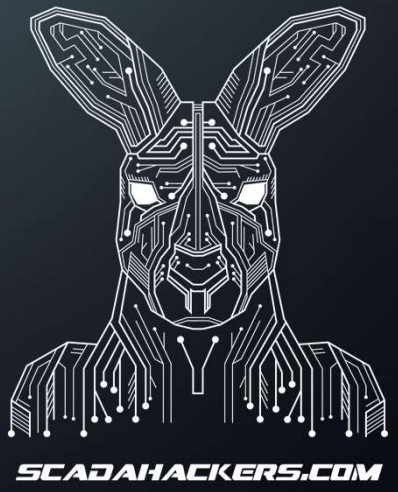
BASIC ROGUE AP DETECTOR

IOT AND SCADA HACKERS AUSTRALIA



HOUSEKEEPING

GROUP INFO

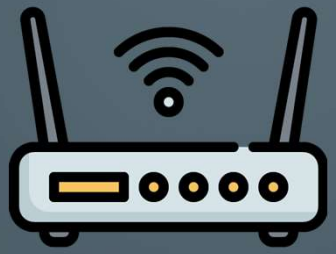
- OPEN COMMUNITY
- IOT, SCADA, ICS, AUTOMATION, PLC, SECURITY
- SHARING CHALLENGES, IDEAS, AND INTERESTS
- SUPPORTIVE AND COLLABORATIVE ENVIRONMENT
- VOLUNTEER-DRIVEN GROUP
- EXPERTS AND BEGINNERS

PRESENTATION

Have an idea?
Present it!

Wireless Architecture

Authenticator



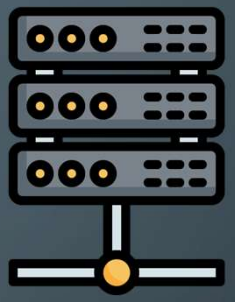
Client / Supplicant

Client / Supplicant

Wireless Architecture - Enterprise

Authenticator

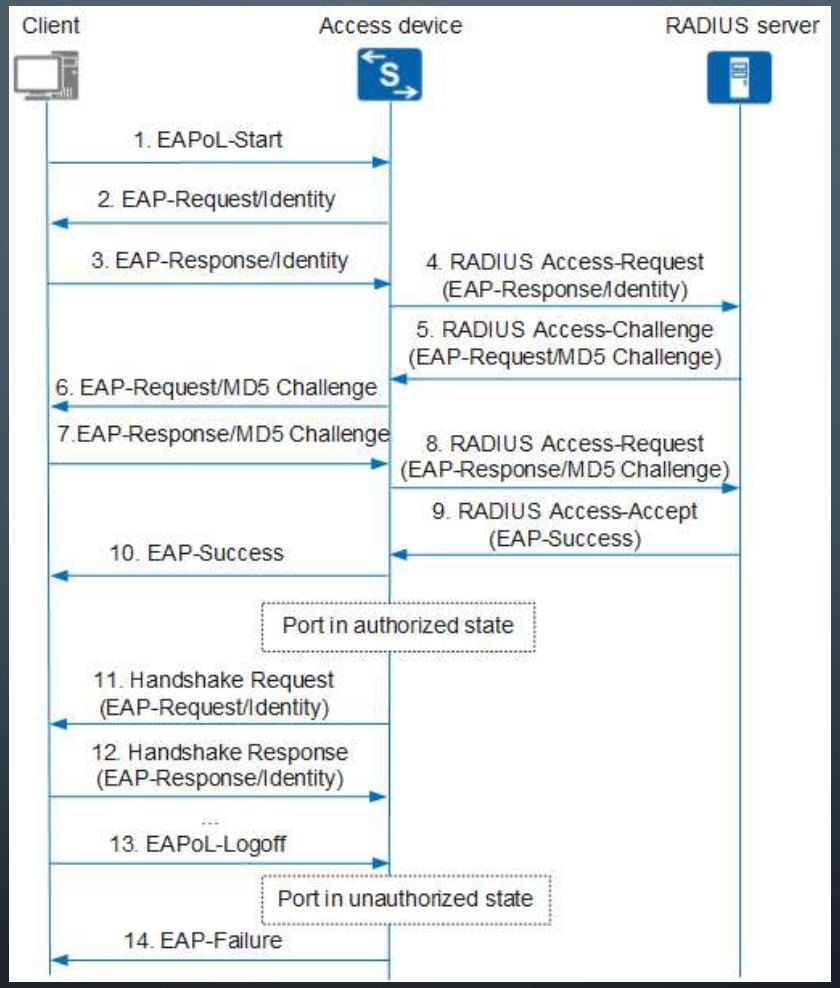
Authentication Server



Client / Supplicant

Client / Supplicant

Wireless Architecture - EAPOL



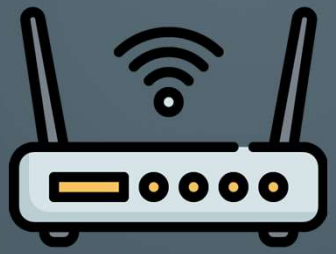
img – Huawei - EDOC1100086527

Wireless Architecture – Common Auth

- Open Wireless (captive portal, etc.)
- Pre-Shared Key (PSK)
- PEAP / MSCHAPv2
- EAP-TLS

