Christian Schindelhauer

Freiburg, den 23. Juli 2014
Besprechung 30. Juli 2014

Übungen zur Vorlesung

Systeme II / Rechnernetze

Sommer 2014

Blatt 12 (10 Punkte)

AUFGABE 1: 6 Pkt.

Aufgrund der kurzen Schlüssellänge von 56 bit kann DES nicht mehr als sicher betrachtet werden. Wir behandeln hier eine vereinfachte Variante von Ron Rivest's vorgeschlagenem DESX.
Für diese Variante gibt es zwei Schlüssel k_1 und k_2 mit Längen 56 bit bzw. 64 bit. Damit hat DESX eine Schlüssellänge von insgesamt 56+64=120 bit. Um eine Nachricht m zu verschlüsseln, wird wie folgt vorgegangen:

$$DESX_{(k_1,k_2)}(m) = DES_{k_1}(m \oplus k_2) \oplus k_2$$

1. Geben Sie eine Formel der Form $m = ...$ an, die zeigt, wie eine verschlüsselte Nachricht entschlüsselt wird. Geben Sie alle Umformungen an.

2. Führen Sie einen Angriff auf die weiter vereinfachte Formel ohne das innere XOR durch:

   $$DESX'_{(k_1,k_2)}(m) = DES_{k_1}(m) \oplus k_2$$

   Sie können davon ausgehen, dass Sie ein Nachrichtenpaar (plain m_1, cipher c_1) besitzen. Benutzen Sie einen "intelligenten"Angriff, d.h. brute force ist nicht erlaubt. Erläutern Sie ihre Vorgehensweise.
   Tipp: Um $DESX'$ mit brute force zu brechen benötigt man $2^{120} = 2^{56+64}$ Berechnungen. Mit einem "intelligenten"Angriff sollten Sie auf 2^{64} Berechnungen kommen.

3. Wozu wird das innere XOR also benötigt?

AUFGABE 2: 4 Pkt.

In der Vorlesung haben Sie bereits gelernt, dass man sich mithilfe von *Nonce* gegen Replay-Attacken schützen kann. Im Folgenden betrachten wir dieses Protokoll zwischen Alice (A) und Bob (B):

$A \to B : (A, n_A)_{eB}$
$B \to A : (n_A, n_B)_{eA}$
$A \to B : (n_B)_{eB}$

$(x)_{eB}$ bedeutet, dass x mit dem Public Key von Bob verschlüsselt wurde. Da nur Bob den Private Key besitzt, kann nur er die Nachricht entschlüsseln.
n_A ist das Nonce von Alice, die Nachricht A ist eine Art "Hallo"von Alice

Betrachten Sie nun folgendes Szenario mit einem Man-in-the-Middle-Angreifer Mallory (M):

(1) $A \rightarrow M : (A, n_A)_{eM}$
(2) $M \rightarrow B : (A, n_A)_{eB}$
(3) $B \rightarrow M : (n_A, n_B)_{eA}$
(4) $M \rightarrow A : (n_A, n_B)_{eA}$
(5) $A \rightarrow M : (n_B)_{eM}$
(6) $M \rightarrow B : (n_B)_{eB}$

1. Kann sich Mallory laut diesem Szenario bei Bob als Alice ausgeben? Ob ja oder nein, erläutern Sie Schritt für Schritt warum.

2. (1) ist in obigem Szenario essenziell, damit Mallory ihr Ziel erreichen kann. Warum?