Wireless Systems Security

EE/NiS/TM-584-A/WS

Bruce McNair
bmcnair@stevens.edu

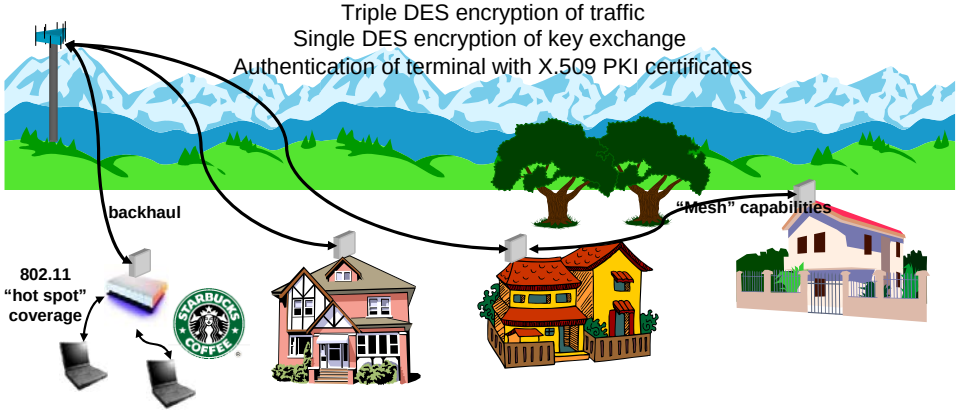
Week 11

Case Study 7
Summary and observations

This was the last case study for the class. As an evolving network, it seems appropriate to examine to use this as an example to finish on.

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

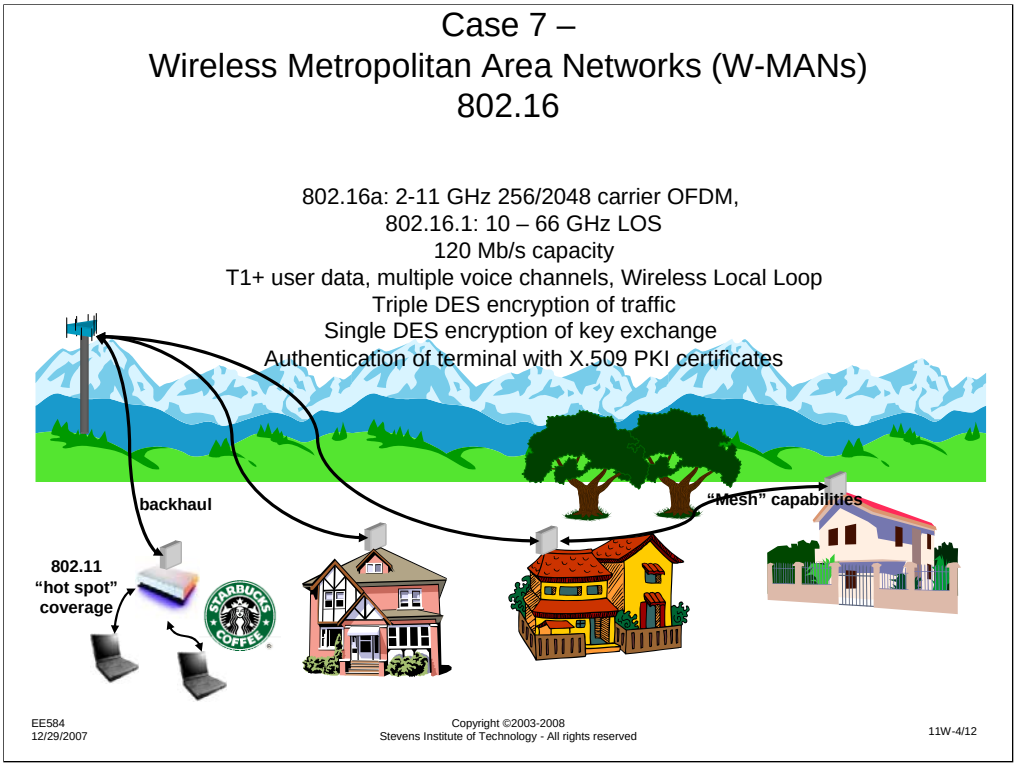


802.16 has a lot of things going for it, from a security perspective, but there are still a lot of open issues.

