Wireless Systems Security

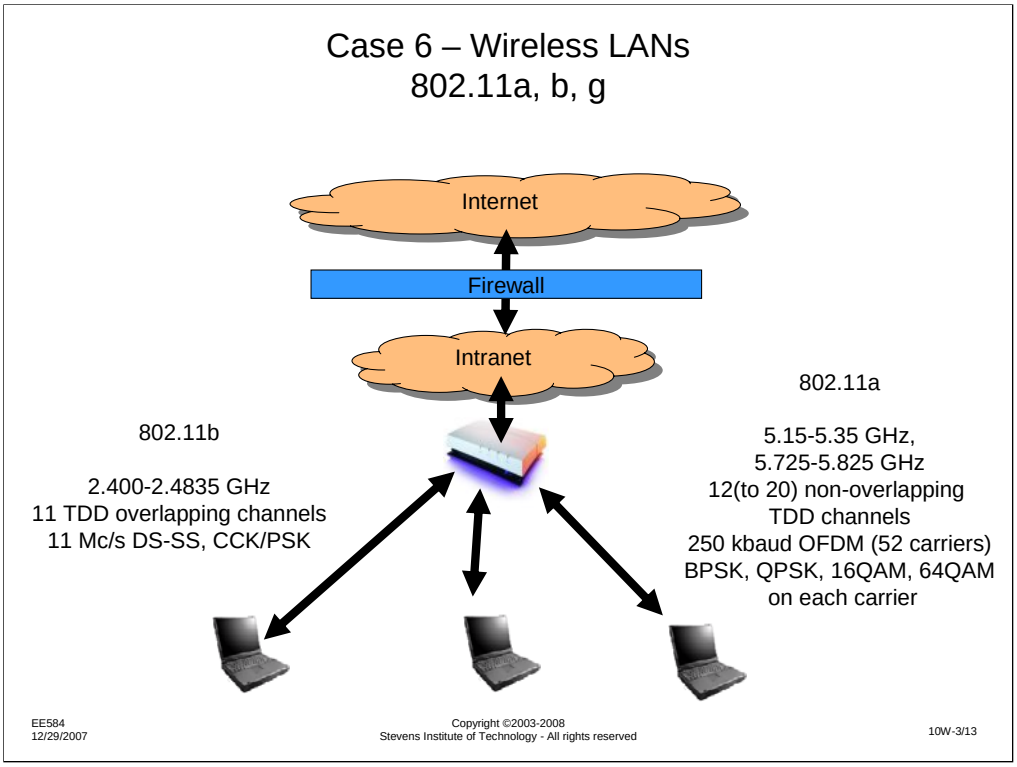
EE/NiS/TM-584-A/WS
Bruce McNair
bmcnair@stevens.edu

.

