JAMES BURGAN

31 March 03

WIRELESS/PERSONAL ELECTRONIC DEVICE SECURITY ISSUES FOR THE US ARMY

INTRODUCTION

The utility and flexibility of wireless communication devices and Personal Electronic Devices (PEDs) appear to make them ideal candidates for military applications. Clearly, reduced size and power requirements make the use of portable information system devices a trend that will continue to rise in the Army as new devices, uses, and applications are developed. Current Army and National security doctrine focuses on countering the threats to and vulnerabilities of more conventional fixed, wire-dependent communications. This paper recognizes and highlights how the use of wireless communications and PEDs may add significant security vulnerability that must be considered in the operational environment.

Currently available commercial wireless products have not been ruggedized against the rigors of combat. Commercially available wireless products have also not been designed to provide military-strength secured transmission capabilities and protection from jamming. Although these issues will not be addressed directly in this report/policy, they are the limiting factors with respect to the usefulness of current wireless products. For these reasons, this report assumes (and suggests) that no wireless product will be forward deployed as the primary means of data dissemination. As advancements are realized in any of these three major areas of vulnerability, deployment strategies for wireless communications devices and PEDs should be reviewed. Even with the challenges noted thus far, wireless devices can offer significant advantages to our forces in terms of productivity and mobility. Policies that govern the use of these devices must be quickly addressed and developed into a flexible security framework. This framework will be adapted and expanded as necessary when newer applications, devices, and wireless communication technologies are introduced. In other words, security policies that accompany the use of these devices must be written to accommodate future technology trends.

Wireless communications are not a set of discrete technologies, applications, and implementations, but an extension of capabilities from the wired networks and telecommunications infrastructures. For purposes of this task, wireless is defined as the set of services and technologies that does not include the more traditional military legacy “radio” communications (e.g., voice radios or data radios operating within military frequency bands). One or more of the following characterizes the systems that are covered in this document:

Radio Frequency (RF) communications in commercial and unlicensed frequency bands.

Low power, short-range communications systems using enhanced processing and multiple transmitters to achieve required range.

Commercially owned and operated infrastructure.

Commercial standards.

Vendor proprietary protocols.

Mobility of users and communications (within the confines of the infrastructure).

Wireless communication devices include data enabled Wireless Application Protocol (WAP) cellular telephones, wireless Local Area Networks (wLANs), pagers, Personal Digital Assistants (PDAs), and laptop computers with wireless communication technology.

Purpose

This paper represents the research and analysis necessary to develop, coordinate, and staff a Department of the Army (DA) security policy for the use of PEDs and wireless data communication devices. The team drafting this paper reviewed existing DA security policies that may have applicability to these devices; reviewed policies of other services and agencies; and reviewed industry policies. The team reviewed current and planned technology used to support PEDs and wireless communications to ensure that the policy would not become outdated with enhancements to the technology. Functional, networking, interoperability, anticipated future requirements, potential attacks, security vulnerabilities, countermeasures, and possible alternative solutions were identified and considered during the policy development process.

Wireless communications presents a unique set of information security challenges that must be addressed in order to mitigate risk through a layered defense system in accordance with the Army's Defense-in-Depth technical strategy. Security requirements focus primarily on Identification and Authentication (I&A), access control, data confidentiality, data integrity, non-repudiation, and service availability. RF transmission of sensitive or Sensitive But Unclassified (SBU) information adds another variable to securing information in terms of ensuring data confidentiality, providing non-repudiation, and preventing Denial of Service (DoS) through techniques such as jamming.

Scope and Content

Wireless voice communications security was not considered within the scope of this report. This report focuses on PEDs with wireless data communication capability. An important issue is the fact that a PED with wireless data communications is an Automated Information System (AIS) and must therefore be managed and maintained as any other AIS (like a desktop computer). It must be used in accordance with established security policies and procedures that would apply to any other AIS. Currently available commercial PED Operating Systems (OS) were not designed to meet, nor would they meet, the Army's documented computer security requirements and will, therefore, require waivers in association with any Army system. Based on the technology, there may also be restrictions on these devices, including prohibiting their use in classified environments. This type of restriction would currently be considered because the only means of de-classification for current-generation wireless data communications devices is physical destruction.

The basic premise of this security policy is that, in addition to any new requirements developed for the use of PEDs with wireless data communications capability, users of any of the PED-communications devices must follow traditional computer security policies. This report acknowledges this reality and addresses only the additional requirements brought about by the unique nature of the PED with wireless data communication capability.

Technical subjects are summarized in the discussions providing in the body of this report.

In completing this paper, the team focused on the following activities:

Researching existing relevant security policies and doctrine applicable to PEDs/wireless communications.

Researching applicable PED and wireless technology

Identifying security vulnerabilities and solutions

Identifying the required security policy components

Drafting the appropriate security policy document. (During the completion of this report, a draft policy was released by the Army.

