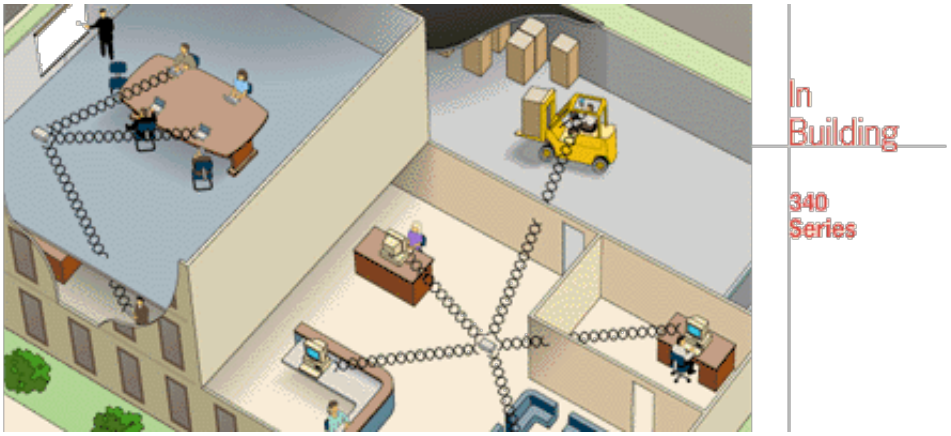
Global Information Assurance Certification Paper

Containing the Wireless LAN Security Risk
B. Justin Ross
November 4, 2000

What is a wireless LAN

One possible definition of a wireless LAN is a collection of two or more devices connected via an open air medium in order to share data. There are many different methods of laying out a wireless LAN. There are a few definitions used by some of the wireless vendors[1]. "Ad Hoc Network: A wireless network composed only of stations without access points[1]." This type of network can be used anywhere. There are very few requirements for this to work. This could potentially be the most dangerous of all wireless networks. Since this type of network is going to be setup on the fly when two people want to share data it is more probable that less consideration is going to be placed on security. "Access Point: A wireless LAN transceiver that acts as a center point and bridges between wireless and wired networks[1]." A wireless network that is installed with access points should be fairly secure in today's networking environments with a few considerations. In the future one of the most common types of wireless LANs will be a LAN deployed inside of a building for the use of laptop computers, hand held devices and other mobile network connected equipment. The illustration[2] below is just one possible use of a wireless LAN.



Both ad hock networks and networks centered around access points may use the IEEE 802.11b standard. "802.11b: The IEEE standard that specifies a carrier sense media access control and physical layer specifications for 5.5 and 11 megabit per second wireless LANs[1]." The 2.4 Gigahertz frequency range is typically used[3]. Typical speeds of 11 Megabits can be achieved depending on the distance from the access point and the type of area the network is being used. Information provided by vendors typically indicate 400 feet in an open air environment and 100 feet in a typical office environment for 11 Megabit traffic. The speed can drop to 5.5 Megabit or even lower depending on many factors.

Security in today's wireless environment

When using a wireless LAN one of the most important considerations is security. In general there is a Service Set ID (SSID). This SSID is nothing more than a network name. This name is sometimes considered secret. In reality it is not really that important. The SSID can typically be found by "sniffing" the network. Therefore this lends very little to securing a network. The next level of security is typically WEP 40 encryption, or 64 bit encryption. "Wired Equivalent Privacy (WEP): Optional security mechanism defined within the 802.11 standard designed to make the link integrity of the wireless medium equal to that of a cable[1]." The next level of encryption is 128 bit. The minimal level of encryption used if security is a concern should be 128 bit. Not only because it is very difficult to decode (because WEP 40 and 64 bit encryption are also very difficult to decode) but also because it uses longer encryption keys. It is more likely that someone can obtain or remember a five or ten byte encryption key than a twenty-six byte encryption key.

Simply using encryption keys and SSIDs is not the optimal solution. If someone were to leave a company on bad terms but keep their wireless network card they could drive up to the outside of the building and capture all of the network data that they would like. Some of the vendors have installed MAC address filters. This in many cases is not

very useful though. If you are administering a network of 400 wireless cards which turn over from one employee to another, keeping track of ownership and MAC addresses could be a nightmare. This in most cases is the limit of today's wireless infrastructure.

