Ludwig-Maximilians-Universität München
Institut für Informatik
Lehr- und Forschungseinheit für Kommunikationssysteme und Systemprogrammierung
Dr. Helmut Reiser

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2009/2010
Übungsblatt 8

Abgabetermin: 13.01.2010 bis 14:00 Uhr

Achtung: Zur Bearbeitung einiger Übungsaufgaben benötigen Sie eine Rechnerkennung für unsere Praktikums Infrastruktur. Um diese zu erhalten, melden Sie sich bitte über die Vorlesungs Webseite zum Übungsberieb an.

Die schriftlichen Lösungen aller mit **H** gekennzeichneten Aufgaben sind **vor Beginn** der jeweils nächsten Übungsveranstaltung abzugeben (per Email, in der Vorlesung oder vor der Übung). Während des Semesters werden vier Übungsblätter korrigiert. Bei vier richtigen Lösungen erfolgt ein Bonus von zwei drittel Notenstufen auf die Klausurnote, bei nur drei oder zwei richtigen Lösungen erhalten Sie einen Notenbonus von einer drittel Notenstufe.

Aufgabe 19: (H) MS-CHAP v2

In der Vorlesung wurde das Point-to-Point-Tunneling Protocol (PPTP) erläutert und dessen Sicherheitseigenschaften betrachtet. Bruce Schneier zeigt in einem Paper Schwachstellen des Protokolls auf. Betrachtet wird darin insbesondere die Authentifizierungsmöglichkeit auf Basis von MS-CHAPv1.

a. Beschreiben Sie den Ablauf von MS-CHAPv1 und zeigen Sie mögliche Sicherheitslücken auf.

b. Microsoft besserte das Challenge/Response-Verfahren nach. Daraus entstand MS-CHAPv2. Skizzieren Sie den Ablauf von MS-CHAPv2. Welche Schwachstellen wurden in Version 2 im Vergleich zu Version 1 beseitigt und welche nicht. Begründen Sie kurz Ihre Antwort.

c. Gegeben sind

   - die 16-Byte Challenge AB12CD34EF56AB12CD34EF56AB78AABB,
   - die Peer Authenticator Challenge 159753AFEDAABBCCDDEEFFAADEFA3579
   - der Benutzername itsecusr
   - das Passwort itsecusr

   Berechnen Sie hierzu die jeweiligen Werte, die bei der Kommunikation von Client und Server im Rahmen von MS-CHAPv2 ausgetauscht werden. Beachten Sie dabei folgende Vereinfachungen:

   (i) Für die Berechnung des NT-Hash ersetzen Sie einfach die 4-höherwertigen Bits durch Null

   (ii) DES wird ersetzt durch eine XOR-Verknüpfung

(iii) MD4 wird ersetzt durch MD5

Die Parameter werden jeweils konkateniert an eine Hashing-Funktion übergeben, d.h. ohne Leerzeichen, Zeilenumbrüche etc.

Aufgabe 20: (H) Wired Equivalent Privacy (WEP)

Besonders in WLAN-Netzen werden an die Sicherheit hohe Anforderungen gestellt. Ein erster Schritt die Vertraulichkeit sicherzustellen war Wired Equivalent Privacy (WEP).

a. Beschreiben Sie textuell den Ablauf von WEP (Verschlüsselung)

b. Gegeben sind

- die Nachricht $M = 27$
- das Generatorpolynom $x^4 + x + 1$
- der Initialisierungsvektor IV = F59CE7
- der Key = 3FC9AB082A

(i) Berechnen Sie die CRC-32 der Nachricht M

(ii) Berechnen Sie den Ciphertext

c. Beschreiben Sie textuell den Ablauf von WEP (Entschlüsselung)