Running Head: WIRELESS NETWORKING FOR SMALL BUSINESSES

Wireless Networking for Small Businesses

Russell Morgan

East Carolina University

Abstract

Computer use in small businesses is arguably one of the biggest enhancements to the business world in recent history. When computers were first introduced to small businesses they were helpful for specific tasks such as running a small inventory database. In the late 1980s and early 1990s when local area networks began appearing in small businesses the benefits of computers increased. Now users could easily and quickly share files and printers. This enhanced productivity greatly for many firms. With the explosion of Internet connectivity and use in the 1990s, many small and medium businesses can now compete on the international stage. The introduction of wireless networking in the late 1990s and early 2000s was another major shift in computing. Wireless networks offer many benefits, but also pose some significant security issues. This paper looks at the potential benefits and security issues of wireless networking from the perspective of small and medium businesses.

Wireless Networking History and Benefits to Businesses

What we know today as wireless, or Wi-Fi networking has evolved from the IEEE 802.11 publication of 1997. This standard called for wireless transmission rates of 1 and 2 megabits per second (Mbits/s) to be transmitted on the 2.4Ghz band. In 1999 the 802.11b amendment was published. This amendment called for wireless transmission speeds with a maximum transmission rate of 11 Mbits/s (Wikipedia, n.d.). This was the first version of wireless networking adopted by mainstream users and the business community.

Wireless networking gained more momentum and speed in 2003 when 802.11g was ratified. The G specification calls for maximum speeds of up to 54Mbits/s and is backwards compatible with 802.11b (Wikipedia, n.d.). The increasing speeds made wireless even more attractive to users. As a result businesses began to deploy more wireless networks. Today it is estimated that there are nearly110 million wireless notebooks in use (Khalil, 2004).

The adoption of wireless networking happened about as fast as the changes in the standards. Businesses and home users alike saw great benefits to going wireless. In 2004 it was estimated that the number of small businesses using wireless LANS increased 28 percent (Simonds, 2004). Among the benefits to going wireless are flexibility and cost savings. Both of these benefits can be seen when companies are looking to expand either their workforce or their workspace. Richard Stone, a wireless mobility manager at HP, estimates that expanding a wireless network is 30 percent cheaper than pulling new

cables (Simonds, 2004). Another benefit of the flexibility is that computers can be used anywhere in the coverage range. Companies are no longer required to wire every wall or desk area. Thanks to wireless networking, areas that were never intended to be collaborative workspaces due to wiring limitations can now be used as such (Welch and Lathrop, 2003).

Printers with wireless networking built in and hand held scanners used by inventory clerks are some other devices that can be used on wireless networks. Maintenance technicians can also use wireless to communicate with the network while working on HVAC or manufacturing systems. Wireless devices are also useable in Wi-Fi Hot Spots, which can be found in many airports, hotels and coffee houses. This allows workers to stay connected while on the road. New Wi-Fi enabled devices are on the way so in the future there will be even more advantages to going wireless. For many businesses and home users there may be no need for wired networks in the near future.

Wireless Disadvantages and Security Threats

When there are so many positive things about a technology there are bound to be some problems as well. One of the first problems with wireless networking is that current equipment operates on the 2.4Ghz ISM band, which is fairly crowded. The 2.4Ghz band is home to a myriad of devices including Wi-Fi, Bluetooth, HomeRF, cordless phones, wireless audio headsets and even microwave ovens (Russell, 2001).

Another potential problem with wireless networking is the fact that signals do not travel as far in some environments as they do in others. Buildings with a lot of metal or

concrete walls will require range extenders or multiple access points to provide the required coverage. Buildings with mostly wood and drywall construction are much easier to cover (Moran, 2002). Crowded wireless bands and building limitations are relatively minor problems when compared to the potential security threats wireless networks face.

Traditional wired networks are generally considered to be more secure than wireless networks due to the fact that they are contained in physically secured buildings. Wireless networks on the other hand can penetrate walls and cross parking lots or streets. 802.11b networks can even be accessed up to one half mile away in some instances (Welch and Lathrop, 2003). This makes wireless networks much less secure due to the fact that someone can access them without being near your facility. Wireless networks are also vulnerable to some of the same attacks that affect wired networks such as session hijacking and man in the middle attacks (Welch and Lathrop, 2003).

Unauthorized wireless network access is probably one of the biggest threats to small and medium sized businesses. This is described as a user from outside the company using the network (Welch and Lathrop, 2003). Unauthorized access can be something as simple as a neighboring business using the wireless LAN to access the Internet. If the unauthorized user is just surfing the Internet it would not present a very big problem except for potentially slowing your network down. As an example, the owner of a video rental store in New York City, was having trouble connecting to his wireless network. When he called for tech support, he learned that many of his neighbors were using his wireless service. At that point, he enabled some security mechanisms on

his network and now his system is fast and reliable (Miller, 2006). In the previous example the only issue was limited access to the wireless network. If the unauthorized user of your wireless network were doing something illegal, however, you could be held liable.

