

The 802.11b Story

or, “not open” systems and semi-secret algorithms and protocols designed by programmers and hardware engineers are likely flawed.

Goal: convince you to be extremely careful and skeptical about “home-brewed” security and encryption solutions. This is an often repeated mistake and therefore qualifies for discussion in this class.

Remind yourself through this presentation that 802.11 was designed by professional software and hardware engineers and reviewed by many such.

Topics in this Presentation

- Wireless networks
 - Vulnerabilities in all wireless networks
 - Range vs power
- 802.11b networks
 - how they work
 - vulnerabilities
 - software solutions

Wireless Vulnerabilities

- All wireless networks are vulnerable to:
 - Jamming (Denial-of-Service, DoS)
 - Eavesdropping
- Unprotected networks are also vulnerable to packet injection

Review Question

- Which property of “CIA” (confidentiality, integrity, availability) can’t you guarantee in any wireless network?
- How about a warship that is steered and controlled through an 802.11b wireless networks. What could happen?

Answer

- You can't guarantee availability, because wireless networks can be jammed.
- A warship controlled through a wireless network could stop responding and continue on a bad course (collision or otherwise)

Wireless Coverage is Risk

- The potential number of locations from which attackers can operate is proportional to the area covered.
 - Areas you physically control may not be as risky
 - The size of the area is not completely under your control, because attackers can use arbitrarily large antennas.
- However, you can control the amount of power used. How does that affect the risk?

Wireless Power

- Area of a sphere = $4\pi r^2$
- Total power is constant
- Power/area decreases $\approx 1/r^2$
- Big antennas capture more power (more area)
- Antenna gain is measured in dB (decibels) as the ratio of power captured compared to a reference antenna.
- Gain usually comes at the cost of increased directionality

Antenna Gain (dB)

$$dB = 10 \log_{10} \left(\frac{P_1}{P_2} \right) ,$$

- A gain of 3 dB means captured power is doubled.
- A gain of 10 dB means captured power is increased 10 times.
- A gain of 20 dB means captured power is increased 100 times.

Variable Power

- Some access points and cards can use varying amounts of power
 - uncommon feature (Cisco, Apple Airport Ex)

- How is the range changed by power?

- $\frac{P_1}{4\pi r_1^2} = \frac{P_2}{4\pi r_2^2}$ So $\frac{P_1}{P_2} = \frac{r_1^2}{r_2^2}$

- How much power do you need to double the range?

Power Calculations

- Double range needs 4x power
- Equivalent statements:
 - An increase in power of 6 dB doubles the range
- Triple range needs 9x power
- Lower the power to decrease the risk area

- Cisco Aironet Antennas Reference Guide
(http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/agder_rg.htm)

Review Question

Your wireless network usually has a range of 100 feet. However you are having a (confidential) meeting in a 10'x10' room but want to use an access point in the room. By how much can you decrease the power to lower the risks?

Answer

- A 10'x10' room approximately fits inside a 5' radius sphere.
- $100/5 = 20x$ range reduction
- Power = $1/(20 \times 20) = 1/400$
- So if the power was 400 mW, 1 mW should now be sufficient.

Review Question

If you want to spy on the meeting mentioned previously, from 100 feet away, what is the gain (in dB) of the antenna you need?

Answer

- Gain (dB) = $10 \log(400) = 10 \log(4) + 10 \log(100) = 6 + 20 = 26 \text{ dB}$

802.11 Wireless Networks

- Ad-hoc networks
 - Similar concept: Peer-to-Peer
- Access-point-based networks (aka infrastructure)
 - All traffic goes through the access point.

802.11 Vocabulary

- BSS: Basic Service Set. An AP connected to a wired network and a set of wireless stations.
- ESS: Extended Service Set. A set of two or more BSSs.

