



Mobile Telephone Forensic Unit.

http://www.sectorforensics.co.uk/mobile_telephone_forensics.shtml

Wireless Handheld Device Security

by: Tom Olzak, 04/12/2005

<http://www.securitydocs.com/library/3188>

The world of business communication is changing. More employees are carrying electronic information in wireless handheld devices than ever before. These devices include smartphones and wireless PDAs. It is predicted that over four/fifths of mobile knowledge workers will have the opportunity to use wireless email by 2008, and smartphones may outnumber PDAs as electronic organizers by the end of 2006 (Dulaney et al, 2004).

This change in the way employees interface with company information presents some special challenges for security managers. The purpose of this paper is to help identify some of those challenges and to provide recommendations for reducing the associated risks to your business.

The Challenges

When an employee connects to your network with a handheld device, your security may be bypassed. Data can be moved in and out of your network without management's knowledge or control. The data that can be found on wireless handheld devices include:

1. Passwords and user ID's used to access corporate resources
2. In-process project information
3. Calendar items
4. Work contacts (fodder for social engineering attacks)
5. Electronic Protected Health Information (defined in HIPAA as ePHI)
6. Price lists
7. Employee information
8. Email
9. Company credit card information

Two major threats to this information are:

1. Loss of the handheld device
2. Malware attack

Loss

The loss of a handheld device containing sensitive information is a very real threat. A recent survey by Pointsec Mobile Technologies shows that, over a six month period, 21,460 PDA/Pocket PCs and 85,619 mobile phones were left in the back of cabs in Chicago alone (Missing in Action, 2005). This does not include devices left in airports and restaurants, stolen, etc. But this should not be a problem since your company's handheld devices are protected, right?

During a recent training session, I asked the attendees to raise their hand if they used a wireless handheld device at the office. About 15 hands went up. I then asked how many configured their device to require a password to gain access to the device. About 3 people raised their hands. I then asked how many displayed their name, address, and phone number on the device so that it could be easily returned to them. No hands went up.

Given the information that can be stored on a handheld device, the fact that password policies with associated enforcement through automated business rules usually do not exist is troubling. Even if the person finding a lost device is ethical and honest, he or she will not be able to return the device since no contact information is provided. This set of circumstances may result in:

1. The compromise of sensitive company information
2. The compromise of regulated information, such as ePHI
3. The unauthorized use of company information resources through the use of compromised user names and passwords
4. The loss of productivity due to the loss of information that was available only on the handheld device

Malware Attack

Prior to 2004, smartphones and wireless PDAs were not a preferred target of Malware developers. However, this is changing with the increasing number of wireless devices used worldwide. Current attacks are primarily focused on Symbian OS and Windows Mobile devices. Table 1 provides a brief history of Malware attacks on these platforms since mid-2004.

First Appeared				
Year	Month	Malware	OS Affected	Impact
2004	June	Cabir	Symbian	Affects mobile phones. Spreads via Bluetooth connections. Many variants appeared throughout 2004. No real damage caused by infection.
2004	August	Brador	Windows Mobile	Allows the remote control of Pocket PCs.
2004	November	Dust(a.k.a. Duts)	Windows Mobile	Pocket PC virus spread by synching with desktop, via Bluetooth connections, email, or Internet. No real damage caused by infection.
2004	November	Skulls	Symbian	Breaks all links to Symbian system applications. Replaces the icons with images of skulls. Variants continue to appear.
2005	January	Gavno	Symbian	Can infect to the point of making a phone unusable.
2005	January	Lasco	Windows Mobile Symbian	Proof of concept malware. The first to infect both Symbian and Windows Mobile platforms. No real damage caused by infection. Primary infection vector is Bluetooth connection.
2005	March	CommWarrior	Symbian	Spreads via Bluetooth connections. Resets phone on the 1st hour of the 14th of any month.

Table 1: Malware Outbreaks

Although most attacks to date have not been malicious, malware attacks may result in:

1. Loss of productivity
2. Exploitation of software vulnerabilities to gain access to resources and data
3. Destruction of information on a SIM card
4. Hi-jacking of air time resulting in increased costs

Risks associated with wireless handheld devices will continue to increase. The following section describes a layered model that will assist in securing your handheld environment.

The Solution

Your security program should manage the risks caused by wireless handheld devices with a layered approach. Figure 1 depicts a model for a layered security model.