One of the biggest threats to today's corporate intranets is attack through people's PCs at home. With cable modems and DSL lines in a great number of homes this threat is now even easier to leverage. This is only made worse by wireless networking products. Most of today's at home wireless networks are very weak on the security side. Most require the equivalent of an SSID. Once that is installed the network is up and running. Most home users are not aware of the security risks that they are imposing on their company's intranet. Lucent Technologies has documentation on how to setup their RG-1000 home access point. In this documentation there are few mentions of security or encryption[4]. Also the RG-1000 only supports 64 bit not 128 bit encryption. The one plus to Lucent's RG-1000 is that by default the SSID is used as an encryption key. Since Lucent uses this SSID as their key encryption is on by default. Some manufacturers do not even support encryption on their home wireless networking equipment.

Security in tomorrow's wireless environment

The next level of wireless networking includes many more features that will help in securing these networks. Up until now encryption and access has been limited to authenticating a piece of hardware. The next step is to authenticate the person at the hardware. Cisco is going to release in the up coming year x.509 certificate authentication. So each person will be required to unlock their x.509 certificate with a password and then present their certificate over an encrypted channel before they are allowed access to the network. Early indications from Cisco are that there will be some sort of session key based on this certificate. So even if you have the keys for the 128 bit encryption you will still not be able to understand or "sniff" the traffic without a session key produced when the individual is authenticated. This multilevel situation lends to fairly strong security. You first have to have the SSID, next the twenty-six byte encryption key, then an approved and password unlocked x.509 certificate. Only then can you communicate on the network.

One theory proposed by a colleague[5] is to place a barcode on the back of every wireless network card. Use these barcodes at a barcode scanner at the help desk or other site inside the building to "unlock" the access to that card. Lucent Technologies uses a MAC address filtering based on a radius authentication server. If the radius server knows the MAC address then it is allowed. The barcode scanner could input the MAC address into the radius server's authentication list. This could then be reset every night. This would ensure that someone could not simply drive up to the side of your building and start talking on the network even if they have the SSID, encryption keys, and a certificate.

What the future of wireless networking may hold

Currently the popular vendor's wireless networking products are limited to 11 megabit. The one noticeable limitation is that the speed of wireless networking is a step back from other methods. Wired networking is now at switched gigabit speeds. Wireless is at shared 11 megabit. The steps taken by wired networking have been from 10 to 100 to 1000 megabit and next to 10000 megabit. But the advancements made in wireless have been much slower, from around 1.6 megabit to 11 megabit. The next step is only to double to 22 megabit. Wired networking increases by a factor of ten while wireless only by a factor of two. Right now with a limited number of users 11 megabit is sufficient, but with a large number of users it may prove to be a bottleneck.

Vendors

Two of the top vendors in this field are Cisco Systems and Lucent Technologies. One concern is interoperability between the different vendors. There are standards, 802.11b and WEP to name two, but these only seem to work with either no encryption or the lowest level of encryption. The different vendors use different length encryption keys. Some of the vendors advertise that their products use proprietary technology to encrypt their traffic. Until the use of wireless networking cards is as mainstream as the use of wired network cards, where interoperability between different vendors is a requirement, there are going to be difficulties with security and usability.

Cisco Systems: http://www.aironet.com

Lucent Technologies: http://www.wavelan.com

References:

1. Cisco Systems. "Wireless Glossary." URL: http://www.aironet.com/wireless/glossary.asp (4 Nov. 2000).
2. Cisco Systems. "Product Families" URL: http://www.aironet.com/products/in_building.asp (4 Nov.

2000).
3. Mitchell, Gordon. "Wireless LANs – the Big New Security Risk." 5 May 2000. URL: http://www.sans.org/infosecFAQ/LAN.htm (4 Nov. 2000).
4. Lucent Technologies. "RG-1000 FAQ." http://www.wavelan.com/products/rg1000.html (4 Nov. 2000).
5. Private Communication