Wireless security attacks and defenses: The state of the art in Wi-Fi network design

Steve Pinkham
Maven Security Consulting

September 4, 2007

Common uses for WiFi

Why do we implement WiFi in the first place?

- Roaming
- Wired replacement
- Conference rooms
- Public hotspots

In short, for convenience.

What does "security" look like?

Security is driven by business case

- Confidentiality?
- Integrity?
- Availability?

Defense against Attackers

- Attackers may want the data flowing over your wireless network
- Attackers may want access to other parts of your network
- Attackers may want to deny service to your network, or a specific client
- Attackers may just want anonymous network access

Defense against your users

- Your users want access
  - Users ~~can~~ *will* put up unauthorized access points if you don't provide wireless
- Your users want convenience
  - Users ~~can~~ *will* put up unauthorized access points if your security mechanisms are too difficult to use
- Your users may already be harboring malware
- Your users don't care about security

Defense against the environment - Interference

2.4 Ghz is very noisy and crowded

- Interference
  - Cordless phones
  - Microwaves
  - Baby monitors
  - Other WiFi users
  - Weather
  - Amateur Radio
    - In US, "Hams" have 1,500W limit on broadcast, most WiFi 0.03 to 0.2W

Defense against the environment - Attenuation

- Attenuation
  - People
  - Walls
  - Trees
  - Weather
  - Basically anything

WEP Security?

- WEP cannot be considered a security measure
- WEP can now be broken in 1 minute
- WEP is equivalent to a "Keep Out" sign
  - May have legal benefits, and keep out casual surfers, but NOT attackers

Associated "security"

- MAC filtering
  - easily broken by changing MAC address
- SSID hiding
  - SSID still broadcast in Management frames
  - Forces clients to broadcast who they are willing to associate with
- Disabling DHCP
  - Trivial to guess a valid IP, or assume someone else's

WPA- Improved security

WPA protocol itself much improved over WEP, attacks target the keys

- WPA-PSK open to offline password attacks
  - Rainbow tables available for quick attacks on common SSIDs
- EAP-LEAP is also open to offline password attacks
- Depending on configuration, PEAP-MSCHAPv2 can make username harvesting possible

Denial of Service Attacks

In addition to normal interference, new protocol specific flaws

- WPA introduces "tilt" protection
  - Will shut off access for 60 seconds if crypto attacks detected
  - Definition of attack is 2 forged packets in a second
  - Only TKIP is affected
  - Necessary because MIC (Message Integrity Code) field too small to withstand attack
  - Designers say won't be changed, since so many other DOS possibilities exist that are as least as easy
- Combined with all the RF, logical, and other DOS attacks, WiFi cannot provide high availability

Rogue APs - The enemy within

First kind of rogue AP - Internal unauthorized wireless

- Traditional AP
- Ad-hoc wireless on laptops
  - Ever wonder what the "Free Public Wifi" spots are at airports?

Rogue APs - The enemy outside

Attackers can plant APs where your users will use them

- If you use crackable security, can clone your AP and steal all traffic
  - With WDS, can be seamless
- If users have insecure settings, will automatically connect to "tmobile" or other common SSID

Driver Attacks

- Many security bugs are being found in drivers
- Allows direct code injection onto a computer with insecure drivers
- Attack now available in point and click tool called metasploit

Configuration Attacks

- Wireless settings on user's computer often insecure
  - XP has EAP certificate validation off by default?!?
  - Automatically connects to known networks
  - By default, broadcasts a list of all access points it is willing to connect to!

WPA

- WPA/WPA2 are your friends
- AES/CCMP much stronger then TKIP, but TKIP is fine for the moment
- All new equipment should support WPA2/AES
- PSK plenty strong with long random passwords
  - Think 20 random char minimum, no dictionary words, etc...
  - 63 char random string easily generated on web
  - Can be put on keyfob for transfer between computers

EAP

- EAP-TLS offers strongest security
  - Comes at the cost of client side certificates = PKI infrastructure
- EAP-TTLS offers strong security with server certificates only
- EAP-PEAP offers similar security, but many implementation flaws make it less desirable

Level 3 auth

- In high security environments, it is advisable to tunnel your traffic over a level 3 encryption layer
- For example, SSL VPN or IPSEC encryption
- Mitigates possible future problems through layering

Wireless IDS/IPS

- WIDS can help detect rogue access points, cloning attacks, deauth floods, etc.
- Can see information your normal IDS cannot
- Some WIPS products can mitigate these attacks to some extent, but don't depend on them for your main security

Network design

- For conference rooms, WPA with key posted on wall
  - Remember to rotate key frequently
  - Connect outside company firewall if possible
  - Use VPN to connect to internal resources
- For open access points recommend:
  - Connecting outside company firewall
  - Firewalling all but HTTP(S) and DNS ports (80, 443, 53)
  - Rate limiting clients to avoid abuse

Configuration

- Products are available to enforce security policy on user's computers
  - Example: Only allow WPA and higher, no association probes, etc
  - Problem: If too restrictive, users will find some way to override
- Tools exist to audit PCs for insecure wireless drivers
  - Free tool: Aruba WiFiDEnum

Review

- Use WPA/WPA2
  - AES w/ TLS or TTLS recommended as long term solution
  - TKIP secure today, but the margin is thinning
  - PSK w/ STRONG passwords is as secure and more useful for very small/temporary deployment
- Don't trust WPA too much
  - Still tunnel sensitive data over encrypted protocols
- Educate end users about rogue access points
- Secure users wireless settings
- If possible, invest in WIDS/WIPS

Maven SECURITY CONSULTING

Thank you

Thank you for joining us today.

- Contact me at steve.pinkham@mavensecurity.com
- Updated resources will available at: http://www.mavensecurity.com/presentations
- Questions?