Wireless LANs, Best Practices Session Two

David W. Borden, CISSP
Senior Systems Engineer
Lockheed Martin Corporation
david.borden@lackland.af.mil
dborden@gvtc.com

II. Best Practices

- After several years of dealing with Wireless LANs, we have learned some things
- Wireless devices can be deployed, but security must be a major consideration
- Turn on 128 bit WEP to protect the network
- Use WPA if your devices will allow it
- Get 802.1i equipment/software when it comes available
- Use End-to-End Encryption to protect data

Best Practice 1

- Turn off beacons, if possible
  - Some manufactures allow this, others do not
  - All your clients know the SSID of the WAP and the correct RF channel to transmit on
  - There may be a problem if you have multiple access points some of which are repeaters
  - Repeaters require beacons to stay coordinated

Best Practice 2

- Cloak SSIDs
  - Some manufacturers allow this
  - If you must have a beacon (i.e. slave repeaters) then do not broadcast the SSID of the WAP
  - This stops casual snoopers using NetStumbler
  - It will not defeat kismet or kismac and the serious hacker

Best Practice 3

- Turn on WEP and Change Keys Often
- Yes, WEP can be broken by a determined hacker - use it anyway - protect the network
- Most hackers go for the low hanging fruit - the WAPs with no WEP turned on
- In my 50 mile commute, I count 210 WAPs with only 34 using WEP (one is my bank)

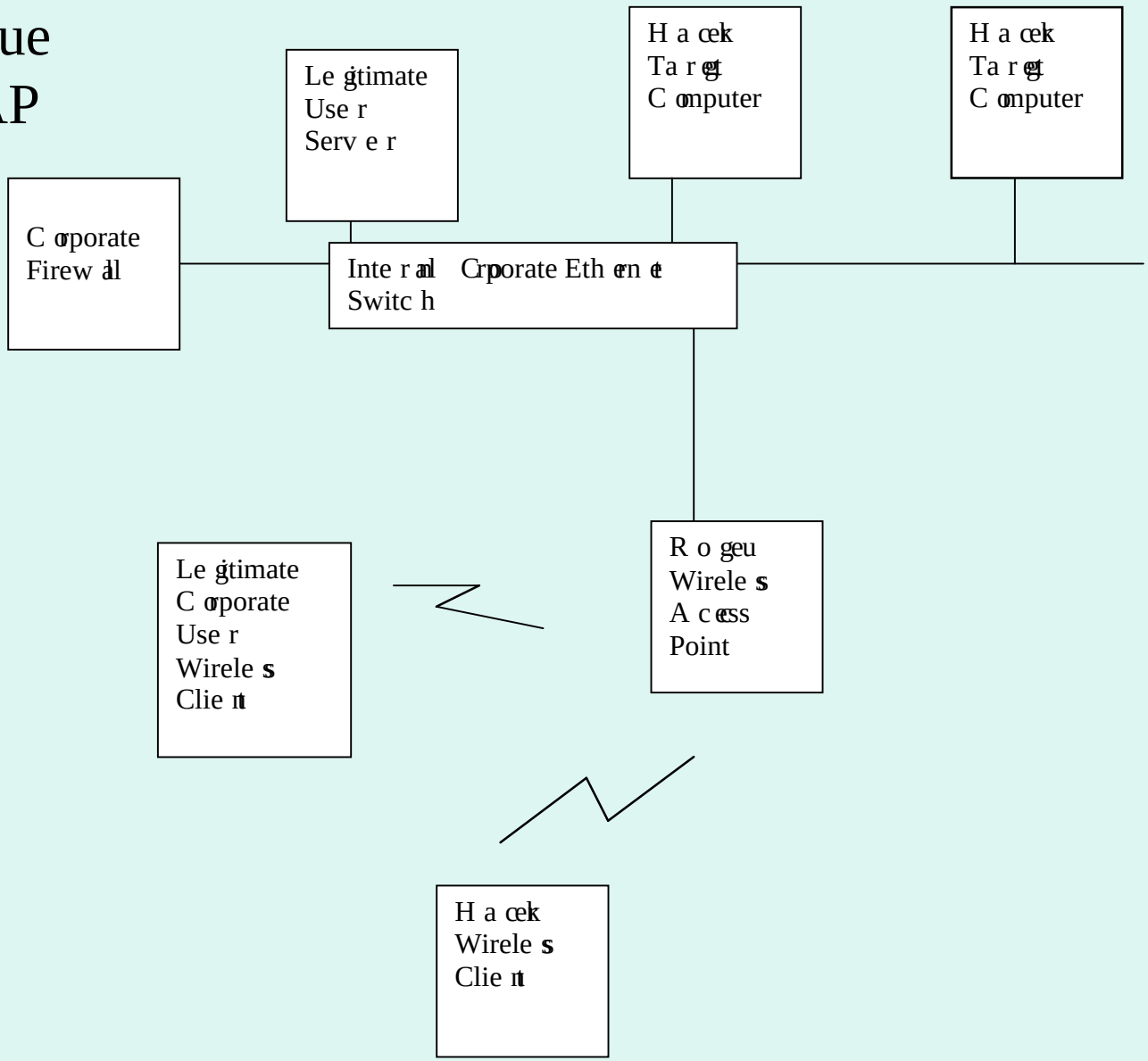
Best Practice 3 (cont)

