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 11

Besprechung: 01.02.2022

Aufgabe 41: (T) 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 42: (H) PPTP, MS-CHAPv2 und 802.1x

In der Vorlesung wurde das Point-to-Point-Tunneling Protocol (PPTP) erläutert und dessen Sicherheitseigenschaften betrachtet. Bruce Schneier zeigt in einem Paper Schwachstellen des Protokolls auf. Betrachtet wird darin insbesondere die Authentifizierungsmöglichkeit auf Basis von MS-CHAPv1.

a. Beschreiben Sie in Stichpunkten den Unterschied zwischen Voluntary Tunneling und Compulsory Tunneling.

b. 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.

c. Sie versuchen Zugang zu einem 802.1x gesicherten WLAN aufzubauen. Welche Nachrichten werden zwischen Supplicant, Authenticator und Authentifizierungsserver ausgetauscht bei Verwendung von EAP-TLS? Beschränken Sie sich bei Ihrer Antwort auf die Authentifizierungsphase, d.h. lassen Sie Phasen wie WLAN-Assoziierung und IP-Adressaushandlung mittels DHCP unberücksichtigt.