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

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2016/2017
Übungsblatt 10

Termin: 07.02.2017 um 12:00 Uhr

Aufgabe 22: (K) 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.

Aufgabe 23: (K) IPSEC Protokollkombinationen

Wie in der Vorlesung beschrieben, können die Protokolle AH und ESP entweder unabhängig voneinander oder in Kombination eingesetzt werden. Dabei ist zu unterscheiden, ob eines oder beide kommunizierenden Endsysteme selbst IPSEC-fähig sind oder ob so genannte Security Gateways eingesetzt werden. In der Vorlesung wurden bereits ausgewählte Kombinationen und deren charakteristische Eigenschaften besprochen

a. Gegeben sei ein Quellsystem mit der IP-Adresse 10.1.1.1 mit Security-Gateway 10.1.1.254 und ein Zielsystem 10.10.1.1 mit Security-Gateway 10.10.1.254. Für die Kommunikation soll

   - ESP soll im Tunnel-Mode zwischen den Security-Gateways

- AH im Transport-Mode zwischen den Endsystemen

verwendet werden. Geben Sie für alle beteiligten Systeme exemplarische Inhalte aller relevanten Security Associations an; gehen Sie dabei davon aus, dass die Vertraulichkeit über AES-Verschlüsselung und die Integritätssicherung über MD5-Prüfsummen sicher gestellt werden soll.

b. Geben Sie, analog zu den Folien im Vorlesungsskript, den Inhalt des Pakets an. Gehen Sie dabei von einem zu übertragenden IPv4-Datagramm aus. Geben Sie für alle relevanten Header-Felder korrekte Werte an.