Not only can neighboring businesses easily detect and use your wireless network there is a whole Internet community devoted to war-driving or war-walking. This involves someone driving or walking around with a wireless scanner searching for wireless networks. When they find an open network they can either use it or submit it to sites on the Internet such as http://www.wifimaps.com . These web sites are great tools for users that are looking for unsecured wireless networks for whatever purpose.

Another threat to wireless networks is traffic analysis. This is like a virtual stakeout where the attacker simply monitors the network activity, compiling information about patterns of wireless communication (Karnik and Passerini, 2005). If this traffic is unencrypted it would be very easy for your private information to be compromised.

Eavesdropping is an attack that can be carried out either actively or passively. Passive eavesdropping is when an attacker monitors network traffic. This can allow the attacker to clearly see unencrypted traffic. If the traffic is encrypted he can still gain information about traffic patterns. Active eavesdropping is when the attacker injects packets into the data stream in an attempt to decode the transmission (Welch and Lathrop, 2003).

Another attack vector is the Denial of Service (DoS) attack. During this attack the network is hit with a strong frequency generator, which disrupts access by legitimate clients (Karnik and Passerini, 2005). Even though they are not legal there are several devices available for purchase over the Internet that can jam cellphones, cordless phones and wireless network communications (Russell, 2001). A different version of the Denial of Service attack is the unauthorized user or users. While they may not be intentionally trying to deny access to your network if they generate enough traffic the connection can still become saturated thus denying legitimate users access.

Most access points are fairly easy to set up and configure. This makes it easy for someone to install a rogue access point. An access point that is not set up by the network administrator is referred to as a rogue access point. Rogue access points can be used to trick users into sending critical information through them in an effort to access the company network.

All they need is access to a network jack and a few minutes and their access point can be up and running. Man in the middle attacks can be used to read data from the wireless session or to modify the traffic violating the session integrity. During the man in the middle attack an attacker will break the initial connection between the wireless client and the access point. Then when the connection is re-established a machine in the middle of the connection can read all the data and take information as needed (Welch and Lathrop, 2003).

One final security issue to think about is the home user connecting to the corporate network via a wireless device. The best corporate security can be compromised

by a home user operating on an unsecured network or PC. Accessing a corporate network from a home network can present hackers with an easy opportunity to enter an otherwise secured site, gaining access to important company data (Hole, Dyrnes and Thorsheim, 2005).

Wireless Security Options Past and Present

Securing a wireless network is more complicated than securing a physical location such as a bank vault (Russell, 2001). To secure the vault placing a lock and a guard at the single entry point would provide enough security in most cases. With a wireless network however, not only does the access point need to be secured, but security must also be provided on the airlink and the end user computers.

As wireless technology has evolved the security mechanisms available to secure the networks have evolved as well. The first security mechanism for 802.11 networks was Wired Equivalent Privacy (WEP). The goals of WEP were to provide access control, confidentiality and data integrity. Access control is defined as keeping unauthorized users off the network. Confidentiality is the prevention of eavesdropping and ensuring that only authorized parties can view network data. Data integrity means ensuring that the network traffic has not been tampered with (Boland and Mousavi, 2004). While the goals of WEP were admirable, it failed to live up to them. WEP uses a relatively weak encryption mechanism. The encryption is a combination of a 40-bit WEP key and a 24-bit Initialization Vector (IV). The limited 24-bit IV meant that eventually the IV would have to be reused, which could allow an attacker to crack the WEP key. The implementation of WEP will probably stop casual war-drivers, but an experienced

attacker can crack the WEP key on a busy network in as little as 15 minutes (Wong, 2003).

Given the weakness of WEP, the industry decided they could not wait on the IEEE to fully develop and finalize 802.11i. 802.11i was going to address all the issues with WEP, but it was slow to develop. So in 1999 the Wi-Fi Alliance was formed. Composed of wireless equipment manufacturers the Wi-Fi Alliance is a nonprofit international organization working to certify the interoperability of wireless local area networking products based on 802.11 (Wong, 2003). The first standard proposed by the Wi-Fi Alliance was Wi-Fi Protected Access (WPA).

