Is Wi-Fi Enterprise so perfect?

Demchenko Oleksandr

Wargaming.NET | Persha Studia

SteelDrum XI 12 Nov 2016

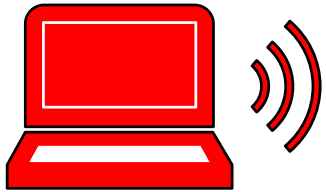
About me

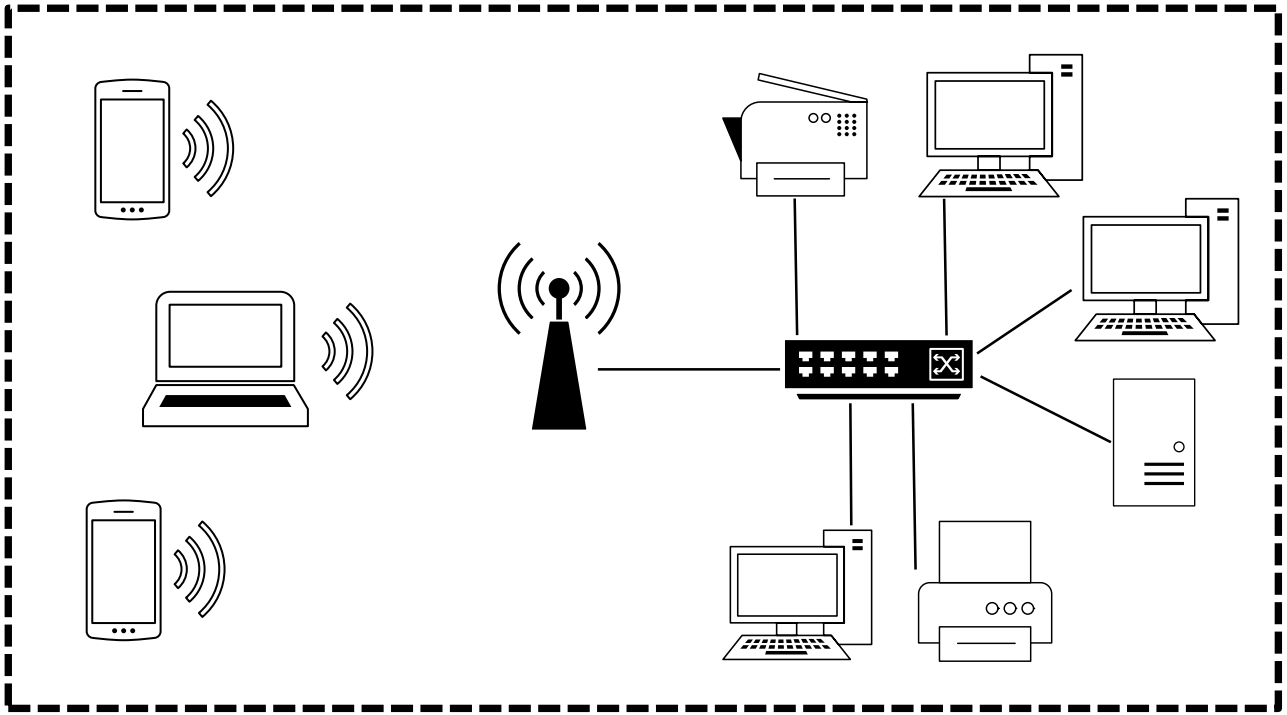
- IT Security Specialist at Persha Studia
- 7 years in IT
- 4 years in Information Security

