NFS Absichern

David Wedekind, Leon Haußknecht

Gliederung

- Grundidee
- Unsere Ziele
- 802.1X
- Radius
- Paketformat
- EAP
- TPM 2.0
- Demo
- Fazit und Future Work

Grundidee

- NFS-Client entscheidet selbst über Rechte im Dateisystem
- Dadurch hohe Anforderung an Integrität
- 1. Idee: Authentifizierung auf Netzwerkebene per 802.1X
- 2. Idee: feste Hardwarebindung der Schlüssel mittels TPM 2.0

Unsere Ziele

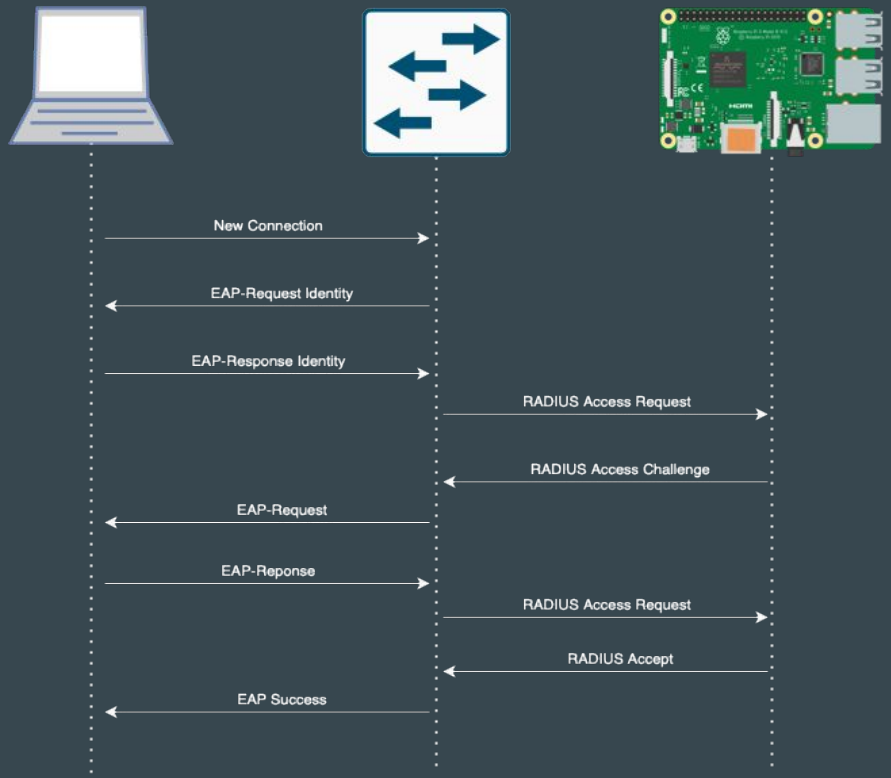
- 3 große Ziele:
  - 1. Funktionierender Testaufbau für eine Authentifizierung mit 802.1x
  - 2. CSR mit Schlüssel aus TPM generieren
  - 3. Schlüssel aus TPM für 802.1x verwenden

802.1X

- Standard zur Authentifizierung in Netzwerken
- Authentifizierung eines Teilnehmers mittels Authenticator und Authentifizierungsserver (RADIUS)
- Teilnehmer übermittelt Authentifizierungsinformationen an den RADIUS Server und dieser entscheidet über die Zulassung
- Motivation: Zugriff nicht an Standort sondern Identität binden

RADIUS

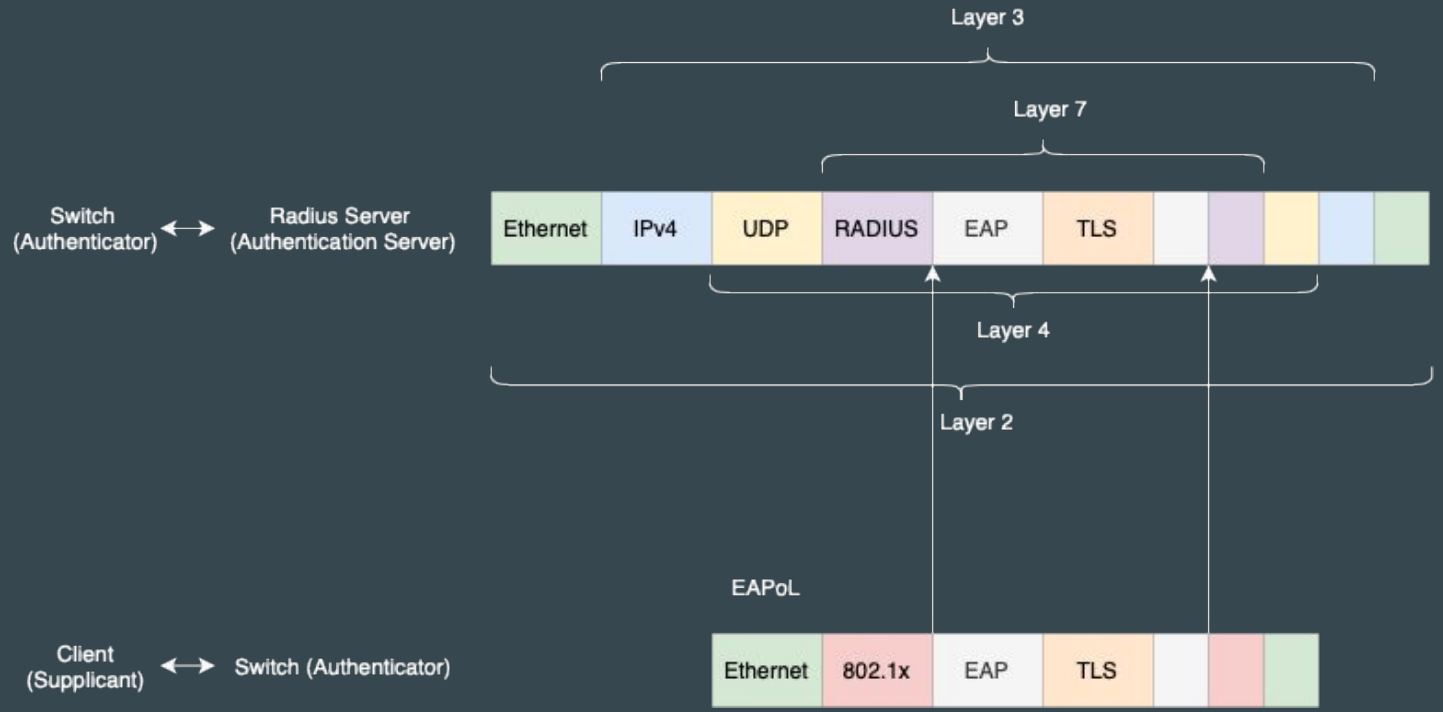
- Protokoll zur Autorisierung, Authentifizierung und Accounting in Netzwerken
- Wird zwischen Authenticator und Authentifizierungsserver gesprochen
- Im RADIUS-Accept Paket können mehrere Attribute zur Auswertung am Authenticator mitgegeben werden