How it works

- Access points may broadcast “beacon frames” to the world to advertise a network
- Hosts need to “associate” with a single access point, which establishes a route.
- Association may require authentication with a challenge-response mechanism.
- Send packets (encrypted or not) to AP

Mechanism #1:SSID

- Short for Service Set Identifier, a 32-character unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to the BSS. The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. A device will not be permitted to join the BSS unless it can provide the unique SSID. Because an SSID can be sniffed in plain text from a packet it does not supply any security to the network.
- An SSID is also referred to as a Network Name because essentially it is a name that identifies a wireless network.
- (<http://www.webopedia.com/TERM/S/SSID.html>)
- Similar to: RIP (Routing Information Protocol) password, telnet password

Beacon Frames

- Broadcast SSIDs
- Optional
 - With BFs: “Open network”
 - Without: “Closed network”
- SSIDs can be sniffed from
any transmission.

MAC addresses

- Media Access Control
 - Globally unique identifier tied to hardware
 - Blocs allocated to companies
 - 6 bytes, e.g., 00:02:B3:11:11:11
- Present in every packet
 - in cleartext in 802.11b wireless packets, whether “encrypted” or not
 - Easy to build a collection of valid MAC addresses

802.11 MAC Address Access Control

- 802.11 access control mechanism: build and maintain a list of allowed MAC addresses
 - Doesn't scale well: the more users you have, the more maintenance you have to do
 - Hardware can be programmed to use any valid MAC address. Example:
 - `ancontrol an0 -m 00:02:B3:11:11:11`
 - So the access control is easy to defeat.

WEP

- Wired Equivalent Privacy
- Attempt to secure wireless networks with encryption and other access control mechanisms
- Flawed
 - Some flaws are ridiculous

XOR Encryption

- $0 \text{ XOR } 0 = 0$
- $1 \text{ XOR } 0 = 1$
- $1 \text{ XOR } 1 = 0$
- $(z \text{ XOR } y) \text{ XOR } z = y$
- $(z \text{ XOR } y) \text{ XOR } y = z$
- Works independently of which of z or y is the “key” or the “data”.

Authenticated Association

- A tells B “I want to associate”
- B tells A “Encrypt this as proof that you are a friend”
- A chooses a pad for the XOR operation and sends the encrypted text back to B
- Malory got the plaintext p and the encrypted version e
- $\text{pad} = p \text{ XOR } e$
- Malory can now “authenticate” by choosing the same pad... :-(
silly, dumb, etc...

Stream Cipher

- pad is generated by a random number generator with a seed value (“initial value”, “IV”)
- Same (IV, key) => same pad
 - send the IV in cleartext
- Pads should not be reused!

WEP

- RC4 encryption (stream cipher)
- Initialization Vector (IV), 24-bit (cleartext)
- Integrity Check (IC), CRC-32 checksum (“encrypted”)
- Deceitful marketing: with a 40-bit key, add the 24-bit IV, and call it 64-bit encryption! Wow!
- What’s the difference? $2^{24} = 16\,777\,216$ times weaker than advertised!

WEP is awful

- When is 64-bit encryption really 40-bit? WEP
- When is 128-bit encryption really 104-bit? WEP
- When is 40-bit encryption more like 24? WEP
- When is 104-bit encryption more like 24? WEP
- When are 24-bits really 18? (A: in Cisco's first implementation of WEP the IVs had only 18 bits)

“Integrity Check”

- Due to the use of XOR encryption, the checksum and message can be manipulated (out of the scope of this class)
- The “integrity check” does not really add to the data integrity vs a malicious attacker
- Mostly helps with bad reception and hardware problems.

Security Principle: “Defense in Depth”

- 802.11b falls like a house of cards
- A depth of bad security leaves you in deep s***
- all possible pads can be collected (a few dozen GB)
- the key can be found cryptographically (out of the scope of this class) with less difficulty than pad collection

LEAP by Cisco

- Since the WEP encryption is very weak, change the key often, hoping to confuse attackers...
- What an ugly hack!
- The system is still flawed
- Imagine having to renegotiate 40-bit SSL every 10 minutes and calling it as secure as 128-bit SSL...

Review Question

If you really want to secure your meeting, which technology is the best?

- a) LEAP
- b) VPN
- c) Program your own encryption
- d) 128-bit WEP
- e) Closed Network

Review Question

- If you hear someone say, “I’ll just XOR this with that and it will be safe enough”, what should you do?
- If you hear “we can’t tell you, the algorithm is secret” or “we’ll tell you how we do it for \$1400”, what should you do?

Q&A