A Whole New World for the 21st Century

Introduction

August 12, 2000 - jurors involved in a murder trial use their personal PDA (Personal Digital Assistant) to verify information obtained during the court trial, unbeknownst to court officials and despite the Judges orders not to bring PDAs into the courtroom. (Harrison, L.)(O'Connell, P.) January 19, 2001 - a program was written that allows malicious users to steal data directly from other PDAs using the PDAs infrared port. (Lynch, I,) February 22, 2001 - Robert Hannsen is arrested after years of downloading Top Secret FBI (Federal Bureau of Investigation) files to a PDA and turning the information over to Russian spies. (McCoullough, D.) ("Affidavit In Support of Criminal Complaint, arrest Warrant and Search Warrants"). March 2, 2001 - a backdoor is discovered that is built into the O.S. (Operating System) of PDAs that allows a person to connect a PDA and laptop together via a serial cable, and crack the PDA's system password. (Lemos, R.) ("Advisory Name: Palm OS Password Lockout Bypass")

These are just a few examples of a threat that is rapidly growing unbeknownst to companies and Security Administrators. This threat may already be lurking in the "backyard" of companies while Security Administrators are busy trying to secure the "front door" to the company's network.

Many PDA users and company officials have a false sense of security believing that PDAs do not pose a security threat. This false belief, the fact that companies are having a difficult time keeping abreast of the rapidly changing technological field and the issues associated with the new technology, and the lack of knowledgeable and competent Security Administrators, will help to increase the magnitude of these threats. (Lee, C.) This paper will discuss how PDAs will add a new dimensional threat to the infrastructure of corporate networks as well as discuss several suggestions to minimize the threats and risks that are associated with PDAs.

Background

Security Administrators have spent significant amounts of resources, building the defensive perimeters around their company's network. Last year alone, Infonetics Research showed that companies spent $835 million on VPN hardware, $1.1 billion on firewalls, and $269 million on VPN software. ("Dedicated VPN Hardware Market Hits $835 Million, Firewall Market Hits $1.1 Billion in 2000)

While, Security Administrators were busy building their defensive perimeter, an internal threat has been growing rapidly over the last year. These internal threats are Personal Digital Assistants (PDAs). PDAs are a growing threat to networks and corporations for three main reasons. First, PDAs are being created with more computing power and wireless features, thus making PDAs powerful enough to threaten network security, but physically small enough that detection of PDAs are difficult. Second, consumers who are purchasing PDAs have increased dramatically over the last year. By the end of the year 2000, manufactures sold more than 2 ½ times the amount of PDAs sold during 1999 –

approximately 3.5 million units were sold in 2000. (Kellner, M.) Third, as security experts agree, it is only a matter of time before the PDA threats become a reality. Once the threats are a reality, the frequency and the sophistication level of the attacks will rise proportionately. (Fisher, D.)

Confidentiality, Integrity, and Availability
PDAs are a major threat to network security, because PDAs exploit all three Bedrock Principles (Confidentiality, Integrity, and Availability). Another way to comprehend the Bedrock Principles, is to think of the terms as Prevent, Detect, and Deter.

Confidentiality will be a major issue with companies when determining how to address the use of PDAs within the workplace. Currently, many companies do not have any policies or procedures in place to specifically address PDAs, let alone having any knowledge as to the types of data that is being stored on PDAs. PDA users store a vast amount of information such as financial data, medical information, prescriptions, passwords, and information from company meetings. Confidentiality of information can be easily breeched without the PDA users knowledge, nor are there any method to determine who is responsible for the theft of data.