The fact that the people writing the 802.16 standard decided to use DES was a good choice, despite the fact that brute force attacks against DES exist. AES hadn't been standardized when 802.16 was first under discussion, so DES was the best alternative available. Further, the use of triple-DES means that a brute force attack will be about 2^56 time more difficult than it would be for 56-bit DES. Even the use of single DES for key exchange is reasonable, since the key exchange involves a random-looking stream of bits, inherently more difficult to predict than user traffic.

But there are weak spots in the 802.16 security. First, the terminal is authenticated to the base station with X.509 PKI certificates. This is good, but what about the reverse path? Nothing in 802.16 serves to authenticate the base station to the terminal. As an aside, the next time you drive up to a bank, take note of the night deposit drawer on the side of the bank. You will probably notice a sign that says not to use the drawer if it is broken and never to use any other container. The reason for this notice is because thieves have disabled real night deposit drawers and left their own for merchants to drop their day's receipts in. Obviously, these deposits were into the thieves pockets and not the bank's. This is a simple physical example of the danger of not authenticating the server to the terminal, despite the fact that the terminal is authenticated to the server.

There is another problem with the operation of an 802.16 network which has to do with the mesh-network operation. One of the students pointed out the seemingly unfairness of using their power and component lifetime to handle another customer's data. The issue goes beyond this – the intermediate may have the power to intercept and/or interrupt the path through their terminal. After all, the terminal is on their property and open to any prying into the device operation they choose to perform. As a minimum, they can cut power to the device any time they choose, breaking the path for remote users. Worse, unless the device has strong physical protection, it is very likely that the intermediate user can read and, perhaps, modify traffic flowing through their terminal.

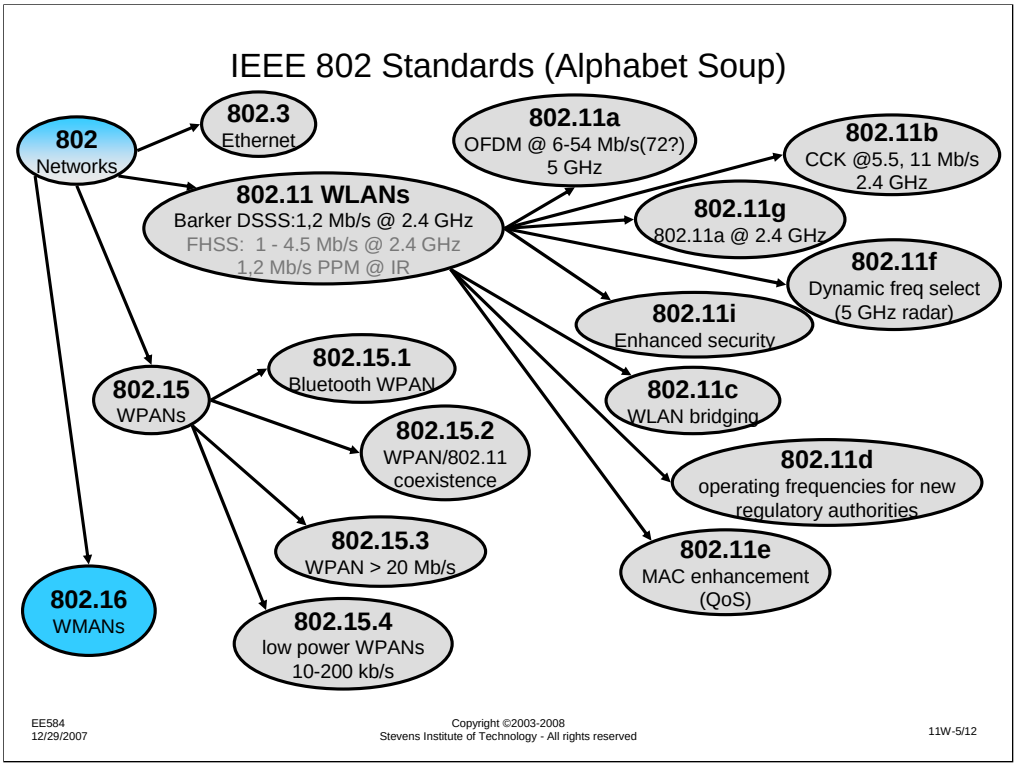


Let me expand on this "intermediary" attack with a personal example.

