IT-Sicherheit – Sicherheit vernetzter Systeme

Übung im Wintersemester 2024/2025 (LMU)

30.01.2024
WS 2024/2025

Organisatorisches
Klausur

- Termin
  - **24.02.2025, 15:45 Uhr s.t.**
  - **Reguläre Bearbeitungszeit: 100 Minuten**
  - **KEINE Nachholklausur**
- Anmeldung über Moodle bis
  - **spätestens** 18.02.2025
- Präsenzklausur (Closed Book) – Räume im bzw. in der Nähe des Biomedical Center der LMU in Planegg-Martinsried
- Für Nachteilsausgleich (Schreibzeitverlängerung) möglichst bald – spätestens bis zum 18.02.2025 – eine E-Mail an uebung-itsec@lrz.de (von Campus E-Mail Adresse) senden

Führung durch den Rechnerwürfel des LRZ

EXKLUSIV für Studis der IT-Sec-VL

Termin:

Di. 18.03.2024 im LRZ in Garching

(https://www.lrz.de/wir/kontakt/weg/)

Anmeldung:

uebung-itsec@lrz.de

spätestens Fr. 14.02.2025 EOD

WICHTIG:

Personalausweis mitbringen und anmelden

- ohne Perso und Anmeldung kein Besuch des Rechners

- Anmeldung: nur über die Campus-Mailadresse

Eingang

Aufgabe 1 (T): Network-Security & 802.1X

30.01.2024
WS 2024/2025

Übungsblatt 12:
Aufgabe 1: (T) Network-Security & 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?

Übungsblatt 12:
Aufgabe 1: (T) Network-Security & 802.1X

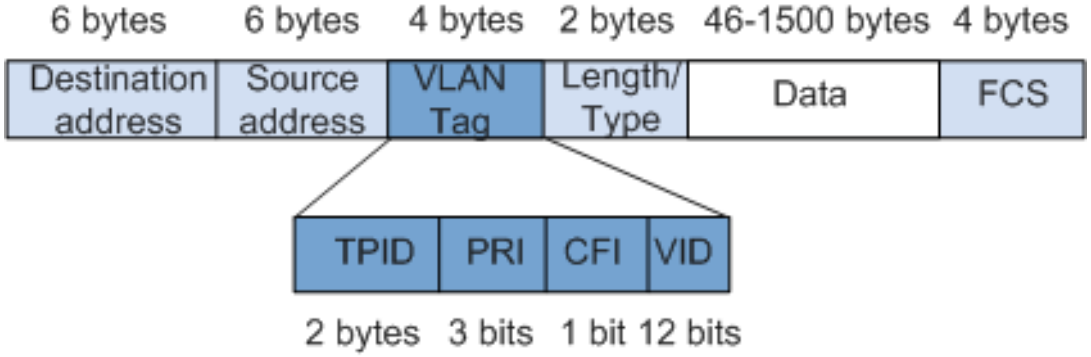
Wdh.: Virtual LAN (VLAN):

- Erlaubt logische Gruppierung/Separierung von IT-Systemen nach Geschäfts- oder Security-Anforderungen
- Mehrere LAN Broadcast Domains über einen physischen Link
- VLAN-Tagging (IEEE 802.1Q)
- VLAN enabled Ports sind kategorisiert in einen von zwei Typen:
  - Untagged / Access: Port akzeptiert nur Daten für ein VLAN, verbindet ein Gerät mit Switch
  - Tagged / Trunked: Port akzeptiert mehrere VLAN's, verbindet Switches

Übungsblatt 12:
Aufgabe 1: (T) Network-Security & 802.1X

Traditional Ethernet data frame

VLAN data frame



- TPID (Tag Protocol Identifier)
- Priority (802.1p, Class Of Service)
- CFI (Canonical Format Indicator)
- VID (VLAN Identifier)

Übungsblatt 12:
Aufgabe 1: (T) Network-Security & 802.1X

PCP value	Priority	Acronym	Traffic types
1	0 (lowest)	BK	Background
0	1 (default)	BE	Best effort
2	2	EE	Excellent effort
3	3	CA	Critical applications
4	4	VI	Video, < 100 ms latency and jitter
5	5	VO	Voice, < 10 ms latency and jitter
6	6	IC	Internetwork control
7	7 (highest)	NC	Network control

Priorität bei Video-/IP-Telefonie: 4 oder 5

- IEEE P802.1p
- Empfehlungen der IEEE
- Tatsächliche Umsetzung hängt von der Implementierung auf der Netzwerkhardware ab

Übungsblatt 12:
Aufgabe 1: (T) Network-Security & 802.1X

(b) […] 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 (WLAN AP) nicht bekannt ist?

