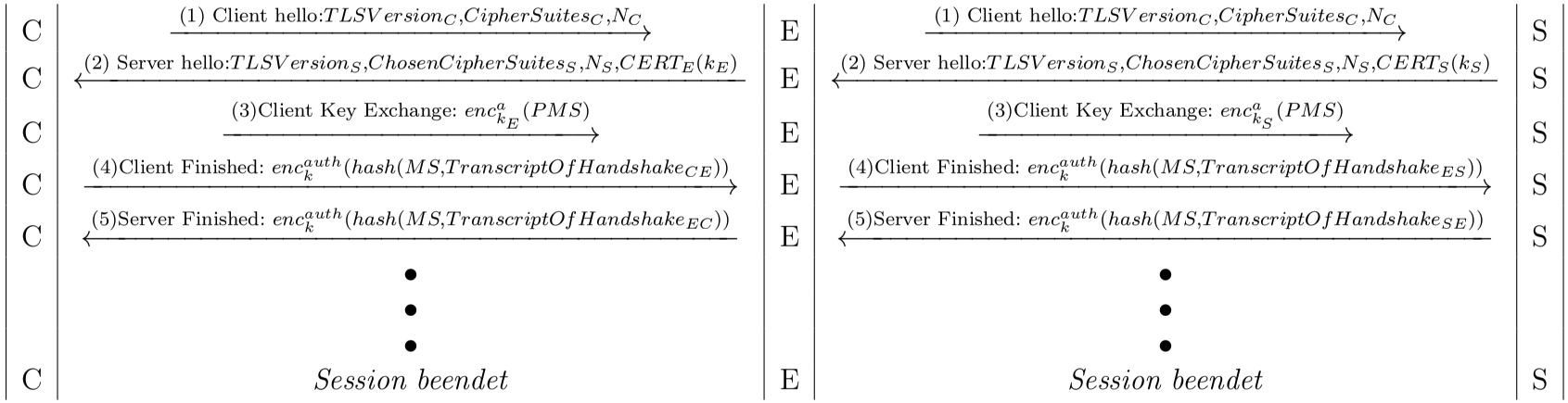
E = Evil (= Attacker)

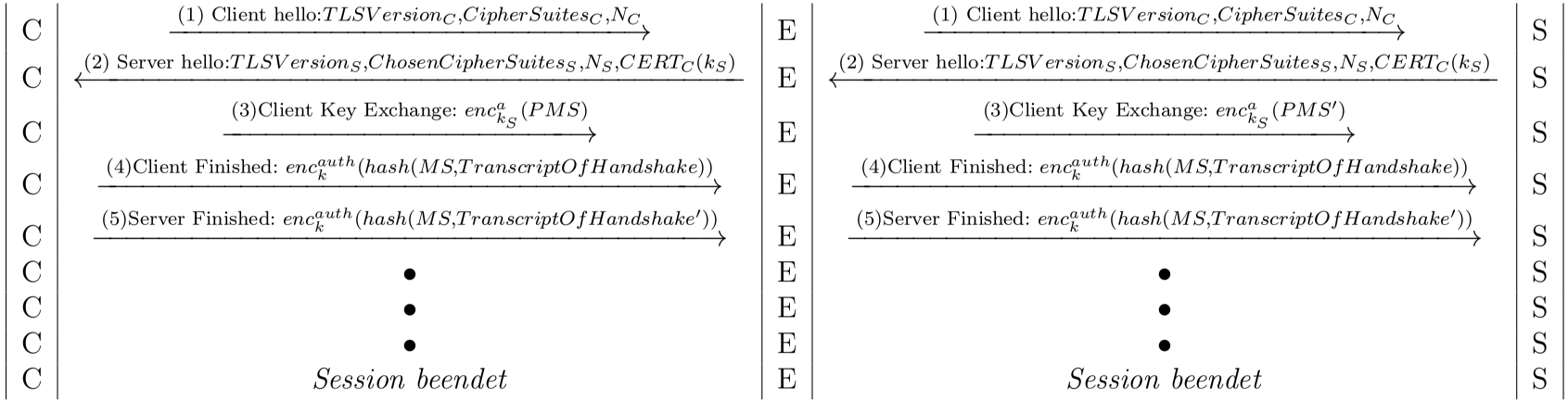
1. Verbindung 1: A $\rightarrow$ B : $enc_s^k(N_A)$
2. Verbindung 1: B $\rightarrow$ A : $enc_s^k(N_B), N_A$
3. Verbindung 1: A $\rightarrow$ B : N_B