- WEP is not to protect information (the data you are sending and receiving)
- WEP is to protect your network
- Even if you use a VPN, turn on WEP, you are responsible for your network
- With no WEP in use, your devices become an instant “Hotspot” (minus the coffee)
- Hackers love hotspots - It hides their identity

Best Practice 4

- Employ Virtual LANs (VLANs)
- Do not just throw a WAP on your wired LAN and declare wireless access
- Segregate your wireless activity from your main organizational wired network using a Firewall
- With no VLAN, you are more vulnerable for an attack

Rogue WAP


Legitimate User Server
Hacker Target Computer
Hacker Target Computer
Corporate Firewall
Internal Corporate Ethernet Switch
Legitimate Corporate User Wireless Client
Rogue Wireless Access Point
Hacker Wireless Client

Best Practice 5

- Employ Virtual Private Network (VPN) tunnels to protect your data
- Only allow traffic using protocol 50, protocol 51, and port 500 (IPSEC)
- If you can not authenticate with the VPN, you can not participate in the network
- You could still have a problem of traffic between WAPs directly (some WAPs do not allow this)
- Some VPNs may cause speed problems requiring the turning off of WEP (modern hardware is better)
- All your “road warriors” should be using the VPN

Best Practice 6

- War drive (or walk/sit) your own territory frequently
- Use kismet CD in your normal Windows laptop (available on WWW for download)
- Use prism2 based PCMCIA wireless card
- Can use kismet on Sharp Zaurus for walking discovery (where in the detected building is the rogue WAP?)

Best Practice 7

- Employ only minimum (as needed) transmit power
  - Find a WAP that allows you to set the power output in software
  - Find PCMCIA wireless cards or devices for your clients that allow setting of output power

Best Practice 8

- Employ only minimum “as needed” antenna gain
  - Use antenna placement to shape your coverage area
  - Probably you do not need coverage in the parking lot or the Burger King down the street
  - Remember hackers use maximum antenna gain to find you and join your network so do not make it easy for them

Best Practice 9

- Change all system defaults that came from the manufacturer
  - Hackers know default settings for all WAPs (they are published on the WWW)
  - Do not allow “ANY” authentication/association (require clients to supply the correct SSID)
  - For administration of the WAP, best is serial wire (avoid WEB, telnet, snmp)

Best Practice 10

- Aggressively manage IP address space - never use DHCP
  - If a rogue client manages to authenticate and associate with your WAP, they will need an address so do not just give them one
  - Know all your addresses and use software tools to detect new addresses appearing (WIDS and IDS can help)

Best Practice 11

- Employ an Access Control List (ACL) - Only your clients work with your WAP(s)
  - Yes, MAC addresses can be spoofed, but use an ACL to control your network
  - These can usually be set right in the WAP
  - Keep your neighbors honest
  - If hacker uses your devices, the FBI visits YOU (hacker is never found) and PATROIT act makes you history (no bail - no lawyer - no trial)

