

## IT-Sicherheit im Wintersemester 2010/2011 Übungsblatt 8

**Abgabetermin:** 19.01.2011 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 Übungsbetrieb 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 20: (H) PPTP, MS-CHAPv2 und 802.1x**

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 in Stichpunkten den Unterschied zwischen Voluntary Tunneling und Compulsory Tunneling.
- b. Microsoft verbesserte das Challenge/Response-Verfahren (MS CHAP) 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 Antworten.
- 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 Vereinbarungen:

- (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.

- d. Sie versuchen Zugang zu einem 802.1x gesicherten WLAN aufzubauen. Welche Nachrichten werden zwischen Supplicant, Authenticator und Authentifizierungsserver ausgetauscht bei Verwendung von EAP-TLS? Beschränken Sie sich bei Ihrer Antwort auf die Authentifizierungsphase, d.h. lassen Sie Phasen wie WLAN-Assoziierung und IP-Adressaushandlung mittels DHCP unberücksichtigt.

## Aufgabe 21: (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. Oftmals wird zur Absicherung von WLAN-Umgebungen vorgeschlagen, das SSID-Broadcasting abzuschalten und die Nutzung des WLANs nur Geräten mit bestimmten MAC-Adressen zu erlauben. Ist das Ihrer Ansicht nach sinnvoll? Begründen Sie kurz ihre Antwort.