4. Verbindung 2: E $\rightarrow$ A : $enc_s^k(N_B)$
5. Verbindung 2: A $\rightarrow$ E : $enc_s^k(N'_A), N_B$
6. Verbindung 3: E $\rightarrow$ A : $enc_s^k(N'_A)$
7. Verbindung 3: A $\rightarrow$ E : $enc_s^k(N''_A), N'_A$
8. Verbindung 2: A $\rightarrow$ E : N'_A

Problem 2: Kerberos

Problem 3: TLS and Randomness


C
E
S
(1) Client hello:$TLSVersion_C$,$CipherSuites_C$,N_C
(2) Server hello:$TLSVersion_S$,$ChosenCipherSuites_S$,N_S,$CERT_E(k_E)$
(3)Client Key Exchange: $enc^a_{k_E}(PMS)$
(4)Client Finished: $enc^{auth}_k(hash(MS,TranscriptOfHandshake_{CE}))$
(5)Server Finished: $enc^{auth}_k(hash(MS,TranscriptOfHandshake_{EC}))$
Session beendet
(1) Client hello:$TLSVersion_C$,$CipherSuites_C$,N_C
(2) Server hello:$TLSVersion_S$,$ChosenCipherSuites_S$,N_S,$CERT_S(k_S)$
(3)Client Key Exchange: $enc^a_{k_S}(PMS)$
(4)Client Finished: $enc^{auth}_k(hash(MS,TranscriptOfHandshake_{ES}))$
(5)Server Finished: $enc^{auth}_k(hash(MS,TranscriptOfHandshake_{SE}))$
Session beendet


C
E
S
(1) Client hello:$TLSVersion_C$,$CipherSuites_C$,N_C
(2) Server hello:$TLSVersion_S$,$ChosenCipherSuites_S$,N_S,$CERT_C(k_S)$
(3)Client Key Exchange: $enc^a_{k_S}(PMS)$
(4)Client Finished: $enc^{auth}_k(hash(MS,TranscriptOfHandshake))$
(5)Server Finished: $enc^{auth}_k(hash(MS,TranscriptOfHandshake'))$
Session beendet
(1) Client hello:$TLSVersion_C$,$CipherSuites_C$,N_C
(2) Server hello:$TLSVersion_S$,$ChosenCipherSuites_S$,N_S,$CERT_C(k_S)$
(3)Client Key Exchange: $enc^a_{k_S}(PMS')$
(4)Client Finished: $enc^{auth}_k(hash(MS,TranscriptOfHandshake))$
(5)Server Finished: $enc^{auth}_k(hash(MS,TranscriptOfHandshake'))$
Session beendet

Problem 4: Attack on IKEv1 Main Mode

Reflection attack:

Der Angriff ist eine einfache Reflexion, die erfordert, dass ein Initiator seine eigene Identität als Gleichrangigen-Peer akzeptiert. In diesem Fall werden die Authentifizierer in dem Protokoll gleich und der Gegner sendet einfach alle Nachrichten, die von dem Initiator kommen, unverändert an sie zurück. In diesem Fall schlägt die schwache Vereinbarung fehl, da kein Agent die Responder-Rolle ausführt. Die Geheimhaltung des Schlüssels ist weiterhin gewährleistet. Wenn eine Selbstkommunikation nicht möglich ist, ist der aufgezeigte Angriff nicht mehr möglich.