Global Information Assurance Certification Paper

Wireless Networks: Are they worth the risk? March 27, 2003
GSLC v1.0
Donough Deutsch

Abstract

Wireless networking provides a convenient and often low cost method of accessing your information from just about anywhere. This rush to ride the wireless wave should be met with a bit of caution. Unchecked installations, and a relative ease of unauthorized access, leave wireless users exposed to some serious security risks.

Introduction

Wireless LANs or WLANs as they are often called are proliferating the business and home-use market spaces. Wireless networking offers a convenience and cost savings that often masks its hidden security implications. A communications medium confined only to the electromagnetic spectrum, which can permeate most walls, floors, and ceilings will invariably be fraught with security concerns.

It's no secret that there are people who seek to compromise intellectual property or at the very least annoy legitimate users of information technology. Those of us in the IT industry have been dealing with this threat for a very long time. The ubiquity of RF makes WLANs all the more vulnerable.

Wireless Vulnerabilities

Companies tend not to invest too much in information security because of the apparent complexity required to render a successful compromise of the organization's assets. WLANs have reduced that level of complexity down to an almost bare minimum. Anyone with a laptop, an antenna, and some spare time can listen in, and even communicate with a wireless network if it is not properly secured. This scheme requires little investment. An antenna can be fabricated from rudimentary objects such as a Pringles can.

This type of "hacking" has become somewhat of a sport known as "war driving" – W.A.R., for Wireless Access Revolution. This activity describes an enthusiast with a Wi-Fi enabled laptop who drives around looking for open and thus vulnerable wireless access ports (ABC Action News). If you're lucky, your organization, should it fall victim to a war driver, will have merely given away free Internet access. However, a malicious attacker could use your organization's network to launch an attack on others that would be traced back to your Internet connection. This would make it very difficult to ascertain the true source of the attack. A graffiti-like marking called "war chalking" marks your location as vulnerable, welcoming other would-be war drivers (Buckler, 2002).

Wireless Security

There are technologies designed to aid in the securing of wireless networks. Wired Equivalent Privacy (WEP) provides up to 128-bit link-level encryption for wireless communications. WEP is said to have its faults however. It can be compromised with relative ease, and render your network exposed. To address this, the IEEE plans to ratify 802.11i by the end of this year. This new standard in wireless security is designed to clear up some of the shortcomings of WEP (Greene & Cox, 2003).

Encryption is designed to ensure the integrity of a transmission. However, it does nothing to ensure the user is who they say they are. This is where authentication becomes important. A consortium of Microsoft, Cisco, and RSA Security developed Protected Extensible Authentication Protocol (PEAP), a wireless security standard for authentication. PEAP provides for the secure transport of authentication information across wireless connections by tunneling between PEAP clients and the authentication server (Messmer, Fontana, & Cox, 2002). Other organizations have developed similar technologies such as TTLS.

There are architectural considerations that can be made to help mitigate the exposure to attacks via your WLAN. For instance, you can place your wireless access point (AP) on the outside of your corporate firewall, and require wireless users to utilize VPN as your remote users would. This would ensure that all transmissions are encrypted and user identification has been verified. This also reduces much of the administrative burden that can accompany securing a wireless network. This is because the added administration is absorbed by your VPN solution.

Much of the problem with wireless security is not a matter of technology. It rather stems from user use, and lack of awareness. Many wireless devices are installed with default configurations, which are typically with all security features turned off. An awareness of these security features and their use would go along way to reducing the exposures WLANs present.

An organization can start by instituting a policy controlling how WLANs are deployed. If it is your goal to restrict wireless access to just your corporate users, it may not be a bad idea to institute the following requirements:

1. Do not broadcast your Service Set Identifier (SSID). The SSID is the name of your wireless network, and is required to access your WLAN.
2. Require only specified MAC addresses to communicate with your WLAN.
3. Enable encryption on all wireless APs.

A corporate security policy is a must in the information age. Inclusions need to be made to your corporate security policy for wireless networking. Regardless of your company's position on the subject, this should be formally stated as policy. Those charged with the security of a company's electronic

information must lead the organization to an awareness of the security implications of wireless networking, and provide direction to protect it.

