Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Wireless Computing - A Technological Breakthrough Laden with Risk?

With all the pluses for wireless computing, cries of dangers of the unknown remain in our mixed. There are unresolved issues of security, privacy, interoperability and possible health hazards associated with long-term-routine exposure to the radio frequencies generated by these systems.

Copyright SANS Institute
Author Retains Full Rights

AD

WIRELESS COMPUTING – A TECHNOLOGICAL BREAKTHROUGH LADEN WITH RISK?

INTRODUCTION

"That which is looked upon by one generation as the apex of human knowledge is often considered an absurdity by the next, and that which is regarded as a superstition in one century, may form the basis of science for the following one!"[2] *Paracelsus*

The above quotation seems a good way to start a discussion about wireless computing. The technology is new, in early stages and exciting to many about its future; yet to others, it is confusing and a source of great anxiety for similar reasons, what the future holds. Both feelings, conflicting as it may be, is legitimate when looked upon from the different perceptive. Innovations in technology are not static; technological innovations always probe for uncharted territories to explore and dominate. Wireless computing seems to be the natural next stage in computer connectivity due to present nature of the business environment. Wireless LANs allow the connection of PCs, printers, servers, and any network devices, by replacing wired cables with radio frequencies or infrared beams.

As many institutions and corporations struggle to find better ways to interconnect local area networks (LANs) that they have in operation at various locations to form a wide area network (WAN), the solution they are looking towards is Wireless connectivity. As more people seek quality-of-life perks in their careers, having the ability to stay connected to the office while travelling wherever they may wish, wireless connectivity is verging to become the de facto standard for doing local, national and international business. To remain competitive, many organizations are being forced to deploy mobile devices to employees. The employees, using handheld wireless devices, such as some mobile phones, PDAs, smart phones and other communicators, are able to access information from corporate networks or web sites. They can engage in mobile commerce (m-commerce) from anywhere and at anytime because businesses are being driven by the need for Internet access wherever they are, not just where their offices are. In addition, consumers are demanding more information in more places - that means mobility, which demands wireless connectivity to the Internet. With all the pluses for wireless computing, cries of dangers of the unknown remain in our mixed. There are unresolved issues of security, privacy, interoperability and possible health hazards associated with long-term-routine exposure to the radio frequencies generated by these systems.

Wireless network bridges, using spread spectrum radio waves or microwaves, can be used to connect LANs that are separated by as much as 25 miles. Wireless links can provide data transfer rates from less than 1 Mbps to more than 10 Mbps.[1]

Wireless computing functions according to prescribed standards. There are different standards out there. Some proprietary, others are non-proprietary. Two popular non-proprietary standards are: Wireless Application Protocol (WAP), and Bluetooth. WAP is an open non-proprietary standard developed by consortium companies organized as WAP Forum. The primary goal of the WAP Forum is to bring together companies from all segments of the wireless industry value chain. This ensures product interoperability and growth of wireless market. WAP Forum

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

members include companies such as IBM, Compaq, Lucent Technologies, Oracle and many others as listed here. For more information about WAP Forum, visit http://www.wapforum.org/.

Bluetooth wireless technology is a specification designed to enable wireless communication between small, mobile devices. Functionally, Bluetooth is no different than a physical cable. The key difference is that Bluetooth uses a radio link to connect devices instead of a cable. The Bluetooth Special Interest Group (SIG) is propagating Bluetooth standard. SIG is headed up by industry leaders 3Com, Ericsson, IBM, Intel, Lucent Technologies, Microsoft, Motorola, Nokia, and Toshiba. For more information about bluetooth, visit http://www.bluetooth.com/. Other standards, proprietary in nature exist, such as NTT DoCoMo's i-Mode service, My Sprint PCS Wireless Web and AT&T's PocketNet solution. These proprietary standards only work on their carrier's network.

ISSUES FOR AND AGAINST WIRELESS COMPUTING

A ground swell of interest in Wireless computing has begun among business entities. They have taken keen interest in the success of secured Wireless technology. The interest is borne out of self-preservation as businesses now realize that the success or failure of the technology will affect the bottom line. Realize that, as corporations embrace the new technology, mobile, handheld computers are accessing growing pools of sensitive information ranging from business plans to financial data. Further more, the trend towards mobile commerce (m-commerce) as an outlet to improve e-commerce has raised the longing of corporate executives for a secured wireless technology. The technology is touching business travelers. One only needs to visitor any major airport in the country to witness the increasing trend towards wireless computing. Busy men and women, with laptops at their sides, Palm Pilots in their pockets and, usually, mobile phones glued to their ears crisscrossing airport terminals. These business officers travel around the globe to negotiate or close transactions of all kinds. To these people, using mobile devices and the interaction it provides with base office is a business advantage. To them, security of wireless devices is paramount.

Many casual talks about wireless computing in offices and elsewhere always hover around challenges confronting the technology. Just as I was writing this project, one of my colleagues asked what my project was on, before I could finish telling him, his comment was “Wireless computing is fraught with problems”[15]. Other remarks I have read or heard include:

- That the increasing sophistication of handheld devices makes them vulnerable to the same type of destructive software already plaguing computer users.
- That more mobile computing will mean more viruses, more malicious code and more hacking.
- That part of the attraction of virus writing is to spread them to as many computers as possible, hence virus writers are waiting to unleash virus mayhem on handheld computers as the number of the device multiply.
- That PDAs run specially written scaled-down operating systems, such as EPOC, PalmOS and PocketPC. They are often connected to home or office PCs to synchronize the data on the two machines. This presents an opportunity for viruses to spread onto them.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- That wireless communications obviously provide potential security issues, as an intruder does not need physical access as in the traditional wired network in order to gain access to data communications.
- That wireless network tends to have intermittent network connectivity -- dropping connections due to temporary signal loss, for example.
- That wireless networks often feature limited bandwidth (9600 bps or less) and long latencies (delays between requests and replies).
- That wireless network may or may not support IP.
- That mobile viruses will be easier to write (due to easy access to information and tools for this environment), and the damage will result from links from the Internet to the existing infrastructure, unlike PC viruses which tend to limit themselves to affecting the computer world only.
- That wireless connectivity poses a number of security risks. First, it is no longer necessary to tap a wire to intrude into a wireless network - the data is everywhere. Second, wireless devices need adequate logical access controls, in particular authentication.
- That an intruder could, for instance, steal sensitive information without being noticed from an unprotected PDA or cell phone in an airport lounge or a restaurant.
- That any device with a wireless port turned on is a potential target for an intruder.
- That the bundling of many wireless services, including the global positioning system (GPS), on a single platform (e.g. a mobile phone or a PDA) may pose new threats to individual privacy.

The prospect of ubiquitous wireless devices in every hand, contributing to wireless computing is very attractive to many. Some have surmised that our imagination and the justifiable concerns for security are the only two things holding back the spread of wireless technology. Yet the potential drawbacks to a wireless solution including environmental factors are not often discussed. For example, terrain may eliminate wireless as an option. Intervening hills and tall buildings or trees can block the radio frequency (RF) signals. Wireless RF technology is referred to as "line-of-sight". This means that the antennas on the wireless bridge units must be able to "see" each other; there must be no obstacles in the way to block or reflect the transmitted signals. Severe weather, such as torrential rains, can adversely affect signal transmission and temporarily down the link. Similarly, the link might be susceptible to other radio frequency interference. Dense fog could possibly be a problem for microwave links.

However, wireless advocates maintain that, wireless connectivity must be seriously considered if the terrain allows its use. They state that microwave links can be more reliable than leased data lines.

The hype and enthusiasm over wireless local area networking is worrisome in some quarters. They cringe at what they see as lack of adequate attention paid to potential health hazards associated with long-term-routine exposure to the radio frequencies generated by the system.

They advice that the issue of wireless networking, for example, ought to be pursued with a lot more prudence and caution than seems to be the case. The prospect of unsuspecting workers or students, as the case may be, using wireless LANs everyday, being exposed to radio frequency emissions at close range, deserves attention given the level of ignorance on this issue, they will

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

argue. They maintain that no one really knows for sure whether this sort of radio frequency exposure is safe or a significant health hazard!

However, The Wireless LAN Association, (WLANA) a trade association of wireless industry companies has tried to dampen concerns about wireless LAN and the health question. WLANA not long ago sponsored a research study titled: "Do Wireless LANs Pose a Health Risk to the Consumer?" [16]. At the end of the research, the study concluded "Manufacturers of Wireless Networking products design their products to operate within the guidelines of these standards and recommendations and, therefore, are considered safe" [16]. What a conclusion! The judgement is yours (the reader). The question one ponders is whether the conclusion reached by the study will alley fears about the safety of wireless computing.

SOLUTIONS FOR SECURITY AND OTHER CONCERNS

The overwhelming concern regarding wireless computing centers on the issue of security. The success or failure of this technology appears to hinge, largely on this one issue. All other concerns seem minuscule in comparison. Any time a new technology is widely adopted, some people will look at ways to understand and exploit it. Wireless computing is no exception.

The security concerns revolve around - Virus infection, theft of mobile devices, and theft of data. The solutions to these concerns are can be found even though none is full proof. Companies or entities can choose combination of solutions that will work best for them.

Virus infection

Viruses can infect wireless devices as other wired computers. In fact, there are records of virus infections to mobile devices. There is a virus called Palm/Phage, which is able to infect Palm OS, but it is not in the wild and poses little threat. Nonetheless, it is sensible to keep backups of any Palm applications and data. There is also a trojan horse known as Palm/Liberty-A, which is able to infect the Palm OS. It deletes Palm OS applications. Like Phage, it is low risk and you are unlikely to ever encounter it. The question one ponders is, can mobile devices be protected from virus? The answer yes, I may add that one of the most efficient way to protect mobile devices is to check data when you transfer it to or from the device. Other ways to guard against virus infection on mobile devices include:

- Do not accept attachments that come by e-mail on handheld devices, and get anti-virus products installed.
- Always backup your information with a trusted, tested system.
- Synchronize your handheld regularly with your PC that has the latest anti-virus software.
- Educate end-users they should verify the source and authenticity of email and email attachments and never install games from unknown sources.
- Take advantage of anti-virus products with small signature file updates for remote updating.

The anti-virus product should not only scan the device, but it should also have the ability to scan the files that are being sent to the PC during synchronization. This protects the device, the PC it is synching with and the network.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Device theft

The theft of unprotected notebooks, PDAs or mobile phones is rampant. According to a recent study by Safeware, a computer insurance company, an estimated 319,000[13] laptops were stolen in the United States in 1999. Laptops, PDA and other wireless devices are certainly the easiest kinds of computers to steal. They are small, light weight, easily concealed, and easily resold on the black market. They can be taken home by a jealous co-worker or stranger, or used to gain access to company systems and proprietary data. Whether it's at the airport, the hotel or the office, thieves are looking for that inattentive moment to grab your wireless device and computer. In reality complex industrial espionage perpetrated by competitors or free agents is still with us. It is possible there are bounties on important laptops and mobile devices. No one can predict where their stolen devices will end up and who will eventually come to peruse the data on them. While there is no single reason for these devices being pilfered, the risk is too high not to protect against them.

The good news is you are not powerless. There are steps you can take to protect your mobile equipment. Here are come safeguard tips:

- Lock your laptop and mobile device in your desk when leaving the office
- Secure your laptop with a cable and put an alarm on your mobile device.
- Permanently engrave your company's name and ID on the equipment
- Keep the serial number, make and model information of your laptop and mobile device separate from the computer.
- Never save passwords in the computer or store them in the computer bag.
- You may even turn to innovative technologies like radio wave-based proximity cards, card keys that shut down computers when the particular users are out of range.

In summary, business travelers should be mindful that mobile device, so easily carried around by them is a major target for thieves. They should always use common sense security measures. Realizing that even a conscientious employee could experience loss and theft underscores the necessity for companies to provide adequate security on mobile devices in advance.

Data theft

Eavesdropping, fraud, identity theft and other invasions are all feasible acts that today's savvy crackers could carry out. A report published in 1999 by Price- waterhouseCoopers revealed that data theft is costing organizations and government entities billions of dollars on an annual basis. It found that breaches of systems were causing about $1.6 trillion[12] in damages worldwide. One can only imagine what that figure will become as wireless devices become the main tools for computing and connectivity to organization's networks.

Without proper security an attacker can 'grab' data that is transmitted through the air without anyone even knowing he or she is listening. If proper hardware security is utilized, and virtual private network (VPN) tunnels are used to transmit data from the handheld through the wireless channel, data can be made safe.

Here are some tips to protect your information from theft:

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- Use access control software to protect proprietary information and the computer
- Use encryption programs to safeguard critical information.
- Use smartcards and biometrics, namely fingerprint authentication, to safeguard data on laptops, cell phones and PDAs. What good is the data if it is not exclusive or not protected?
- User wireless VPN, PKI solutions, encryption products, other authorization security tools and access control systems to strengthen security in wireless computing.
- Before widespread adoption of mobile devices, ensure practical defensive techniques, such as data encryption are in place.

Professionals are reminded that since mobile devices are not directly linked to the overall corporate security environment, they remain vulnerable points. Often outside the corporate firewalls and used in public areas, wireless devices can cost a tremendous amount of losses if not protected.

General issues.

The increasing use of laptop computers within the enterprise, and the increase in worker mobility has fuelled the demand for wireless networks. Wireless technology used to be a patchwork of incompatible systems from a variety of vendors. The technology was slow, expensive and reserved for mobile situations or hostile environments where cabling was impractical or impossible. With the maturing of industry standards and the deployment of lightweight wireless networking hardware across a broad market section, wireless technology has come of age.

To make the technology work better is the business of every user. Stakeholders should make effort to secure communications in wireless computing, just as they have done to safeguard wired networks.

Prudent managers will minimize risk of mobile devices by deploying a combination of access controls, user authentication and automatic encryption to the devices. The access control prevents illicit users from even getting to the operating system where the thief could then employ widely available software tools that subvert the operating system or extract passwords.

In addition to making employee security awareness and training a component of organization's overall security approach, listed below are tips for a more secure wireless computing:

- Make corporate wireless security proactive and preventive. Every wireless device used in business should have layered and credible security measures.
- To convince employees to take security policy seriously, managers and upper level management should take strong stance on security, and enforce the policy by encouraging people to use the security tools provided properly and effectively. Research bears out that losses to companies that use wireless devices are usually due to lax mobile security policies and too few protective measures
- Reduce the complexity and security risks created by adding mobile devices to the network by deploying a single security system that provides access management for both web and wireless web applications. This provides a single point of control for setting, monitoring and enforcing security policies. Furthermore, a single-access management system that uses

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

business rules to protect individual resources and control user access eliminates the need for human intervention every time a change occurs in a user's profile.

- Assign trained people to maintain security since a good security is a process that requires continuous monitoring and improvement.
- Be mindful of how much money your company's reputation is worth.
- Before letting remote systems into the corporate network, audit them for compliance with security policies.

Even as progress are made to unresolved issues in wireless computing such as Security, interoperability, scalability and other concerns, groups like WAP forum, SIG and other standardization bodies across the world are busy working on these issues to ensure wireless technology wins the approval and confidence it deserves.

© SANS Institute 2001, Author retains full rights.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Bibliography

1. Wireless Computer Networking: WANs and LANs, http://www.tcet.unt.edu/wlan.htm.

2. How Safe Is Wireless Computer Networking by Charles Moore, December 1999. http://macopinion.com/columns/roadwarrior/99/12/09/

3. Home Networking's Bitter Brawl, http://www.wired.com/news/technology/0,1282,38703,00.html

4. Fast WAN could rival Bluetooth. http://www.netimperative.com/technology/newsarticle.asp?ArticleID=11550&ChannelID=3&ArticleType=1

5. Introduction to WAP: WAP supports the delivery of Web content over wireless networks http://compnetworking.about.com/library/weekly/aa123000c.htm

6. Wireless Networking Q&A, http://compnetworking.about.com/gi/dynamic/offsite.htm?site=http%3A%2F%2Fwww.vicomsoft.com%2Fknowledge%2Freference%2Fwireless1.html%231

7. Mobile Device Viruses, Nothing to Worry about? by Graham Cluley. Dec' 2000 http://www.scmagazine.com/scmagazine/sc-online/2000/mobile_device_viruses/article.html

8. Fighting for Mobile Security by Illena Armstrong. SC Info Security Magazine, Feb. 2001.

9. WAP Forum http://www.wapforum.org/what/index.htm

10. FAQ about Bluetooth Wireless Technology: http://compnetworking.about.com/gi/dynamic/offsite.htm?site=http%3A%2F%2Fwww.anywhereyougo.com%2Fayg%2Fayg%2Fbluetooth%2FArticle.po%3Ftype%3DBluetooth_FAQ

11. What's Happening with WAP? by Illena Armstrong. SC Info Security Magazine, Feb. 2001.

12. Plugging the Holes in Bluetooth by Illena Armstrong SC Info Security Magazine, Feb.2001.

13. Laptop theft. Security Sense, © National Security Institute, Inc. January 2001

14. Wireless Wonders with Security Risks by *Angelo Tosi, Ph.D. Manager, Technology Risk Services, PricewaterhouseCoopers in InfoSecurity* .

15. Comment by my colleague at work.

16. WLANA research study http://www.wlana.com/learn/health.htm

17. Mobile Code Stakes its Claim by Illena Armstrong SC Info Security Magazine, Nov. 2000

18. Fighting for Mobile Security by Illena Armstrong. SC Info Security Magazine, Feb. 2001

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 24th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced