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

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2012/2013
Übungsblatt 10

Abgabetermin: 30.01.2013 bis 14:00 Uhr

Achtung: Zur Bearbeitung einiger Übungsaufgaben ist es notwendig sich über den Vorlesungsinhalt hinaus, durch Internet- und Literaturrecherche mit dem Thema zu beschäftigen.

Die schriftlichen Lösungen aller mit **H** gekennzeichneten Aufgaben sind **vor Beginn** der jeweils nächsten Übungsveranstaltung abzugeben (per Email 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 24: (H) Network-Security & 802.1X

Zur Absicherung von Netzen existieren verschiedene Verfahren. Eine sehr einfache, aber effiziente Möglichkeit, Netztraffic zu separieren, stellt der Einsatz von Virtual LANs (VLANs) dar. Eine im WLAN-Umfeld häufig anzutreffende Maßnahme ist der Einsatz von 802.1X.

a. Erläutern Sie knapp den Aufbau eines VLAN-Tags. Beschreiben Sie kurz die Priorisierung. Welche Prioritätseinstufung schlagen Sie für Video- bzw. IP-Telefonie vor?

b. 802.1X ist ein in WLAN- und VLAN-Infrastrukturen häufig verwendeter Network Access Control-Mechanismus. Sie benötigen in einem Besprechungsraum am LRZ Internet-Zugang über das dort zur Verfügung stehende, 802.1X-gesicherte WLAN. Welche erste Nachricht sendet der Supplicant üblicherweise, wenn der Authenticator nicht bekannt ist?

c. Welche Gefahr besteht beim Senden der Identitätsinformationen des Supplicants auf Ihrem Notebook an den WLAN-Access Point?

d. Skizzieren Sie die weitere Kommunikation zwischen ihrem Notebook, dem WLAN-Access Point und dem RADIUS-Server generell. Welchen großen Vorteil bietet die Verwendung von EAP-TLS? Was ist hierbei jedoch zwingende Voraussetzung?

Aufgabe 25: (H) MS-CHAPv2 & WLAN-Security

a. Microsoft besserte 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.

b. Gegeben sind

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

   (i) Berechnen Sie die CRC der Nachricht M, verwenden Sie hierzu das vereinfachte Generatorpolynom.

   (ii) Berechnen Sie den Ciphertext, der nun übertragen wird. Verwenden Sie für die Berechnung den RC4-Calculator unter http://www.fyneworks.com/encryption/rc4-encryption/. Verwenden Sie für den Calculator den String *ITSEC* als Key.

c. 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?

Aufgabe 26: (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.