Wireless Architecture

FE-ED-41-AA-47-4E
(BSSID)
Basic Service Set IDentifier



Wireless Name: ISHA
(SSID or ESSID)
Extended Service Set IDentifier

BE-EF-66-17-67-8A
(BSSID)

BE-EF-87-E4-67-04
(BSSID)

BE-EF-66-17-67-8A
(BSSID)

Wireless Architecture

Wireless Name: ISHA
(SSID or ESSID)

FE-ED-41-AA-47-4D

FE-ED-41-AA-47-4E

FE-ED-41-AA-47-4F

BE-EF-66-17-67-8A
(BSSID)

BE-EF-87-E4-67-04
(BSSID)

BE-EF-66-17-67-8A
(BSSID)

Wireless Architecture – Common Attacks

- Open Wireless (captive portal, etc.)
  - MAC Address Cloning, Session Hijacking, Authentication Bypass
- Pre-Shared Key (PSK)
  - Capture Handshake and Brute Force, Half-Handshake Attacks (no AP required)
  - WPS / PIN
  - KRACK
- PEAP / MSCHAPv2
  - Rogue Access Point – security is heavily reliant on device management
  - EAP relaying
  - KRACK
- EAP-TLS
  - Rogue Access Point – security is heavily reliant on device management
  - KRACK

Wireless Architecture

Wireless Name: ISHA
(SSID or ESSID)

DE-AD-41-AA-47-5A

Wireless Name: ISHA
(SSID or ESSID)

FE-ED-41-AA-47-4E FE-ED-41-AA-47-4F

BE-EF-66-17-67-8A
(BSSID)

BE-EF-87-E4-67-04
(BSSID)

BE-EF-66-17-67-8A
(BSSID)

Wireless Architecture – Active Defence

Wireless Name: ISHA
(SSID or ESSID)

DE-AD-41-AA-47-5A

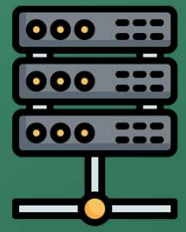
Wireless Name: ISHA
(SSID or ESSID)

FE-ED-41-AA-47-4E FE-ED-41-AA-47-4F

BE-EF-87-E4-67-04
(BSSID)

WLC

Good BSSIDs:
FE-ED-41-AA-47-4E
FE-ED-41-AA-47-4F



Wireless Architecture – Active Defence

Wireless Name: ISHA
(SSID or ESSID)

DE-AD-41-AA-47-5A

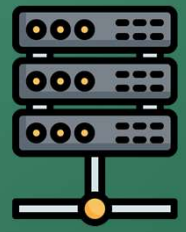
Wireless Name: ISHA
(SSID or ESSID)

FE-ED-41-AA-47-4E FE-ED-41-AA-47-4F

BE-EF-87-E4-67-04
(BSSID)

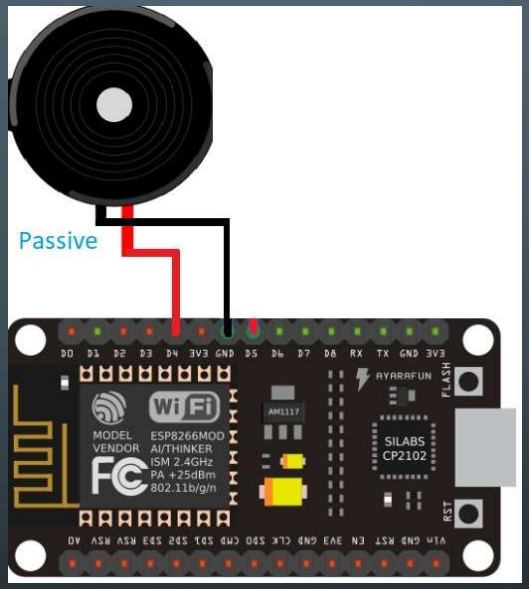
WLC

Good BSSIDs:
FE-ED-41-AA-47-4E
FE-ED-41-AA-47-4F



PROJECT INFO

- HTTPS://GITHUB.COM/SCADAHACKERS/PRESENTATIONS



img - https://www.geekering.com/

THANKS FOR COMING!

- Twitter @IoTSCADA_AU
- Web scadahackers.com