WPA Enterprise

Petri Riihikallio, CWNE#307
Metis Oy

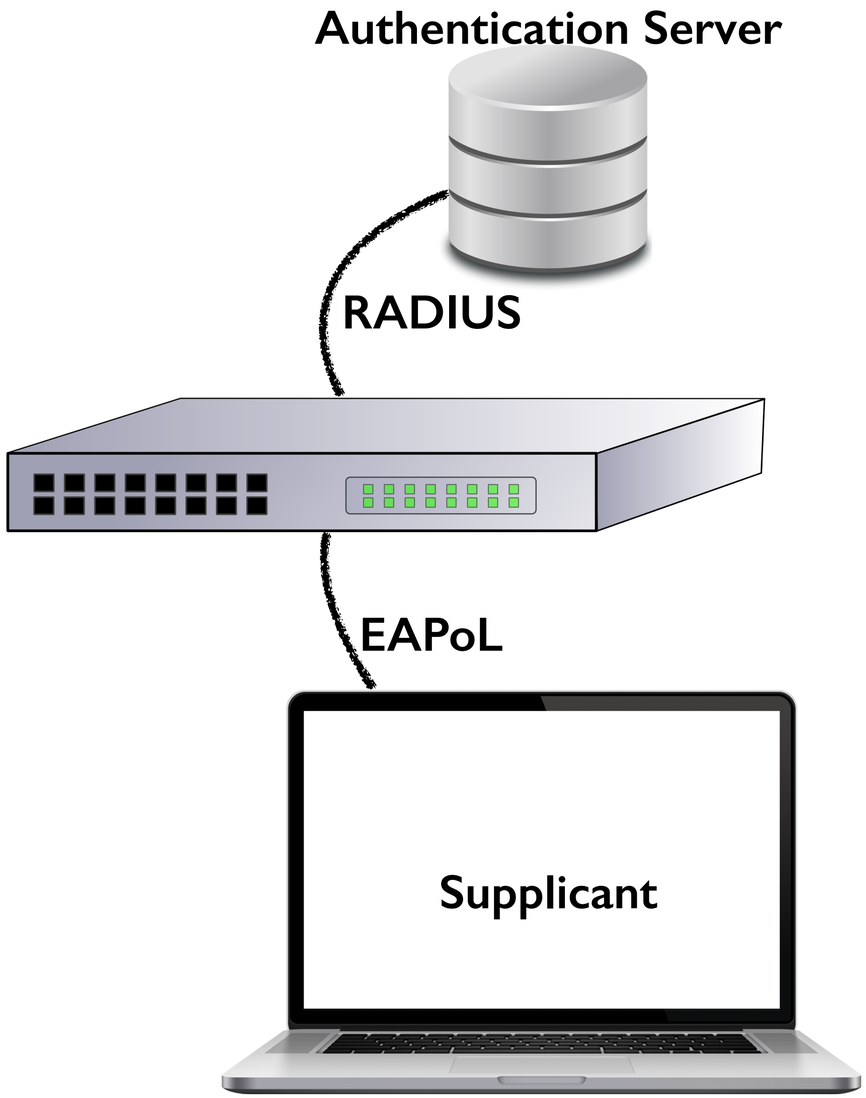
The case

- WPA Personal or Pre-Shared key (PSK)
  - The same password is used by all
  - The password should be changed every time someone is denied access
- WPA Enterprise
  - Users authenticate with an account and a password
  - Easy to control access per user
  - Users can be directed to different VLANs (802.1Q)