Following is a list of hardware, protocols, and OSs as an example of the breadth of this report:

Traditional PDA (like the Palm VII, V), with and without wireless capability

Cellular phones with data capability

Two-way pagers

Wireless physical infrastructure (wireless modems and wLANs)

Wireless protocols (e.g., Institute of Electrical & Electronics Engineers (IEEE) 802.11)

Communication applications (may be based on infrastructure and/or protocols (e.g., BlackBerry)

PED OSs (e.g., PalmOS, Windows CE)

Applicable Encryption Standards (e.g., 3DES, AES)

The policy includes recommendations regarding I&A, access control, encryption, antivirus software, and physical security.

Structure of Report

This report is divided into five sections:

Section 1 is an introduction to the report.

Section 2 is an assessment of PED security.

Section 3 provides an assessment of communications security.

Section 4 introduces security initiatives and considerations.

Section 5 summarizes the major findings and recommendations.

Referenced Documents

The following references were used in preparation of this report.

National Security Agency

CCIB-98-026, Common Criteria for Information Technology Security Evaluation, Version 2.0, May 1998.

Department of Defense

a. Department of Defense (DoD) Directive 5200.28-STD, Trusted Computer Security Evaluation Criteria (TCSEC), December 1985.

b. DoD Directive 5200.28, Security Requirements for Automated Information Systems (AIS), 21 March 1988.

c. DoD 5200.40 Instruction, DoD Information Technology Security Certification and Accreditation Process (DITSCAP), 30 December 1999.

Department of the Army

a. Army Regulation (AR) 380-19, Information Systems Security, 27 February 1998.

b. AR 380-53, Security Information Systems Security Monitoring, 29 April 1998.

IEEE/International Standards Organization

a. IEEE/International Standards Organization (ISO) Standard 802.11 Wireless Local Area Network, 1999.

b. IEEE 802.15 Wireless Personal Area Network (Draft)

World Wide Web (WWW) Resources

Note that these pages may have changed or become unavailable after the publication of this report.

802.11 Wired Equivalent Privacy (WEP)

a. www.nwfusion.com/cgi-bin/mailto/x.cgi

b. www.wireless-nets.com/whitepaper_overview_80211.htm

c. http://developer.intel.com/technology/itj/q22000/articles/art_5c.htm

d. http://www.3com.com/promotions/wireless/whitepaper.pdf

Bluetooth

a. www.bluetooth.com

b. www.socketcom.com/btfaq.htm

c. http://sysopt.earthweb.com/articles/bluetooth/index2.html

d. http://sysop.earthweb.com/articles/bluetooth/index3.html

e. www.cmptr.com/print.php?id=274

f. http://sysopt.earthweb.com/articles/bluetooth/index.html

g. http://www.networkcomputing.com/1013/1013colwittmann.html

h. www.zdnet.com/filters/printfriendly/0,6061,2650172-54,00.html

i. www.infotooth.com/tutorial.htm

j. http://www.nwfusion.com/news/1999/1208bluetooth.html

k. http://static.hellodirect.net/2852.htm

l. http://www.ambicom.com/products/air2net/btfaqs.htm

Wireless Application Protocol (WAP)

a. www.voicestream.com/products/coverage/global.asp

b. www.networkcomputing.com/1121/1121f42.html

c. www.cellular.co.za/ericsson_i888.htm

d. www.mindlogic.com/GSM_NOKI_8890_DTL.shtml

e. www.cis.ohio-state.edu/htbin/rfc/rfc2420.html

f. http://csrc.nist.gov/encryption

g. www.blackberry.net

h. www.6.compaq.com/products/handhelds/H1100/index.html

i. www.cellular.co.za/celltech.htm

j. http://news.cnet.com/news/0-1006-202-3366904.html

k. http://www5.Compaq.com/emea/ipaq/pocketpc/intro.html

l. www.attws.com/personal/explore/pocketnet/mitsubishi_phone_details.html

m. www.zdnet.com/products/stories/specs/0,8828,259093,00.html

n. www.libcom.com/wireless/5160i.htm

o. www.attws.com/personal/explore/pocketnet/ericsson_phone_details.html

p. http://e10.sprintpcs.com/learn/show_phone.asp?sku=MOTVKIT

q. http://e10.sprintpcs.com/learn/show_phone.asp?sku=SCH6100GHS

r. http://e10.sprintpcs.com/learn/show_phone.asp?sku=LGTP1100HK

s. http://www.cerberussystems.com/INFOSEC/stds/fip46-3.htm

PED Security

a. http://www.mcafeeb2b.com/

b. www.cmptr.com/print.php?id=313

c. www.fcw.com/print.asp

d. www.softwinter.com/dentryce.htm

e. http://www.pgp.com/

f. www.vnutet.com/Download/1111548

g. www.pcworld.com/resource/printable/article.asp?aid=33921

h. http://biz.yahoo.com/prnews/000828/ca_mcafee_.html

i. www.imimg.org/cellular/news_2000/news-08072000_mcafee_avert_wap.htm

j. www.datafellows.com/news/2000/news_2000080900.html

k. www.f-secure.com/news/2000/20000215.html

l. www.allnetdevices.com/wired/news/2000/08/30/more_vendors.html

m. www.allnetdevices.com/wired/news/2000/08/28/mcafee_ships.html

n. www.infoworld.com/articles/hn/xml/00/09/26/000926hnantivirus.xml

o. www.cnn.com/2000/TECH/computing/09/27/virus.vendors.idg/

PERSONAL ELECTRONIC DEVICE SECURITY

The PED and wireless communications technology area is changing rapidly as new products and technologies are realized. In some respects this field remains unpredictable, as changes are occurring so rapidly. During the course of research for this paper a number of new products were introduced in the technology area, as well as reports of vulnerabilities being found in current products. This section will summarize high-level security factors associated with the use of PEDs.

An out-of-the-box PED is much less secure than the standard desktop computer deployed in most units. Most of the desktop computers deployed in the Army have at least a minimal set of OS security features, they are installed and controlled in accordance with physical security guidelines, and where appropriate utilize the appropriate level of communication security protection. PEDs have not necessarily been designed to the same standards, nor exposed to the same rigorous examination as desktop OSs. Current research shows that there are some technical solutions available to counter some of the OS security deficiencies and most of the communications security deficiencies noted. None of these technical solutions provides a countermeasure to the physical security concerns associated with the use of PEDs; quite simply, the devices are so compact and portable, loss of the device and any information contained on the device seems inevitable (the only effective countermeasure in this case is data encryption, covered below). This document addresses OS and physical security vulnerabilities, countermeasures, and recommendations in this section. Communications security vulnerabilities, countermeasures, and recommendations are discussed in Section 3 of this document.

Operating System Security Requirements

OS security requirements for Army systems are derived from AR 380-19, and DoD 5200.28-STD (also know as the Orange Book). Techniques to evaluate and test products against security functional requirements are spelled out in the ISO standard 15408, normally referred to as the Common Criteria. When grading the OS against security requirements reflected in AR 380-19 and DoD 5200.28-STD, most PEDs receive a "very poor," based on the assessment here. In an evaluation of several PED OSs, it was found they did not provide provisions to separate one user's data from another (Discretionary Access Control (DAC)); they lacked audit capabilities; they had no support for object reuse control through the implementation of I&A; and they did not provide data integrity protection. An exception to this finding is a laptop computer running the Windows NT OS configured in accordance with DoD guidance. A Windows NT OS meets many of the security requirements called out in DoD and Army regulations for use with SBU or even Secret System-High operating environments.

Identification and Authentication

I&A is required to provide a means of identifying who is authorized to use a particular system, and providing a means of validating that the individual accessing the system is who they say they are. A very basic, commonly understood method of I&A is the use of a user ID and password to access a system. Many of the PEDs evaluated did not require I&A techniques to be employed before using the device. This appears to have been identified as a concern to commercial vendors, because it was noted during the study that progress has been in implementing I&A, primarily in the form of third-party additions to the basic PED. (For example, the Restrictor product from IS/Complete for use with the Palm OS – currently being used by the Navy.)

Vulnerabilities

For those PEDs that had OS passwords, this was often an optional feature, and a feature that is easily turned off. Additionally it appears that the mechanism that implements them is easily circumvented. Some exceptions to this concern seem to be the use of Basic Input/Output System (BIOS) passwords and the properly configured WindowsNT system.

Countermeasures

Below are listed the currently available countermeasures for the vulnerabilities identified previously.

2.1.1.2.1 BIOS Passwords

The BIOS password mechanism is a feature on most laptop computers and some palmtops. It is implemented in the power-up instructions that are initiated when the power is turned on. For this reason it is nearly impossible to circumvent. Unfortunately, the BIOS password mechanism is often not enabled because if the BIOS password is forgotten, then the only way to start the device is to remove and replace the Read-Only Memory (ROM) chip in the device. If a typical user password mechanism is also enabled on the device, the use of a BIOS password requires that the user remembers and enters two passwords in order to use the device.

2.1.1.2.2 WindowsNT

WindowsNT is a general-purpose OS supportable on some laptops and some palmtops. It supports most required security features; can be configured to support DAC and other advanced security features; and includes robust password management. The password management includes a mechanism for protecting the password and for ensuring that a password is used, prior to allowing access to the device.

2.1.1.2.3 Smart Cards and Two-Factor Authentication

There are now available third-party additions for PEDs that use smart cards or Personal Computer Memory Card International Association (PCMCIA) cards to implement a secure challenge/response that takes the place of the basic password mechanism. These devices enforce a two-factor authentication by requiring the user to have the smart card (or PCMCIA card) and to know a pass code or unlock code (similar to the Personal Identification Number (PIN) used with bank automated teller machines).

2.1.1.2.4 Biometrics

Biometrics of several types are becoming available for a limited number of PEDs, but promise to be fairly widespread within a year or two. The most common types are fingerprint and voice recognition. The available fingerprint technology can be added to a PED that has a PCMCIA slot and replaces the native password mechanism. Voice recognition is available on certain phones, but must be purchased with the phone, not as an add-on. Both of these technologies are in their infancy for this application area, but bear watching.

2.1.1.2.5 Third Party Authentication Server

There are several third party authentication servers available, but one of note is a wireless server based on the Internet Engineering Task Force's Remote Authentication Dial-In User Service (RADIUS) protocol. It allows the user to be authenticated via a digital key system and also restricts the access to pre-authorized areas per user. It is scheduled to be available next year, but more information can be found at www.informationweek.com/810/funk.htm.

Recommendations/Implications for Army Use

Except for the case of WindowsNT, PED OSs have not been rigorously evaluated and should not be considered to be secure. If the OS has not been evaluated, it is impossible to consider built-in password mechanisms as secure. Although, as noted above BIOS passwords provide an implementation challenge in that if you lose them, you cannot use the device, they do protect the device from general snooping.

Because the current state of PED OSs is that they are unevaluated, any third party I&A mechanism such as smart cards and PCMCIA cards and biometrics that rely on such cards must be self-protecting and not rely on the OS in order to function properly. The same is true for third party authentication servers. Voice recognition, available on some phones, is considered a reasonably high level of I&A assurance for unclassified operations.

Based on the items noted above, it is recommended that PEDs without strong I&A built in or added to the system, should only be used for administrative tasks such as maintaining calendars and non-sensitive contact lists. In no instance should a PED without strong I&A be used to store, process, or transmit official Army information.

Encrypt of Data at Rest

A focus of concern for PEDs is the loss (or theft) of a device. This is particularly true if the PED contains sensitive information and does not support strong I&A. Because of this, encryption of the information stored on the PED should be implemented. There are currently available, add-on software products that can be installed on the PED to maintain all files and messages in an encrypted format, making it more difficult for someone to access and read the data. A variety of encryption algorithms are supported, which provide varying degrees of protection (e.g., seNTry 2020 for Windows CE).

Vulnerabilities

All encryption is not created equal. The same considerations that are used in choosing an algorithm and implementation strategy for a traditional computing device is required. This may sometimes require forsaking some ease of use. Assuming a strong encryption algorithm, the protection provided by the encryption also relies on a benign environment, one in which the encryption technique is not circumvented by hostile code, such as a Trojan Horse program. Utilization of encryption for protection of data at rest on the PED also requires that all copies of the data to be protected are encrypted, including such things as temp files if they exist on the system.

2.1.2.2 Countermeasures

DoD-level policies and programs such as the DoD PKI program govern the choice of an encryption algorithm and implementation scheme for use in a military environment.

Nationally known and government-endorsed standards such as Triple Data Encryption System (3DES) or the new Advance Encryption System (AES) are available for some PEDs and will soon be available for many more. Protection from a Trojan Horse program falls within the purview of anti-virus software and malicious code security covered in the next section.

Recommendations/Implications for Army Use

The recommendation is that encryption of data at rest be implemented for all PEDs that will be utilized outside the physical security confines of a user's assigned physical workspace. A strong, National Security Agency (NSA) approved algorithm should be utilized. Serviceability, ease of use, and proper implementation analyses should be completed on several products before selecting one. Serious consideration must be given to encryption key management techniques and procedures. Several Companies including Certicom and Baltimore Technologies offer PED-base PKIs to help manage encryption keys. Also, interoperability testing should be done with these products and ones proposed to be used in the protection of communications (see section on communications security below).

1.1.1 Viruses, Worms and Malicious Code

Viruses, worms and malicious code are facts of life in the computer world. Every OS that has any market share is susceptible to its share of viruses, worms and (other) malicious code (sometimes called malware).

1.1.1.1 Vulnerabilities

The debate on the susceptibility of PEDs and web-enabled cell phone to viruses continues. Many experts in the field attest that mobile devices are not yet powerful enough to allow viruses to thrive. These same experts contend however, that with improvements in technology it is only a matter of a short period of time, perhaps as little as a year, when viruses will become a threat for mobile devices. It is worth noting however, that even though many experts have claimed viruses cannot yet thrive in the mobile environment, there have been at least three viruses discovered to date for the Palm operating system. At the time this report was completed, a number of vendors, including McAfee and Symantec, were working on anti-virus product offerings for mobile devices. Even if the PED itself does not support anti-virus software, their supporting desktop and server computers can (and should) support anti-virus software that is PED-aware. There is still the risk that an as-yet-undocumented virus, worm, or Trojan Horse program could circumvent the virus protection before it is discovered and cause damage to the system by deleting data or copying files. This risk is not only to the PED, but the desktop computer (or network server) that it connects to in order to synchronize its files. In fact, a virus that is not harmful to the PED (and not detected by its anti virus software) could be transmitted over the synchronization connection to a computer that may not be able to detect the virus coming in that way.

1.1.1.2 Countermeasures

Anti-virus (and malicious code detection) software is available for most PEDs (except data-enabled cellular phones) and is available for desktops and servers that interact with PEDs. This software tests for and detects known virus implementations and many forms of malicious code. The countermeasure against the threat of viruses and malicious code is to properly install and configure anti-virus software, and to update the virus signature files as new computer viruses are discovered. Also, one must ensure that both the support environment and the PED always check files passed between the PED and the support environment. Example products are: Network Associates' McAfee division's McAfee VirusScan Wireless, which resides on the desktop and scans for viruses as files are synchronized with a PED running the Palm OS, Windows CE, or one of the new EPOC devices; F-Secure's F-Secure for EPOC, which resides on the EPOC device and scans for viruses locally; and the Symantec's Sysmatec AntiVirus for Palm OS that resides on a Palm device and scans for viruses locally. For complete protection, both PED-based and desktop-based virus scanning software should be utilized.

1.1.1.3 Recommendations/Implications for Army Use

The use of Anti-virus software on PEDs and their associated workstations must be mandatory. To ensure the level of protection required against viruses it is important to maintain the database(s) they use to profile and identify viruses, worms and malicious code. The network infrastructure must accommodate virus software updates for all PEDs and their supporting desktops and servers. Also, the Army should have a program for testing and certifying antivirus products for PEDs and investigate Army-wide licensing of PED-base antivirus software, as it currently does for desktop antivirus software.

Physical Device Security

This section addresses the challenge of and implementation of security for the device itself.

Vulnerabilities

By their very nature, PEDs are inherently at greater physical security risk than desktop computers. They are smaller, lighter, and have fewer connections to the physical environment. In addition, their mode of use puts them at greater risk, since they are generally removed from controlled environments and utilized in an open environment. Even laptops with wireless Local Area Network (LAN) cards tend be utilized in a more mobile configuration, because the restrictions of having to connect into a particular physical location are removed. Their identities as "mobile devices" encourage movement, without much consideration to the security needs of the device, the data it may contain or the sensitive system it may interact with. Once a device has been lost or acquired," by the wrong party, little stands between the snoop and the data in the device (see encryption of data at rest, above). If the device has any sensitive information on it, that information must be considered compromised. For example, official government documents, marked "For Official Use Only,"/SBU are sometimes permitted to be sent via e-mail over a government network. If such a message were received by a PED, while it was connected to the network, it would be available to the new owner of the device.

Countermeasures

An ounce of prevention is worth a pound of cure according to an old saying. User security awareness training is central to the physical protection of PEDs. Helping users to understand their responsibilities and the dangers posed by loss of an official PED will aid in PED retention. Cabling systems to attach PEDs to work surfaces can reduce the number of lost PEDs although this also greatly restricts their mobility. Sensitive information could be protected by stronger implementations of encryption (see encryption section above), or filtered at a mail or file transfer server. Should the device accidentally receive classified information, destruction of the device is the only authorized form of "sanitation."

Recommendations/Implications for Army Use

User security awareness training regarding the proper control and use of PEDs will help to eliminate some lose of the devices. Providing a securing mechanism for a PED that must be left unattended (in a lab or in a hotel) may help prevent theft. . Using encryption, as mentioned above, will not recover the PED, but will protect the data on it from illicit use. The support environment can and should be set up to implement the local policy of SBU data and PED use. Only official PEDs should be used, since they may have to be destroyed if they become contaminated with classified or unauthorized SBU information.

COMMUNICATIONS SECURITY

A PED uses one of the following for communications: serial cable (with or without cradle), infrared transceiver, wired modem, wireless modem, wired networking card, or wireless networking card. Of these devices, the wired solutions are generally considered more secure than their wireless counterparts. Obviously, if the wired connection is used to enter an unsafe environment (such as the Internet), even the wired connections can be unsafe, particularly in light of the fact that the PEDs are not self-protecting (i.e., do not meet OS security requirements), as discussed above.

Wireless Local Area Networks

The best example of the wLAN technology is the wireless Ethernet-like connectivity, as identified with the IEEE 802.11 standard suite (which support extensions of existing wire-based LANs into the wireless realm). The devices' functional range is reported to be approximately 200 feet. IEEE 802.11b supports maximum data rates of 1 – 3 Mbps in the 2.4-GHz range. A later version of IEEE 802.11b supports data rates up to 11 Mbps in the 5-GHz range. Although IEEE 802.11a is still in committee, some devices have been built to the draft standard that support data rates up to 54 Mbps (there are actually two competing groups associated with IEEE 802.11a that are not compatible). A using agency normally implements the Access Point (AP) (a transceiver that manages communications between wLAN devices) as well as the wLAN device(s), and maintains the entire system (with system administration and security responsibility for the entire system). It is noted that, in the absence of an AP, wLAN devices can still communicate to one another.

Vulnerabilities

Any wLAN device is at risk of having its communications monitored, interrupted, or even taken over (that is, a third party could replace or augment communications from one (or both) of the original two communicating parties). Many currently available commercial wireless LAN devices transmit all data "in the clear" (unencrypted). With these devices, stray but useable signals are not uncommon at half a mile distance. Monitoring Wireless LANs is simple. Unless specifically configured up not to accept another wLAN device joining the network, a wLAN device will accept communications from any device within its range (some business are setting up wLAN transmitters that will continuously broadcast messages that will be received and displayed on any compatible wLAN devices that come within range). This is the network version of an I&A vulnerability (the operating system version was addressed in Section 2.1.1). Even on a wired network there is a vulnerability that a person might connect a computer to a network for which they are not authorized to do so by spoofing the Media Access Code (MAC) or Internet Protocol (IP) address and monitoring unencrypted communications using a network sniffer. The same is true in the wireless world. The only real difference is that the person doesn't need physical access in order to attempt the connection. They only have to be within signal range.

Countermeasures

Network Access Control

The AP provides central management and a connection point to the wired LAN infrastructure. It supports device identification and communications security, and thus increases the general security of a wLAN. IEEE 802.11 devices can be set to only respond to a specific set of other devices, based on a list of MAC addresses (which can be cryptographically sealed to prevent spoofing. These devices can also be set to require a secret key that has to be installed in each such device that is permitted to communicate over a particular wireless segment (Extended Service Set Identification (ESSID)). The features available in the 802.11 compliant PED for setting up groups of communicating devices should be used (particularly in an environment that can not or does not use APs).

