Global Information Assurance Certification Paper

Dianna E. White
GSEC Practical Assignment Version 1.3
Law Enforcement, Just Another Layer in Security; Handheld Devices, Just Another Layer in Law Enforcement
May 15, 2002

Introduction

Wireless technology and handheld devices are growing in popularity in various aspects of business, academia, healthcare, financial markets, government, and law enforcement. The focus of this paper is on the rising interest of handheld devices to the law enforcement community. This technology is still relatively new for most law enforcement agencies yet the growing need for mobility and immediate responses to inquiries make it a very attractive option. The objective of this paper is to evaluate the wireless and handheld technology and its benefits, while identifying and evaluating its vulnerabilities. There are numerous Personal Data Assistants (PDA's) on the market and it's not my intent to select one product over another but to evaluate the wireless technology and its protocols. This paper is based on my research, three years as an Information Security Officer, and twelve years of law enforcement experience. It is my intent to share this research with other law enforcement agencies still trying to decide whether Personal Data Assistants (PDA's) are worth the risks and efforts to secure it.

History of Wireless

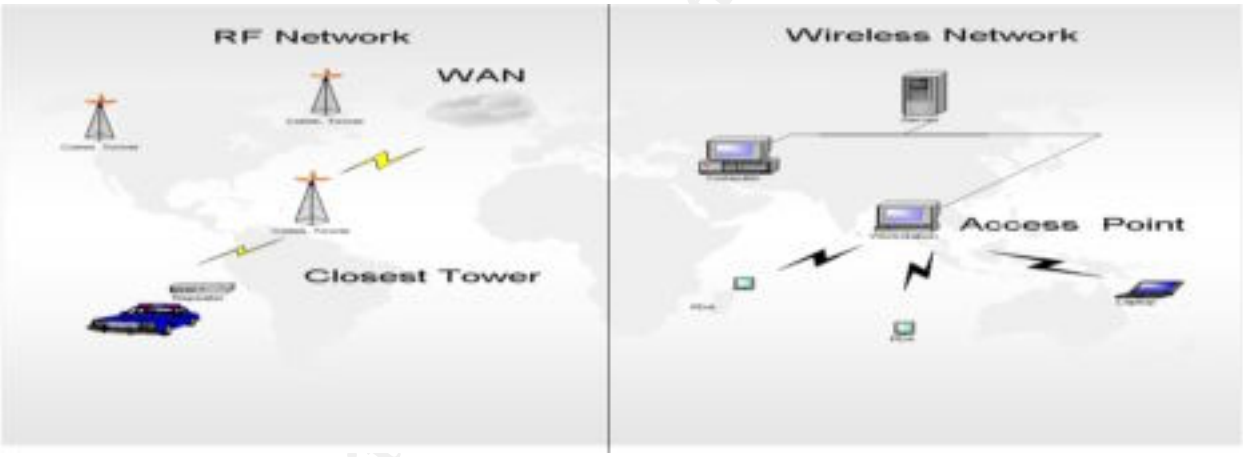
Wireless technology is based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11x protocol standards. The 802.11x protocol is also referred to as "Wi-Fi" technology. This technology uses Direct Sequence Spread Spectrum (DSSS) to generate the bitstreams to be transferred in the 2.45-GHz Instrumental, Scientific, and Medical (ISM) band.[1] The other spread spectrum technology used is Frequency Hopping Spread Spectrum (FHSS) that tends to have a lower overall performance.[2] The 802.11(b) technology provides speeds up to 11 Mb, 802.11(a) promises 50 Mb+, and 802.11(g) also promises 50 Mb+ along with backwards compatibility to 802.11(b) which is not found in 802.11(a). The disadvantages of 802.11(a) and (g) are higher costs and reduced battery life while 802.11(b) is cheaper and has a longer battery life it will eventually be phased out. However, 802.11(a) is predicted to be the de facto standard because 802.11(g) will not offer the density of users corporations need for large enterprises. [3]