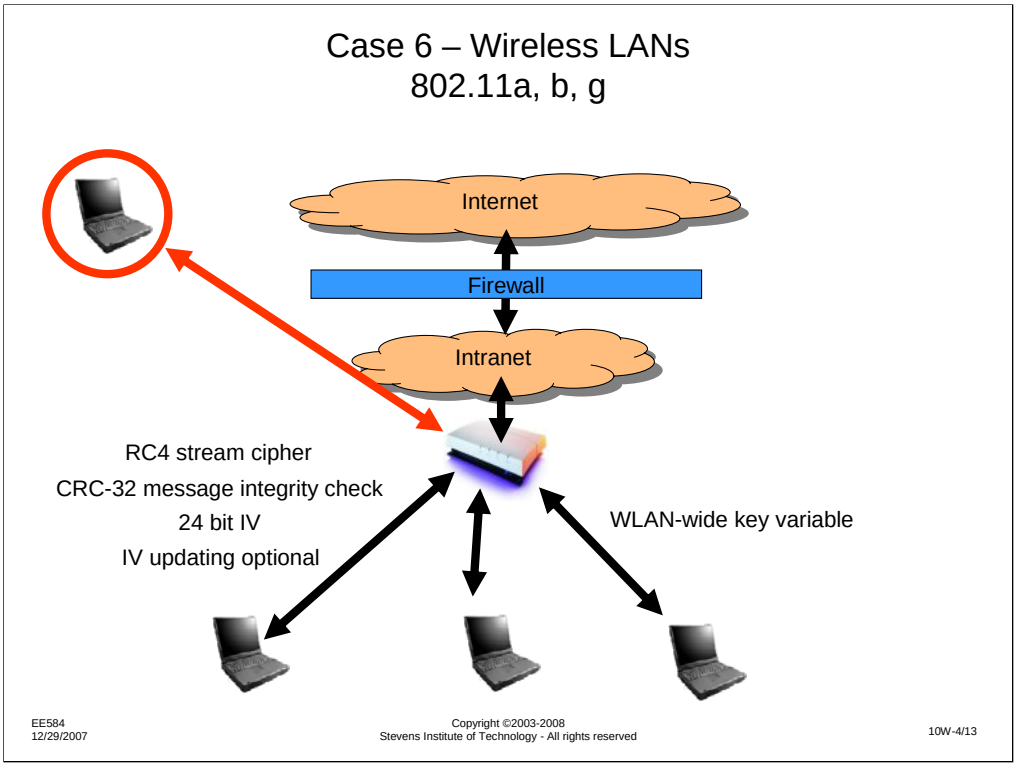
Week 10

Case Study 6

At this point, you have completed the discussions for the sixth case study. I wanted to make some observations about the system we have assessed and summarize the assessment. For the later, I am using assessment results from previous groups who have taken this class. I will add your assessment results to future versions of this class.



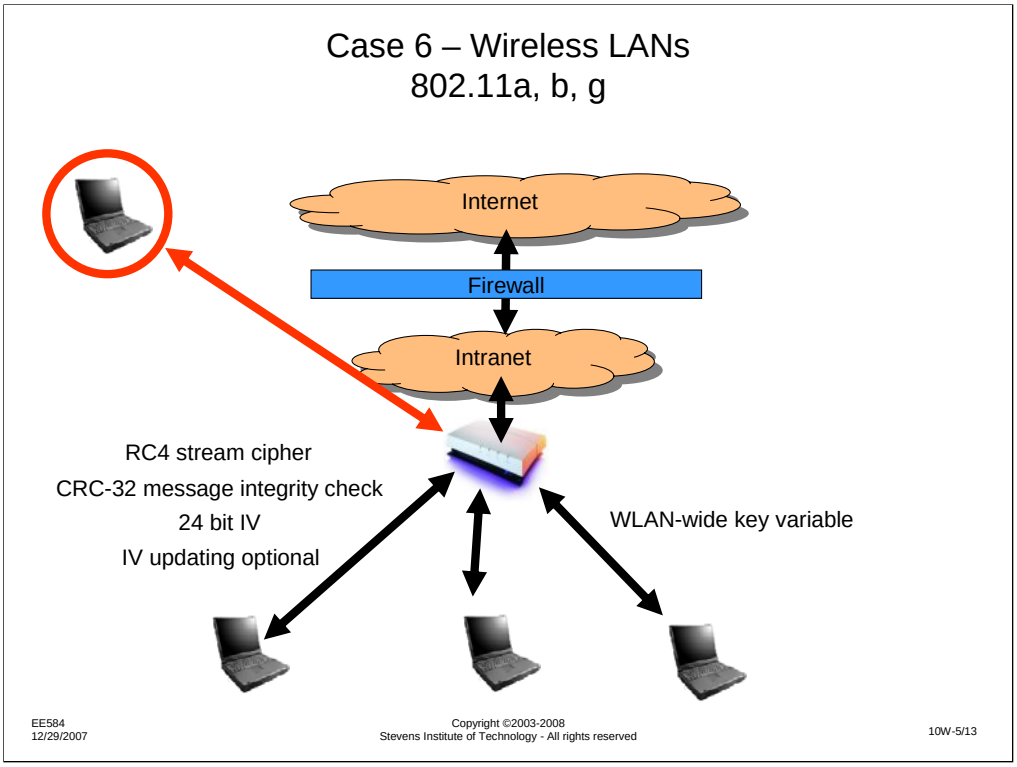
For all of the 802.11 WLANs, we can examine the architecture of a system with a WLAN inside a corporate firewall, which is intended to allow secure communications within a closed user group, blocking outside access.



The external attacker, that is someone outside the corporate firewall, should not be able to access resources inside the firewall. If they were coming over the wired path from the Internet, via the firewall, this might work, if the firewall is configured correctly. Unfortunately, the 802.11 WLAN provides a backdoor into the corporate network that completely bypasses the firewall.

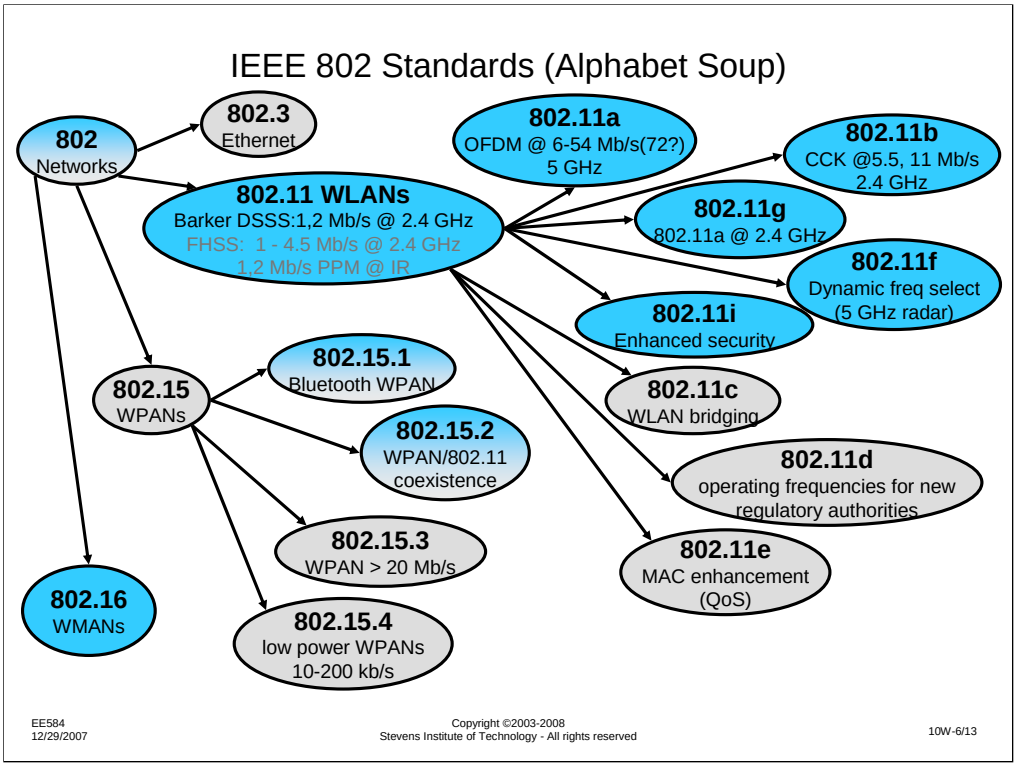
Wired Equivalent Privacy (WEP) is **supposed** to protect the wireless LAN, making it as secure as a wired LAN. There are, unfortunately, a few design decisions that were made in the 802.11 security features that make WEP quite weak. Let's consider a few of them to see how they compromise 802.11 security and how they could have been implemented in a more secure manner.

First, 802.11 uses the RC-4 stream cipher. While this encryption technique is not particularly weak, its application in 802.11 is inappropriate. Had a block cipher been used instead of a stream cipher, the biggest hole in 802.11 security could have been easily avoided. Remember back to our discussion of encryption in the early part of this course. Even the strongest encryption system, the one-time-pad, the only provably secure encryption method is easily attacked if key sequence is reused. It turns out that the RC-4 stream cipher has this vulnerability, just as every encryption algorithm has. How do we know that an RC-4 key stream is going to be reused? Two reasons: First, the same key variable is generally used throughout the WLAN. This increases the amount of candidate traffic for key variable reuse. Second, a stream cipher requires state synchronization for the receiver to be able to decrypt the transmission. To do this, a crypto initialization vector must be conveyed from the transmitter to the receiver. In the case of 802.11 WEP, that IV is 24 bits.



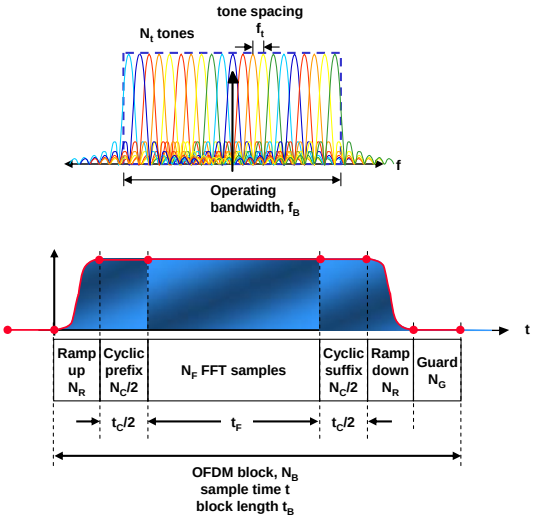
Now, 24 bits corresponds to 16 million possible IVs, which seems like a large number. However, consider how long it takes before an IV collision occurs: If we assume a WLAN that is carrying a moderate amount of traffic, we can expect 1 Mb/s utilization (this is about 15% of the system capacity, since an 11 Mb/s WLAN actually has a 7 Mb/s throughput). If we make a very conservative assumption that blocks are about 1500 bytes long (actually, they are likely to be much shorter), this means that about 83 blocks/second will be sent on a single WLAN segment. This means that it will take about 96000 seconds, on average, to repeat IVs. This is about 26 hours, or 1 day before we expect IVs to be reused! Remember, this is for one WLAN segment with very conservative assumptions about utilization. It is very likely that the IV will be reused much sooner, giving the attacker a better opportunity to compromise the link.

There is another significant problem here, as well. How does the attacker know that an IV collision has occurred? If there were no redundancy in the plaintext messages, it would be difficult for them to be sure. However, there are two forms of redundancy that give the attacker an unnecessary advantage. First, there is the inherent redundancy in the 802.11 protocol. If we know a series of messages are conveyed from the mobile unit to the access point, we can look for fields in the messages that are constant, e.g., information about the session. However, there is another redundancy that is completely unnecessary – the 32 bit CRC. This field is used to provide error detection, in case a packet is damaged in transmission. The CRC provides an independent calculation that allows the receiver to detect if the packet is a valid one or not. However, because the CRC is attached to the plaintext message, it provides a mechanism for the attacker to verify that they have correctly decrypted a packet. It is very unlikely that a packet will pass the CRC test if it was decrypted incorrectly. However, there is no reason to give the attacker this advantage. The CRC will work just as well if it is applied to the encrypted packet, which will **not** add any extra redundancy to the message and will deny the attacker that advantage. Besides all the other insecurities of 802.11's WEP, IV updating is optional. Standards-consistent systems can be deployed that use a constant IV – every packet sent uses the same key sequence, so guaranteed IV collision occurs with only two packets!



So, for this assessment, we concentrated on 802.11 WLANs, but there are other standards that touch on the 802.11 networks. For one, 802.15 WPANs (Wireless Personal Area Networks) like Bluetooth™ are likely to be called on to interoperate with 802.11 networks. This opens a new set of security issues – availability of each system in the presence of the other. Experiments that I did at AT&T Labs with some summer students suggests that in a head-to-head competition for RF resources, 802.11 will not fare well, since it operates on a set of channels and does not move from channel to channel. Bluetooth™ hops from channel to channel and has the potential to wipe out a 802.11 packet during one hop, while Bluetooth™ can squeeze in transmissions while having hopped to a channel where interference from 802.11 is minimal. There is obvious opportunity to use a Bluetooth™ device to jam 802.11 links.

OFDM Basics



Total bandwidth $f_B = N_t f_t$

Tone spacing vs active block time $f_t = \frac{1}{t_F}$

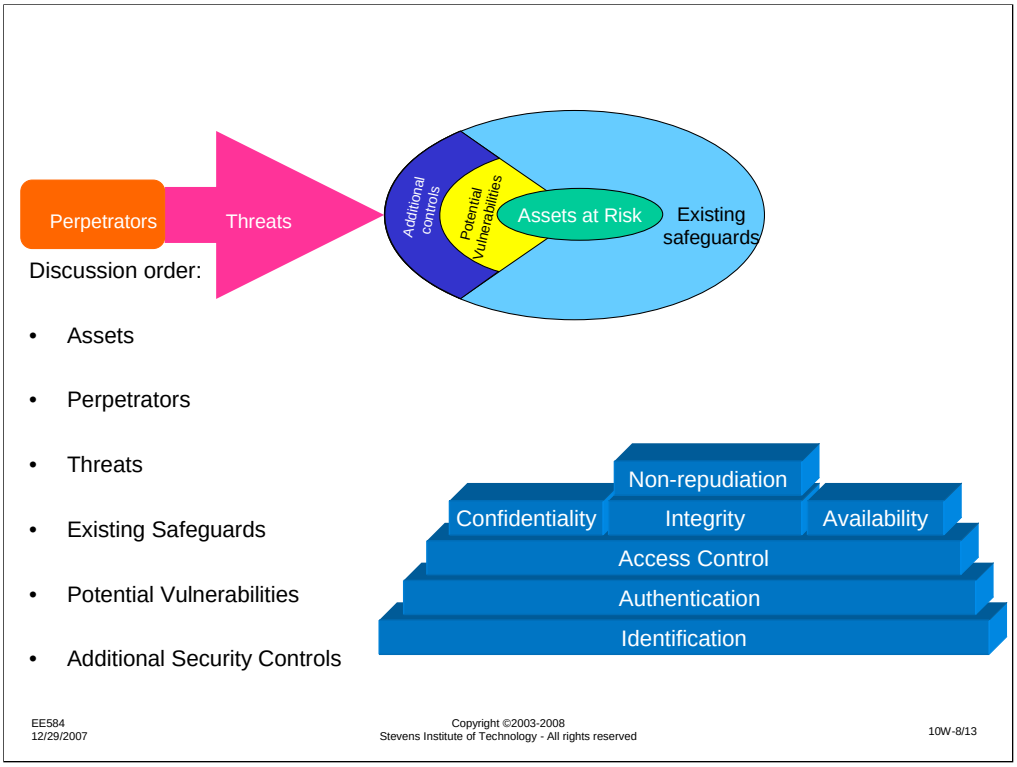
$$N_B = 2N_R + N_C + N_G + N_F$$

Block efficiency $\eta = \frac{N_F}{N_B} = \frac{N_F}{N_F + N_C + 2N_R + N_G}$

Tolerance to delay spread $\approx t_C \propto N_C$

Raw capacity for M-ary tone modulation $N_t M$

802.11a and 802.11g are the newest in the series of 802.11 standards. They both provide data rates up to 54 Mb/s, compared to the 11 Mb/s of 802.11b. Both 802.11a and 11g are based on OFDM, the same modulation technique that is used in cable modems, DSL, and other new communications systems. One major security advantage of OFDM over other techniques is the coding of information across a range of frequencies. With a well-designed code and channel assignment, individual carrier's information can be destroyed, while the coding redundancy of another carrier allows the errors to be corrected. One recent application of OFDM is to so-called Broadband Powerline communications, where medium voltage (~10-50 kV) power feeder lines are used to distribute power into a neighborhood, and carry wideband communications along with power. Although the BPL power systems are inherently noisy, were not really designed for broadband data transmission, and are subject to narrowband interference from amateur radio, shortwave broadcast, and other services, the ability to adaptively use and avoid certain channels makes this data transmission technique a possible alternative to fiber, cable modems, DSL, etc.



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?

