A Defense-in-Depth Approach for Securing Mobile Devices and Wireless LANs

Sean P. McAleer

January 24, 2001

With the trend towards wireless LAN access and mobile computing devices such as PDAs, one would think that the walls are coming down on Information Security. These devices are here to stay and managers are looking for full connectivity and functionality with the corporate network. While securing these devices offers some new challenges, it is not a new challenge. Information Security managers need the same defense-in-depth approach to securing these devices as they have used to secure laptop computers with dial-up access.

Since the owner of the device is also a system administrator, a physical security manager, and a network security manager, there is the same requirement for strong security policies, technical standards, user awareness, and auditing as with the case with laptops. The first steps are to determine what information access the device will have and what will be the required security for the communications link. Then the manager must balance how much flexibility users need to do their job while still completing security requirements.

A Frame Work for Risk Analysis

In order for us to begin our analysis, we need to define what we are protecting. For the purposes of this paper, we will define the information asset as a large corporate network containing confidential information and transaction data for a financial institution. This environment requires strict access control to the corporate security network, as well as measures to ensure the integrity and availability of information.

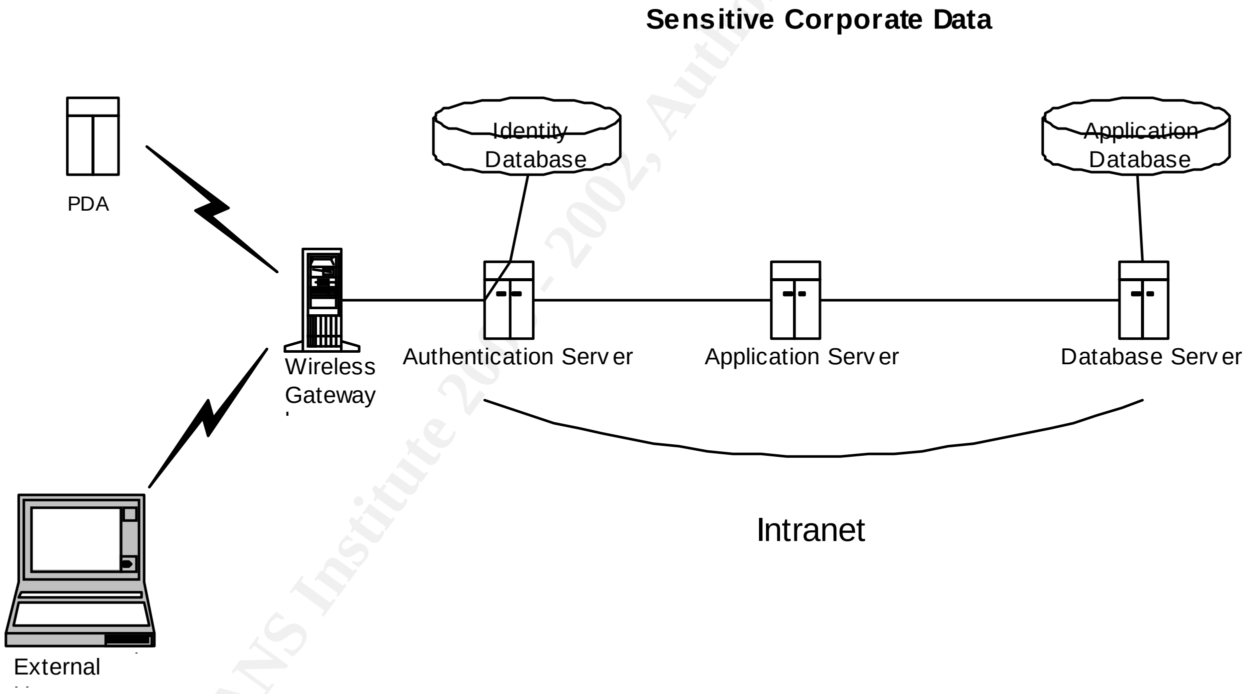
During the risk analysis, we can identify several scenarios that may cause a loss of confidentiality, integrity, or availability of information. However, the identification of "worst nightmare" or catastrophic cases for will be especially valuable during the definition of potential losses.

When outlining the risks associated with mobile devices, it will be hard to sell a security program unless there is a consensus about the risks involved. While it is beyond the scope of this paper to quantify the below risks in financial terms, this exercise may provide valuable insight as to which risks are tolerable.

Once the vulnerabilities have been identified, then we must decide how they will be eliminated, transferred, or reduced to achieve an acceptable level of security.

Our Wireless Application

For the purposes of this analysis, we will assume the following network topology and no direct Internet access from the mobile device. We will also define our LAN as a connection inside the corporate intranet that employs security zones to protect information through the use of access control servers, firewalls, and packet filtering. The LAN connection will use the 2.4 Ghz band.



Addressing the Threats for the Device

The information security threats to the devices (such as PDAs) with default configurations in a wireless LAN environment are very similar to those associated with a remote dial-up laptop or PC connection. These vulnerabilities can be addressed with different security policies and controls. However, there are always residual risks when users do not follow requirements:

POTENTIAL INCIDENT	POTENTIAL LOSS	COUNTERMEASURE	RESIDUAL RISK
Loss of plain text confidential files through the loss or theft of the device.	*-Loss of confidentiality and availability*	*-Data classification* *-Data back-up* *-Device Access Controls and secure configuration*	*-Poor control and physical security measures*
Attacker gains access to corporate network with stolen device	*-Loss of confidentiality and data integrity*	*- Device Access controls and secure configuration* *- Strong authentication*	*-User enables password caches* *-Passwords written down*
Attacker gains access to corporate network through the device.	*-Loss of confidentiality and data integrity*	*-Modem policy* *-Password policies* *-Authorized software* *-Device access controls and secure configuration*	*-Unauthorized external network connections and software*
Malware enters network from device	*-Loss of availability and integrity*	*-Anti-virus policy* *-Application filtering* *-Personal use restrictions*	*-Disabling anti-virus software*

Anti-virus Software: Several recent articles have highlighted the existence of viruses for the PalmOS and Windows CE operating systems. One virus, Phage, has already been identified on the Palm operating system.[1] Anti-virus software products for the PalmOS are now available from the major vendors and should be used on all devices. Incidentally, these risks would exist on both sides of the network connection with PCs and laptops accessing the wireless LAN.

Restricted downloading: In our example environment and of a corporate network, downloading of illegal software through a corporate network would pose the same risk and liability as it would if a normal PC that was conducting the illegal activity. Users also have the opportunity to install other connections on these devices and download files from other sources. These issues must be addressed in policies and audited for compliance.

Threats to the Communications Link

The communications link is the key difference in a wireless LAN. There have been many improvements in the development of secure protocols and security infrastructure in recent years.

The user will clearly have less control over threats to the communications link. However, one of the major concerns for the wireless communications link under Wireless Equivalency Privacy (WEP) mentioned in the IEEE 802.11b standard is the issue of using symmetric encryption.[2] With this type of a system, the entire group of participants in a distributed environment would need new keys if one device's key were compromised through loss or theft. What is possibly worse, the device could be trusted by the network or other devices if other authentication controls are not in use. While this could be managed with a small number of devices, this re-keying task becomes unmanageable in an application with hundreds of devices. Under the new proposed standard 802.1x, this is solved with Extensible Authentication Protocol (EAP).[3] This process will assign dynamic WEP keys and interface with strong authentication applications such as RADIUS. In addition to using an RC4 algorithm with a strong 128 bit key length, EAP is also resistant against man-in-the-middle attacks and repeat attacks. If interception of the transmission is a concern, the current system used with Palm devices does not provide adequate authentication and encryption for connection to secure networks.[4]

RISK/INCIDENT	POTENTIAL LOSS	COUNTERMEASURE	RESIDUAL RISK
Interception of signal by unauthorized person or other user *-plain text confidential information* *-login user id and password* *-Service Set Identifier information*	*-Loss of confidentiality, availability, and integrity.*	*-Data classification* *-Use of strong encryption in communications or Wireless Equivalency Protocol (WEP)* *-Strong authentication with Extensible Authorization Protocol (EAP)*	*Social engineering*
Unauthorized access to corporate network through wireless gateway using repeat attack	*-Loss of confidentiality and integrity*	*-Strong encryption or WEP* *-Strong authentication with EAP*	*Social engineering (difficult if biometrics are used)*
Unauthorized Device connects to Network	*-Loss of confidentiality and integrity*	*-Secure configuration of wireless access point* *-Strong authentication*	*Social engineering (difficult if biometrics are used)*
Man-in-the-middle attack	*-Loss of confidentiality and integrity*	*-Secure configuration of wireless access point* *-Strong authentication with EAP*	*-*
Denial of Service from signal jamming or interference	*-Loss of availability*	*-Frequency hopping*	*-The 2.4 Ghz band is an unlicensed broadcasts on band.*
Device Connects to unauthorized Wireless Gateway	*-Loss of availability, confidentiality, and integrity*	*-Secure configuration* *-Use of strong authentication with EAP*	*-User changes configuration or loads unauthorized software*

Malware uploaded from other Device or Network	*Loss of Integrity and availability*	*-Strong authentication* *-Packet filtering*	*-New virus not detected* *-User disables anti-virus software*

Authentication: Our corporate environment probably requires that we have a strong authentication process that uses two types of authentication and is resistant to repeat attacks. This requirement is addressed in 802.1x standards. Wireless devices that do not have 802.1x compliant network interface may not be allowed in this environment. Early versions of WTLS used weak encryption algorithms, delivered revealing error messages in the clear and provided plain text data during the initial connection calls.[5]

A Checklist for Policy, Procedure, and Technical Requirements

To begin our defense in depth, policies must be crafted. If not already addressed in current information security policies, then new policies for these devices need to be established. As we have already seen, may of these requirements will already be addressed in policies pertaining to remote access computing and network security.

If there is a "Wireless LAN and Mobile Computing Policy," then it should stipulate at least the following:

- What classification level of information may be stored on mobile devices and transmitted on the wireless LAN connections?
- How often must the information be backed-up?
- Can the computer be used for personal use?
- Is encryption required?
- Is anti-virus software required?

Sample policy statement:

Mobile computing devices such as laptop computers and PDAs may be connected to the corporate network through approved wireless gateways. The devices may be used for e-mail access and must have approved encryption software loaded for the storage of secret information. The user is required to back-up all information as required to ensure availability of data.

Procedures and Technical Requirements for Mobile Computing Devices

Once the appropriate policies have been referenced or established, the procedures for use of the devices in the network environment and technical requirements must be defined. Some of the procedural and technical issues that should be addressed are listed below:

- What hardware devices are authorized?
- What are the requirements and baseline configurations for mobile devices?
- What are the remote access devices to be used (wireless NICs)
- Restrictions for the use of IR ports and external connections
- Which configurations must be disabled on approved operating systems?
- What software applications are authorized?

- What network access controls will be used?
- What anti-virus software will be used and how will it be updated?
- Which device access controls must be in place such as automatic shutdown and disabled password caches?
- Which encryption program must be used for confidential data?

Procedures and Technical Requirements for Gateways

- What gateway devices may be used?
- What are required baseline configurations for the gateway?
- What services should the gateway allow to pass in and out?
- What secure protocols will the gateway use to communicate with devices (WEP)?
- What protocols will the gateway use to communicate with the corporate network (HTTP)?
- How must the gateway device be secured physically?
- How must the gateway device be secured logically?
- How much transmission power can be used and what type of antenna restrictions will be used?

User Training

Users of mobile computing devices require a much higher level of awareness training than does the normal PC user; however, the training requirements are not much different than the training required for laptop users. They are required not only to ensure the physical security of these devices, but they must also use extra caution to avoid writing down passwords, allowing cached passwords, and leaving confidential files unencrypted. As is true with laptop computers, there is also a significant risk of inappropriate use and excessive personal use of these devices that must be addressed with policy and understood.

Auditing for Compliance

One of the most difficult challenges is auditing for compliance. Users could be asked at random to bring in the device for a physical check, however, this is not very practical. Another option is imaging drives and storage media or conducting checks similar to that used with push applications such as anti-virus software updates. At any rate, this requirement cannot be overstated given the control and latitude users will have to modify default configurations on the devices.

Bibliography

[1] Todd, Susan "Threat of the New Computer Virus – The Palm/OS Phage Virus," SANS http://www.sans.org/infosecFAQ/wireless/phage_virus.htm
[2] "Wireless LAN Security," Cisco Systems, 2000

www.cisco.com

[3] Cisco Product Document, Cisco Systems, 2000 http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/350cards/pc350rn.htm#xtocid2911712

[4] Yen, Lumin and Polizo, James, “Network Security Architectures for Wireless Systems: The Palm VII Case – a First Look,” International Information Integrity Institute, September 2000

[5] Gillian, Stephen, “Vulnerabilities within the Wireless Application Protocol,” August 31, 2000 http://www.sans.org/infosecFAQ/wireless/WAP.htm