Global Information Assurance Certification Paper

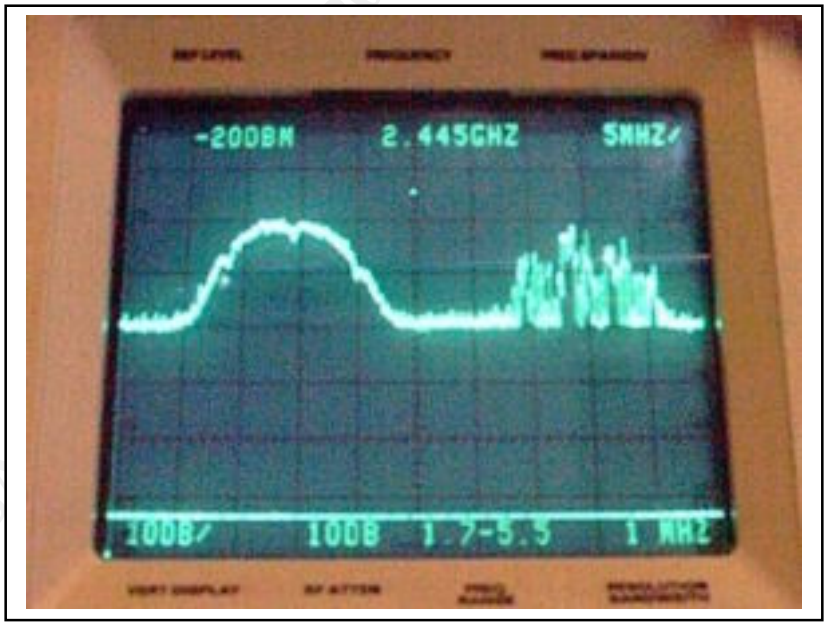
Wireless LANs – the big new security risk
Gordon L. Mitchell, PhD, CISSP
May 5, 2000

SANS has educated thousands of network security folks. Users are beginning to employ powerful firewalls, intrusion detection and auditing tools. Just when the world looks a bit safer, wireless networks begin to appear everywhere. Do they threaten basic network security allowing bad guys to sniff from the parking lot?

A colleague[1] in Boston recently told me about an authorized network penetration that he performed as part of a vulnerability analysis. He was able to sniff the network effectively from an area outside the building. His customer used a common unencrypted LAN with access points (the transmitter/receiver modules which communicate to mobile users) that could communicate outside the building. This sort of vulnerability presents major risks to LAN security.

Wireless means radio transmissions

Wireless LAN systems conform to IEEE 802.11, a standard that allows both frequency hopping and direct sequence spread spectrum communications. Typically this is at a frequency of 2.4 Gigahertz. Near an access point, signals can be observed using a spectrum analyzer. The screen photo below[2] shows transmissions from two nearby access points.



On the left is an 11 megabit direct sequence spread spectrum signal which is transmitting information continuously. The signal on the right is from an access point which is not so busy and (because of the way the spectrum analyzer gathers data) appears less well defined.

Spread spectrum techniques are used to avoid the fading associated with narrow band transmissions[3] as well as providing processing gain in situations where the bandwidth is substantially greater than the signal bandwidth. The spread spectrum modulation also is a small measure of security since it requires at least an intermediate piece of hardware, e.g., a stolen PC card, to intercept network signals.

Two basic types of spread spectrum modulations are used in wireless LANs. They are frequency hopping (FH) and direct sequence (DS). Reasonably good interoperability between manufacturers is possible for either FH or DS systems but not between them. The two flavors of spread spectrum transmission remain a nonstandard part of standard 802.11. All of these 802.11 systems can be operated as unlicensed transmitters.

These radio signals can be detected hundreds of feet from the access point, especially when high gain antennas are used on the mobile portion of the link. Virtually all the wireless LANs installed to date (Spring 2000) feature unencrypted transmissions. That means that the signals illustrated above contain live net traffic. Sniffers do not need to be attached to a wire to grab this network information.

User authentication

Users are typically using a PC (PCMCIA) card in a laptop to associate with (connect to) the wireless network access points. Often access points are mounted in ceiling areas where they connect to power, Ethernet and RS-232 wiring.

Many administrators trust Extended Service Set ID (ESSID) numbers to keep intruders from associating with their networks. The ESSID is essentially a workgroup identification used by individual network cards to identify themselves to the access point. We have sniffed ESSIDs transmitted on the clear on the wired network connected to access points; it is possible that they are also available over the air. ESSIDs do not provide adequate security. A stolen laptop can connect to the network easily.

Security solutions and headaches

Some wireless link manufacturers are beginning to offer encryption with their products. They use symmetric algorithms[4] which are implemented in hardware to keep throughput speed up. The most important encryption issue that must be resolved before a cryptosystem of this sort is implemented is key management. How will secret keys be distributed (certainly not via e-mail). When an employee is fired how will his ability to intercept and decrypt wireless LAN traffic be revoked?

Having employees with wireless LAN cards in their laptops certainly adds mobility to a workforce but it requires another layer of network management. Interface issues with wireless LANs are much more significant than with Ethernet jacks in the wall. If access control lists (ACLs) are used it is important to know how they are to be loaded, checked and changed. System integrity may require being able to connect to individual access point serial ports; this is difficult if the access points are installed in ceiling areas.

Denial of service via radio inteference

Since most wireless LANs use the unlicensed 2.4 Gigahertz band[5] which is shared with other services interference is certain. The most significant interference sources are high powered transmitters that share the same frequency band. Microwave ovens with leaky door gaskets are the most threatening but other transmitters can also be problems. We have tracked interference problems to car alarms designed to detect intruders through a convertible roof.

In wireless LANs which use encryption radio interference will cause an increase in decrypt errors. This is because any corruption of the cyphertext will produce garbage out of the encryption engine.

Vendors

Vendor information on wireless LANs often sidesteps network security issues; call and ask directly about ACL management schemes, the use of strong (at least 112 bit) encryption and other security features.

Vendors web pages include:

http://www.cisco.com/warp/public/44/jump/wireless.shtml
http://www.symbol.com/products/wireless/wireless_products_lit.html
http://wwwdb.lucent.com/bcs/syst.main?p_id=65&p_keyword=
http://www.intermec.com/local_area/wireless.htm
http://www.breezecom.com/

---

[1] Private communication
[2] Photo courtesy of FutureFocus, www.Bug-Killer.com
[3] T.S. Rappaport, **Wireless Communications**, Prentice Hall, 1996, page 274
[4] B. Schneier, **Applied Cryptography**, John Wiley, 1996
[5] E. Jordan, editor, **Reference Data for Engineers**, SAMS, 1989

Last Updated: February 24th, 2018

Upcoming Training

SANS New York City Winter 2018	New York, NY	Feb 26, 2018 - Mar 03, 2018	Live Event
Mentor Session - AW SEC401	Melbourne, FL	Mar 01, 2018 - May 10, 2018	Mentor
SANS London March 2018	London, United Kingdom	Mar 05, 2018 - Mar 10, 2018	Live Event
Mentor Session - SEC401	Vancouver, BC	Mar 06, 2018 - May 15, 2018	Mentor
Mentor Session - SEC401	Grand Rapids, MI	Mar 09, 2018 - Apr 13, 2018	Mentor
SANS Paris March 2018	Paris, France	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS Secure Singapore 2018	Singapore, Singapore	Mar 12, 2018 - Mar 24, 2018	Live Event
SANS Secure Osaka 2018	Osaka, Japan	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS San Francisco Spring 2018	San Francisco, CA	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS Northern VA Spring - Tysons 2018	McLean, VA	Mar 17, 2018 - Mar 24, 2018	Live Event
SANS Pen Test Austin 2018	Austin, TX	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS Munich March 2018	Munich, Germany	Mar 19, 2018 - Mar 24, 2018	Live Event
Mentor Session - SEC401	Studio City, CA	Mar 20, 2018 - May 01, 2018	Mentor
Mentor Session - AW SEC401	Mayfield Village, OH	Mar 21, 2018 - May 23, 2018	Mentor
SANS Boston Spring 2018	Boston, MA	Mar 25, 2018 - Mar 30, 2018	Live Event
SANS 2018 - SEC401: Security Essentials Bootcamp Style	Orlando, FL	Apr 03, 2018 - Apr 08, 2018	vLive
SANS 2018	Orlando, FL	Apr 03, 2018 - Apr 10, 2018	Live Event
Community SANS Charleston SEC401	Charleston, SC	Apr 09, 2018 - Apr 14, 2018	Community SANS
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201804,	Apr 09, 2018 - May 16, 2018	vLive
Community SANS St. Louis SEC401	St Louis, MO	Apr 16, 2018 - Apr 21, 2018	Community SANS
SANS London April 2018	London, United Kingdom	Apr 16, 2018 - Apr 21, 2018	Live Event
SANS Zurich 2018	Zurich, Switzerland	Apr 16, 2018 - Apr 21, 2018	Live Event
Mentor Session - AW SEC401	Memphis, TN	Apr 17, 2018 - May 17, 2018	Mentor
SANS Baltimore Spring 2018	Baltimore, MD	Apr 21, 2018 - Apr 28, 2018	Live Event
Baltimore Spring 2018 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Apr 23, 2018 - Apr 28, 2018	vLive
SANS Seattle Spring 2018	Seattle, WA	Apr 23, 2018 - Apr 28, 2018	Live Event
SANS Riyadh April 2018	Riyadh, Saudi Arabia	Apr 28, 2018 - May 03, 2018	Live Event
Automotive Cybersecurity Summit & Training 2018	Chicago, IL	May 01, 2018 - May 08, 2018	Live Event
Community SANS Houston SEC401	Houston, TX	May 07, 2018 - May 12, 2018	Community SANS
SANS Security West 2018	San Diego, CA	May 11, 2018 - May 18, 2018	Live Event
SANS Northern VA Reston Spring 2018	Reston, VA	May 20, 2018 - May 25, 2018	Live Event