There are several other protocol standards used in the area of wireless and handheld devices including Wireless Application Protocol (WAP), Bluetooth, Cellular Digital Packet Data (CDPD), and HyperLAN/2. HyperLAN/2 has been approved by the European Telecommunications Standards Institute but is used predominately in Europe.[4] Since HyperLAN/2 is not as popular in the U.S. I will focus more on CDPD, WAP and

Bluetooth. Wireless networks can use radio waves, infrared, or laser to transmit data between two network nodes.[5]

Wireless networks can either be configured as ad-hoc (Independent Basic Service Set), which have no access points or infrastructure mode (Basic Service Set), which have at least one access point.[6] Ad-hoc mode means each client talks to the other clients on the network while infrastructure mode requires communication through an Access Point (AP). A disadvantage of a single AP is the loss of the client's signal strength as proximity to the AP decreases. Multiple access points strengthen the signal as the client moves out of range of one AP and is picked up by another stronger signal. An analogy can be drawn between police radios using repeaters in the trunks of their cruisers to strengthen the Radio Frequency (RF) signal and an AP client being used to strengthen the degraded signal for wireless communications.

Illustration by Dianna White:



An association process must take place before two wireless clients can exchange data. This involves the exchange of messages called management frames.[7] After the request has been authenticated and the association process is complete the client becomes a peer on the network.[8] This allows communication to take place as it would in a trust relationship on a traditional wired network.

Cellular Digital Packet Data

Cellular Digital Packet Data is a wireless IP network that uses the existing cellular infrastructure and a packet switch network to transport data. Data is sent in packets and short bursts instead of one steady stream, which eliminates the need for a constant connection. This means a more efficient and less costly method to send and receive data. The costs are cut The CDPD raw channel modulation rate is 19.2 kbps, but throughputs can vary from 5-6 kbps up to 12-13 kbps.[9]

Law enforcement agencies are taking advantage of this technology to transport and encrypt wireless transmissions from the towers to the Mobile Data Terminals (MDT's) in the patrol cars. This provides a secure communications path while another type of encryption must be deployed on the landline from the host to the tower in order to meet Federal standards. Federal standards require encryption on all law enforcement traffic traversing over a wireless or public network. This knowledge is based on my experience working to meet those federal standards.

Wired Application Protocol WAP

WAP has some security issues because it is encrypted until it hits the gateway then it is decrypted and once again re-encrypted. During this transition the message is exposed at the WAP gateway, also referred to as the "WAP Gap". Any point in wireless communication that is decrypted could create vulnerabilities. Several steps can be taken to make it more secure such as ensuring the gateway does not store decrypted data, only give administrators access to the physical device, do not allow remote access, implement other levels of security, and disconnect WAP devices from the rest of your network.[10] Nothing is foolproof, but the more dimensions in the security architecture the better.

Bluetooth

Bluetooth is a fairly simple protocol that serves to connect various devices including peripherals. It operates in a 2.4 GHz range and uses the FHSS to keep communications flowing even in spaces that are "noisy". Bluetooth utilizes synchronous bands for high-quality voice and asynchronous bands for data.[11] This protocol is relatively low cost, it can accommodate multiple devices, and it does not require a physical connection. Bluetooth technology is designed to serve as a Personal Area Network (PAN) to achieve seamless data synchronization.[12]

There are concerns such as encryption, which needs to be deployed at the application level and authentication beyond just an access control list.[13] Security issues like these need to be addressed in order to effectively utilize the Bluetooth protocol. The type of security solution used could be dependant upon various factors such as budget, vendor's proprietary products, politics and/or personal preference.

Personal Data Assistants (PDA's)

During the 2001 Super Bowl, Aether (www.aether.com) provided the Louisiana State Police with their PocketBlue handheld unit to help improve security. These handheld units allowed police officers to make inquiries into the National Crime Information Center's (NCIC) nationwide database to check suspicious persons for arrest warrants, terrorist suspect lists, and to check commercial vehicles or large trucks that could be used to transport explosives or used as a vehicle of mass destruction.[14] NCIC is accessed through each state's Control Terminal Agency (CTA), which also provides access into

the state's local warrant and stolen vehicle databases, the Department of Motor Vehicles (DMV) – driver's license and registration databases, Bureau of Criminal Identification and Investigation (BCI&I) – state criminal history repository, Department of Rehabilitation and Corrections (DRC) – inmate progression system, and various other databases. The availability of this information is tantamount to the law enforcement officer's ability to do his/her job effectively. This information is based on my law enforcement experience and knowledge of the state/federal computer systems.

