Global Information Assurance Certification Paper

The Wireless Confusion

Craig V. Harrison, CEA,CBT
November 13, 2000

Many of us working in the computer security field, with our sophisticated firewalls, intrusion detection systems and logging analysis each have our own completely different understanding and harbor misconceptions about the wireless networking business. When you mention wireless, one person may conjure up images of sitting on the beach while surfing the Internet on his laptop interfaced with his cellular phone, while another may think of transferring mega Jpeg files from one office to another across the street, and yet another dreams of wall street updates and stock purchases from his handheld computer while sitting at a very boring political rally. Wireless, really boils down to using Radio Transmissions in the UHF (Ultra High Frequency) or SHF (Super High Frequency) range to communicate data for an unbelievable number of uses. This paper will attempt to reduce the confusion at least were it is applicable to the computer security industry.

The frequency ranges generally referred to as wireless, although all radio transmissions are wireless, are 900MHz, 2.4GHz, and 5.8GHz. The proliferation of devices using these narrow spectrums is growing at an unbelievable rate. Examples are: Cellular phones, paging services, message boards, Palm connections, mobile information services, mobile emergency location services, video and audio surveillance services, auto security systems, home security systems, household control systems, mobile and remote control systems, LAN's (Local Area Networks), WAN's (Wide Area Networks), MAN's (Metropolitan Area Networks), PAN's (Personal Area Networks), and many others. Each of these has it's own unique security issues or in some cases non issues. Full duplex port to port or base station multiport applications at competitive pricing are resulting in private carrier networks, government networks, campus networks, office networks, temporary network infrastructure, backup links, and disaster recovery networks. Return on investment for replacing current technologies such as leased land lines, ISDN,ASDL, and cable modems makes it very attractive technology, as the initial investment payback time can be as little as one year. Then, you have almost "free service." Pretty tempting from a corporate viewpoint.

Physical security as it applies to the wired Ethernet network is no longer applicable in world of the wireless network. The transmission media is truly ethereal in nature. Your data is literally hanging all around you, your proximity and in some cases even further. Claims are now made for wireless networks at speeds of up to 100 Mbps at ranges exceeding 50 miles. The one room local wireless LAN can now stretch clear across town without your knowledge if it is not designed properly. The fact that there is no frequency coordination or FCC licensing required results in a somewhat chaotic environment. The availability of antennas, amplifiers (up to 1 watt) and various accessories from a variety of manufacturers that can be interconnected makes it inevitable that interference related and unintentional DOS (Denial Of Service) attacks will occur. Although this is a benign attack it can become one of the most serious and expensive to track down and cure. It would also be very easy for a prankster or ill intended hacker to modify the safety door switch on a microwave oven and wreck total havoc with all the wireless

networks within blocks. After all, they are really not concerned with the legality of it. These wireless systems need to be designed with much better RF protection and filtering before they are deployed on mission critical sites. Care must be taken to limit the possibility of interference by installing band pass filters and notch filters wherever necessary.

Another physical security aspect is theft of an authorized wireless laptop from a campus or corporate wireless LAN. A hacker with an authorized (stolen) box can snoop and attack practically at will. He could be in the same room, next door, at home, down the street or possibly miles away and be virtually untraceable. Until you discover the intrusion or are notified of the theft you will be vulnerable from the inside via the outside. Spoofing of these laptops is also currently possible to the enlightened hacker.

Likewise we have the issues involved with point to point wireless WAN's and MAN's . Many of the units now deployed use only frequency hoping or sequence spread spectrum communications as a means of preventing eavesdropping without any from of encryption. The newer better-designed units that use proprietary encapsulation and encryption are more secure. However, the pricing of these units makes it possible for a hacker to purchase one and simply snoop the airways with impunity for valuable information from miles away. The snooping would be difficult if not impossible to detect, however, if the hacker became active it might be possible to track it down to an RF MAC address, although this would have limited usefulness. PKI using key management and encryption of all data sent over the wireless would essentially make the data useless to the snooper. However, it would add considerable data overhead and possibly render the wireless network useless during certain weather conditions such as heavy rain or snow due to bit error sensitivity of encrypted packages.

