Kristof Van Laerhoven
Thomas Janson

Freiburg, den 15. Mai 2015
Besprechung 22. Mai 2015

Übungen zur Vorlesung

Systeme II / Rechnernetze

Sommer 2015

Blatt 3 (15 Punkte)

AUFGABE 1: 6 Punkte

Sie möchten das Admin-Passwort eines Online-Forums rekonstruieren und besitzen nur noch den MD5-Hash-Code des Passworts: *71808c53ad4af7bd07875a99dfadc318*

1. Beschreiben Sie MD5 und diskutieren die Sicherheit von MD5.
2. Wie kann man die Sicherheit der mit MD5 verschleierten Passwörter erhöhen?
3. Finden Sie das verschlüsselte Passwort, indem Sie ein Programm schreiben, das eine BruteForce-Attacke durchführt. Sie können hierbei annehmen, dass das Passwort aus 8 Buchstaben besteht und nur die Buchstaben aus $\{a, b, c, d, e, f, g, h, i, j, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, \#, \$\}$
4. Nutzen Sie eine alternative Technik um den MD5-Hash zu entschlüsseln. Geben Sie an wie Sie dabei vorgehen. Vergleichen Sie die Technik mit der BruteForce-Attacke.

AUFGABE 2: 6 Punkte

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 3: 3 Punkte

Ein Unternehmen möchte den Inhalt aller http(s)-Verbindungen im Unternehmensnetzwerk kontrollieren.
Welche Sicherheitsziele sind verletzt?
Betrachten Sie:

1. http
2. https mit selbstsignierten Zertifikaten
3. https mit von einer CA signierten Zertifikaten

Beschreiben Sie für die drei Verbindungsarten was getan werden muss um die Verbindungen abzuhören.