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

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2008/2009
Übungsblatt 8

Abgabetermin: 07.01.2009 bis 14:00 Uhr

Achtung: Die schriftlichen Lösungen aller mit H gekennzeichneten Aufgaben sind **vor Beginn** der jeweils nächsten Übungsveranstaltung abzugeben. Während des Semesters werden drei Übungsblätter korrigiert. Bei drei richtigen Lösungen erfolgt ein Bonus von zwei drittel Notenstufen auf die Klausurnote, bei zwei richtigen Lösungen erhalten Sie einen Notenbonus von einer drittel Notenstufe.

Aufgabe 16: (K) WLAN-Sicherheit

a. Skizzieren Sie die Funktionsweise von WEP!

b. Während der Authentifizierungsphase von WEP sendet der AccessPoint eine unverschlüsselte 128 Bit lange Challenge an den zu authentifizierenden Client, welcher im nächsten Schritt mit der verschlüsselten Challange sowie dem verwendeten Initialisierungsvektor antwortet. Zeigen Sie, dass ein Angreifer mit nur einem einzigen vollständig mitgehörten Authentifizierungsvorgang in der Lage ist, sich selbst belig oft zu authentifizieren!

c. Datenpakete, die mit WEP gesichert sind, können von Dritten ohne dass diese den Schlüssel kennen manipuliert werden. Die Integrität der Nachricht kann dabei erhalten bleiben. Im Folgenden sei Δ die gewünschte Änderung an der Nachricht M. Zeigen Sie, dass der Hash der manipulierten Nachricht korrekt bleibt, wenn man den Hash von Δ addiert.

d. WEP ist wegen seiner Liniarität kryptographisch unsicher. Aus diesem Grund wurde WPA entwickelt. Stellen Sie die Erweiterungen und Veränderungen von WPA gegenüber WEP dar!

e. WPA2 ist die IEEE 802.11i konforme Variante von WPA. Unter anderem verwendet WPA2 AES als Verschlüsselungsalgorithmus. Warum ist es meist nicht möglich, WPA2-Unterstützung per Firmware-Update nachtzurüsten?

Aufgabe 17: (H) Protokoll

Entwerfen Sie ein Protokoll, das Authorisierung, Vertraulichkeit, Integrität, Verbindlichkeit des Sendens und Verbindlichkeit des Empfangs zwischen zwei Teilnehmern realisiert.