PDA's are also being used in Boston at the Logan International Airport since the terrorist attack on September 11, 2001. The Research in Motion or RIM Blackberry (www.blackberry.net) made by Waterloo was piloted there after ten terrorists boarded two passenger jets and crashed them into the World Trade Center.[15] More pilots projects are being conducted with airports and law enforcement agencies around the country and the results remain consistent; immediate results, no intervention by a dispatcher and mobility add to the value of this technology.

The Franklin County Sheriff's Department in Columbus, Ohio, was one of the first law enforcement agencies in the country to utilize PDA's. In May 2002 I met with their System Administrator to see a demonstration of their system and to get some feedback on how the users like the handheld units. This department has 671 officers and a total of 50 PDA's issued to detectives and special investigators (i.e. mounted police, officers on foot and bicycle patrol.) The Franklin County Sheriff's Department is utilizing the PocketBlue handheld application by Aether Systems on the RIM Blackberry PDA. When asked why they selected the RIM, they provided the following reasons: Thin and less bulky PDA compared to competitors, 1.5 Watt Modem provides great range, and long battery life - up to a week. Like many law enforcement agencies they are using CDPD wireless because of its range, reliability, and security. Below is a list of several popular PDA's and their websites:[16]

Table 1

PDA's	**Processor**	**RAM/ROM**	**Cost**	**Web Site**
IPAQ 38355	206 MHz	64/32 MB	$599	www.compaq.com
Casio E-200	206 MHz	64/32 MB	$599	www.casio.com
HP Jornada 565	206 MHz	32/32 MB	$599	www.hp.com
NEC Mobile Pro	206 MHz	32/32 MB	$599	www.neccomp.com
RIM 857/957	Intel 386	5MB	$499	www.rim.com
Intermec 700 Series	206 MHz	64/32 MB	$1575	www.intermec.com

Most of the examples sited in this paper have been the Aether PocketBlue application but there are numerous other software vendors who have created or are creating law enforcement applications. See the table below for more details:

Table 3

Vendor	Website
Datamaxx	www.datamaxx.com
Unysis	www.unisys.com
VisionAir	www.visionsair.com

PDA Advantages

There are obvious advantages and benefits to the police officer such as mobility and immediate response. Valuable time is lost when officers must call a dispatch center via radio to run a transaction and then wait for a response. Dispatchers make answering the radio a priority but that is not their only job responsibility, many dispatchers answer 911 calls and talk the caller through first aid over the phone or until the ambulance arrives. Also, budgetary constraints and short staffing do not always provide enough dispatchers on a shift to offset the number of units on the road. Giving officers the ability to access records themselves could actually increase the number of felony arrests made while also improving officer safety.

The PDA's can be programmed to utilize voice notification or a colored warning screen when a warrant or "hit" is received. Many police officers currently have the availability of laptop computers in their cruisers that utilize radio frequency (RF) and CDPD technology but not all law enforcement officers have a properly equipped cruiser available. Officers such as undercover investigators, park rangers, mounted police, and officers on foot or bicycle patrol would benefit immensely from this mobile technology. Some additional benefits of wireless PDA's to an officer would be access to chat, spreadsheets, databases, and internal email. Report writing is still easier on a mobile data terminal because of the size of the keyboard and screen. Because most law enforcement agencies work from a limited budget the decrease in WAN deployment costs would also be a major benefit.[17]

Another good example would be the ability to conduct a "sting" operation in an old warehouse where a wired network may not be possible or may not be timely enough for the investigation. In a case like this a wired network would be too slow and cumbersome. The ability to deploy a quick wireless network is most advantageous in investigations of crimes that may operate in a temporary or limited fashion. (Crack houses, chop shops, telemarketing scams are just a few examples of businesses that can be set up temporarily and relocated quickly.)

PDA Disadvantages

So why aren't more agencies taking advantage of this new technology? Wireless technology does not come without its own security risks and concerns. There are physical security concerns, encryptions issues, wireless viruses and Trojans, and fears of message interceptions. Law enforcement and criminal justice agencies must also adhere to the Criminal Justice Information System (CJIS) security requirements in order to gain access to the FBI federal database. The CJIS Security Policy is provided to all of law enforcement but it is not a public document and therefore difficult to reference. This document outlines the security requirements for wireless communications, data transmitted over any public network, Internet access, authentication requirements, and various other security issues. I have worked with these requirements for the past three years to ensure our agency was in compliance.

Physical Security

Physical security concerns encompass possibly losing the PDA or even theft of the unit. Either scenario could cause disclosure of confidential information, access to unprotected passwords and potential liability issues. "Gartner Group estimates that more than a quarter million PDA'S and mobile phones were lost or stolen in airports worldwide in 2001".[18] If a device is lost or stolen replacement costs for the units would need to be considered. And since the unit could easily be dropped or broken during a resisting or some form of officer/violator contact extra devices should be purchased and stored for cases like these. There are other considerations such as exposures to hostile environments when the PDA gets knocked around in the patrol car or falls onto the floor during patrol car acceleration or rapid turning.

If the PDA were to be lost or stolen protecting the data would become the primary concern. Some ways to increase security would be to require password protection on the device, 5-8 character minimum password length, automatic log off after a preset amount of time, and passwords should not be changed more often than every 10 days. Security could be increased even more by requiring robust passwords or a combination of letters, numbers, and characters. The system administrator could remotely deactivate the device by disabling the IP address at the server making the wireless abilities non-active. Some PDAs could be programmed to erase its data after a designated number of log on attempts are made on the device. Another alternative available in some PDA's is the use of a Global Positioning System (GPS) chip inside the device that could aid in its recovery. The GPS chip would be an additional expense but may still be an option.

Encryption (Wired Equivalent Privacy)

Many PDA's do not possess enough Central Processing Unit (CPU) power to employ encryption therefore, when selecting a PDA this should be taken into consideration. Encryption is a valuable security tool and an important part of a "Defense in Depth"

approach. (This is a phrase coined by the Department of Justice.) Any messages sent in cleartext can be intercepted by a third party and read, unless it is made unreadable by ciphertext. Wireless IEEE 802.11x is protected with Wired Equivalent Privacy (WEP) but several vulnerabilities in WEP have already been discovered.[19] There are ways to exploit WEP's vulnerabilities with cracker tools such as Airsnort www.airsnort.net and WEP Crack www.wepcrack.sourceforge.net. WEP uses the RC4 encryption algorithm to protect from wireless eavesdropping and to prevent unauthorized access to the wireless network.[20]

There is a process referred to as "Exclusive OR" or "XORing" that can be utilized to protect data. "The sender XOR's the key stream with the plaintext to produce cipertext. The receiver has a copy of the same key, and uses it to generate identical key stream. XORing the key stream with the ciphertext yields the original plaintext."[21] Once one side of the plaintext is known it's easy to figure out the other.[22] To make a system more secure WEP needs to first be enabled and then the default password needs to be changed.[23]

Also, the use of Virtual Private Network's (VPN) are a more secure method used to protect wireless data, as well as solutions such as Internet Protocol Security (IPSEC), Secure Socket Layer (SSL), and Pretty Good Privacy (PGP). VPN tunneling is becoming a more popular solution that can provide encryption and secure communications across a public network infrastructure. The most secure encryption is true end-to-end encryption that does not decrypt the message along the path like the "WAP Gap" discussed earlier. Encryption should be at least Triple DES (Data Encryption Standard) 128 bit key or AES (Advanced Encryption Standard) 256 bit-key to adequately protect wireless transmissions. A VPN using Network Address Translation (NAT) and an all hardware solution is also a good security solution.

