Wireless Systems Security

EE/NiS/TM-584-A/WS

Bruce McNair
bmcnair@stevens.edu

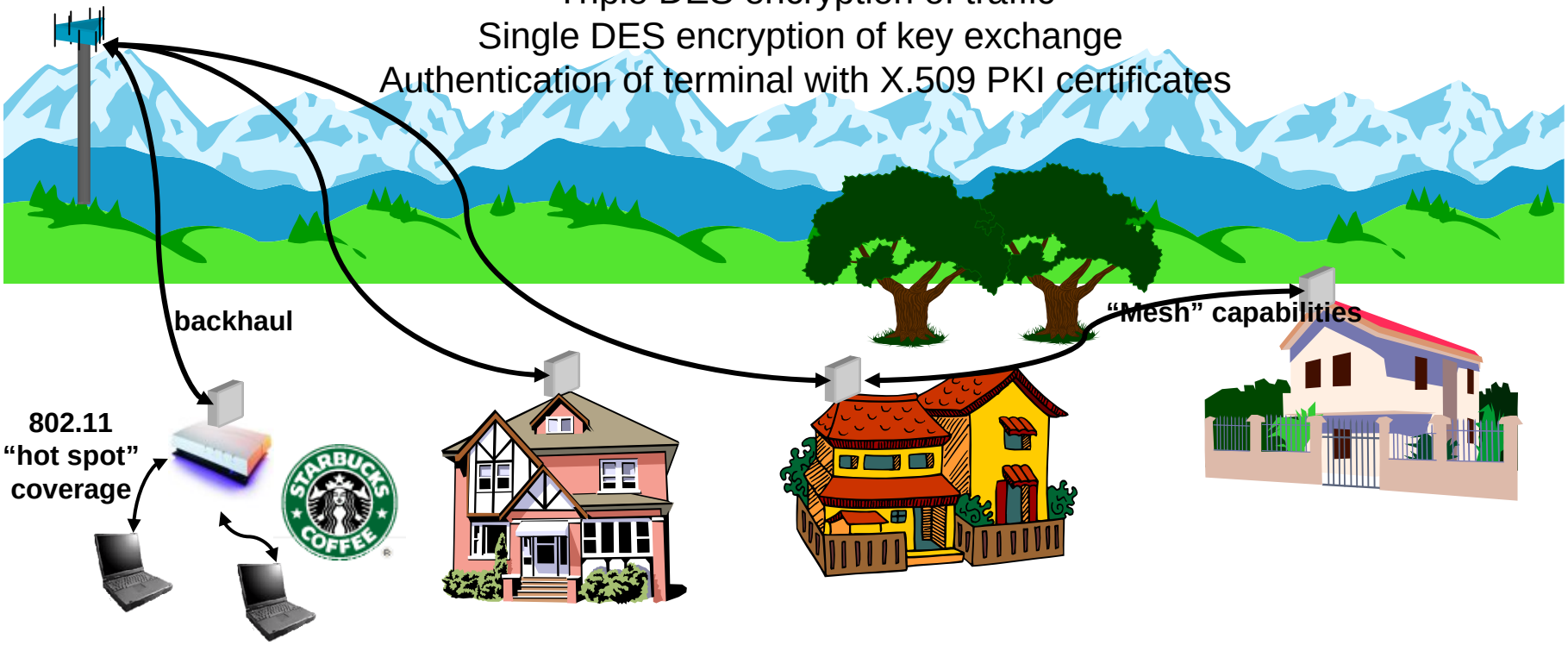
Week 11

Case Study 7

Summary and observations

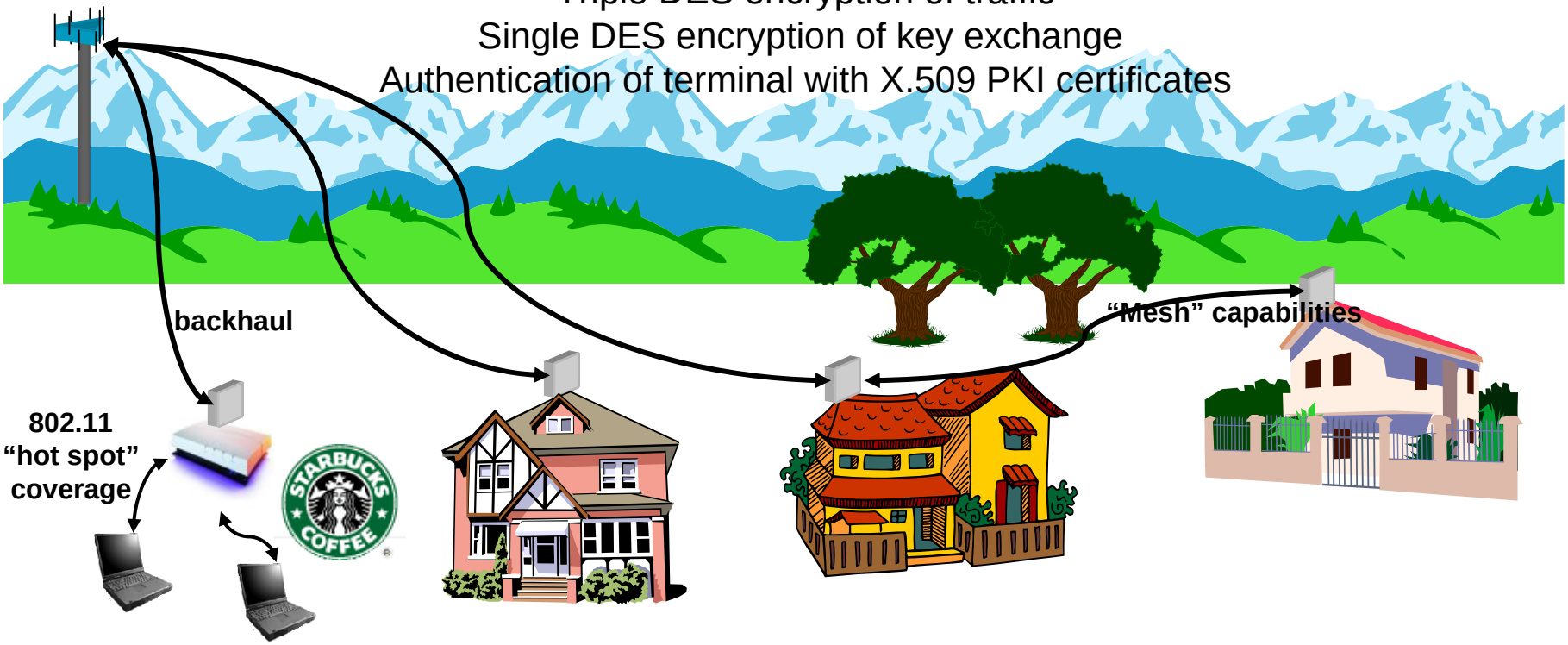
Case 7 –
Wireless Metropolitan Area Networks (W-MANs)
802.16

802.16a: 2-11 GHz 256/2048 carrier OFDM,
802.16.1: 10 – 66 GHz LOS
120 Mb/s capacity
T1+ user data, multiple voice channels, Wireless Local Loop
Triple DES encryption of traffic
Single DES encryption of key exchange
Authentication of terminal with X.509 PKI certificates