WPA was an interim solution to address the shortcomings of WEP. WPA was developed using a subset of the upcoming 802.11i standard. The main advantages of WPA over WEP are the use of Temporal Key Integrity Protocol (TKIP), easier setup using a pre-shared key and the ability to use RADIUS-based 802.1x for user authentication (Moran, 2002). WPA can operate in Personal or Enterprise mode. The Personal mode uses a shared key while the Enterprise version incorporates RADIUS authentication and 802.1x port based authentication.

In June 2004 the 802.11i amendment was ratified bringing a much more advanced security standard to the wireless world. Several months later in September 2004 the Wi-Fi Alliance released WPA2 based on the 802.11i standards. The main difference between WPA and WPA2 is that WPA2 implements government level security by using National Institutes of Standards and Technology FIPS 140-2 compliant Advanced Encryption Standard (AES) (WI-FI Alliance, n.d.). AES is an encryption algorithm for securing

sensitive but unclassified material by the US government (Pacchiano, n.d.). Like WPA the stronger WPA2 also operates in Personal and Enterprise mode.

Methods Small Businesses Can Use to Secure Their Networks

Attacks to wireless networks can be either targeted attacks or attacks of opportunity. Targeted attacks are explicitly aimed at a network because the attacker wants something specific from that network. These attacks, while potentially being the most severe are not all that likely. Most networks are attacked because they are good targets of opportunity. A target of opportunity is when someone sees open or lightly secured network and connects to see what they can find (Potter, 2003).

Given the large number of threats to wireless networks many business owners would ask if the benefits of wireless networking outweigh the threats. For many small and medium sized businesses the answer to that question would be yes. By taking the appropriate steps to secure your wireless access points your business can enjoy the benefits of wireless networking without worrying about attacks of opportunity. Targeted attacks still pose a threat, but the risks can be mitigated.

Security for wireless networks is a layered process just as it is for wired networks. None of the steps listed below are sufficient by themselves to secure the wireless network. When you combine several, or all, of them however, a robust solution can be implemented that will keep all but the most determined and skilled hackers out.

The first step towards securing the wireless network is to change the Service Set Identifier or SSID of the access point. The SSID is essentially the network name. Every

wireless network has a name and most devices come with one pre-configured. For example the default SSID on a Linksys device is Wireless or Linksys (Cirt.net, n.d.). While the name itself is not a security device it is important to change it from the default. These access points also have a default username and password configured on them. If the name of the device is being broadcast, a quick Google search will return the default login credentials (Google, 2006). This would allow a malicious user free reign on the access point. They could then give their computers full access or even lock you out of your own network. Besides changing the SSID some people recommend disabling SSID broadcasting. This is a means of security by obscurity. It does not give you any security against someone with a wireless sniffer, but it would keep out the low-level war-drivers or war-walkers.

Every networking device comes with a unique Media Access Control address commonly known as a MAC address or sometimes a hardware address. Many access points allow you to set up access lists so only devices with their MAC address listed in the table can use the network. Filtering with MAC addresses is not a foolproof security measure, but it will help keep the common war-driver out. Determined hackers with the proper scanning devices can intercept network traffic and pick out legitimate MAC addresses. They can then fake a legitimate address on their device and access the network. This is something to worry about, but it is not a huge issue unless you are a frequent target of attacks.

Most, if not all, wireless access points come with some kind of built in encryption mechanism. These are usually very easy to turn on, but amazingly enough many

networks are operating unencrypted (Hole, Dyrnes and Thorsheim, 2005). Older devices only supported WEP, which was not a very strong encryption algorithm. Even though WEP is not a strong security algorithm it is better than nothing and will keep many casual war-drivers out of your network.

Newer devices come with WPA or WPA2 encryption. This is a much stronger encryption algorithm than WEP and was developed to address the weaknesses in WEP (WI-FI Alliance, n.d.). WPA and WPA2 can operate in Personal mode, which would be suitable for most home and small offices. This is a shared key mode and would be easily compromised and hard to manage in a large environment. For larger networks WPA or WPA2 would be used in Enterprise mode. This mode allows users to be validated on a RADIUS server, which would prevent random computers from attaching to the network. Some WPA devices can be upgraded to WPA2 via software patches (Pacchiano, 2005) giving some older devices a longer lifespan. If the networking devices currently in use are not WPA2 compatible it is recommended they be replaced with devices that are.

Sometimes a security mechanism can be fairly low tech and still provide significant protection. One example of this can be seen with the wireless network signal. Using a directional antenna can direct the wireless signal so that it does not broadcast as far outside the intended area. Another option available on some access points is to limit the signal strength, which would also keep the signal from traveling too far outside the company's walls. Both of these methods can be used to help keep unauthorized users off the network (Pacchiano, n.d.).

