Global Information Assurance Certification Paper

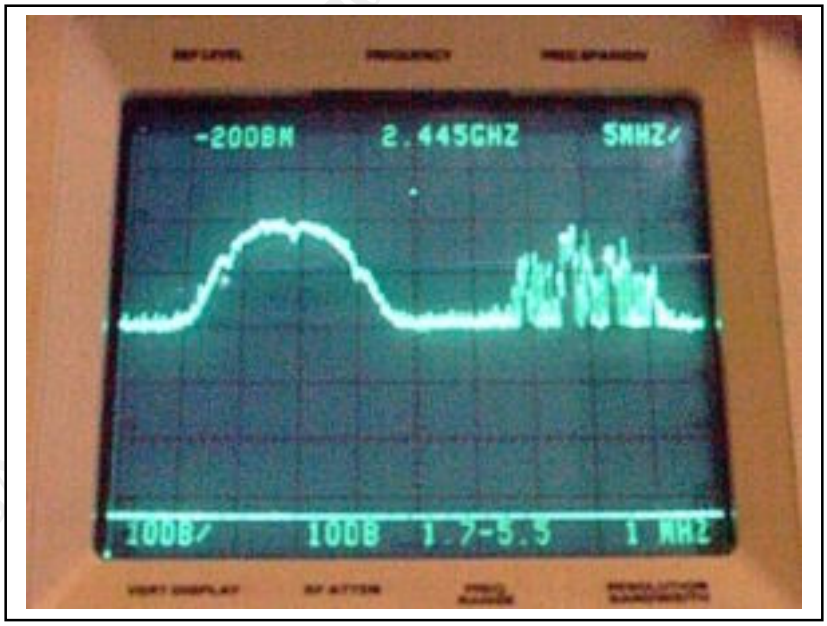
Wireless LANs – the big new security risk
Gordon L. Mitchell, PhD, CISSP
May 5, 2000

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: June 25th, 2017

Upcoming Training

SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS San Diego SEC401	San Diego, CA	Aug 21, 2017 - Aug 26, 2017	Community SANS
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor