3.4

Thursday, September 21, 2023 5:48 PM

Increase service in large office

- Separate channels by 20 MHz
  - channels have 5mHz spacing
    - but WiFi requires 20
- WPA3 w/ enterprise sec requires all users to auth w/ creds
- Place WAP in red areas of heat map because signal strong

Authentication Protocols

- EAP
  - pairwise master key PMK
- Protected EAP PEAP
  - TLS

Cert on server

Microsoft challenge handshake Authentication certificate MS-CHAP v2

or

Generic token card GTC

- EAP-FAST
  - secure tunneling
  - CISCO
  - secure version of LEAP
  - instead of cert for tunnel, use Protected Access Credential
  - PAC - made for each user from master key
- EAP-TLS
  - cert on both
- EAP-TTLS

- ~~EAP-FAST~~
  like peap
  can use older CHAP or PAP
  server cert

LEAP vuln to pword cracking

802.1x is port-based NAC framework
  EAP is the actual auth mechanism

Pre-shared key = wifi pword

Can't setup with WPS
- need compatible NIC
- connect w/out WPS using passphrase or PIN

Wireless controller connects to RADIUS via shared secret key

WiFi Analyzer - software tool to scan for wireless signals in area

Wifi [illegible]

for wireless signals in [illegible]

can catch rogue AP

Site survey - arch map of site
mark walls, reflective surface, motors,
ovens that could interfere w/ signal

heat map = wifi analyzer + site survey

best settings for WPA2

- PSK
- AES-CCMP

counter mode w/ cipher block
chaining message auth code

standard enc method, works
w/ WPA2

Enhanced open - feature of WPA3
that enables encryption for

open mode

SAE - Simultaneous authentication of equals

feature of WPA3 that replaces WPA 4-way handshake auth

WPA3 uses updated crypto proto

AES Galois Counter mode protocol

AES GCMP

WPA2 uses RC4 and temporal key integrity protocol

802.1x defines use of EAP over wireless

EAPoW to allow access point to forward auth data w/out allowing any other type of net access

AP isolate - prevents connected clients from communicating w/ each other

Enterprise wireless implement wireless controllers for central manage and monitor hardware/software

I guess MSCHAP better than EAP-TTLS?