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 2021/2022
Übungsblatt 12

Aufgabe 43: (H) Wired Equivalent Privacy (WEP)

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

a. Beschreiben Sie knapp 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 Prüfsumme CRC der Nachricht M (verwenden Sie hierfür das gegebene Generatorpolynom)

   (ii) Berechnen Sie den resultierenden 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 44: (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-Algorithmus 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?