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 2018/2019
# Übungsblatt 10

**Termin:** 22.01.2019 bis 12:00 Uhr

## Aufgabe 22: (K) 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 23: (K) 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.