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

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2011/2012
Übungsblatt 10

Abgabetermin: 25.01.2012 bis 14:00 Uhr

Achtung: Zur Bearbeitung einiger Übungsaufgaben benötigen Sie eine Rechnerkennung für unsere Praktikumsinfrastruktur. Um diese zu erhalten, melden Sie sich bitte über die Vorlesungswebseite zum Übungsbetrieb an.

Die schriftlichen Lösungen aller mit **H** gekennzeichneten Aufgaben sind **vor Beginn** der jeweils nächsten Übungsveranstaltung abzugeben (per **E-Mail** an die Adresse **uebung-itsec_AT_lrz.de** oder schriftlich 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 22: (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. Gegeben sind
   - die dezimale Nachricht $M = 27$
   - das Generatorpolynom $x^4 + x + 1$
   - der Initialisierungsvektor IV = F59CE7
   - der Key = 3FC9AB082A

   (i) Berechnen Sie die CRC der Nachricht M.

   (ii) Berechnen Sie den Ciphertext, der nun übertragen wird. Verwenden Sie für die Berechnung den RC4-Calculator unter http://farhadi.ir/works/rc4.

b. Zeigen Sie, dass bei Verwendung von Shared Key Authentication ein Angreifer Eve in der Lage ist, durch Abhören der Kommunikation den Keystream zu berechnen und sich damit selbst zu authentifizieren.

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: (H) WiFi Protected Access (WPA)

Leider zeigt sich bald, dass die Sicherheitsaspekte von WEP unzureichend waren. Verbesserung versprach sich die IEEE durch Definition von WiFi Protected Access (WPA), insbesondere WPA-TKIP.

a. Beschreiben Sie knapp den Integritätscheck-Algorithmus *Michael*. Der Schlüssel werde mit K^* bezeichnet, der unverschlüsselte Datensatz mit A. Welche Werte nutzt *Michael* für die Berechnung? Welche Bestandteile hat der Wert D, der dem RC4-Alogrithmus als Eingabe übergeben wird?

b. Um sich vor Replay-Angriffen zu schützen, wurde in WPA-TKIP ein TKIP Sequence Counter (TSC) eingeführt. Beschreiben Sie in Stichpunkten diesen Wert. Was passiert nach jeder Übertragung damit?

c. Auf Empfängerseite wird der TSC geprüft. Was passiert, wenn der Wert des TSC kleiner oder gleich dem beim Empfänger gespeicherten TSC-Wert ist?

d. Mit WPA-TKIP wurde eine Schlüsselhierarchie eingeführt. Beschreiben Sie knapp die einzelnen Hierarchiestufen.

e. Beschreiben Sie den Ablauf eines WPA Chop-Chop-Angriff! Nennen Sie wichtige Voraussetzungen/Annahmen. Welche Nachrichtenteile sind dem Angreifer trotz passivem Sniffing unbekannt und bilden den Ausgangspunkt des Angriffs?