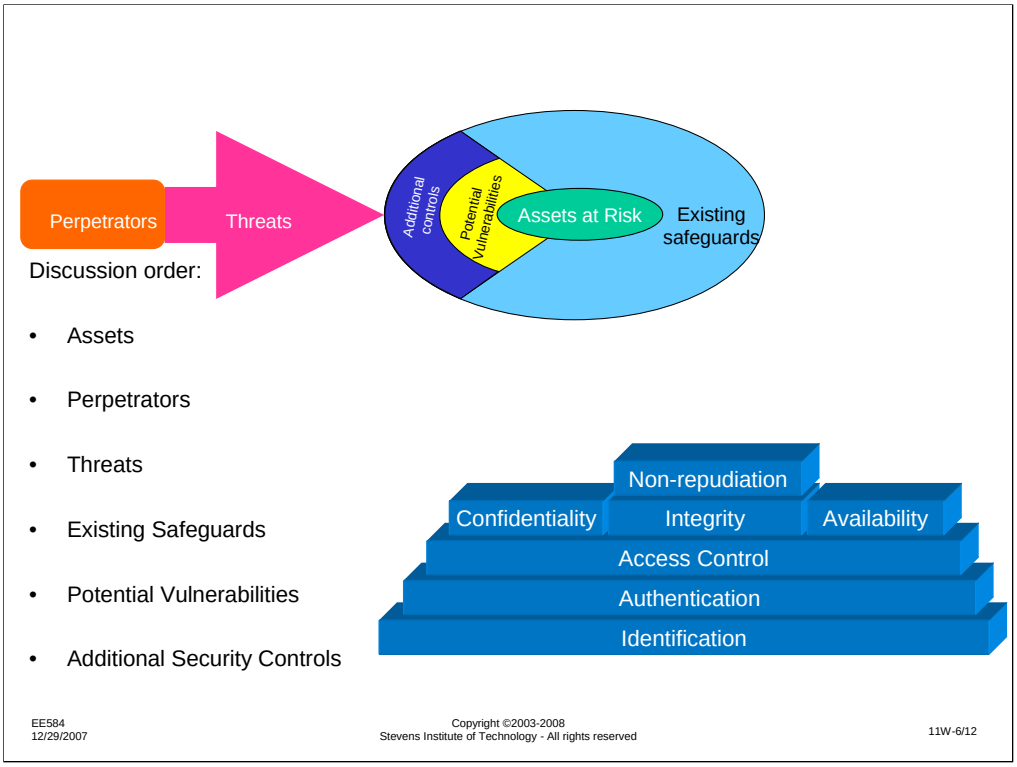
When I worked at Bell Labs, I happened to have one of the first PCs running UNIX. I tend to name my computer systems with particular themes. For a long time, I have used the theme of crypto system names (a few of my current machines are named vernam, enigma, caesar, and saville). When I was at Bell Labs, my PC running UNIX was attbash, a pun on the Hebrew atbash cipher and the company name, AT&T. My machine also happened to have a login on the Bell Labs email network as well as the attmail network that AT&T corporate users favored. Since the concept of DNS and automatic route detection didn't exist at the time, one had to prespecify the route email would take to the destination, using the so-called bang-addressing. Somehow, other users at AT&T and Bell Labs discovered that my machine was one of the few potential gateways between Bell Labs email and attmail, so I started noticing CPU activity when there should be none. They were sending email with a route like: mymachine!attbash!attmail!yourname. It was a simple matter to change attbash's /bin/mail command from an executable to a shell command. The shell command I wrote was a simple two line shell which executed the following function: "if the recipient or originator of the email is bmcnair, process it normally, running the real /bin/mail command. Otherwise, use the tee command to make a copy of the message and put it in a local directory, and then forward the mail normally."

After spending a few days capturing the email addresses of the people who were using my machine as a gateway, I sent them all email asking why they thought it was a good idea to forward their proprietary mail through an untrusted system.

The lesson: the person who has physical control of an intermediate node is very likely able to do whatever they want to at the node. If you depend on the security of the node for your message security, you had better either trust the node administrator or have some other means to keep your message out of their hands.



