Threats and Countermeasures in Wireless Networking

Sean Wang
December 20, 2000

"Wireless" was the most frequently used word in describing the latest gear showcased at this year's ***Comdex*****.**[1, 2] While the "*connect anywhere and anytime*" promise by wireless vendors is beginning to provide real opportunities, there is plenty of confusion among prospective users when it comes to security. A recent survey by "***Network Magazine***" found that 25% of those who were yet to use Wireless LANs (WLANs) had cited security as the top concern. [3]

Are WLANs intrinsically more vulnerable than the wired counterparts? There are three recent SANS papers discussing the topic.[4,5,6] This paper attempts to further clear the confusion and misconceptions associated with security aspects unique to the wireless networks. We conclude that with proper countermeasures and best practices in place, wireless networks can actually be more secure than the wired networks.

The Standards

Today's various wireless specifications such as IEEE802.11b, IEEE802.11a, HiperLAN1/2, HomeRF, and Bluetooth are all close cousins to IEEE802.11.[7] Although commonly referred to as the wireless Ethernet, IEEE802.11, in fact, defines a Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) network at the MAC layer. There are three physical layers defined in IEEE802.11:

- **IR - infrared.** IR has limitations such as its short range (a few feet) and the line-of-sight requirement. It is mostly used in point to point communications in applications such as connectionless docking function for laptops.

- **FHSS - Frequency Hopping Spread Spectrum radio.** FHSS originated from the military during WWII. It employs a narrow band carrier, shifting frequency in a pattern known only to the transmitter and the receiver. FHSS is popular among standards mostly associated with wireless networks connecting PDAs, cell phones, printers, and other gadgets, often known as Wireless Personal Area Networks (WPANs) in implementations of Bluetooth, HomeRF, and OpenAir. [8]

- **DSSS - Direct Sequence Spread Spectrum radio.** DSSS is the same technique used in Satellite broadcast industry, for example, in GPS.[8] It is a broadband carrier, which takes the signal at a given frequency and spreads it across a band of frequencies. The center of the band is the original signal. DSSS generates a redundant bit pattern (called a chip) for every bit of data to be transmitted. Unlike FHSS, DSSS changes its frequency spreading range with time in a pseudo random manner, making the signal appears to be a random noise source.

It is important to bear in mind that the majority of IEEE802.11 family WLANs, and applications based on Bluetooth, and HomeRF in the market place are all non-exclusive members of the 2.4 GHz to 2.48 GHz band, the unregulated Industrial, Scientific, and Medical (ISM) band.

The most widely implemented WLANs adopt the recently approved IEEE802.11b. The nominal speed is 11 Mbit/sec, with a maximum throughput around 5 Mbit/sec. The actual mileage varies according to the distance between the transmitter and the receiver.

A typical WLAN implementation is an adjunct to an existing wired network. Here, Access Points (APs) bridge the wireless and wired networks. An AP performs two additional functions, authentication and association. Authentication determines if a given wireless device is permitted to connect to the network, and this is commonly done via a password or the MAC address. Association is unique to the wireless communications and is a handshaking mechanism between the AP and the wireless devices. It ensures that one client is only connected to one AP at any given time.[9] Things start to get more complicated for multiple APs to work together and for the clients to switch from AP to AP (roaming). An Extended Service Set (ESS) is a collection of logical communication channels. A unique ESS ID number is used to avoid interference.

Vulnerabilities and Countermeasures

The foundation upon which any security model is built has the same objective: to protect *confidentiality, integrity, and availability*. Security issues, threats and vulnerabilities faced by wireless networks are largely the same as those faced by the wired networks. There are a few added twists unique to the wireless network.

- **Eavesdropping.** Given the radio-based nature of wireless network, eavesdropping is always a possibility since communication is through open air (*confidentiality and integrity attack*). Here the common confusion is to mix up intercepting a signal and "sniffing" a network.
- **Radio Interference and Denial of Service.** Another misconception is that it is easy to launch denial-of-service attacks against wireless network. The basis for this belief is the following; since the resonant frequency of water molecule is centered around 2.45 GHz, microwave ovens and medical scanners (for example, MRI) all have to operate near the ISM band. A typical scenario is a leaky microwave oven disrupting a wireless network (*availability attack*).