Segregating wireless traffic from wired traffic with a VLAN or a DMZ is another option businesses can consider. By segregating wired and wireless traffic, users could be allowed to access wireless devices to access certain servers or an Internet connection without putting high security servers or data stores at risk.

Another security option is to have wireless clients connect through a Virtual Private Network (VPN). VPNs provide a secure, encrypted link between client and server so if the wireless traffic was being analyzed the data would still be encrypted. This is a great option for users connecting from Wi-Fi Hot Spots or from home networks.

WPA or WPA2 operating in Personal mode would be sufficient for many small businesses. Some, however, may want to use the stronger authentication features of Enterprise mode. Even though it is called Enterprise mode these features can be deployed on a small business budget. Windows Server 2003 has the necessary features built in to authenticate 802.1x wireless clients. Internet Authentication Server is the Microsoft implementation of a RADIUS server. IAS can handle authentication and authorization of wireless clients (Weston, 2005).

Conclusion

Wireless networking technology is relatively new and is still evolving in performance and security. A lot of progress has been made in regards to speed, reliability and security since the original 802.11 standard was ratified. Wireless networks are capable of performing as well as wired networks for many purposes. As the technology matures they will replace wired networks in many cases due to the flexibility and cost

savings. With proper planning and implementation any business should be able to benefit from a wireless network.

References

Anonymous (n.d.) *Default Wireless Configurations.* Retrieved April 8, 2006 from http://www.cirt.net/cgi-bin/ssids.pl?method=showven&ven=Linksys

Anonymous (n.d.) *Google search: Default Password Linksys Router.* Retrieved April 8, 2006 from http://www.google.com/search?hs=Btz&hl=en&lr=&client=firefox-a&rls=org.mozilla%3Aen-US%3Aofficial_s&q=default+password+linksys+router&btnG=Search

Anonymous (n.d.) *IEEE 802.11.* Retrieved April 2, 2006 from http://en.wikipedia.org/wiki/802.11

Anonymous (n.d.) *WI-Fi Alliance Knowledge Center.* Retrieved April 2, 2006 from http://www.wi-fi.org/glossary.php?letter=W&glossary_id=162

*Arbaugh, W. A. (2003) *Wireless Security is Different.* Computer, Aug 2003 Volume 36, Issue: 8. pp 99-101

*Boland, H and Mousavi, H. (2004) *Security Issues of the IEEE 802.11b Wireless LAN.* Canadian Conference on Electrical and Computer Engineering May 2-5, 2004 Volume 1. pp 333-336

*Hole, K.J, Dyrnes, E Thorsheim, P. (2005, July) *Securing Wi-Fi Networks*. Computer Volume 38, Issue 7 pp 28-34

*Karnik, A. and Passerini, K. (2005) *Wireless network security – A discussion from a business perspective.* 2005 Wireless Telecommunications Symposium, April 6-7 2005. pp 261-267

Khalil, M. A. (2004) Vision to Reality: Applications of Wireless Laptops in Accessing Information from Digital Libraries: End-Users' Viewpoints.* Library Hi Tech News. Number 7 2004, pp25-29

Miller, D.I. (2006) *Protect your business's wireless network.* Retrieved April 1, 2006 from http://www.cnet.com/4520-10192_1-6411694-1.html

Moran, J. (2002) Wireless Home Networking, Part V - Interference and Range Extension. Retrieved April 2, 2006 from http://www.wi-fiplanet.com/tutorials/article.php/1497111

Pacchiano, R.(n.d.) *Making a Case for Wireless Network Security: Going to the Extreme with Wireless Security.* Retrieved April 2, 2006 from http://www.winplanet.com/article/3074-.htm

*Potter, B. (2003, July-Aug) *Wireless Security's Future.* Security & Privacy Magazine, IEEE pp68-72

*Russell, S. (2001, April) *Wireless Network Security for Users.* International Conference on Information Technology: Coding and Computing, 2001 Proceedings. pp. 172-177

Simonds, L. (n.d.) *Step Up to Wireless Networking*. Retrieved April 2, 2006 from http://www.wi-fiplanet.com/tutorials/article.php/3360721

*Welch, D. and Lathrop S (2003) *Wireless Security Threat Taxonomy.* Information Assurance Workshop, 2003 IEEE Systems, Man and Cybernetics Society June 18-20 pp 76-83

Weston, B. (2005) *Step-by-Step Secure Wireless for Home / Small Office and Small Organizations.* Retrieved April 2, 2006 from http://www.microsoft.com/downloads/details.aspx?familyid=269902e8-fc41-4eb1-9374-44612e64f0fb&displaylang=en

* Wong, S. (2003) *The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards*. May 20, 2003. Retrieved April 2, 2006 from http://www.sans.org/rr/whitepapers/wireless/1109.php