Security and Privacy, Blatt 0

Franziska Hutter (3295896)
Felix Truger (3331705)
Felix Bühler (2973410)

23. April 2018

Problem 1: Needham-Schroeder Protocol

a)

The attack on the Needham-Schroeder protocol is based on the fact that only the initiator (A) explicitly mentions who he is in an encrypted message. The identity of the correspondent (B) however is implied in the use of certain keys for encryption. This enables an adversary (E) to use the identity of the initiator towards another correspondent (B). In the improved NSL protocol this is fixed by including the name of the correspondent in his first reply. Since this message is encrypted with the public key of the impersonated participant, the adversary cannot read or alter it. So the attack fails, since the impersonated participant will know that the reply came from another participant, who he did not aim to communicate with.

b)

Replay attack:
E = Evil (= Attacker)
Bei der ersten Verbindung zeichnet der Angreifer alle Pakete auf und merkt sich diese.

1. Verbindung 1: A $\rightarrow$ B : $\{N_A, A\}^a_{k_B}$
2. Verbindung 1: B $\rightarrow$ A : $\{N_A, N_B, B\}^a_{k_A}$
3. Verbindung 1: A $\rightarrow$ B : $\{N_B\}^a_{k_B}$

4. Verbindung 2: A $\rightarrow$ E : $\{N_A, A\}^a_{k_B}$
5. Verbindung 2: E $\rightarrow$ A : $\{N_A, N_B, B\}^a_{k_A}$
6. Verbindung 2: A $\rightarrow$ E : $\{N_B\}^a_{k_B}$

Bei der 2. Verbindung wählt A exakt die gleiche Nonce. Hierdurch kann der Angreifer einfach die alte Nachricht von B senden. A denkt somit B ist auf der anderen Seite des Kanals. In Wirklichkeit ist es aber E. E bekommt allerdings keinen Zugriff auf die Keys um Nachrichten zu entschlüsseln. Alice denkt, dass die Verbindung also erfolgreich war. Es kann sozusagen vorgetäuscht werden, dass B Nachrichten schon bekommen hat, was aber nicht der Fall ist.

Problem 2: Another attack

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 aufzeichnen und später nochmal senden und sich damit als Alice ausgeben.

E = Evil (= Attacker)

1. Verbindung 1: A $\rightarrow$ B : $\{N_A\}_k^s$
2. Verbindung 1: B $\rightarrow$ A : $\{N_B\}_k^s, N_A$
3. Verbindung 1: A $\rightarrow$ B : N_B

4. Verbindung 2: E $\rightarrow$ A : $\{N_B\}_k^s$
5. Verbindung 2: A $\rightarrow$ E : $\{N'_A\}_k^s, N_B$
6. Verbindung 3: E $\rightarrow$ A : $\{N'_A\}_k^s$
7. Verbindung 3: A $\rightarrow$ E : $\{N''_A\}_k^s, N'_A$
8. Verbindung 2: A $\rightarrow$ E : N'_A

Problem 3: Woo and Lam Mutual Authentication Protocol

E = Evil (= Attacker)

1. Verbindung 1: $E_A \rightarrow$ B : A, B
2. Verbindung 1: B $\rightarrow E_A$: B, N_B
3. Verbindung 1: $E_A \rightarrow$ B : $\{A, B, B, N_B\}^s_{K_{AS}}$
4. Verbindung 1: B $\rightarrow E_S$: $\{A, B, B, N_B\}^s_{K_{AS}}, \{A, B, B, N_B\}^s_{K_{BS}}$

5. Verbindung 2: $E_A \rightarrow$ B : A, N_B
6. Verbindung 2: B $\rightarrow E_A$: B, N'_B
7. Verbindung 2: $E_A \rightarrow$ B : $\{A, B, N_B, N'_B\}^s_{K_{AS}}$
8. Verbindung 2: B $\rightarrow E_S$: $\{A, B, N_B, N'_B\}^s_{K_{AS}}, \{A, B, N_B, N'_B\}^s_{K_{BS}}$

9. Verbindung 1: $E_S \rightarrow$ B : $\{A, B, N_B, N'_B\}^s_{K_{AS}}, \{A, B, N_B, N'_B\}^s_{K_{BS}}$
10. Verbindung 1: B $\rightarrow E_A$: $\{A, B, N_B, N'_B\}^s_{K_{AS}}, \{B, N_B\}^s_{N'_B}$
11. Verbindung 1: $E_A \rightarrow$ B : $\{N_B\}^s_{N'_B}$