WI-FI SECURITY ESSENTIALS

RICHARD SHELFORD

openreality

Value Added Wireless Distribution

About Me

RICHARD SHELFORD
Consultant Sales Engineer

- Joined Open Reality in 2018
- Worked for major security and networking distribution companies for the last 19 years in technical support and technical pre-sales roles
- Experience with Aruba, Ruckus, Siemens, Arista, Cambium and Aerohive
- ECSE Design accredited
- Instructor certifications for Arista, Ruckus and Symantec.

Our Agenda

- Reducing your attack surface
- Preventing accidental associations
- Defending against evil twin attacks
- Identifying rogue access points and personal hotspots
- Enforcing web and application control

REDUCING YOUR ATTACK SURFACE

The CIA Triad

- **C**onfidentiality
- **I**ntegrity
- **A**vailability

CONFIDENTIALITY
INTEGRITY
AVAILABILITY

Reducing Your Attack Surface

- PSK – who knows the key?
- Keys can be shared, when do they get changed?
- Per device / user PSK may be an answer.
- 802.1x – secure but requires the client to be configured correctly.
- BYOD needs to be simple.

PREVENTING ACCIDENTAL ASSOCIATIONS

Preventing Accidental Associations

- Corporate devices using the guest network – self sign-up is convenient but may be open to abuse.
- Prohibit corporate devices from joining the guest network - MAC blacklist or ideally automatic blacklisting.
- Corporate devices connecting to 3rd party neighbouring guest networks.

EVIL TWIN

Evil Twin

- This may not be just your corporate wireless, cloned public Wi-Fi like the cloud for example or other well known ones can be just as effective at intercepting users traffic.
- Clients may not be aware of this activity.

ROGUE AP AND PERSONAL HOTSPOTS

Rogue AP and Personal Hotspot

- Corporate devices making mobile hotspots sharing either their wired or wireless connection.
- Users making phones into hotspots.
- How you want to deal with these will be different.
- Isolation of rogue devices from wired and wireless network?

- Is some form of WIPS required?

WEB AND APPLICATION CONTROL

Web and Application Control

- What is the wireless for?
- Updates:
  - Is it better to block updates instead of controlling bandwidth or rate limiting?
  - Are users aware that updates are happening? Limiting client bandwidth or rate will affect clients user experience.
  - Do you want to allow updates on the guest network?
- Streaming content may still work with reduced bandwidth or rate whilst still consuming air time.
- Application control may be a better solution by blocking the traffic at the access point.

THANK YOU

ANY QUESTIONS?

openreality
Value Added Wireless Distribution