

IT-Sicherheit im Wintersemester 2019/2020

Übungsblatt 11

Termin: 28.01.2020 bis 12:00 Uhr

Aufgabe 22: (K) X.509

- Fassen Sie kurz das Aufgabenspektrum einer CA zusammen.
- Welche grundsätzlichen Ansätze existieren für den Widerruf eines Zertifikats? Erläutern Sie diese!
- Für die Echtzeit-Überprüfung des Status eines Zertifikats wurde das Online Certificate Status Protocol entwickelt. Beschreiben Sie dessen grundsätzlichen Ablauf.

Aufgabe 23: (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.

- Erläutern Sie knapp den Aufbau eines VLAN-Tags. Beschreiben Sie kurz die Priorisierung. Welche Prioritätseinstufung schlagen Sie für Video- bzw. IP-Telefonie vor?
- 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?
- Welche Gefahr besteht beim Senden der Identitätsinformationen des Supplicants auf Ihrem Notebook an den WLAN-Access Point?
- 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?