Here's a scenario, a malicious user decides what type of data that he/she wants to gather. In this case, the malicious user wants to gather hospital / patient data. The malicious user goes to an area where that data would most likely be highly accessible, so the user goes to a hospital cafeteria during lunchtime and sits in an area that is highly crowded with doctors. The malicious user using software such as Notsync, allows the malicious user to remotely "hotsync" information from surrounding doctor's PDA to the malicious user's PDA, as long as the distance between the two PDAs do not exceed a maximum radius of approximately 10'. (Cope, J.) With Bluetooth technology emerging, this distance will expanded to over a 30' radius. (Bernatchez, E.) Transference of the data is done by spoofing the victim's PDA into thinking that the malicious user's PDA is actually the victims desktop. Thus, while the doctor is eating lunch, data stored on the doctor's PDA can be stolen directly from the doctor's PDA without his knowledge. Confidentiality is now lost since the data on the PDA has been compromised. In addition to breech of confidentiality, possible litigation could ensue as a result of the question, did the doctor do everything to protect the data stored on the PDA that a reasonable and prudent person would do?

PDAs also exploit Integrity. On March 1, 2001, @Stake issued a vulnerability regarding the Palm OS v.3.5.2 and below. ("Advisory Name: Palm OS Password Lockout Bypass"). This is a significant advisory since the majority of PDAs, despite the vendor, are built on the same O.S platform. Even if the PDA is password protected, by using the Palm debug mode, a "malicious" user can retrieve the password of the victims PDA. The actual password can then be decoded using the PalmCrypt tool. Another possibility is that even with the O.S. password locked, applications can still be installed onto the Palm O.S. without the owners knowledge. Therefore, the integrity of the data has been compromised.

Once the password is bypassed, all the information on the PDA is fully readable by the "malicious user". Security administrators currently do not have the ability to determine if this type of attack has occurred, because the attack is non-traceable. Therefore, security administrators have no method to determine who was responsible for the attack. Therefore, availability has now been exploited.

A good example of how PDAs can be used to exploit all three Bedrock Principles is the recent incident involving Philip Hannsen and the FBI (Federal Bureau of Investigation). Philip Hannsen breached the confidentiality of the FBI's (Federal Bureau of Investigation) sensitive information by gaining access to sensitive data, downloading the data to his Palm Pilot and turning the information over to the Russians. During the years of Philip Hannsen's espionage, the FBI was not able to prevent, detect, nor deter this breach in security. The Palm Pilot was so valuable to Philip Hannsen in accomplishing his mission that he even requested the Russians purchase the Palm VII so that he could encrypt and transmit data in faster and secure method. (McCoullough, D.) ("Affidavit In Support of Criminal Complaint, arrest Warrant and Search Warrants")

Level One Threat Model

As stated in the SANS Security Level 1 class, the Level One Threat Model can be stated as the following equation:

$$\text{Risk} = (\text{Threat}) \times (\text{Vulnerability})$$

Therefore, if the threat or vulnerability variable can be made to zero, then the risk factor is zero. However, with PDAs, the risk factor will never be zero for the following reasons:

First, companies are spending billions of dollars to reduce the external threats to their network. However, PDAs make it easier for external and internal threats to by-pass the companies security measures that are in place. To heighten the internal threat level, PDAs due to their physical size and non-essential need for a network connectivity, make it difficult for a Security Administrator to determine if a PDA is being used internally.

The threats of PDAs are not only limited to desktops operating on a Windows platform, but also include Unix and Linux machines. On February 21, 2001, Sharp introduced a new PDA designed to operate on the Linux O.S. ("Sharp announces Linux PDA "). With Sharp's introduction of a Linux based PDA, malicious users can now launch attacks on different servers using different types of PDAs. No longer will PDA attacks be limited only to the Window platform. "Hacking tools" for Linux machines are already available on the Internet. Now it is only a matter of time before malicious users develop and / or modify existing tools to hack Linux PDAs and even possibly use Linux based PDAs as a launching platform for attacks against the network.

Second, PDAs are not only a vulnerability in itself, but are also a vulnerability to a company's network. This paper has discussed the backdoor vulnerability in the majority of PDA O.S. systems. Yet, @Stake identified another vulnerability of PDAs - the infrared ports. (Lynch, I.) Even if PDA users encrypt their data on their PDAs, when "beaming" data to and from other PDAs, the data is not encrypted. Data during the time of transmittal between two IR ports, becomes vulnerable as plain data. Therefore, the data can be easily intercepted and read by a malicious user. (Lynch, I.)

Another vulnerability of the IR port is the ability of the PDA to record IR signals. This will allow a malicious user to control devices that operate via IR signals or spoof a device into thinking that the IR signal is coming from a legitimate source. For example, PDAs can record the signal to auto alarms that use the IR signal to lock and unlock vehicles. Once the signal has been recorded on the PDA, the signal can be re-emitted from the PDA, to unlock the vehicle and disable the vehicle alarm. (Graham-Rowe, D.) Granted, not a lot of devices on a network emit IR signals or use IR signals other than printers and peripherals, but this is another vulnerability, and may only be a matter of time before this flaw is exploited as wireless communication becomes more abundant.

Third, the majority of PDAs do not have Anti-Virus (AV) software installed on the device nor do desktop AV software scan for viruses during the "hotsync" process. A recent survey in Information Security Magazine showed that 98% of all PDAs do not have any anti-virus protection. ("By the Numbers") The chance of a PDA obtaining a virus has increased with Microsoft's announcement of a beta version of Microsoft's Outlook for PDAs. ("Microsoft Outlook goes Mobile") Therefore, viruses that exploit Microsoft's Outlook vulnerabilities such as "I Love You", "Melisa", and "Anna Kournikova" soon will not only infect desktops, but have the potential to infect PDAs as well. At the very least, PDAs could be used to launch viruses onto desktops, via the "hotsync" or IR connection, thereby bypassing any AV software on desktops.

Fourth, PDAs can be used to exploit vulnerabilities on desktops. A search of Palm Hacking Software on Astalavista Search Engine produced numerous PDA hacking software available on the Internet. Hacking software ranged from Buffer Overflows to decrypting Cisco password files, to brute force attacks, spoofing attacks, Denial of Service attacks, hijacking pcs with PDAs, to even remotely rebooting systems with a PDA. Some people may argue that PDAs do not possess the processing power of systems used by malicious users. True, but that does not mean that a PDA can't be used as a means to launch attacks. It only means that it more time will be needed to execute the attack. However, what would stop a "malicious user" from starting a Denial of Service attack using a PDA and wireless connection and tossing the PDA into a ceiling or concealing the device in a trash can? The "malicious user" now has all the time in the world to execute the attack despite the lack of processing speed and power.

Therefore, based on the high level of threat and the increasing vulnerabilities of PDAs, the risk level for corporations will become increasingly higher. The bad news is the threat and vulnerability level will get worse before it gets better. With the increase in PDA sales and PDAs being integrated with wireless devices, it is only a matter of time before "malicous users" start using PDAs for more sophisticated attacks.

Houston We Have A Problem

Another problem that security administrators will have to contend with are PDA's features of wireless communication. A general rule of thumb for network security is that all connections must pass through the networks firewall. How will security administrators enforce this rule if a PDA using a wireless modem does not need a physical telephone connection? Despite the technological advances, a modem's physical size has not gotten much smaller over the last few years, the noise of two modems "handshaking", and the fact that modems must be connected to a desktop either internally or externally, makes detecting a modem relatively easy. With a PDA's physical size being smaller than a modem, no physical connection is needed to the desktop to use the modem, and the sound of "handshaking" is relatively quiet. Thus, how is an Security Administrator going to detect the use of a PDA using a wireless connection? One advertisement for a PDA wardialer, advertises its software as the following: "throw it in a phone can to retrieve later, toss it up in the ceiling during a security audit - the possibilities are endless". (http://neworder.box.sk/box.php3?gfx=neworder&prj=neworder&key=palmg&txt=Palmtop%20related%20tools) As PDAs and wireless devices become built into one single device, such as Kyocera's new $500 dollar cellular telephone and PDA built into one (Arara, Y.), the possibilities will become endless.

The internal threat that PDAs bring is widened even more with Kodak's input into the PDA market. In May 2000, Kodak announced the development of PalmPix, which will allow users to take pictures using their PDAs and emailing the pictures in a BMP or JPEG format. (Viotti, V.) Combine this with Kyocera's PDA and wireless communication device, and the risk has increased significantly. What's to stop a disgruntled employee from taking photos of company documents using his / her PDA and emailing the pictures via a wireless device connected to the PDA by simply throwing the device into the ceiling? The damage is done before anyone will be able to determine that the company's data has been compromised.

What Can Be Done

Unfortunately, there is no "silver bullet" that will resolve all the vulnerabilities and concerns regarding the use of PDAs. Security Administrators will need to implement several methods to minimize the threat and vulnerabilities that PDAs will bring to a corporate environment to bring the risk factor as close to zero as possible. Capslock a provider of security for wireless infrastructure software, outlined a few of the following points:

One of the first methods that should be implemented is a sound policy with enforceable procedures. As with any incident of network security, policies and procedures are the cornerstone / foundation to any good security. A policy should be created to specifically address PDAs and wireless communication tools. By incorporating PDAs and wireless communication into one policy, it will address future technology such as the incorporation of both cellular and PDAs into one device and Bluetooth Technology. Other concerns that need to also be addressed are the types of data that are authorized to be stored on PDAs and wireless communication devices and what areas of the company are these devices authorized for usage. By addressing these concerns, Security Administrators can ban the usage of wireless devices within the physical boundaries of the company, thereby enforcing the general security guideline – "all connections must go through the firewall".

A good place to start creating the "dos and don'ts" is to reference NASA's ("Palm PDA User Security Notice") web site on Palm Pilots. NASA explains to its employees, what type of data is acceptable to be placed on a PDA and what type of acceptable data can be "hot synced" to an employee's workstation. (See http://www.hq.nasa.gov/office/codec/codeci/help/hardware/palm.htm).

The second method is user awareness. Security Administrators need to make PDA users aware of the dangers that are inherent to PDA devices. For example, the website Contradicting the Norm (http://www.noncon.org/noncon/product_info.html) has free software designed specifically for the Palm Pilot to crack single encrypted passwords on Windows NT, Unix, and Cisco. As the organization's main web page states "The concept behind this program is primarily to show that a diminutive computing device like the Palm Pilot can break passwords". There are other companies such as Ernest & Young that conduct programs where they show users how PDAs can be used to crack passwords, launch Denial of Service Attacks, launch viruses, and even hi-jacking a desktop remotely. (Hayes, D.) If a user actually see both ends of the spectrum, the vulnerabilities of PDAs, as well as how to maliciously use PDAs, it will help users become more security conscious about their PDAs.

The third method that should be implemented is the purchase of software specifically addressing the vulnerabilities of PDAs. Companies spend large resources on security software such as Anti-virus, sniffers, encryption software, and firewalls to protect desktops, servers, and the corporate network. However, as previously mentioned, very little funding is spent on protecting the PDAs themselves. If companies want to allow PDA usage by its employees, allocated resources must be dedicated to protecting PDAs , since PDAs will become part of the internal infrastructure. Some security companies feel that by putting security software on PDAs to prevent viruses, Trojans, and other malicious codes, is overkill or paranoia since there have been no major attacks. (Lemos, R.) However, remember the original desktop viruses? The original desktop viruses were very simple in nature and were non-destructive. (Fox, J.) However, today's viruses and malicious code have evolved from being simplistic to complex and non-destructive to destructive.

This area of security software for PDAs is still relatively new. Many companies are rapidly trying to enter this new market with a wide array of software. For example, during the week of March 5, 2001, three companies announced plans for development of anti-virus software for PDAs (F-Secure Corp., Symanetc and Network Associates). Blueice Research (http://blueiceresearch.com/products/index.html) have developed Multipass which encrypts data on PDAs using PKI (Public Key Infrastructure) structure, Trivoli Systems Inc. has developed software to detect PDAs that are "hotsync" to workstations (Cope, J.) Password Protect, Secret, and Cryptinfo protect passwords stored on PDAs. (Green, J.) Security software for PDAs are available on the market and are not difficult to find. Not all of the software will cost the company an "arm and a leg". For example, Password Protect costs $5 to download. (Green, J.) Five dollars to protect company data on a PDA is relatively nothing as compared to the cost of cleaning up after an attack.

The fourth method is the concept of "user with the least amount of privilege". Servers should be located in a locked cabinet within a secured room. Users should be restricted to only the files and data that are needed to accomplish their task description. This will prevent users from gaining access to systems and data that are not necessary for users to accomplish their specified duties. This concept will play an even more important role in the future as new technology will allow PDAs to "hotsync" directly to servers rather than desktop systems. As of March 20, 2000, Palm has already developed Ethernet "hotsync" cradles that will bypass desktop systems and allow direct connection from PDAs to servers. Palm has also developed a "hotsync" server that can link between mail servers, database severs, and PDA applications. (Cope, J.) By also applying "user with least amount of privilege", even with the use of Kodak's PalmPix, the amount of pictures that can be taken of company documents are limited only to the amount of access the user has privilege to, thereby reducing the amount of risk.

Summary

PDAs and wireless communications are a major threat to networks and company security due to the vulnerabilities and threats that are associated with these devices. These devices will bring a whole new facet to the job of security administrators and it will only get worse as new technology allows the integration of PDAs and wireless communication to integrate into one. New technology and development of new software is quickly allowing PDAs to interface with every aspect of technology within a corporate structure. However, unless security administrators are aware of what is occurring both internally and externally, what is the use of strengthening the front door of a network, when the backdoor is wide open?

There are two philosophies about how to deal with this new emergence of technology. The first group believes that protecting corporate networks from PDA threats is being overly paranoid since no major attack has occurred on PDAs or with the use of PDAs. (Lemos, R.) The second group believes that it is only a matter of time before PDAs come under attack and are used as another method for attacking networks. (Lee, C.) Before deciding which stance your company will follow, ponder this statistic:

The Forensic Challenge, put on by Lance Spitzner, took data from an actual 30 minute hacking incident and challenged incident handlers to see what type of data could be extracted from their findings. From this challenge, this is what resulted: Based on a 30 minute hacking session, it took incident handlers approximately 1 week to clean up the damage done to a system. Based on the average rate for this type of position, it would cost a company on the average, a little over $2,000 US dollars. If the task was contracted out to a consulting firm, the cost escalated to over $22,500 US dollars. ("The Forensic Challenge"). However, this price does not include the lost of intellectual property which will significantly add to the cost.

So, based on the above statistics, would a company rather spend a few dollars to protect their system upfront before something significant occurs or wait until after an attack occurs before taking action. Either way, money will be spent as a result of PDAs. It just boils down to wanting to spend a few dollars upfront to protect your network or spend several thousand in the backend cleaning up the mess – its your choice.

References

"Advisory Name: Palm OS Password Lockout Bypass". 1 March 2001. @Stake, Inc. http://www.atstake.com/research/advisories/2001/a030101-1.txt (26 March 2001)

"Affidavit In Support of Criminal Complaint, arrest Warrant and Search Warrants". http://www.fas.org/irp/ops/ci/hanssen_affidavit.html (26 March 2001)

Arar, Yardena. "PDA-Based Cell Phones Deliver All-in-One Convenience". 28 November 2000, http://www.pcworld.com/news/article/0,aid,35241,00.asp (26 March 2001)

Bernatchez E. "What is Bluetooth - often spelled Blue Tooth?" About. http://cellphones.about.com/gadgets/cellphones/library/glossary/bldef_blue_tooth.htm (26 March 2001)

"By the Numbers". Information Security. January 2001: 24

Capslock. "Securing the Wireless Internet-Seven Critical Success Factors". http://www.itsecurity.com/papers/capslock1.htm (26 March 2001)

Cope, James. "Palms pose new demands on IT Managers". Computerworld. 20 March 2001. http://www.computerworld.com/cwi/story/0,1199,NAV47_STO41923,00.html (26 March 2001)

"Dedicated VPN Hardware Market Hits $835 Million, Firewall Market Hits $1.1 Billion in 2000". 21 February 2001. http://www.itsecurity.com/tecsnews/feb2001/feb452.htm (26 March 2001)

Fisher, Dennis "Symantec Offers Virus Protection for Palm". ZDNet E-Week. 5 March 2001. http://www.zdnet.com/zdnn/stories/news/0,4586,2692857,00.html (26 March 2001)

Fox, Jim. "A Computer Virus Primer". WinPlanet. http://www.winplanet.com/winplanet/reports/1256/1/ (26 March 2001)

Graham-Rowe, Duncan. "Palmtop Plunder". New Scientist. 5 December 1998. http://www.newscientist.com/ns/981205/newsstory6.html (26 March 2001)

Green, Jeff. "Keeping Your Palm Closed Tightly". Business Week On-Line. 8 March 2001. http://www.businessweek.com/bwdaily/dnflash/mar2001/nf2001038_563.htm (26 March 2001)

Hayes, D. "Hacker U: Company Offers Security Service, Training Against Computer Invaders". Infowar.com. 21 June 1999. http://www.infowar.com/hacker/99/hack_062199b_j.shtml (26 March 2001)

Harrison, Linda. “Judge slams Palm Pilot and Web use in Las Vegas Murder Case”. The Register. 18 September 2000. http://www.theregister.co.uk/content/1/13347.html. (26 March 2001)

Kellner, Mark A. “Technology: Handheld devices are viruses next target”. The Nando Times. 15 March 2001. http://www.nandotimes.com/technology/story/0,1643,500463911-500708023-503889379-0,00.html (26 March 2001)

Lee, Chris. “Virus Attacks Pick Up Pace”. ZDNet E-Week. 19 March 2001. http://www.zdnet.com/eweek/stories/main/0,10228,2698615,00.html (26 March 2001)

Lemos, Robert. “Handhelds: Here Comes the Bugs?”. ZDNet E-News. 19 March 2001. http://www.zdnet.com/zdnn/stories/news/0,4586,5079712,00.html (26 March 2001)

Lemos, Robert. “Passwords don't protect Palm data, security firm warns “. ZDNet E-News. 2 March 2001. http://news.cnet.com/news/0-1006-201-5005917-0.html?tag=cd_pr (26 March 2001)

Lynch, Ian. “Crackers can zap data off Palm Pilots”. Vnunet.com. 19 January 2001. http://www.vnunet.com/News/1116644 (26 March 2001)

McCoullough, Declan. “Old Spy, New Tricks”. 22 February 2001. http://www.wired.com/news/wireless/0,1382,41950,00.html (26 March 2001)

“Microsoft Outlook goes Mobile”. PDA News. 14 February 2001. http://www.pdanews.com.au/index.php?dir=10018&show=10879&layout=10010 (26 March 2001)

O’Connell, Peter. “Binion Jurors Take the Stand”. Las Vegas Journal – Review. 12 August 2000. http://12.9.217.5/plweb-cgi/fastweb?state_id=984878063&view=rjsearch&docrank=2&numhitsfound=65&query=Palm%20Pilot&query_rule=%28%28$query%29%29%20AND%20%28%23date%28$query1%29%29%3ADATE%20AND%20%28%28$query4%29%29%3AHEADLINE&docid=15752&docdb=2000&dbname=2000&TemplateName=predoc.tmpl&setCookie=1 (26 March 2001)

“Palm PDA User Security Notice”. NASA Headquarters Information & Technology Division. http://www.hq.nasa.gov/office/codec/codeci/help/hardware/palm.htm (26 March 2001)

“Sharp announces Linux PDA”. PDA News. 21 February 2001. http://www.pdanews.com.au/index.php?dir=10018&show=10955&layout=10010 (26 March 2001)

"The Forensic Challenge". The Honeynet Project. http://project.honeynet.org/challenge/ (26 March 2001)

Viotti, Vicki. "Didgets: Turning your Palm Pilot into a camera". The Honolulu Advertiser. 5 May 2000. http://the.honoluluadvertiser.com/2000/May/05/business13.html (26 March 2001)