Best Practice 12

- Administer your WAP from the wired side, if possible
  - Best way is to connect by separate serial connection direct to the WAP
  - Turn off SNMP, Web Access, and TELNET administration
    - If you must use these, make the password strong (no dictionary words even with substitutions)

Best Practice 13

- If you can afford it (and if you are a for-profit enterprise, you cannot afford not to) employ a Wireless Intrusion Detection System (WIDS)
- New systems do not accept WAP authentication/association outside of approved physical areas

Best Practice 13 (continued)

- A modern WIDS will deploy many sensors (really converted wireless access points)
- The sensors listen to all wireless emitters and report strength and MAC address to a server
- At the server, software performs geolocation of the emitter
- A stored profile of what is authorized is checked for each emitter
- If an emitter is detected that does not fit the profile (in the wrong place - no parking lot) the WAP is informed to not let the emitter authenticate/associate

Best Practice 14

- You should employ a wired IDS also (SNORT is free and great)
- Reminder - Address Resolution Protocol (ARP) is in use everywhere
- Your wired IDS should detect OSI Level 2 attacks like ARP Cache Poison, ensure your IDS has “ARPWATCH” capability
- ARPWATCH is an open source program that monitors ethernet-IP address pairings and reports mischief

Best Practice 14 (continued)

- The mischief centers around your VPN
- Remember we said only allow protocol 50, protocol 51 and port 500 traffic on your network (everything else is in the encrypted tunnel)
- What I did not tell you is your VPN passes ARP traffic - you find life hard without ARP
- Some VPNs allow you to turn ARP off, but you have big routing troubles without it
- So, leave ARP on, but check for mischief with your wired IDS

Best Practice 15

- Draft your Wireless LAN Policy as a part of your Computer Network policy
- Disseminate your policy to all employees
- Employees should not be able to deploy their own computer equipment or software
- If you have no policy, you can be sure you will get a rouge WAP eventually (you may anyway - but remember the lawyers)

Best Practice 16

- Plan First
- Perform System Engineering Study and determine Wireless LAN requirements
- Identify and Mitigate Risks (our Keynote speaker mentioned this)
- Deploy Wireless LAN WAPs and Clients
  - During site survey, determine best placement for minimum RF footprint
- Monitor wireless and wired network for intrusion

Best Practice 17

- If throughput or device sophistication allows, use Wi-Fi Protected Access (WPA)
- This uses a WEP session key with a new key every packet (not based on the IV)
- Some handheld devices with built in wireless can not do this
  - Bar Code Scanners, an example

Example One - Good Security

- Maintenance handheld computers using wireless network cards (maintenance personnel get manual pages online and log maintenance done online)
  - Security: Use VLAN, WPA, and VPN
- In the military, Operational Security (OPSEC) concerns “sensitive but unclassified” data
- In the commercial world, OPSEC would mean “sensitive but not proprietary” data
- Perform an OPSEC study (risk assessment) to determine if your data needs the VPN - maybe not

Example Two - Good Security

- Handheld bar code readers using wireless network cards (logistic personnel perform inventory online)
  - Security: Use VLAN and WEP
  - As mentioned, WPA probably not available on these devices (yet)

Example 3 - Good Wireless Security

- Cash registers report all transactions to server
  - TURN WEP ON (remember credit/debit card transactions)
  - Security: Use VLAN and WEP (WAP probably not available)

More Examples of Wireless Systems with Security

- Road warrior salesman gets latest catalog information while at Starbucks hot spot
  - Use VPN (so competitor sitting at Starbucks does not share the same information)
- Road warrior salesman gets latest catalog information wireless in guest cubicle of corporate headquarters
  - Use VPN

Case Study One

- High ranking executives use lap top computers to wireless access the corporate network
- They connect to a WAP using WPA (requiring a WEP key), ACL, RADIUS server authentication, VPN authentication
- They have to type their user name and password several times and have the right WEP key (which changes every 90 days)
- They do not like all this username and password stuff, they want “single sign on”

Case Study One (continued)

- A system engineer (not me) figures the VPN is protecting the data, so set up the WAP with WPA off and forget the RADIUS server, but leave the ACLs
- Remember only protocol 50, protocol 51, and port 500 allowed on the network
- System engineer figures everything is still secure
- So the high ranking executive only needs to provide their user name and password once (single sign on)
- Do you see the Problem?