Skype: exmodding

Email: exmodding@gmail.com

Wireless vs Wired





Wi-Fi protocol

Protocol =

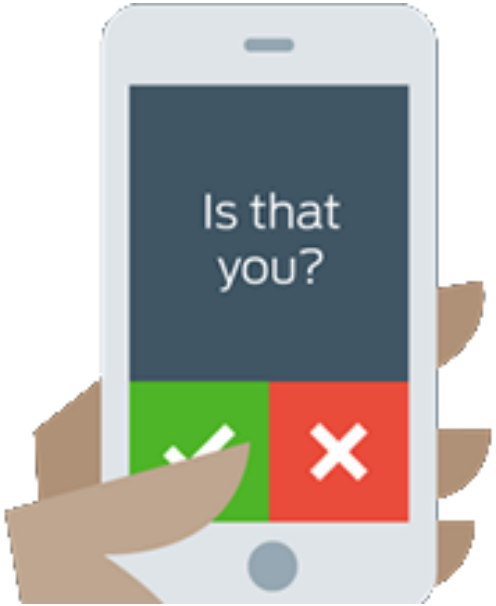
Authentication + Encryption

Encryption

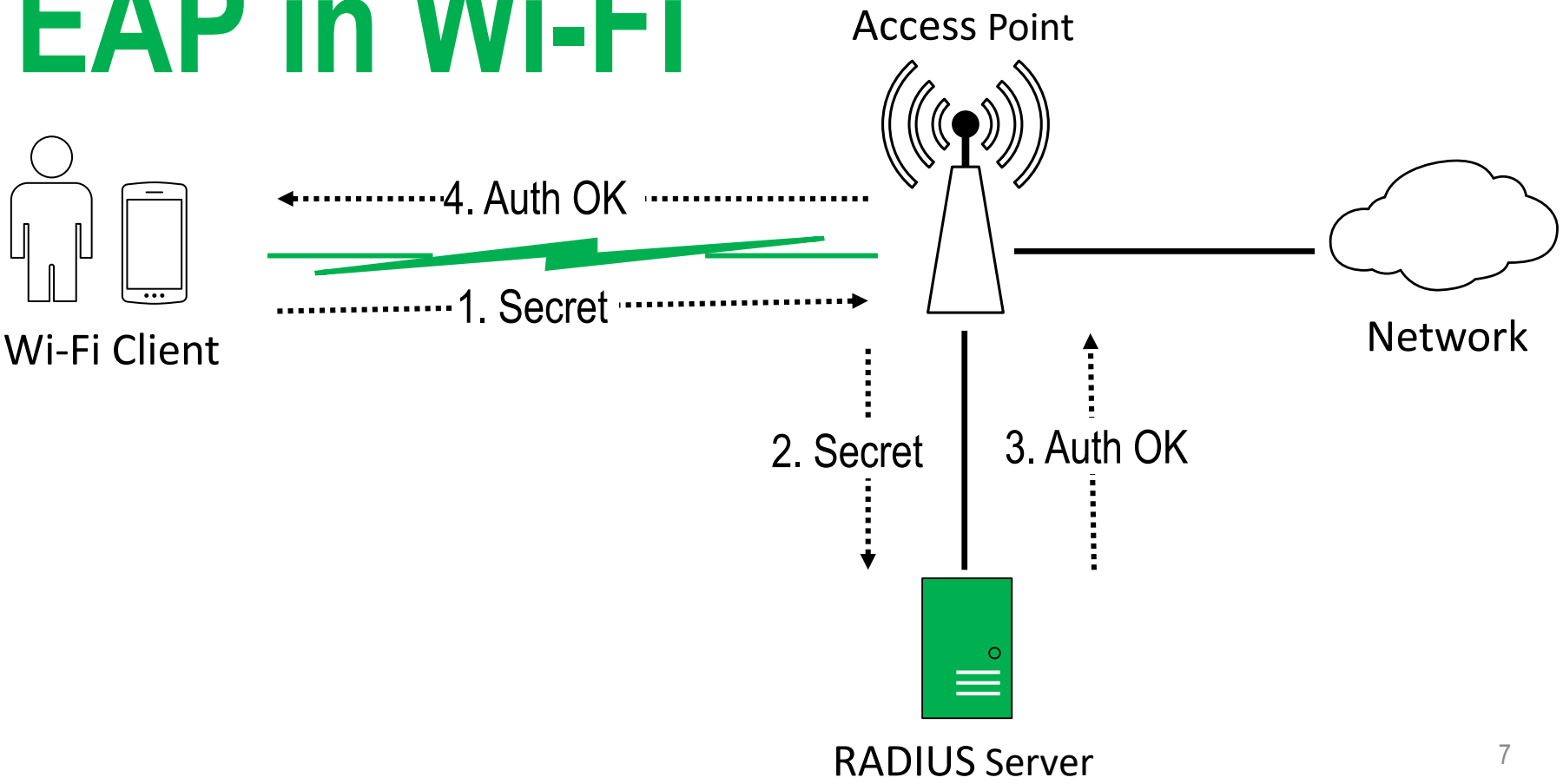
- None
- RC4 (WEP)
- TKIP (WPA)
- CCMP-AES (WPA2)