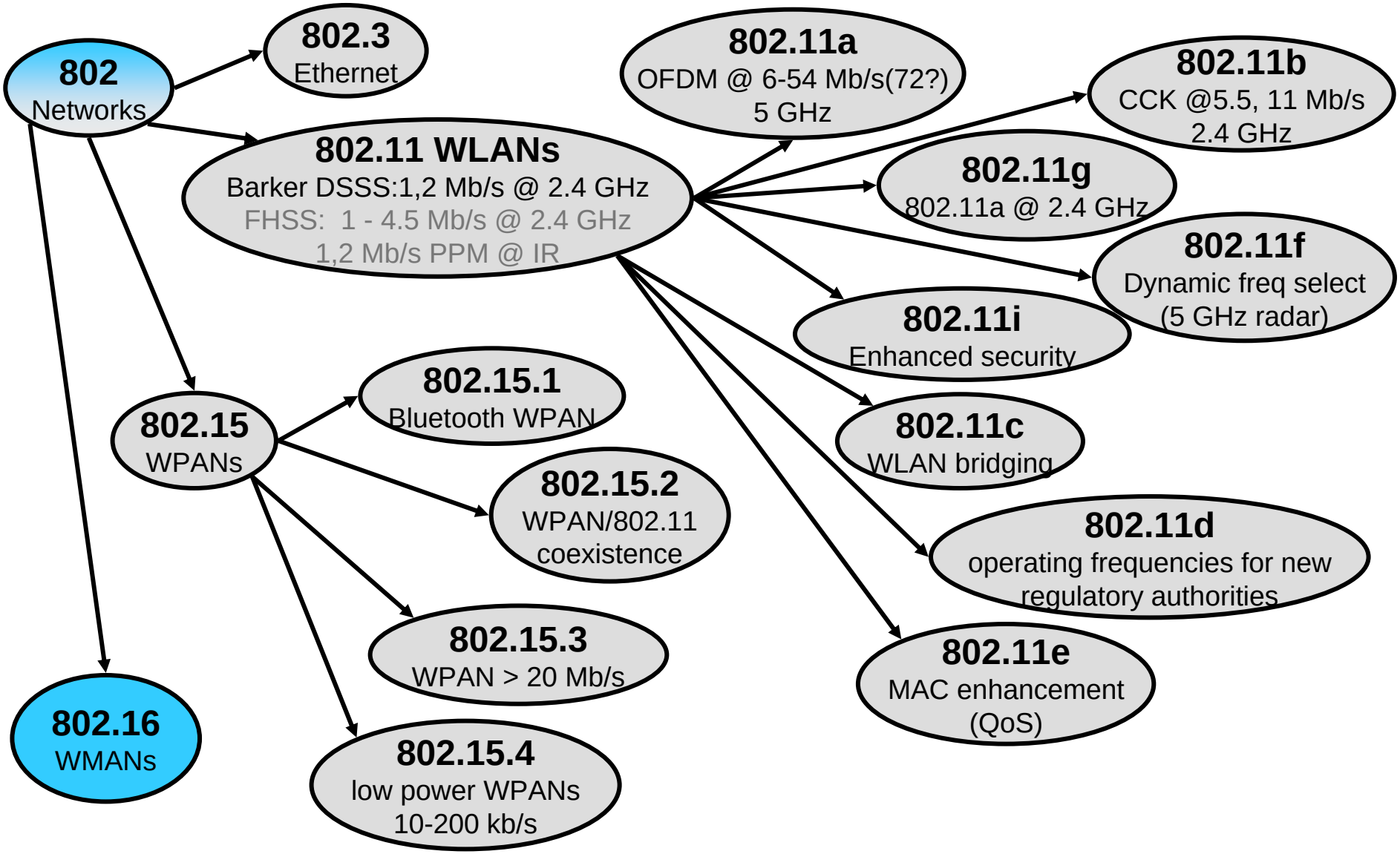


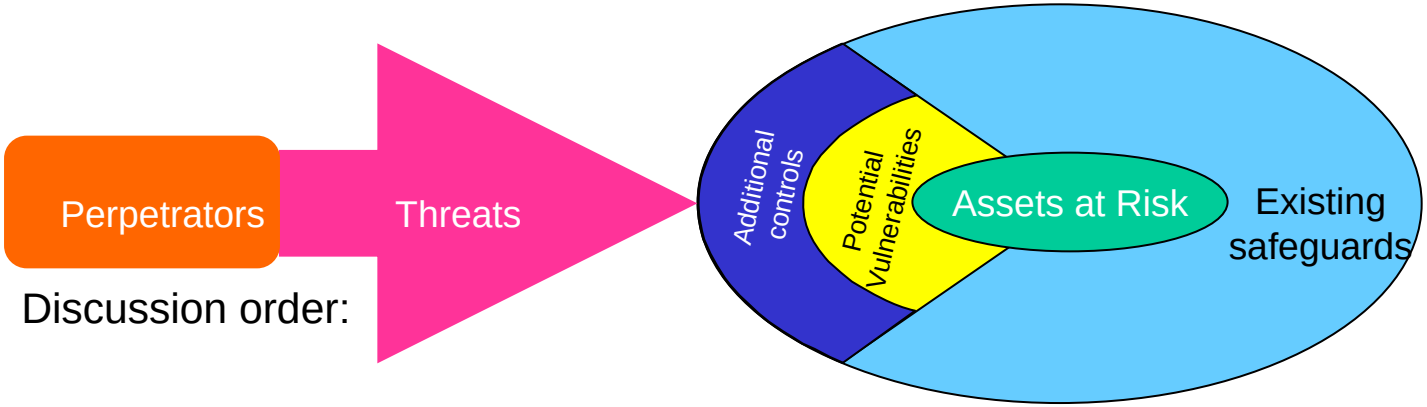
Case 7 –
Wireless Metropolitan Area Networks (W-MANs)
802.16

802.16a: 2-11 GHz 256/2048 carrier OFDM,
802.16.1: 10 – 66 GHz LOS
120 Mb/s capacity
T1+ user data, multiple voice channels, Wireless Local Loop
Triple DES encryption of traffic
Single DES encryption of key exchange
Authentication of terminal with X.509 PKI certificates



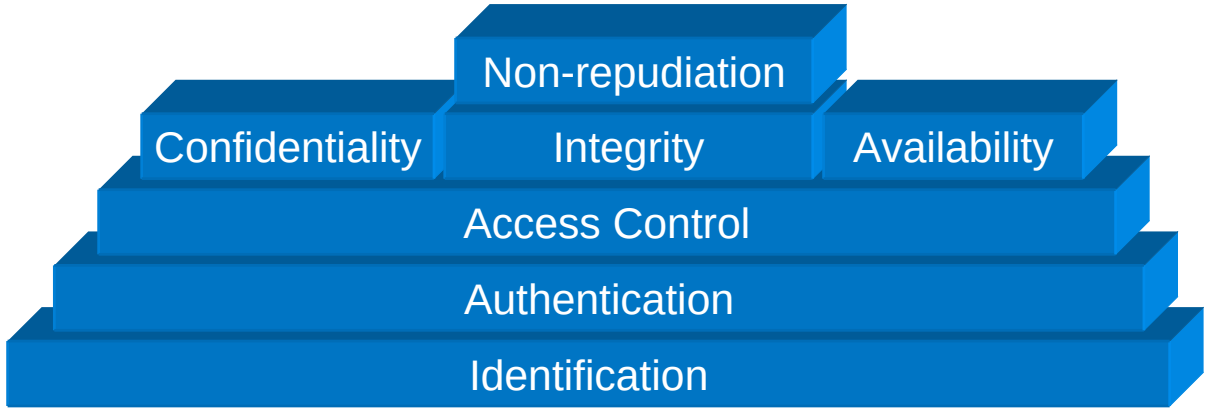
IEEE 802 Standards (Alphabet Soup)

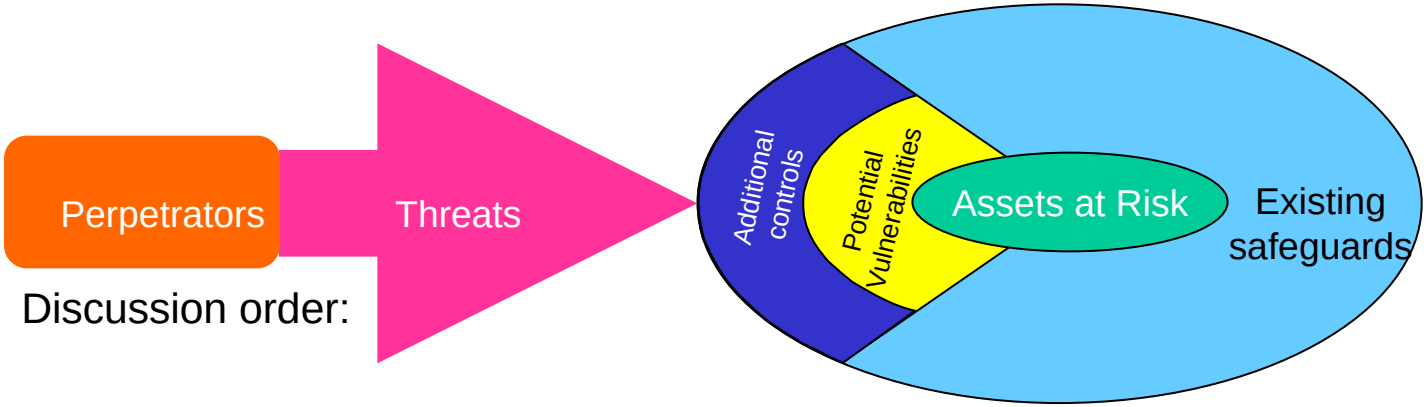




Discussion order:

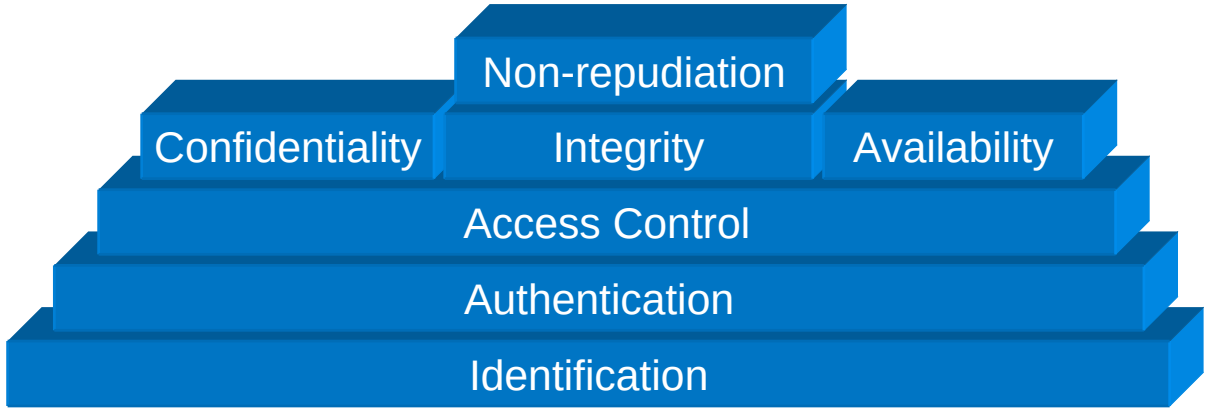
- Assets
- Perpetrators
- Threats
- Existing Safeguards
- Potential Vulnerabilities
- Additional Security Controls





Discussion order:

- Assets
- Perpetrators
- Threats
- Existing Safeguards
- Potential Vulnerabilities
- Additional Security Controls



Assets

- Equipment
  - Terminal
  - Base station
  - Antennas
- Infrastructure
- Frequencies
- Bandwidth
- Terminal/relay nodes
- Connectivity
- User workstation
- Data, protocols
  - Content
  - Integrity
  - Availability
- RF/AP equipment
  - Forwarding function

Perpetrators

Hackers
Teenage kid next door
Disgruntled employee
Users looking at other users information
    "fix it myself"
Organized crime
Competitors (DSL, cable modem, …)
Resellers
Reselling users
Communities
    New buildings
    Antenna and tower restrictions
Nature
Other services competing for spectrum (interference)
Federal government (CALEA)

Threats

User hacks the firewall/modem and snoops on relay traffic
Denial of service
- Denial of relaying
- Injecting extraneous traffic

Another service creating interference
Wind damage
- Reposition terminal antenna
- Bends trees to block Line-of-sight

Steal service or bandwidth

Existing Safeguards

Encryption of data
Updating of keys
Firewall capabilities??
One-way authentication (should be two way)
Accountability of network operators
Auditing capabilities
    And penalty for malfeasance
Education of users/operators
Early reporting of attacks
Non-trivial password???

Vulnerabilities

- Broadband RF-based system
  - Interference
  - Jamming
  - Monitoring
- User/operator configurability
  - Turn on security features
  - Leave default password
- Maintenance mode for RF modem allowing snooping
- Lack of mutual authentication