Message Interceptions

According to Hacking Exposed Third Edition, intercepting messages through "war driving" and "parking-lot-attacks" are popular and simple attacks. To perform these types of attacks it merely requires a laptop, wireless network card, an antenna, and a wireless sniffing program. This exploit is a matter of driving around until an access point (AP) is found and the network traffic can be intercepted. This could prove very costly to a corporation if trade secrets or confidential information is being transmitted in the clear.

The book also recommends utilizing standard access control mechanisms such as Service Set Identifier (SSID) and Medium Address Control (MAC) address restrictions, an internal firewall, and security protocols such as IPSEC.[24] These should be treated as external connections with the same authentication requirements to protect your network. There are several on-line tools available to intercept wireless traffic: Airopeek, Sniffer Wireless, and NetStumbler.

For more information on Airopeek see URL: www.wildpackets.com/products/airopeek

For more information on Sniffer Wireless see URL:
www.sniffer.com/products/wireless/default.asp?A=5

For more information on NetStumbler see URL:
http://www.netstumbler.org

Viruses and Trojans

PDA's are still just computers and face the same vulnerabilities as computers including viruses and Trojans. While the popularity of handheld wireless devices increase due to their functionality and accessibility so do the risks of virus and Trojan attacks. These stealthy attacks may occur through the infrared transmitters, wireless modems, telephone connections, or even during the synchronization process with the host desktop. "If the device can automatically receive and process data, it can also automatically propagate viruses."[25] Two well-known wireless Trojans written for the Palm OS are Vapor Trojan and the Liberty Trojan. More viruses, Trojans, and other types of nefarious codes like these will continue to plague wireless as its use becomes more popular.

Antivirus solutions

The AV solution must be applied at the desktop level wherever the PDA is synchronized and also to the PDA itself. This dual approach will help prevent re-infection that can occur if only one side is protected.[26]
Here is a list of AV programs for Palm OS according to the Sans Security Institute [27]

Table 3

Antivirus	**Website**
Trend Micro	www.antivirus.com/free_tools/wireless
McAfee	www.mcafeeb2b.com/products/virusscan-wireless/default.asp
F-Secure	www.f-secure.com/wireless
Symantec	www.symantec.com/sav

Future advancements:

Current second generation or 2G technology wireless networks carry voice, limited data applications and short messaging service. The 2.5G and 3G enhanced wireless networks will offer more capacity, enhanced data applications beyond just email and Internet access.[28] The following devices commonly use second and third generation technology; mobile phones, smartphones, laptop computers, and personal digital assistants.

Wireless security issues must be addressed according to the risks associated to the user. Texas Instrument (TI) is a supplier of the basic architecture used in the vast majority of 2G wireless devices. They like many others are working to develop acceptable security solutions for 2.5G and 3G wireless applications. TI does not believe in a one-size-fits-all solution when it comes to meeting security needs. For example, valuable computation power wouldn't be wasted on encryption for a user who just wants to access local movie listings or lottery numbers via the Internet. However, TI recommends law enforcement applications start with very strong encryption and Public/Private Key Infrastructure (PKI) algorithms, a dedicated hardware/software security module consisting of hardware-based random number generators, hardware protected memory where root keys can be stored, secured input/output (I/O) channels, accelerator modules to improve processing performance, smartcards, biometrics, and even a VPN. [29]

The ability to send data streams and images to a PDA are also possible with 3G technology. This would be even a greater advantage over "still" photos but for the time being photo images can be downloaded from the Internet or scanned onto the network and sent to a PDA. Using a PDA to access photo images is an extremely valuable tool for law enforcement officers. If a suspect were stopped for a traffic violation, a positive identification could be made in real-time even if the suspect does not have identification on them. This would aid in the battle against identity theft and fraudulent use of social security numbers.

Summary

The utilization of PDA's by law enforcement agencies is inevitable although with the current security issues in the wireless protocols there are still some risk factors. The benefits of mobility and instant response still must be weighed against the need to protect confidential data from being lost, stolen, or modified. Awareness of message interception attacks, wireless viruses and Trojans, weak encryption algorithms, changing default passwords, and other security issues will help mitigate many security exploits. Wireless technology is a valuable asset to law enforcement but poorly managed it can become a detriment to the officer, the department, and private citizens. Protecting the integrity, confidentiality, and authenticity of the data is critical. Law enforcement is a layer of security in this country that plays a vital role in protecting life and property. Exploring ways through technology to give the officers critical data in a timely manner is part of that process. Handheld and wireless devices are becoming an integral layer in law enforcement.