Authentication

- Open – no password
- Shared – one password
- EAP – multi passwords



EAP in Wi-Fi


Access Point
4. Auth OK
1. Secret
Wi-Fi Client
Network
2. Secret
3. Auth OK
RADIUS Server

EAP methods

LEAP
PEAP
EAP-TLS
EAP-MD5
EAP-POTP
EAP-PSK
EAP-PWD
EAP-TTLS
EAP-IKEv2
EAP-FAST
EAP-SIM
EAP-AKA
EAP-AKA Prime
EAP-GTC
EAP-EKE

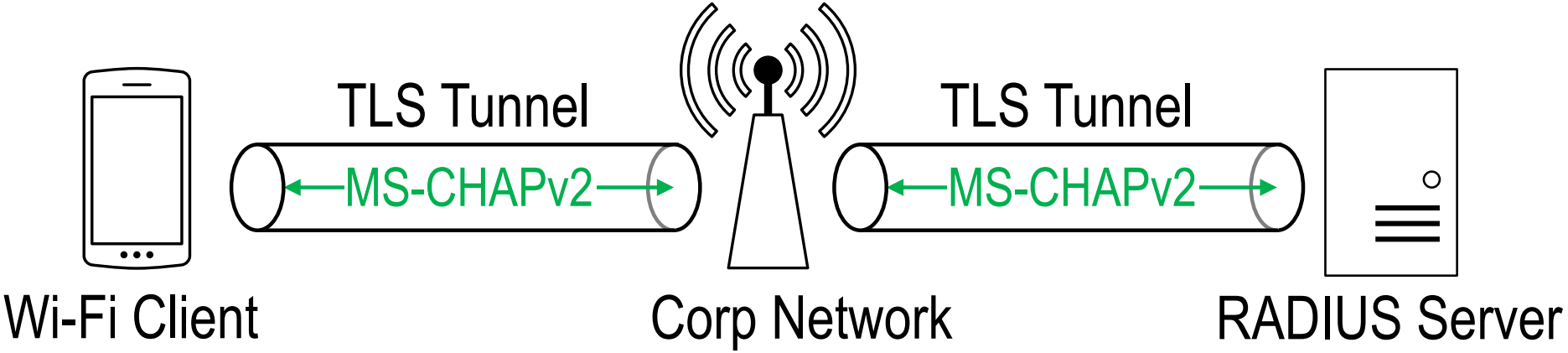
EAP-FAST
PEAP
EAP-TLS

EAP-FAST

- Q. Why did Cisco develop EAP-FAST?
- A. Cisco developed EAP-FAST to support customers who cannot enforce a strong password policy and wish to deploy an 802.1X EAP type that does not require digital certificates…

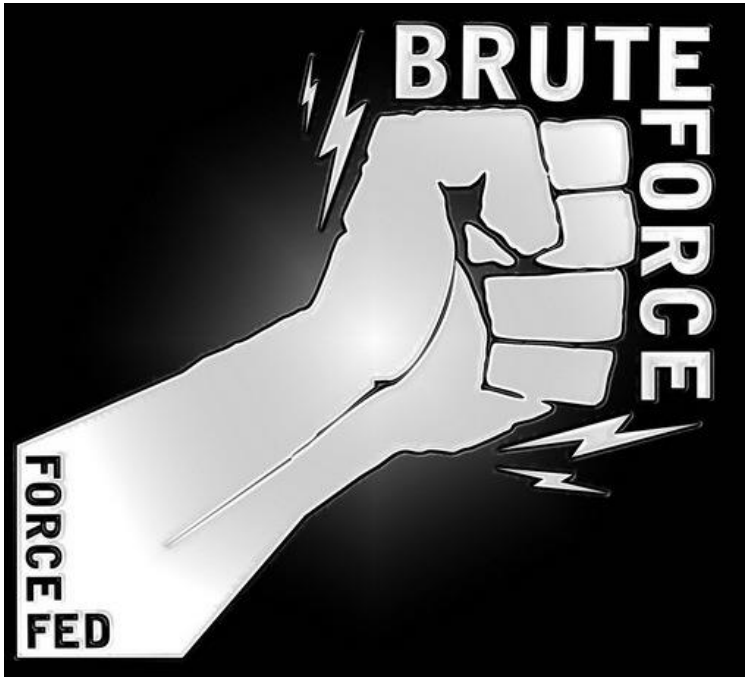
@Cisco Q&A at http://goo.gl/1ACNXa

PEAP


TLS Tunnel
MS-CHAPv2
TLS Tunnel
MS-CHAPv2
Wi-Fi Client
Corp Network
RADIUS Server