Wireless in Business

Wireless customers spent $1.6 billion in 2002 in the technology, and are expected to spend $2.72 billion by 2006 (Greene & Cox, 2003). This expected growth further exacerbates the potential risks of wireless security, and increases the need to raise awareness, and develop supporting technology.

A number of businesses are offering free wireless access. These "hot spots" as they are known, are an extremely convenient means of gaining Internet access from a variety of public places such as hotel lobbies, airports, and Starbucks coffee shops.

Starbucks has created a new revenue stimulus for the company with its roll out of more than 2,100 wireless hot spots in the U.S. Estimates say wireless customers are staying in the coffee shop twice as long as regular customers (Cox, 2003). That's more coffee to sell to the weary web surfer.

Even fast food giant McDonald's is getting in on the action. They plan to offer an hour's worth of free wireless Internet access with the purchase of a combination meal (Pruitt, 2003).

Not all businesses are convinced the technology is where it needs to be for full adoption into corporate networks. Electronics retailer Best Buy ordered its wireless networks shutdown upon learning they had been compromised (Communications Today). The Minneapolis-based company had deployed WLANs to connect some of its cash registers to the corporate network. Once the network was hacked into, the exploitability of wireless networks became apparent to the organization. Thus a need to further examine its use in environments where data integrity is essential.

Conclusion

Wireless networking has a great deal to offer an organization. It provides un-tethered access to its information resources. Corporations can appreciate increased productivity will reducing cabling costs. The omnipresent network access adds a level of convenience that often overshadows the lurking threats of an unsecured medium.

As a result of the rapidly growing popularity of wireless networking, management will need to weigh heavily the benefits of WLANs and the risks they pose to the organization. The information security professional will need to be evermore vigilant in his/her efforts to protect against the misuse of wireless technology. The information security leadership within an organization will need to assess and measure the risks posed by this technology, and make sound decisions regarding the deployment of wireless networks.

References

ABC Action News. A news report on war driving. Retrieved March 18, 2003 from the World Wide Web: http://www.abcactionnews.com/video/news/2003/02/0226wardrivers.html

Buckler, G. (Sep. 13, 2002). Warchalking a threat to LANs: WEP isn't enough to secure your wireless LAN as it's only 40-bit encryption technology. You want at least 128-bit encryption. Retrieved March 18, 2003 from the World Wide Web: http://www.findarticles.com/cf_0/m0CGC/2002_Sept_13/91929326/print.jhtml

Communications Today (May 3, 2002). Retailer Cites Wireless LAN Issues. Retrieved March 18, 2003 from the World Wide Web: http://search.pbimedia.com/search97cgi/s97_cgi?action=View&VdkVgwKey=%2E%2E%2Fdocuments%2Farchive%2Fct%2F2002%2Fct05030207%2Ehtml&DocOffset=12&DocsFound=121&QueryZip=best+buy&SourceQueryZip=%28%28%28ba%2Cbbn%2Cbm%2Cct%2Cecn%2Cfon%2Cis%2Cidtv%2Csatn%2Cst%2Cta%2Cvia%2Cwdn%29%3Cin%3Epublication%29%3Cor%3E%28%28%27www%2Etelecomweb%2Ecom%27%3Cin%3Evdkvgwkey%29%29%29&Collection=sites&Collection=archive&SortSpec=&&ViewTemplate=new_tweb_view_wrap.hts

Cox J. (March 20, 2003). Starbucks Gives Update On Wireless Rollout. Retrieved March 26, 2003 from the World Wide Web: http://www.nwfusion.com/news/2003/0320starbucks.htm

Greene, T., & Cox, J. (March 10, 2003). Securing WLANs still a hit or miss proposition. NetworkWorld, 20(10), 74.

Messmer, E., Fontana, J., & Cox, J. (Sept. 23, 2002). Microsoft, Cisco Prepare for PEAP Show. Retrieved March 18, 2003 from the World Wide Web: http://www.nwfusion.com/news/2002/0923peap.html

Pruitt, S. (March 11, 2003). Intel, Microsoft Pair Fast Access With Fast Food. Retrieved March 26, 2003 from the World Wide Web: http://www.nwfusion.com/news/2003/0311intelmcdon.html