MetisGuest2018

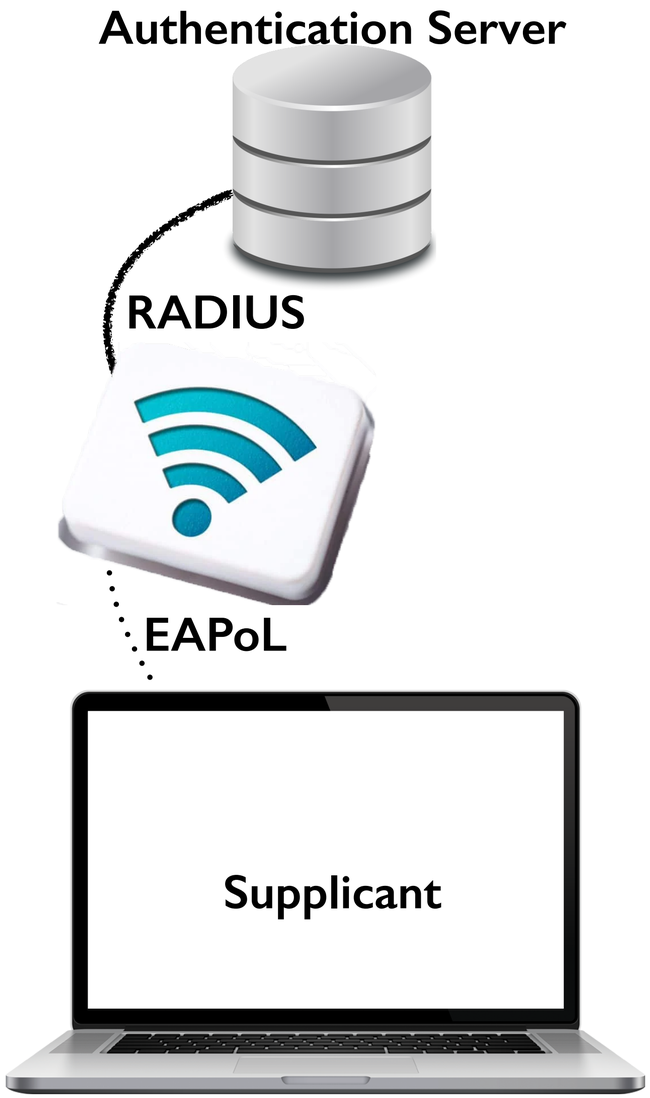
802.1X

- Wired port authentication
- At layer 2
  - Before DHCP!
- Authentication Server
  - RADIUS
- Extensible Authentication Protocol (EAP)
  - EAP-over-LAN or EAPoL
- Wi-Fi Access Points (APs) are layer 2 hubs
  - Thus Wi-Fi + 802.1X = WPA Enterprise



802.1X

- Wired port authentication
- At layer 2
  - Before DHCP!
- Authentication Server
  - RADIUS
- Extensible Authentication Protocol (EAP)
  - EAP-over-LAN or EAPoL
- Wi-Fi Access Points (APs) are layer 2 hubs
  - Thus Wi-Fi + 802.1X = WPA Enterprise



RADIUS

- Remote Authentication of Dial-In User Service
  - Originally to authenticate users in Internet access modem pools
- Poor security
  - Shared secret
  - Often enhanced with IP filtering and/or dedicated VLAN
- Common software packages:
  - Windows Network Policy Server (NPS)
  - FreeRADIUS
  - Aruba ClearPass
  - …and many others

EAP types

- Supported by Apple operating systems:
  - EAP-TLS
  - EAP-TTLS (MSCHAPv2)
  - EAP-FAST
  - EAP-SIM
  - EAP-AKA
  - PEAP-MSCHAPv2
  - PEAP-GTC
- RADIUS server must support the same type!

X.509 Certificates

- Originally created for public key encryption
- Certificates must be signed by a trusted signee
  - Multi-level certification paths are common
- Certificates expire after a definite validity period
- For servers public Certicate Authorities (CAs) only sign public DNS names
- It is common to run an internal CA for 802.1X
  - All devices need to trust the CA's certificate
    - The CA certificate must be added to the trusted certificates on each device
    - Requires Mobile Device Management (MDM)

Pain points

- Chosen EAP type must be supported by all devices and the RADIUS server
- Running a CA is not trivial
  - Renewing certificates is even trickier (SCEP and ACME protocols)
- MDM must install the root certificate with the Wi-Fi profile
  - Still the certificate selection dialog keeps popping up
- Do you want to authenticate devices or users?
  - Device authentication happens automatically after boot by MAC address
  - User authentication happens after user logs on
  - (Windows does both)
- In Active Directory (AD) environment: Are Macs bound to the AD?

Combinations

Wi-Fi Systems	12
Clients	12
RADIUS Servers	6
EAP Types	7
Certificate Authorities	5
MDM Systems	10
Machine or User Authentication	2
AD Binding	2
	1 210 000

Recommendations

- Decide whether WPA Enterprise is worth the effort
  - What are you trying to protect?
  - Do you still need a WPA Personal SSID for unsupported devices?
  - How about a zero trust network?
- Sign up to MacAdmins slack channel #8021x
- All environments are different
  - e.g. “Do the RADIUS requests come from the Wi-Fi controller or the APs?”
- Test the certificate renewal process!
  - In the pilot phase use one or two week expiration time for all certificates

WPA3 Enterprise v2

- The AS's certificate contains the server's common name (cn)
  - The DNS name
  - Not the SSID
- Attack vector: an Evil Twin directs authentication attempts to a rogue AS
- Version 2 adds Trust Override Disable (TOD) policy:
  - Never trust certificates from the AS (TOD-STRICT)
    - The certificate must be in the network profile
  - Trust the certificate On First Use (TOD-TOFU)
  - Ask to accept certificates when the AS changes (TOD-NONE) is the default
- User Override of Server Certificate (UOSC) pop-up

Thank you!