We now have wireless networks competing for the home Internet access market. "Sprint Broadband is a multimegabit asymmetric service that works over Multichannel Multipoint Distribution System (MMDS) fixed wireless. It uses the reserved frequency ranges at 2.1 GHz and 2.5 through 2.7 GHz that at one time were reserved for television signals."[2] If and when these wireless networks become competitive, it opens up a whole new security issue for home users depending on how they are implemented. Since pricing is the motivating factor it would not be surprising to find many home users all hooked to the same hub like network. Neighbors will truly become network neighbors knowingly or unknowingly and freely have access to shared drives. Home users will have to become security conscious and personal firewalls will become a must.

Now we come to yet another new wireless media "Bluetooth." Bluetooth is a wireless standard designed to replace cables and bring interconnectivity between all kinds of local consumer devices such as cell phones, voice, printers, remote control devices, personal PC's, network connectivity, intranets, extranets, and the Internet. It operates in the globally available unlicensed 2.45MHz radio band and supports speeds up to 721 Kps as well as three voice channels. It employs frequency hopping at a rate of 1600 hops per second. It also employs an automatic power reduction scheme for in room or in home requirements. Both of these improve security by making it more difficult to snoop. However, the frequency hopping is algorithmic in nature and local snooping is still possible although difficult. Software controls and identity coding built into each microchip help to ensure that only those units preset by their owners can communicate.

Bluetooth supports point to point and multipoint connections creating what is know as "piconets," several of which can be linked together in what is know as a "scatternet" arrangement. This gives a user the ability to participate in a conference like scenario freely exchanging messages, E-mail, files, and whatever else they wish to exchange in a localized environment. This in itself is a serious security problem in that viruses and Trojan software can be unknowingly passed around only to be transferred to an important network server all without the users knowledge. Visualize yourself attending a conference and exchanging a few messages or chats with other conferees using your handheld, and returning to your office and having your desktop PC (connected to the corporate network) automatically synchronized as you open your door. Neat feature, but a little scary perhaps! We are now hearing of plans to implement Bluetooth on web servers for user convenience. Bluetooth depending on just how it is implemented is a security disaster just waiting to happen.

In conclusion, we can see that the unregulated nature of the wireless network makes it a security issue of great importance if your organization chooses to deploy it. Vendors tend to sell the equipment as a cost effective solution to network needs with simple plug and play like installation requirements. First, it can render your firewall and intrusion detention system mute unless all wireless systems are connected only on the outside. Not a very practical solution, as deployments will be scattered throughout the organization as the cost benefits become apparent. Your Intranet communications will literally be leaking through the walls if not down the street. Great care, expert advise and engineering should be used when designing the deployment of a wireless network. Where is the system to be installed, how will it be connected to the network, what accesses will be given it, how will it be used, and the sensitivity of the data accessible to it are all questions to be asked before the installation. The methods of authentication between point to point and multipoint wireless networks must be brought to standards. Spread spectrum and frequency hopping with I.D. numbers is not enough. It will be up to the purchaser to demand better technology such as radio fingerprinting of the transmitters and receivers used to insure there is no spoofing. This technology is now used in cellular systems to prevent fraud. SIM's (Subscriber Identification Modules) are also used in cell phones to reduce fraud. If these types of technology can economically be used in cell phones, which are essentially given away free, surely they can be employed in wireless network equipment. It's going to be up to the purchaser to demand these changes by making decisions based on security needs and not just price. Security is just as important a part of total cost of ownership as product cost.

Bibliography

:

1. Ross, Patrick, "FCC to aid wireless carriers growth."9 Nov 2000 http://www.news.cnet.com/news/0-1004-200-3605698.html/
2. Shah, Rawn, "Analysis The next great Net connection" 23 Aug, 2000 http://www.cnn.com/2000/Tech/computing/08/23/next.great.connection /index.html/
3. Mitchell, Gordon L.,"Wireless LAN's-the Big New Security Risk" 5 May 2000 http://www.sans.org/infosecFAQ/LAN.htm
4. Wilcox, Joe,"As Bluetooth nibbles, competion lurks,"15 Sept 2000 http://www.canada.cnet.com/news/0-1006-200-2784702.html/

5. Gibilisco,Stan,Handbook of Radioand Wireless Technology, McGraw-Hill, 1998

Vendor Web pages:

http://www.mat-c0.com/as1000.htm.as1004
http://www.securtek.net/images/nav-left-products/html
http://www.overlan.com/pages/prod/bridgerouter.html
http://www.bluetooth.com/bluetoothguide/models/automatic.asp