These two frequently quoted threats against wireless networks are actually readily addressed by today's WLAN implementations. Intercepting a wireless signal is trivial. However, when dealing with a FHSS signal, while mathematically possible, it would take extreme efforts to sniff unless the black hats know the exact frequency hop sequence and the timing. With DSSS, the transmitter maps bits into "chips" and the receiver maps "chips" back to restore data. Depending on how chips map into bits, (or in the wireless terminology, the "spreading ratio", number of chips per bit), it takes special knowledge and equipment to go through the tedious procedure to map in real time the chips into meaningful data streams. In the worst case, even if the data streams are successfully sniffed off the air, they ***should*** be encrypted (see next section). Gaining unauthorized access to a WLAN is even more difficult as it requires passing additional AP authentication and association.

What about the DoS attack? It turns out that a higher "spreading ratio" in DSSS also makes the signal more resilient to interference. It is fairly easy for today's DSSS to survive a leaky microwave. But a more powerful MRI scanner can definitely cause disruption against a WLAN. In the case of DoS attacks against WLANs, the sources of attack can be easily identified and therefore, it can be argued that DoS attacks are easier to stop in a wireless network than in a wired network. For in the wired world, identifying the source of a DoS attack is usually difficult because IP address spoofing. Further, the microwave scenario will soon become irrelevant with the next generation WLAN, IEEE802.11a, due out 2001, as it will operate in the 5 GHz band.

Encryption: Size (Length) Matters

IEEE802.11b has an optional shared-key encryption known as Wired Equivalent Privacy (WEP) [9.] It employs an RC4 encryption algorithm with either a 40-bit or a 128-bit key. While still useful, a 40-bit symmetric key is too weak against even low-budget brute force attacks. This has been demonstrated in the classical paper by some of the creators of RC4 and other leading experts in cryptography.[10] The minimal key length considered secure against well-funded attackers (for example, a government intelligence agency) in 1996 for the next 20 years was 90 bits long. A recent cryptanalysis of RC4 advocates 128-bit keys. [11]

Vendors were limited to 40-bit keys largely due to US export controls over encryption technology. With the politics of cryptography settling in the past year, all major vendors now offer 128-bit encryption for APs.

We have surveyed about a dozen major 802.11b vendors and found good news and bad (Table 1). The good news: all major vendors we checked ship 128-bit RC4 or some equivalently strong encryption. The bad news is for consumers: the enhanced security usually comes at a much higher price (usually 30-40% more for 128-bit encryption than for 40 bit or 64 bit!). The well-known truth in cryptography is that the computation cost for 128-bit encryption is really no greater than 40-bit encryption. [9]

The Latest Trends

In recent months, some vendors started providing solutions to get around the basic WEP limitations on scalability and manageability. NoWiresNeeded's AirLock [12] employs the Diffie-Hellman public key algorithm between the AP and the connecting clients with a 128-bit key. Capslock, a wireless access service provider, rolled out Secure Wireless Access Technology, using 56 bit Triple DES (the US government sanctioned standards until not too long ago), as well as the latest AES standard, Rijndael.[13]

A promising technique with great potential for scalability is 3Com's Layer3 tunneling.[14] Here, Layer 3 tunneling utilize private keys that are automatically negotiated and frequently changed rather than manually entered shared keys as supported by WEP.

Wireless networking is not limited to just LANs. We will briefly review the emerging technologies that are on the horizon and look at the related security issues.

- **PANs.** In the near term, PANs based on Bluetooth and HomeRF promise to revolutionize how people live. An MIT study predicts that by 2010, each person will have 5,000 Internet connected products, from wristwatch to coffee makers to refrigerators.[15] To bear in mind that FHSS is used in PANs so privacy is essentially achieved via obscurity.

- **The New WLAN.** In the coming year, WLANs will see HiperLAN2 and IEEE802.11a, both at 54 Mbits/sec**.** Gartner Group predicts that IEEE802.11a will win the competition due to its lower cost.[16] Both standards will operate at the 5.2 or 5.8 GHz bands, leaving behind the interference concerns specific to the ISM band.

- **The Last Mile.** Broadband wireless solutions may eventually win the war of the "last mile" over the local exchange carriers. While the WirelessMAN 802.16 specifications are still work in progress,[17] service providers have already started the competition in the wireless access market.[18] Without going into the nuances of the broadband wireless technology, we want to point out that the popular Code Division Multiple Access (CDMA) is also based on spread-spectrum technique. Security technique used in this area is similar to these employed in WLANs and due to the lack of a uniform standard, they tend to be more proprietary in nature.[19]

Wireless Advantages

Wireless networking has made great strides in recent months in addressing the security issues. However, there is no absolutely secure network, wired or wireless. Countermeasures and best practices are the only hope to secure any network.

We argue that with a strong encryption wireless network is more secure than a lot of the existing wired networks where information is transmitted and received in clear text. It is a misconception that information is more secure only because it transmits through a wire. Some APs in the market place have Network Address Translation (NAT) and authentication built-in, making WLANs already a step ahead of most of the wired networks for SOHOs.

Wireless technology and security do not have to be mutually exclusive. In fact, some vendors started taking advantages of wireless technology and integrating it to security solutions. One example is Ensure Technology's Bluetooth-enabled, wearable smart card, which authenticates users based on proximity.[20] Therefore they can lock or unlock desktops/laptops or be used to track assets to ensure physical security.

Finally, we should keep in mind that technology alone will not solve all security problems. There is no substitution for sound security policies and best practices.

Table 1. SOHO AP Survey

Vendor	AP Model	Encryption	NAT	DHCP
Lucent	OriNOCO RG1000	60 bit/128 bit WEP	Yes	Yes
3Com	AirConnect	40 bit/128 bit WEP	No	Yes
Cisco	Aironet 340	40 bit/128 bit WEP	No	Yes
Compaq	WL400	64 bit/128 bit WEP	No	No
NoWires Needed	Small Business AP	40 bit/128 bit WEP	No	No
Enterasys	RoamAbout	40 bit/128 bit WEP	No	No
Apple	AirPort	40 bit WEP	No	No
Linksys	WAP11	40 bit WEP	No	No
Intel	PRO/wireless 2011	40 bit/128 WEP	No	Yes
D-Link	DWL-1000AP	40 bit WEP	No	Yes

References:

1. Edwards, Cliff, “Cutting the Cord” April 21, 2000
   http://more.abcnews.go.com/sections/tech/DailyNews/comdex000421.html
2. Nobel, Carmen, “Wireless needs a wing to fly on” November 13, 2000
   eWeek, Vol. 17 Number 46
3. Angel, Jonathan, “Look ma, no cables” November 5, 2000
   http://www.networkmagazine.com/article/NMG20001106S0004
4. Harrison, Craig, “Wireless Confusion” November 13, 2000
   http://www.sans.org/infosecFAQ/wireless_confusion.htm
5. Ross, B. Justin, “Containing the wireless LAN security risk” November 4, 2000
   http://www.sans.org/infosecFAQ/wireless_LAN.htm
6. Mitchell, Gordon L., “Wireless LANs – the big new security risk” May 5, 2000
   http://www.sans.org/infosecFAQ/LAN.htm
7. O’Hara, Bob and Petrick, Al “The IEEE 802.11 Handbook” IEEE Press (See also http://ieee802.org/11 for recent developments)
8. NDC Communications, Inc. “Wireless LAN Systems- Technology and Specifications”
   http://www.ndclan.com/Wireless/wlanW1.htm
9. Wexler, Joanie“Why use a wireless LAN?” July 17, 2000
   http://www.nwfusion.com/newsletters/wireless/2000/0717wire2.html
10. Blaze, M., Diffie, W., Rivest, R. L., Schneier, B., Shimomura, T., Thompson, E., and Wiener, M. “Minimal Key Lengths For Symmetric Ciphers to Provide Adequate Commercial Security” January 1996
    http://theory.lcs.mit.edu/~rivest/bsa-final-report.ascii)
11. Grosul, Alexander and Wallach, Dan “A Related-Key Cryptanalysis of RC4” June 8, 2000
    http://cs-tr.cs.rice.edu/Dienst/UI/2.0/Describe/ncstrl.rice_cs/TR00-358
12. NoWires Needed “Enhanced Protection for Wireless LANs”
    http://www.nwn.com/docs/AirLock.pdf
13. Williams, Aisha M. “Wireless Data Transaction Get Safer” November 20, 2000

http://www.informationweek.com/813/secure.htm

14. 3Com "3Com Introduces Industry's First Layer 3 WLAN Security Solution" July 5,2000
http://www.3com.com/news/releases/pr00/jul0500a.html
15. Dornan, Andy "Can Bluetooth Sink Its Teeth into Networking?" November 2000
http://www.networkmagazine.com/article/NMG20001103S0002
16. Egan, Bob "Are wireless LANs a viable option for mainstream companies and what will be their future?
http://www.networkmagazine.com/article/NMG20001103S0002
17. IEEE802.16 Work Group
http://wirelessman.org
18. Clark, Elizabeth "Pulling the Plug on the Local Loop" June 1999
http://www.networkmagazine.com/article/NMG20000509S0025
19. Clearwire Service "Fixed Wireless Internet Access"
http://www.clearwire.com/get_connected/ClearwireSvc.cfm
20. Ensure Technology Inc. "XyLoc Wireless PC Security Solution" June, 2000
http://ensuretech.com/cgibin/dp/frameset.dt/company2/pressroom/releases/PCExpo06-26-00.html