Case Study One (continued)

- The problem is the VPN protects the data
- The network is wide open to hackers
- Hacker observes network packets (at level two - management frames)
- She sees the clients of the WAP, obtains the SSID of the WAP (after first use by any client)
- She sets her MAC to the MAC of a valid client
- She uses software that allows her poison the ARP cache and become “lady in the middle”
- Now she hacks the network (she has no interest in the data on the network, she wants the hacking platform)

Case Study Two

- Senior executive lives near his office
- Information Technology Department installs fiber direct to his house so he can get on corporate network and work from home
- Suspend reality for a minute and forget about the fiber tap we studied
- Executive goes to a nearby large computer retail store and buys a WAP, connecting it to the fiber connection
- Now, he can do his work from his patio

Case Study Two (continued)

- Now it is possible to sit in a parking lot near the senior executives house and collect all his data
- If the executive is smart enough to buy a VPN and encrypts his data, then we still have a problem
- The corporate network now becomes a hacking platform for our wiley hacker who no longer needs to get in the middle of anything, just hook up to the WAP
- Solution: The executive makes his requirement know to IT, and IT provides the proper equipment, monitors use, and enforces WEP initial key change often with WPA features turned on

III. Conclusions

- Be sure employees know your computer network policy - remind them often
- Remind employees of the importance of not self deploying network devices of any kind
- Road warriors need to call back home with wireless devices - use encrypted VPN tunnels for this
- Use WEP (WPA if you can) to protect your network
- Use VPNs to protect your data

Conclusions (continued)

- Wireless access points are not just another set of “network jacks” to plug into - radio goes further than intended
- With proper attention to security, wireless LANs are useful and desired in our new mobile world
- There is significant ROI using wireless LANs, but do the risk assessment, risk management, risk mitigation, risk consensus
- Policy - Requirements - Document Risk - Planning - Managed Deployment - Monitoring

Conclusions (continued)

- You must know the RF environment of your enterprise at all times
- Employ a Wireless IDS to detect rogue WAPs or rogue Clients or even Net Stumblers in the parking lot
- Employ ARPWATCH in a Wired IDS if you deployed VPNs for your road warriors
- You might like a Kismet bootable CD for War Driving
- You might like Kismet on Zaurus for War Walking

References

- Poulsen, K. (2001). War Driving by the Bay. On-line. Available:

  http://www.securityfocus.com/news/192

- Stubblefield, A., Ioannidis, J., Rubin, A. (2001). Using the Fluhrer, Mantin, and Shamir Attack to Break WEP. On-line. Available:

  http://www.cs.rice.edu/~astubble/wep

- Program kismet available:

  http://www.kismetwireless.net/

- Program airsnort available:

  http://airsnort.sourceforge.net/

- Program wep-crack available:

  http://sourceforge.net/projects/wepcrack

References (continued)

- ARPWATCH software On-line. Available:

  http://www.securityfocus.com/tools/142

- WarLinux, a bootable Linux CD with Kismet. On-line. Available:

  http://metatag.tripod.com/software.htm

- Kismet on Zaurus. On-line. Available:

  WarLinux, a bootable Linux CD with Kismet. On-line. Available:

  http://kismetwireless.net/download.shtml

References (continued)

- Arbaugh, W. (2001). An Inductive Chosen Plaintext Attack against WEP/WEP2. On-line. Available: www.cs.umd.edu/~waa/attack/v3dcmnt.htm
- Walker, J. (2000). Unsafe at any key size; An analysis of the WEP encapsulation. On-line. Available: www.netsys.com/library/papers/walker-2000-10-27.pdf
- Vacca, J. R. (2001). Wireless Broadband Networks Handbook. McGraw-Hill. New York
- Davis, H., Mansfield, R. (2002). The Wi-Fi Experience: Everyone's Guide to 802.11b Wireless Networking. Que. Indianapolis, Indiana
- Doraswamyk, N., Harkins, D. (1999). IPSEC The New Standard for the Internet, Intranets, and Virtual Private Networks. Prentice Hall. Upper Saddle River, NJ

Questions

?