Übungsblatt 12:
Aufgabe 1: (T) Network-Security & 802.1X

Welche erste Nachricht sendet der Supplicant üblicherweise, wenn der Authenticator (WLAN AP) nicht bekannt ist?

- Supplicant sendet IEEE 802.11 Management Frame: Probe Request
  - **Active Scanning** kann bestimmte SSID enthalten (um sich mit Hidden SSID zu verbinden) oder „any" SSID suchen. Supplicant wartet auf Probe Response
  - **Passive Scanning** → AP's senden Beacon Frame die SSID enthalten. Supplicant lauscht auf allen Kanälen

Übungsblatt 12:
Aufgabe 1: (T) Network-Security & 802.1X

(c) Welche Gefahr besteht beim Senden der Identitätsinformationen des Supplicants auf ihrem Notebook an den WLAN-Access Point?

→ Fehlende Authentisierung des Authenticators gegenüber dem Supplicant (Rogue Authenticator)

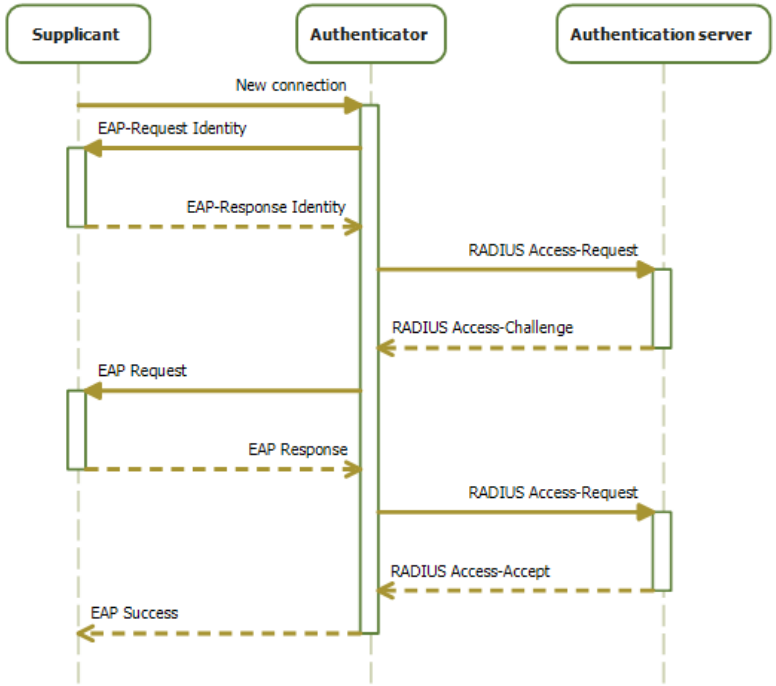
→ Mangels verschlüsselter Übertragung Credential-Diebstahl/ -Ausspähen möglich

Übungsblatt 12:
Aufgabe 1: (T) Network-Security & 802.1X

(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?

Übungsblatt 12:
Aufgabe 1: (T) Network-Security & 802.1X

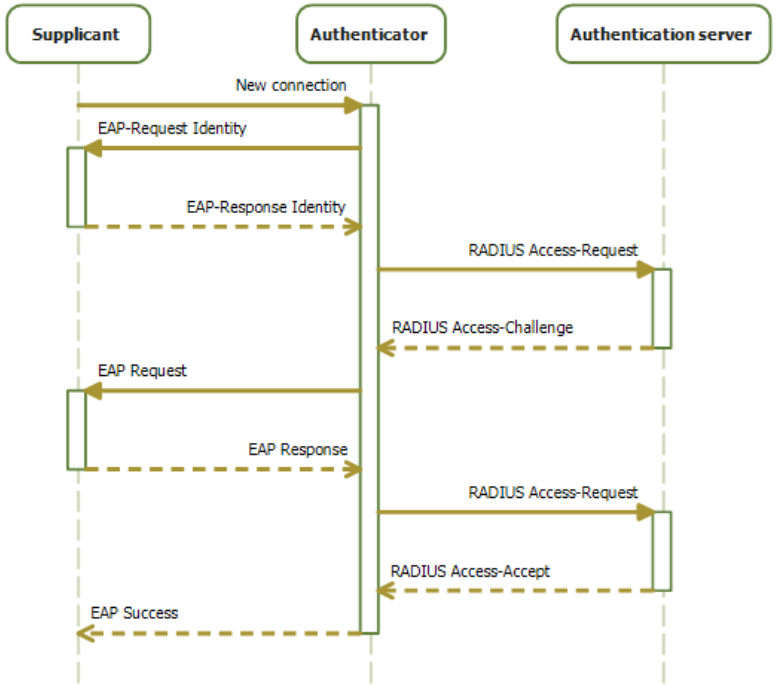


1. **Initialization:** wenn neuer Supplicant erkannt wird, Port in „unauthorized" State. Nur 802.1X Traffic erlaubt, Rest wird verworfen

2. **Initiation:** Authenticator sendet EAP-Request frames. Supplikant antwortet mit EAP-Response (enthält **User ID**). Authenticator leitet es als Access-Request an Authentication Server weiter.

   Supplicant kann auch EAPOL-Start an Authenticator schicken, um eine EAP-Request Antwort zu triggern

Übungsblatt 12:
Aufgabe 1: (T) Network-Security & 802.1X



3. **Negotation:** Authentication Server schickt Access-Challenge und spezifiziert EAP Methode. Supplicant kann EAP Methode akzeptieren oder mit NAK und alternativen Methoden antworten

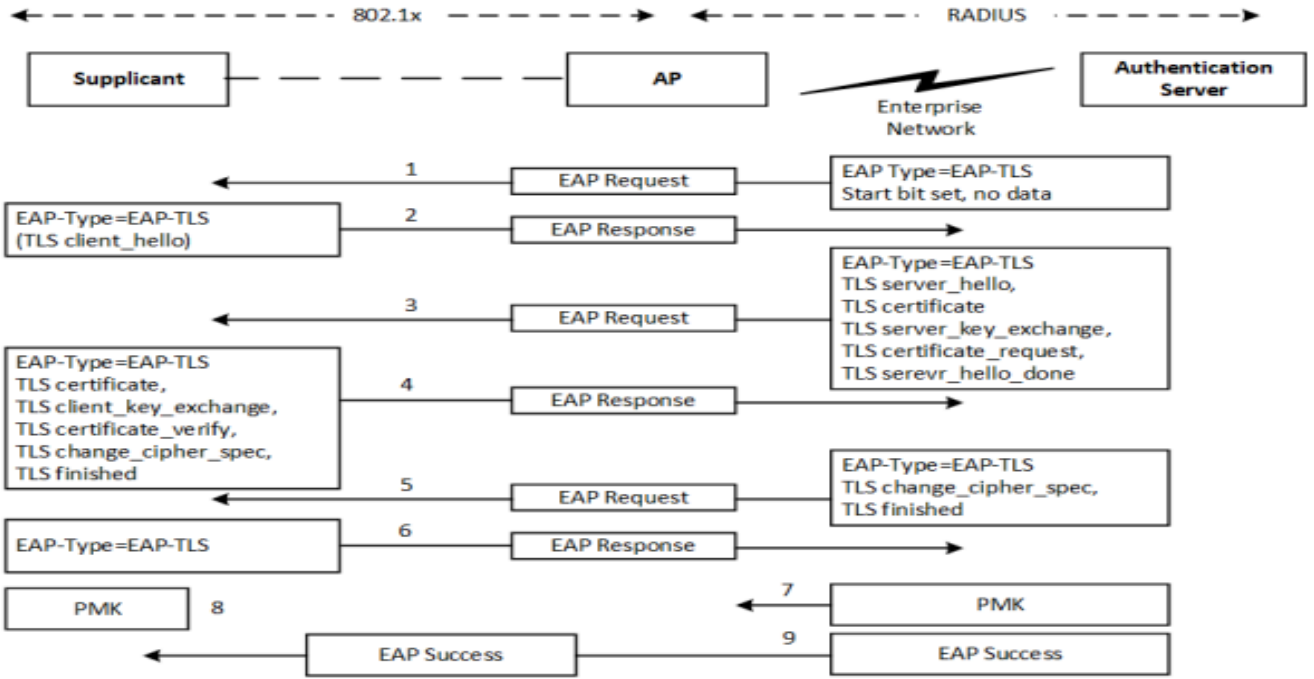
4. **Authentication:** Haben sich Supplicant und Authentication Server auf eine Methode geeignet wird EAP Response geschickt. Es folgt entweder EAP-Success oder EAP-Failure. Im Success-Fall setzt Authenticator Port auf „authorized“ und lässt normale Datenverbindungen zu.

Übungsblatt 12:
Aufgabe 1: (T) Network-Security & 802.1X

- EAP-TLS (EAP-Transport Layer Security):
  - Zwingende Verwendung von Zertifikaten
  - **Benutzer**- und Server-Zertifikat zur gegenseitigen Authentisierung

- Hinweis: EAP-TTLS (EAP-Tunneled Transport Layer Security):
  - Server authentisiert sich mittels Zertifikat → Sicherer Kanal
  - Client muss sich **nicht** über Zertifikat authentisieren, kann sich mittels Username/Passwort über sicheren Kanal authentisieren

Übungsblatt 12:
Aufgabe 1: (T) Network-Security & 802.1X



Aufgabe 2 (T):
Firewalls und Intrusion Detection

30.01.2024
WS 2024/2025

Übungsblatt 12: Aufgabe 2: (T) Firewalls und Intrusion Detection
a) Firewall-Techniken und Einsatzzwecke

- (a) Welche Firewall-Techniken lassen sich im Allgemeinen unterscheiden? Beschreiben Sie die jeweilige Technik und zeigen Sie mindestens einen sinnvollen Einsatzzweck auf.

- Lösung:
  - Paketfilter
  - Applikationsfilter
  - Verbindungsgateways
  - Kombinationen aus den 3 erstgenannten

Wiederholung: Das OSI OSI Schichtenmodell

https://de.wikipedia.org/wiki/OSI-Modell

30.01.2024

OSI-Schicht		Einordnung	TCP/IP-Referenzmodell	Einordnung	Protokollbeispiele	Einheiten	Kopplungselemente
7	Anwendung (Application)	Anwendungs-orientiert	Anwendung	Ende zu Ende (Multihop)	DHCP DNS FTP HTTP HTTPS LDAP MQTT NCP RTP SMTP XMPP	Daten	Gateway, Content-Switch, Proxy, Layer-4-7-Switch
6	Darstellung (Presentation)						
5	Sitzung (Session)						
4	Transport (Transport)	Transport-orientiert	Transport		TCP UDP SCTP SPX	TCP = Segmente UDP = Datagramme	
3	Vermittlung-/Paket (Network)		Internet		ICMP IGMP IP IPsec IPX	Pakete	Router, Layer-3-Switch
2	Sicherung (Data Link)		Netzzugriff	Punkt zu Punkt	IEEE 802.3 Ethernet IEEE 802.11 WLAN TLAP FDDI MAC Token Ring ARCNET	Rahmen (Frames)	Bridge, Layer-2-Switch, Wireless Access Point
1	Bitübertragung (Physical)				1000BASE-T Token Ring ARCNET	Bits, Symbole	Netzwerkkabel, Repeater, Hub

Übungsblatt 12: Aufgabe 2: (T) Firewalls und Intrusion Detection
a) Firewall-Techniken und Einsatzzwecke | **Paketfilter**

Paketfilter:

- OSI – Schicht 3 und 4
- Filterung auf Header-Felder
  - Layer 3: Flags, **Protokoll, Source Address, Destination Address,** IP Optionen
  - Layer 4: **Source Port, Destination Port,** Flags, Optionen
- Erkennung von IP-Spoofing?
  - Ja, wenn Paket mit interner Quell-IP an externem FW-Interface

Übungsblatt 12: Aufgabe 2: (T) Firewalls und Intrusion Detection
a) Firewall-Techniken und Einsatzzwecke | **Paketfilter**

- Einsatz:
  - Screening Router (ACLs)
  - Sehr einfach und preiswert
  - Hohe Performanz (effizient)

- Probleme
  - Header-Felder leicht fälschbar
  - Logging-Funktionalität beschränkt
  - Statische Filterung hat Probleme mit dynamischer Port-Öffnung (z.B. FTP)

Übungsblatt 12: Aufgabe 2: (T) Firewalls und Intrusion Detection
a) Firewall-Techniken und Einsatzzwecke | **Applikationsfilter**