Use Cases

- Dynamische VLAN Zuweisung
  - Port basiert
  - MAC basiert
- IP Zuweisung
- WLAN ohne WPA-PSK

Paketformat



EAP

- Extensible Authentication Protocol
- Verschiedene Varianten
  - EAP-PWD
  - EAP-TLS
  - EAP-TTLS
  - EAP-MD5

TPM 2.0

- Hardware, in der man Schlüssel speichern kann
- Relevant für uns, weil:
  - Generieren des Schlüssels im TPM möglich
  - Schlüssel nicht exportierbar
  - Programme wie openssl können den TPM dazu bringen, mit dem Schlüssel Daten zu signieren
- Dadurch feste Bindung der Zertifikate an die Hardware
- Bietet Schutz vor Software basierten Angriffen

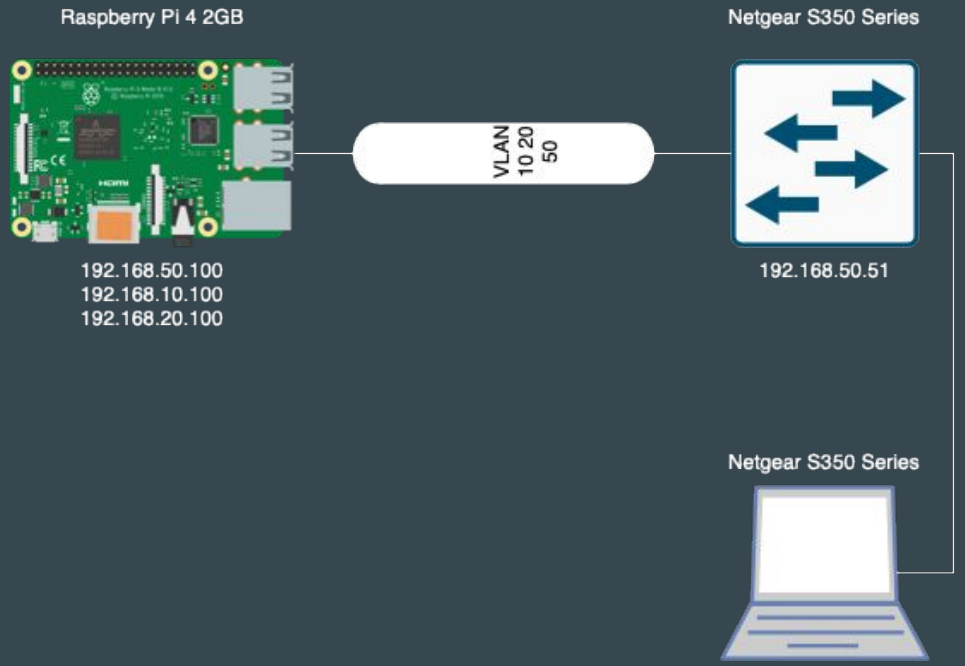
Demo Aufbau - Hardware

- Client: Lenovo X390 Yoga
  - TPM 2.0: Nuvoton NPCT75x
  - Rankie USB 3.0 zu RJ45 Gigabit Ethernet Adapter, Modell: 2724571630609
- Radius Server: Raspberry Pi 4
  - 2GB RAM
- Switch: Netgear 8 Port GS3508T
  - Softwareversion: 1.0.0.12

Demo Aufbau - Software

- Linux TPM2 & TSS 2 Software
  - Unterstützte Schlüssel:
    - rsa1024, rsa2048, rsa3072, rsa4096
    - aes128, aes256
    - ecc224, ecc256, ecc384, ecc521 (NIST Kurven)
    - hmac:sha1, hmac:sha256, hmac:sha384. hmac:sha512
- OpenSSL 3.0
- Ubuntu 22.04 LTS
- FreeRADIUS 3.0
- ISC-DHCP Server

Demo aufbau


Raspberry Pi 4 2GB
Netgear S350 Series
VLAN
10 20
50
192.168.50.100
192.168.10.100
192.168.20.100
192.168.50.51
Netgear S350 Series

Demo

Fazit und Future Work

- Proof of Concept ist erbracht
- Installations und Konfigurationsaufwand noch sehr hoch
- Austesten und Anwenden auf mehr verschiedener Software und Hardware
- Stabiles Installationsskript schreiben