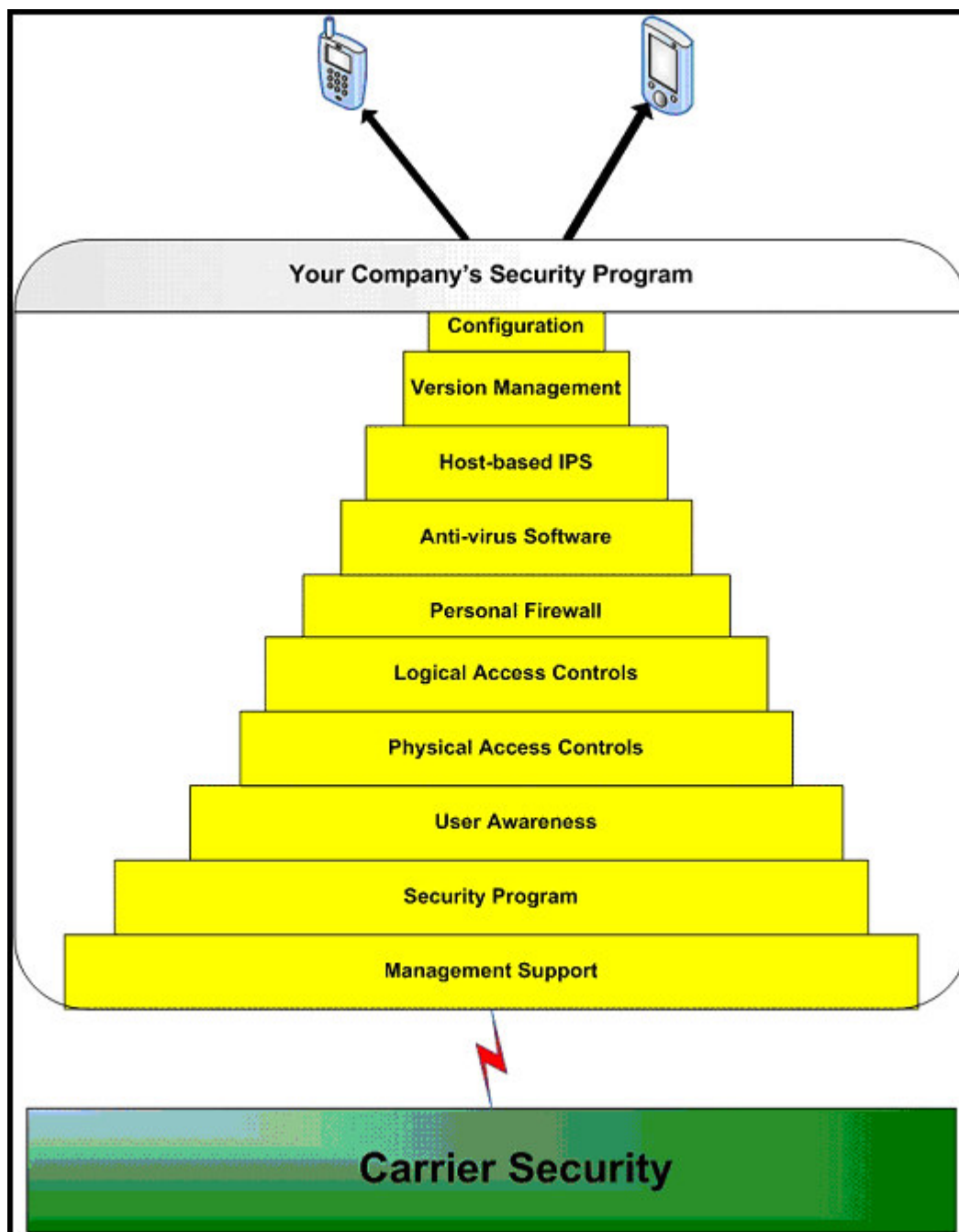


Figure 1: Wireless Handheld Device Security Model

The objective of layered security is to implement a variety of controls that, in their entirety, effectively neutralize incoming threats. Information moving to and from a wireless handheld device must pass through several different tests, both actual and virtual, before reaching its target. These layers comprise administrative, physical, and technical safeguards. The effectiveness of this model must extend to all devices, whether located on the company network, at home, or at a customer site.

Is it necessary to implement all layers to ensure end-user device security? Not necessarily. Which layers to implement, and to what extent, is a risk management decision. To help with this decision, each of the layers is discussed below.

Elements of Layered End-user Device Security

Carrier Security

If the wireless carrier you use for company handheld device communication is short on security practices, it will make your job much more difficult. Ensure the carrier you use has a well defined and operational security program that:

1. Keeps the handheld operating system (OS) up to date in order to take advantage of improved security technology, such as firewalls, code signing, intrusion prevention, encryption, etc.
2. Secures information in the carrier's data stores
3. Filters unwanted activity, including known and unknown
4. Provides strong end-to-end encryption

When you interface your network with that of a wireless carrier, make sure the carrier is as concerned about the security of your information as you.