- **Applikationsfilter (Application Level Firewalls):**
  - Filter auf Anwendungsschicht (Schicht 7)
  - Anwendungsprotokoll und Nutzdaten
  - Für jeden Dienst/Protokoll ist eigener Proxy notwendig (z.B. HTTP-Proxy)
  - **Nutzerauthentisierung (Active-Directory-Integration)**
  - Proxy agiert als Stellvertreter des internen Clients
  - **Content filtering (z.B. Antivirus / URL-Filtering)**
  - Caching-Funktionalität

Übungsblatt 12: Aufgabe 2: (T) Firewalls und Intrusion Detection
a) Firewall-Techniken und Einsatzzwecke | **Verbindungsgateway**

- **Verbindungsgateway** (Circuit Level Firewall)
  - Filter auf Schicht 3 und 4
  - **Generischer Proxy** (Multiprotokollproxy)
  - **Nutzerauthentisierung & Nutzer-abhängige Filterung**
  - Trennt Verbindung zwischen Client und Server
  - Beispiel SOCKS:
    - Filtert auf Quelle, Ziel, Art des Verbindungsaufbaus, Protokoll, Nutzer

Übungsblatt 12: Aufgabe 2: (T) Firewalls und Intrusion Detection
b) Firewall-Regeln

- (b) Erstellen Sie exemplarisch Firewall-Regeln, um die folgenden Anforderungen zu erfüllen:
  - Zugriff auf Webserver von extern (Internet) per HTTP und HTTPS
  - Zugriff auf Webserver von intern (LAN) per SSH
  - Zugriff auf Webserver von intern (LAN) per Telnet verbieten
  - Security-Policy verbietet Aufruf von Jobsearch-Seiten

  - External FW-Interface: 212.34.128.12
  - Webserver-IP in DMZ: 10.10.19.6
  - LAN: 10.10.18.0/24
  - Zugriff auf Webserver erfordert weitere Konfiguration. Welche?

Übungsblatt 12: Aufgabe 2: (T) Firewalls und Intrusion Detection
b) Firewall-Regeln

Nr	Source	Dest	Protocol	S-Port	D-Port	Action
1	**212.34.128.12**	10.10.19.6	TCP	any	80,443	Allow
2	LAN	10.10.19.6	TCP	Any	80,443, 22	Allow
3	LAN	10.10.19.6	TCP	Any	23	Deny
4	Any	Any	Any	Any	Any	Deny

- (Optional) IP **212.34.128.12**: Alias auf External FW-Interface
- DNAT: 212.34.128.13:80,443 → 10.10.19.6:80,443

Übungsblatt 12: Aufgabe 2: (T) Firewalls und Intrusion Detection
b) Firewall-Regeln

- Beispiel: Aufruf von Jobsearch-Seiten verbieten?
- Lösung:
  - Application Level Firewall (Schicht 7)
  - Content Filtering / URL – Filtering mittels HTTP-Proxy
    - Blacklist „Job-Search" (Kategorie-basiertes URL-Filtering)
    - „*.monster.de", „*.jobscout24.de", „*.stepstone.de", „*.indeed.de"
  - In Verbindung mit Nutzerauthentisierung (AD-Integration)
    - Mitarbeiter „deny"
    - Personal-Abteilung „allow"

Übungsblatt 12: Aufgabe 2: (T) Firewalls und Intrusion Detection
c) Erkennungstechniken von IDS

- (c) Welche grundsätzlichen Erkennungstechniken findet man bei Netz-basierten Intrusion Detection Systemen (IDS)?
  Nennen Sie Vor- und Nachteile.

- Lösung:
  - Signatur-basiert
    - Erkennt nur bekannte Angriffe
    - Kleinste Änderungen am Angriffsmuster → Nicht-Erkennung
  - Anomalie-Detection
    - Lernt „Normalverhalten" (Longterm profile)
    - Abweichung (Shortterm profile) → Angriff

Übungsblatt 12: Aufgabe 2: (T) Firewalls und Intrusion Detection
d) Umgehen von IDS

- (d) Intrusion Detection Systeme lassen sich umgehen. Beschreiben Sie eine mögliche Vorgehensweise
- Lösung:
  - Verschlüsselung des Traffics
  - Fragmentierung von Angriffen (Aufteilung des Angriffs auf mehrere Pakete)

Übungsblatt 12: Vorlesungsfolien zu Firewalls

- https://www.nm.ifi.lmu.de/teaching/Vorlesungen/2012ws/itsec/_skript/itsec-k14-v8.0.pdf