1.1.1.4 Spread Spectrum Transmission

The IEEE 802.11 suite of standards indicate that the use of spread spectrum radio frequency technology may reduce the amount of interference between PEDs and also reduce the effectiveness of monitoring and attempted service interruption.

1.1.1.5 Wired Equivalent Privacy (WEP)

WEP was designed as a security overlay to be used with IEEE 802.11b. The concept behind WEP is that, using encryption, the protocol could protect the data being transmitted with the same robustness as a wired LAN would. WEP was not designed to withstand a directed cryptographic attack. In fact, it uses a hashing algorithm for its encryption and does not meet the Army's 3DES or AES encryption requirements.

Wireless Virtual Private Network(s)

Several wireless Virtual Private Network (wVPN) products are available (e.g., from F-Secure and Certicom) that support encryption of transmitted data. Like their wired counterparts, wVPNs provide encrypted communications from the PED, via wireless or wired connectivity, to a local server or firewall that serves as the VPN gateway. Certicom's product can use their Elliptical Curve Cryptography or 3DES and is shipping now. F-Secure's VPN+ product is ISEC compliant and can encrypt data at speeds as high as 24 Mbps with 3DES encryption (168 bit).

Recommendations/Implications for Army Use

Where wLANs are to be implemented, thorough analysis, testing, and risk assessment should be done to determine the risk of information intercept, monitoring, etc. An IEEE 802.11x system should be used, supporting the spread spectrum technology. In a neutral or safe environment, the WEP implementation can be used to ensure data confidentiality. In any other case, a wVPN or other data encryption implementation should be utilized. It should be understood that none of these encryption implementations are secure from traffic (packet header) analysis because only the data payload of the packets are encrypted. Furthermore, protection against interruption of communications through jamming is not provided (although the spread spectrum will help). Interoperability specification and testing should be accomplished prior to investing in equipment.

Wireless Personal Area Networks

Although they are wireless, they are generally referred to as a Personal Area Networks (PANs). There were no popular PANs before the wireless version, so there should be no confusion. A representative example of a PAN is the Bluetooth technology/system, which is assessed here. The Bluetooth technology (which supports the short-range radio frequency transmitters operating at 2.4GHz for interconnectivity of devices with a maximum range of approximately 3 feet/10 meters) is being used to support a wide variety of PANs, such as in cars or even on a person (wireless headphones for cellular telephone). A concern for users of PANs (e.g., Bluetooth) is that support for this technology is not available in all geographic locations. Also, the standard for PANs (IEEE 802.15 with subparts 1-3) is still in draft and subject to change.

Vulnerabilities

The general PAN has the same vulnerabilities that a wLAN does. In addition, it is a low power system that can be interrupted by more powerful transmitters operating in or near its frequency range (such as the IEEE 802.11b).

Countermeasures

The Bluetooth devices utilize spread spectrum communications at very low power. This makes their signal difficult to intercept or to interrupt. Bluetooth data devices use collision avoidance and error detection/retransmission technologies because of the noise communications bandwidth they operate in, which enhances their overall performance and reduces the risk for interruptions.

Recommendations/Implications for Army Use

PAN devices, should not be used for transmitting sensitive data and must be used in a well-controlled physical environment.

Data-Enabled Cellular Phones, Two-Way Pagers, and Web-Enabled PEDs

Examples of mobile communications devices/systems are laptops and Personal Data Assistant (PDAs) with wireless modems, data-enabled cellular phones, and two-way pagers. These devices are usually used by subscribing to commercial (e.g., Internet or message) service provider that is not under the direct control of the DoD for maintenance or security.

Vulnerabilities

Any one of the above listed devices is at risk of having its communications monitored, interrupted, or even taken over (that is, a third party could replace or augment communications from one (or both) of the original two communicating parties). It transmits all data "in the clear" (unencrypted) and monitoring is simple.

This is the wide area network version of the I&A vulnerability (the operating system version was addressed in Section 2.1.1 and the local area network version was addressed in Section 3.1.1). Just as with a wired WAN connection, the data passes through many uncontrolled paths between the two communicating elements (e.g., a data-enabled cellular phone and the data gateway it connects to could even be in different states, like the Blackberry-based RCN system, whose primary gateway is in Virginia, but services customers across the United States). The major difference is that the AP(s) and their associated servers are usually under the management and control of a commercial entity, and not the implementing DoD organization. A good example of the kind of problems this can cause is the "WAP-gap." The problem stems from the way security is implemented with a WAP gateway (AP) and its accompanying interconnected wired service. The messages being transmitted via a WAP-enabled device are encrypted using Wireless Transport Layer Security (WTLS), thus protecting them during the wireless transmission. The packets are transmitted to a WAP gateway, decrypted, checked for correctness and final destination address, encrypted using Secure Socket Layer (SSL), and transmitted over the wired service. The problem (the "WAP-gap"), comes from the message being stored in the clear on the WAP gateway between the time it is decrypted from WTLS and encrypted to SSL. Someone wanting to monitor or interfere with the message need only compromise the WAP gateway (or the associated server, depending on where the re-encryption takes place). The WAP-gap problem can be countered by utilizing end-to-end encryption techniques.

Another major vulnerability with these types of devices is that they are meant to be used with "outside" systems. If they are also used in conjunction with internal systems (for example, a PDA that is used to surf the web via a wireless modem and then also connected to a desktop PC in a DoD organization, to check/synchronize e-mail), they become an additional entry point into the DoD organization's network.

Countermeasures

There are VPN solutions for mobile/wireless devices and encrypted messaging services (such as BlackBerry) available using commercially available encryption technology that can be implemented to compensate for the "service in the middle" security vulnerability of the communications process. Products that communicate using WTLS, which is the wireless version of the SSL protocol, will round out the communications security for PEDs. The solution(s) chosen should be thoroughly tested, along with other proposed security and application technologies, to ensure that the system components interoperate and meet the security requirements.

Recommendations/Implications for Army Use

The line between these last two technology areas seems to blur when a PED can be connected directly to a LAN, via wLAN technology, one moment and then connected to the same LAN, via a wireless modem connection, the next. The difference is that, in the former case, the connecting media is under the control (and responsibility) of the local unit while, in the latter, an outside element (at least a phone company) is involved and, therefore, different security implementations are indicated. As suggested for the wLAN PEDs, VPN systems for mobile and wireless devices (such as that available from Certicom) should be assessed. Furthermore, for basic messaging services a BlackBerry enabled system might be appropriate. The commercial infrastructure that supports such a service needs to be reviewed, since the location of the distribution server could be in another state or in another country.

As stated earlier, the PED must always be treated as an AIS (and must be managed accordingly), but the connection technology changes the "context" within which the device is assessed for communications security requirements. An individual PED should be designated as either being part of an unrestricted environment (no SBU data) or as being part of a sensitive environment. If a PED is designated for use in a sensitive environment, it should not be connected via wireless connections outside of the sensitive environment.

SECURITY INITIATIVES AND CONSIDERATIONS

This section is used to identify initiatives discovered during the writing of this report or technologies that are close to being implemented, but will not be generally available in the next two-three years.

Department of Defense Public Key Infrastructure Initiative

The DoD Public Key Infrastructure (PKI) initiative has established the facilities, specifications, and policies needed by the DoD to use public key-based digital certificates for information system security, workflow processing, electronic commerce, secure communications, and e-mail within the DoD, as well as with organizations of other branches of the federal government. Standards provide the basis for the facilities that the PKI provides. Standards that influence the PKI include those of the ISO, the Internet Engineering Task Force (IETF), and the National Institute of Standards & Technology (NIST).

The DoD PKI provides the services to receive requests for certificates; issue certificates and otherwise respond to requests for certificates; revoke certificates; publish the Certificate Revocation Lists (CRLs); and maintain a directory service allowing users to retrieve certificates, CRLs, and subscriber contact information.

Utilization of the DoD PKI, with certificates bound to an individual user, will enable wireless devices to implement strong I&A and nonrepudiation. Nonrepudiation is a mechanism that validates the information sender's identity to the receiver so that the receiver can be sure the user is who he says he is, an important consideration in some types of electronic transactions.

With respect to wireless devices, many of the current security products such as wVPNs for 802.11 wLANS and mobile VPNs for hand-held PEDs are being designed to utilize the standard X.509v3 certificate that is supported by the DoD PKI initiative. Compatibility with the DoD PKI is a national level requirement for purchases involving the user of encryption technology; therefore, compatibility should be assured prior to equipment purchase. The roadmap for the implementation of the DoD PKI is evolving; the most current information is available from the Defense Information Systems Agency, via their website, accessible from a computer that has a valid ".mil" or ".gov" address.

At issue with the use of certificates (DoD PKI or commercial) is how they will actually make it into the wireless device or PED. A current initiative within the DoD is the use of the Common Access Card, a smart card to be used for distribution of a users' individual certificate. While the CAC holds promise that it will be compatible with wireless devices which are being designed to operate with smartcards, there is still the issue of loss of the device with the smartcard inserted. One method of helping with this vulnerability is the use of a PIN in addition to the smartcard for access to the user certificate. Currently, issues of this type have not been fully addressed in the planning for the DoD PKI and CAC programs. Additionally, as of the date of this report, there are ongoing issues with the available memory on DoD CACs, and it is unclear that the DoD CAC will be able to hold certificates for several different applications (i.e. a separate certificate for wireless devices).

SUMMARY OF FINDINGS AND RECOMMENDATIONS

This section summarizes the ISEC Security Team's major findings and recommendations for the Army's wireless policy. It summarizes current wireless technologies and application's strengths and vulnerabilities, and offers a high-level view of both technical and security policy recommendations. This discussion does not present all findings and recommendations, but offers a high-level view of major issues.

Summary of Wireless Technology Strengths

At a sustaining base, using wireless technologies may provide capabilities for a workforce that do not currently exist within the current environment. For mobile environments wireless technologies provide the Army with the capability to quickly move to new locations and continue with networked communications. Nearly immediate network connectivity during short stops is available, as is the rapid deployment of networked communications at a deployed location. Using a wireless network helps to create a more mobile environment for a host data user. Additionally, the use of wireless technologies may help limit the maintenance costs associated with constant rewiring.

Wireless technologies based on the IEEE standard 802.11 series begin to provide the capability for protecting communications over wireless devices. The standard paves the way for interoperability among systems, and for a more common implementation of the technology. Commercial products are already in the marketplace that have been designed with some security features; this appears to be a focus area for some PED vendors and definitely for some vendors who are providing add-on security devices. During the course of research for this paper, we have identified product families that are working towards implementation of PCMCIA devices in the PED, which will help enable future compatibility with the DoD PKI.

Summary of Wireless Technology Vulnerabilities

There have been a number of wireless technology, specifically PED, vulnerabilities identified in this paper. Wireless technology vulnerabilities include susceptibility to eavesdropping, which is made easier by not having to physically tap into a network. PED-specific vulnerabilities include the standard OS vulnerabilities found with personal computers as well as the additional vulnerability that the device itself may be very easy to lose. A wireless LAN may be at risk for having communications invaded; unless the wLAN is set up to not accept signals from outside a specified user group, a third party could set up a communication device within the range and join in the network.

As noted in the draft Army Wireless policy, the following must also be considered:

Wireless solutions may create backdoors into Army LANs. This can allow all perimeter and host based security mechanisms to be bypassed. If a wireless solution is to be considered, it must be planned for implementation behind network perimeter access control devices, and be connected through an approved Wireless gateway. The choice of an approved wireless gateway will require further study to determine which gateways will best protect against vulnerabilities such as the "WAP-gap" discussed in this paper.

Media Access Control (MAC) addresses for wireless LAN cards are easily copied and can be spoofed.

Wireless LANs are susceptible to interference, interception and can often be easily jammed.

There are currently at least three different wireless LAN standards in the world. Each standard specifies a different transmission technique and is incompatible with the others. Equipment operating under one standard cannot communicate with equipment using other standards. Therefore it is not unlikely that a wireless solution planned for implementation in one location will not work in another geographic location. Army program managers planning wireless connectivity in non-US locations will have to consider the need for Host nation approval to use the devices.

Critical Wireless Technology Vulnerabilities

Critical wireless technology vulnerabilities include basic computer security such as auditing, object reuse, DAC, and strong I&A. Also, there are several standards for encryption (which are not compatible with one another) that are optional and must be added to the PED. A less critical vulnerability is the fact that many of these systems, particularly PEDs were not designed to withstand the ruggedized environments required by the military. Because of this factor, information availability is potentially at risk and reliance on these tools as the sole communications means is not recommended. Additionally, the vulnerability of losing the device and all data contained therein, is significant.

An additional significant factor that must be considered for deployment is that there are currently three different radio frequency wireless LAN standards throughout the world. Each of these standards specifies a different transmission technique that is incompatible with the others.

Critical Security Policy and Procedure Vulnerabilities

Security procedure vulnerabilities relate primarily to the mobility, small size, and ease of use of the PEDs. The same features that make these devices so promising to support the military, also provide the opportunity to lose a significant amount of data that is being stored on these devices.

Summary of Wireless Technology Recommendations

The summary recommendation for the use of wireless technologies for the Army relates back to the Army's risk management strategy, which is aided by the computer security certification and accreditation process. All proposed uses of wireless technology for communications should be reviewed as part of a certification and accreditation process before they are allowed to be used in an operational environment. The certification and accreditation of these devices and proposed networks which will utilize these devices should be initiated during the design phase of the program or project.

Summary of Wireless Technology Security Design Recommendations

Any Army program or project that is considering the use of wireless technologies and PEDs should first identify the protection requirements of the data to be processed, stored, handled and communicated in the system. A suggested method of identifying and tracing these requirements is through the development of a Common Criteria protection profile. This will allow the program to specify to vendors or integrators the features that are required for the successful security implementation of a wireless technology solution. To date Considering that the PED is essentially a miniature Personal Computer (PC) can help in the development of the security requirements document. At the Common Criteria

Working Group meeting sponsored by Space and Naval Warfare Systems Center, Charleston, in November 2000, it was noted that work was beginning on a protection profile for wireless technology. To date, the study team has not been able to obtain a copy of this protection profile, but we are tracking the progress through the working groups formed at the November conference.

Summary of Critical Security Policy and Procedure Recommendations

It appears that a significant security factor associated with the proper use of wireless technologies and in particular PEDs is the acknowledgment by the user that the PED is in fact functioning in the same capacity as a standard PC or workstation. Reinforcing the standard information security training, and discussion of the Army's Defense in Depth program as part of this training can help to raise user awareness of the vulnerabilities associated with these systems. The Army's Defense in Depth program is a security strategy endorsed by the Army as a means to counter security vulnerabilities. Additionally, since the PEDs are so susceptible to being lost or stolen, we recommend that the Army initiate a policy to require that all data stored on PEDs be encrypted.

Conclusion

The wireless technology policy recommendations will only be effective if implemented in concert and parity with existing security measures. Protecting, monitoring, and managing the security of wired and wireless assets is required for optimal security.