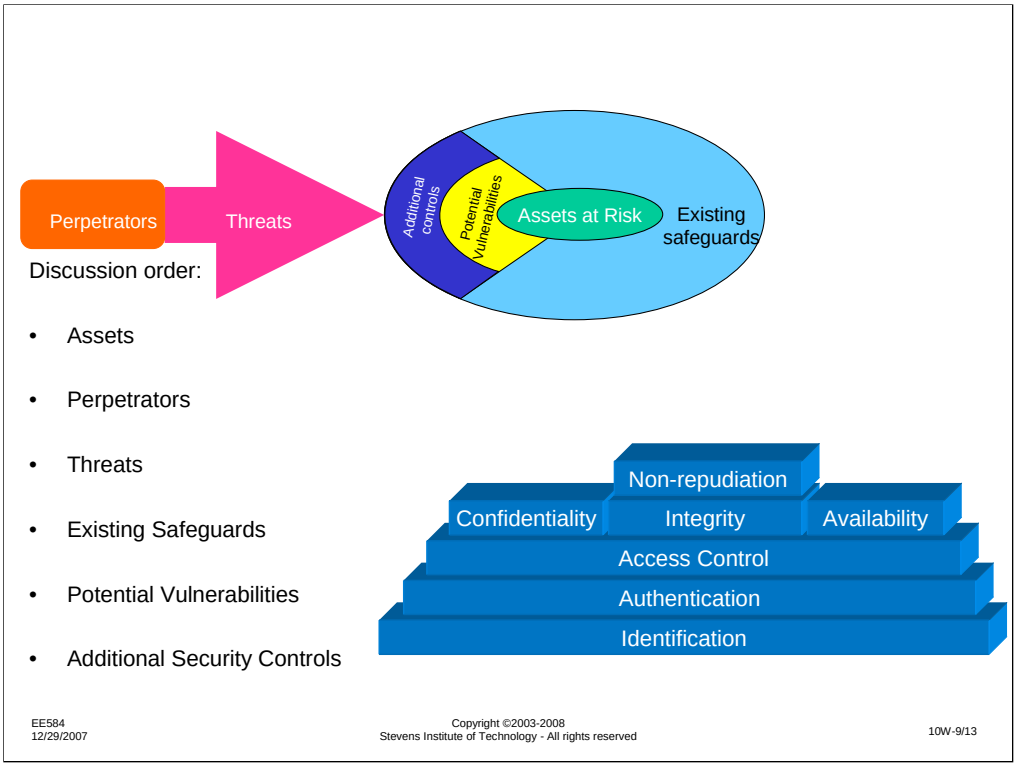
Threats: What mischief can you get into? How would you do it?

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

- Access Point
  - Physical
  - Parameters
  - MAC address
- Initialization Vector
- Encryption key
- Channel bandwidth
- Data content
- User authentication over channel
- Access to intranet
- Capacity on wireless network
- Capacity on public internet (accessed via wireless network)
- Reputation
  - IP address of traffic originated through wireless network to intranet

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

War drivers
Free riders
    Your neighbors
Mesh network users
Hackers
Competitive WLAN provider
Curious eavesdroppers
Competitors to user corporation
    Corporate spies

One perpetrator bears explanation here. "War drivers" are hackers who spend their spare time driving around a neighborhood listening for open access points that allow them to identify and potentially connect to the AP. Software is freely available on the Internet which will force an 802.11 WLAN card to continually scan for activity. Finding activity, the software will record all pertinent information about the AP, including it's latitude and longitude, if a GPS receiver is connected to the computer being used for scanning.

The term "war driving" comes from the term "war dialing," which was a popular hacking pasttime in the 1980s and 1990s. A hacker with a computer and dial-up modem would program the computer to attempt to dial one phone number after another within a central office code. For instance, the Bell Labs Holmdel location has exclusive use of the telephone exchange 732-949-xxxx. A war dialer, looking for a modem connection at Bell Labs, might program their PC to dial 732-949-0000, followed by –0001, -0002, etc. Any numbers with modems connected would provide modem answer tone, and the program would note this fact.

The term "war dialing," in turn, is derived from the movie "War Games," where a teenage hacker used the method of war dialing to find a backdoor into a Department of Defense computer system that controlled the North American missile defense system.

Threats

Scan for open AP
Associate with open AP
Intercept/monitor data/interaction
Jam communications
Insert spurious traffic
    Hijack a session
Observe wireless MAC addresses
    Impersonate terminal
Guess default SSID
Guess common SSID
Monitor to learn SSID
attack WEP and break it
Denial of service
Theft of service
Engage in peer-peer communications
    Break into others' PCs

Vulnerabilities

- Misconfiguration of AP
  - AP bridging: broadcast Ethernet traffic
    - Overload wireless network
    - Compromise Ethernet traffic
- Lack of standards on key entry
- IV implementation
- Rogue APs are not authenticated as official ones are
  - Rogue DHCP servers
- WEP is broken
- Faulty AP design (e.g., Cisco association table overflow)
- Faulty implementation of SNMP
- No provision in 802.11a, b, or g for key variable change
  - Fixed, system wide key variable
- Powerful networking (plus) design flaws (plus) inexperienced network “administrators”
- Homogenous encryption standards/keys
  - Any valid user has wide access