We are seeing a proliferation of networking standards, all addressing a slightly different set of applications, from wired networks to wireless networks, personal area networks to metropolitan area networks. Where we can reuse good ideas from one application to another, we can improve overall system security. Unfortunately, sometimes, we don't learn from previous mistakes and are bound to repeat them.



Once again, as for the previous assessments, if you have been assigned to a Red Team, you should be concentrating on the following items:

Assets: What is it about the system that you would be interested in stealing, destroying, disrupting, etc.?

Perpetrators: Who are you? Why do you do the evil things you do? Who is backing you, or what resources are available to you?

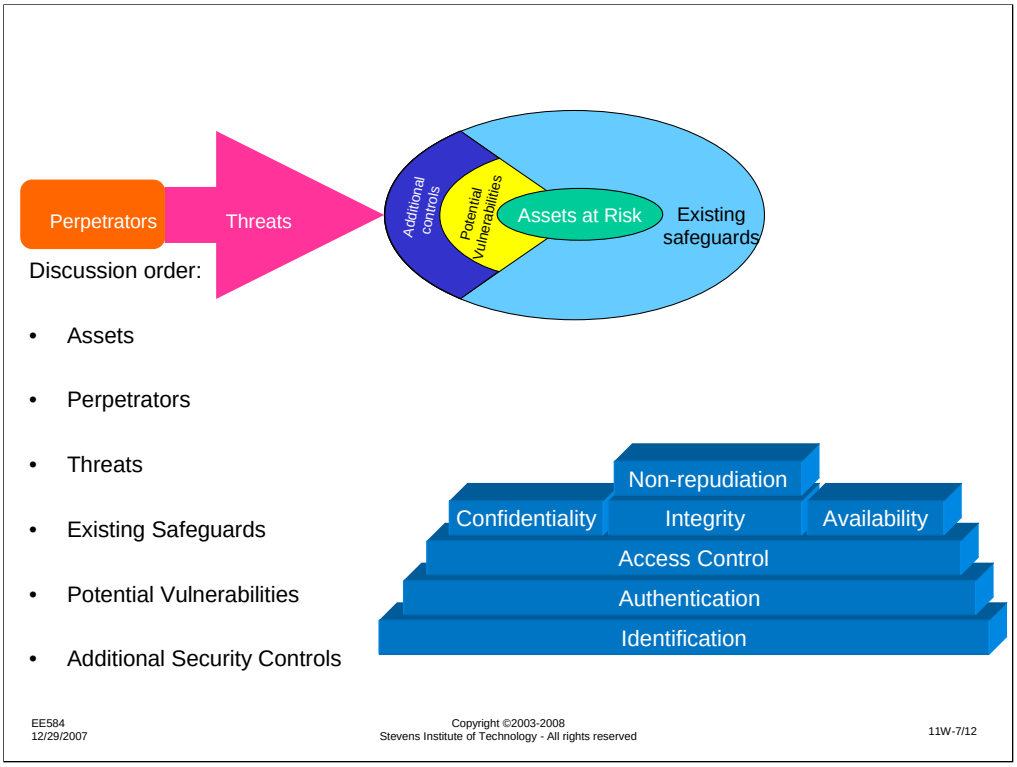
Threats: What mischief can you get into? How would you do it?

Safeguards: What are the things that are, or might be, in your way?

Vulnerabilities: What unlocked doors, open windows, unprotected ways in might exist?

Additional Controls: What might the defender do to make you life harder?

Again, keep in mind the security architecture at the bottom right. For each security service, there might be something that you can do, steal, break, etc.



Likewise, if you have been assigned to a Blue Team, you should be concentrating on the following items:

Assets: What is valuable to you in your system? What might the attacker be after?

Perpetrators: Who should you be on the lookout for? How do they operate? What are they capable of?

Threats: How might someone try to attack your system?

Safeguards: What protection is already in place?

Vulnerabilities: What might have been missed? Where are they most likely to try to enter?

Additional Controls: How could you make the system stronger? Would it be worth it?

Again, keep in mind the security architecture at the bottom right. For each security service, there might be something in your system that needs protecting.

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

Listed above are a set of assets identified by other sections of this class. Not attempt has been made to filter or sort the concepts, so there may be redundancy between the different groups. Items in italics are those that were considered to be especially important.

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???

Note: Some of these existing controls aren't actually existing controls, but are more additional controls.

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