Brute-force

- CPU
- GPU
- Special devices

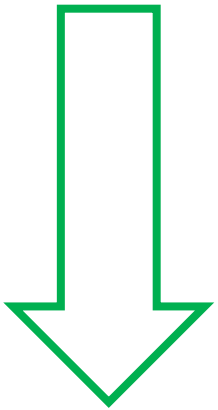


Brute-force

Password

- 8 characters (********)
- [a-z], [A-Z], [0-9], [~!@...]
- 85 options per character
- Total 2,7 × 10^{15} passwords

vs



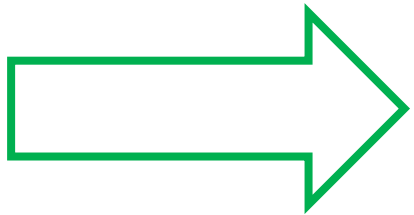
102 hours

GPU

- AMD 7970
- Price 250 $
- 7,3 × 10^{9} hash / sec

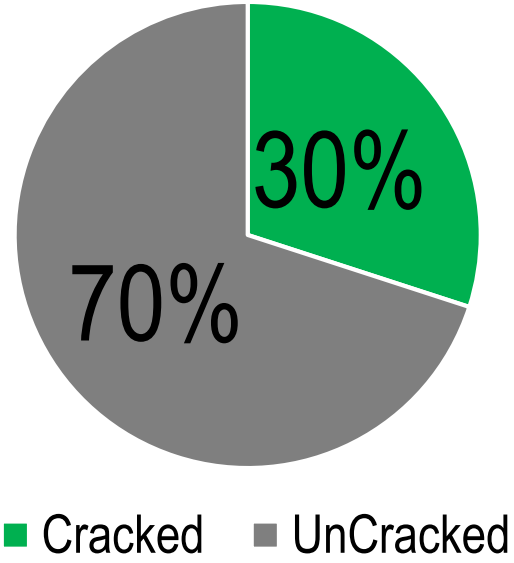
Password length

Length	Time
8	102 hours
9	1 year
10	85 years
11	17270 years

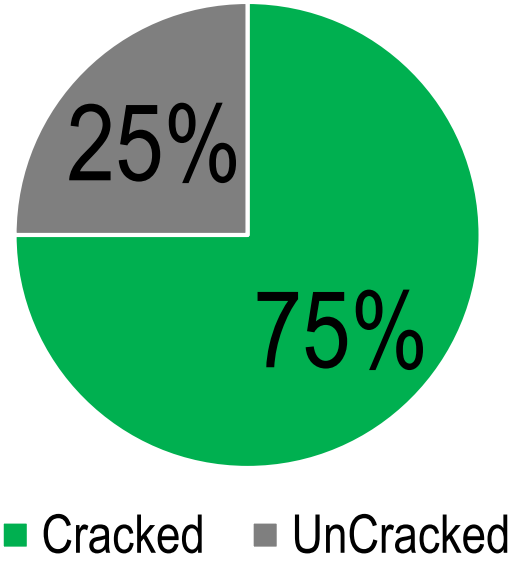


Time to guess the pass

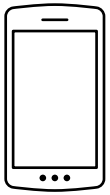
After 30 minutes



After 96 hours



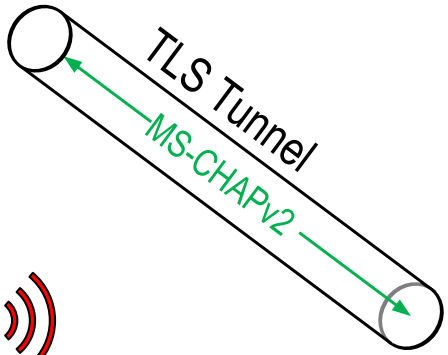
PEAP Attack

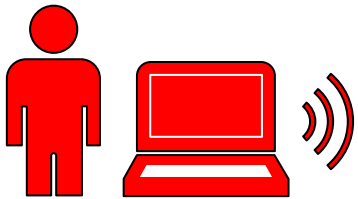


Wi-Fi Client

Corp Access Point

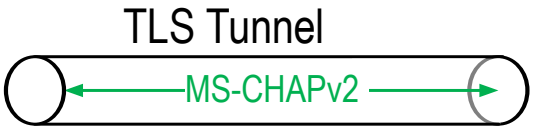
RADIUS Server

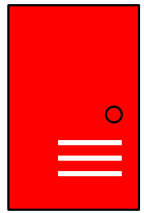




Attacker

Corp Access Point
(Fake)





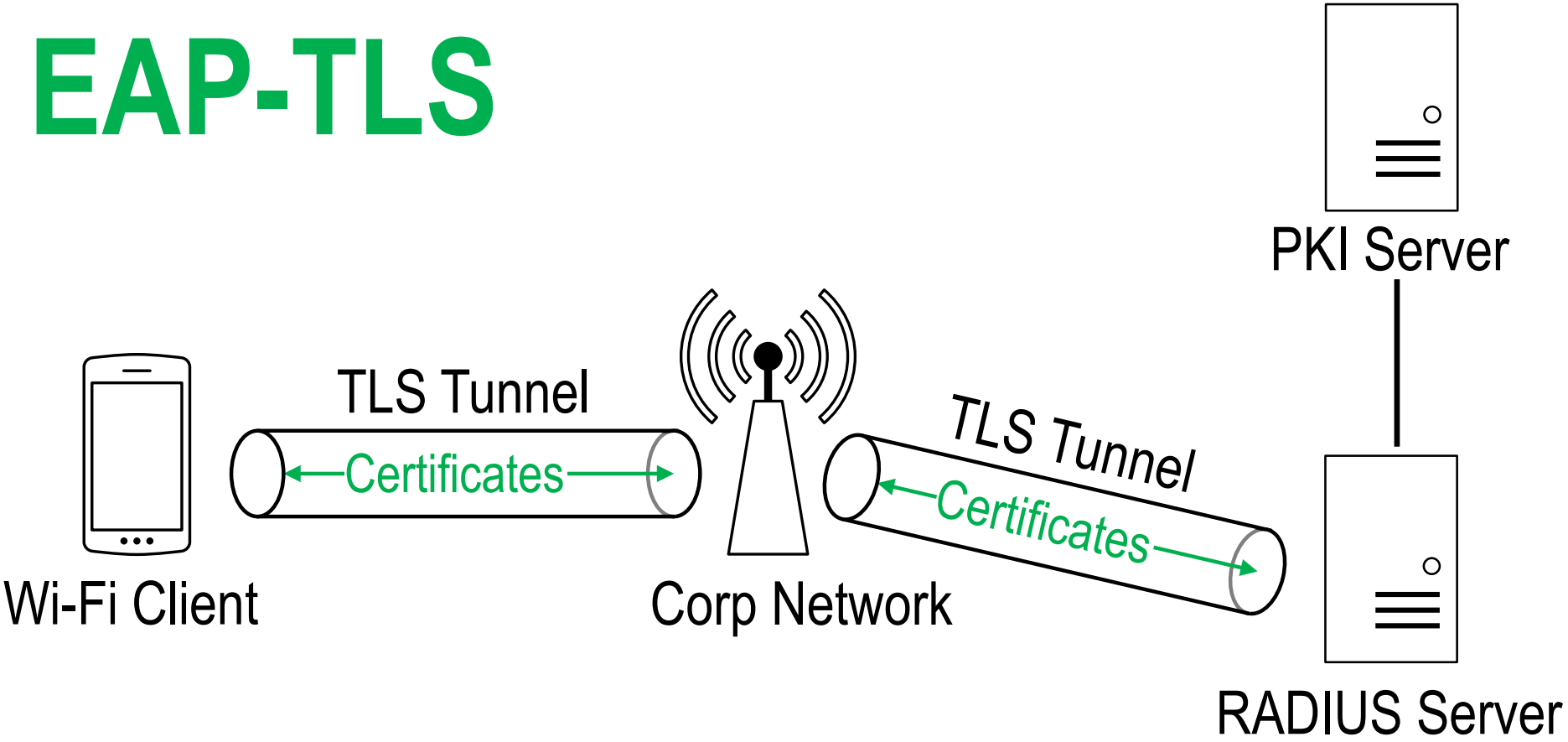
RADIUS Server
(Fake)

Audit steps

1. Detect authorization type
2. Start fake RADIUS and Access Point
3. Intercept user credentials
4. Brute-force the credentials

Life Demo!

EAP-TLS


PKI Server
TLS Tunnel
Certificates
TLS Tunnel
Certificates
Wi-Fi Client
Corp Network
RADIUS Server

THANK YOU!