Whatever the wireless protocol used be it 802.11x, Bluetooth, CDPD, WAP, or HyperLAN/2, there is a certain amount of personal responsibility of the network/security administrators to make sure they are aware of and effectively addressing the known vulnerabilities. Selecting the best PDA, application package, vendor and security solution must be based on the needs and requirements of the department. Each department will have to customize a solution that works best for them. Improvements to

the protocols and to the wireless technology itself will continue to become more enhanced but it is still my belief the benefits far outweigh the risks.

---

[1] McClure, Stuart

[2] Sans

[3] Hayden, David

[4] Hayden, David

[5] McClure, Stuart

[6] McClure, David

[7] Arbaugh, William

[8] Arbaugh, William

[9] Taylor, Grant

[10] Sans

[11] Wittman, Art

[12] Hayden, David

[13] Wittman, Art

[14] Aether

[15] Barnett, Shawn

[16] Miller, Leslie

[17] Chen, James

[18] Gardner, Dale

[19] McClure, Stuart

[20] Borisov, Nikita

[21] Borisov, Nikita

[22] Borisov, Nikita

[23] Ellison, Craig

[24] McClure, Stuart

[25] DeJesus, Edmund

[26] DeJesus, Edmund

[27] Sans

[28] Commworks

[29] Hattangady, Sunil

References

"Aether PocketBlue Handhelds Help Louisiana State Police Enhance Security in New Orleans for the Super Bowl." 2 Feb. 2002 <www.aethersystems.com/news_events/details.asp?ID=554>.

Arbaugh, William A., Narendar Shankar, and Justin Y. C. Wan. "Your 802.11 Network has No Clothes." 30 March 2001. <http://www.cs.umd.edu/~waa/wireless.html>.

Barnett, Shawn, and Conrad Blickenstorfer. "Consumer Handhelds." Pen Computing Winter/Spring 2002: 20 – 81.

Borisov, Nikita, Ian Goldberg, and David Wagner. "Security of the WEP Algorithm." <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>.

Chen, James C., and Jeffrey M. Gilbert. "Measured Performance of 5-Ghz 802.11a Wireless LAN Systems." 27 August 2001. <http://www.cs.umd.edu/~waa/wireless.pdf>.

CommWorks. "Wireless Access." <http://www.commworks.com/Wireless_Access/?source=Overture>.

DeJesus, Edmund X. "Airborne Viruses." Information Security April 2001: 80-88.

Ellison, Craig. "Exploiting and Protecting 802.11b Wireless Networks." PC Magazine 4 Sep. 2001: 1-8.

Gardner, Dale. "Wireless Insecurities." Information Security Jan. 2002: 28-40.

Hattangady, Sunil, and Chris Davis. "Reducing the Security Threats to 2.5G and 3G Wireless Applications." Jan. 2002 Texas Instrument White Paper

Hayden, David, and Valerie Rosenblatt. "Wi-Fi: The Winding Road to Utopia." Pocket PC May 2002: 63 – 64.

McClure, Stuart, Joel Scambray, and George Kurtz. Hacking Exposed Third Edition 2001 McGraw-Hill

Miller, Leslie. "Handhelds Join Handcuffs at Boston Airport in Fight Against Terrorism." 8 March 2002 <http://digitalmass.boston.com/news/2002/01/14/handhelds.html>.

Sans Security Institute. "Sans Security Essentials." Sans Online Security 9 April 2002 < http://giactc.giac.org/cgi-bin/momaudio/s=10.4.6/a=wzpxgyBunO8/SE_46>.

Taylor, Grant. "Cellular Digitial Packet Data." 13 May 2002 <http://www2.picante.com:81/~gtaylor/cdpd.html>.

Wittmann, Art. "Brush Up on Bluetooth." Network Computing 28 June 1999 <http://www.networkcomputing.com/1013/1013colwittmann.html>.