Management Support

The foundation of any security program is management support. This support should be comprised, at a minimum, of effective policies, adequate budgets, and consistent enforcement. Efforts to change user behavior and to implement security measures carry no weight unless there is visible executive management support.

Security Program

An organization's security program facilitates the security objectives of management. It consists of policies and procedures.

Policies are high level statements of management's goals and objectives. They do not provide step-by-step directions to reach those goals and objectives; these directions are provided by procedures. A policy should consist of three elements:

1. Purpose
2. Scope
3. Compliance

The purpose of the policy clearly explains the objectives it is intended to achieve. It should also reflect management commitment to a secure enterprise. Scope describes all enterprise technology and activities affected by the policy. Finally, compliance defines consequences if the policy is not followed. It is the compliance piece – necessary to strongly encourage implementation - that is often missing from security policies.

Procedures are the administrative, physical, and technical recipes for producing a secure enterprise. They are derived from and support management policies. The step-by-step nature of procedures helps to ensure consistent compliance with security policy.

User Awareness

Unless fully engaged in the company's security efforts, end-users can be an organization's greatest vulnerability. Awareness training, and related activities, is the best way to obtain end-user participation in a security program. Training should include:

1. Review of policies
2. Procedure implementation
3. Password protection
4. How to deal with social engineering attacks
5. Proper protection of devices
 - a. Locking the device when finished

- b. Preventing the use of systems by unauthorized users
 - c. Elimination of potential shoulder surfing opportunities
 - d. Protecting the devices from loss or theft
6. Ensuring the information on a handheld device is absolutely necessary
 7. Ensuring the information on a handheld device is also stored on the company network where it is regularly backed up
 8. How to encrypt sensitive information

Enhancing user awareness should begin with new hire orientation. Existing employees should receive the same training at least annually. In addition to formal training, daily reminders should be everywhere in the workplace; posters and login messages are two good vehicles for reminder distribution. Finally, first line managers must ensure that security compliance is part of every operational task.

Physical Access Controls

The effectiveness of the security program is directly proportional to the effectiveness of the physical access controls surrounding electronic information. Strong passwords, biometrics, and other logical access methods will not prevent the financial loss associated with the theft or loss of critical business information. In addition, the level of effort applied to extracting information from secure devices within the normal business environment will probably fall far short of the effort applied in a cracker's basement.

Continuous effort is necessary to ensure that employees remain aware of the importance of maintaining physical control of their mobile information. Policies governing physical control may include:

1. Physically securing the device when it is not in use
2. Sanctions for failure to maintain physical control of the device

Logical Access Controls

Logical access controls prevent either unauthorized users from gaining access to any information resources or authorized users from gaining access to information for which they have no permissions. Logical controls include passwords, biometrics, and tokens. Regardless of the controls used, they should:

1. Have minimal impact on end-user productivity
2. Be reliable
3. Be effective with a ROI resulting from their initial and ongoing deployment costs

An analysis of the various logical access controls is beyond the scope of this paper. However, the following principles are provided as a guide:

1. Relying on strong, easy to forget passwords may be a mistake for your organization. Users often write down their passwords where can be potentially accessed by unauthorized individuals.
2. Establishing an effective account policy is crucial to a logical access control implementation. The policy should include
 - a. Automatic password expiration, usually 60 to 90 days
 - b. A minimum password length
 - c. Password history to ensure that a password is not reused when it expires
 - d. A threshold of login attempts that when exceeded locks the user account, usually set at 3
 - e. An effective lockout duration that will deter brute force attacks

Finally, it is a good idea to combine password controls with another access control, such as biometrics. This is known as two factor authentication. If a password is compromised, the second control will help stop unauthorized use of system resources.

Personal Firewall

A personal firewall should not be confused with the hardware firewall that is commonly found on company network perimeters. Rather, it is a set of related programs "...installed and administered on end-user devices to protect a single Internet-connected

computer from intruders” (Noakes-Fry & Diamond, 2004). The personal firewall acts as the first logical line of defense against penetration attacks. Some of the functions performed by a personal firewall are:

1. To screen incoming traffic and block suspicious code
2. To screen outgoing messages that infect other company resources
3. To prevent the unauthorized use of logical ports by hiding them from malicious code or human penetration attempts

Although I have separated antivirus and personal firewall software into two separate layers, most security software vendors provide solution suites that consist of both.

Antivirus Software

Malicious code attacks, including spyware, are the most common type of penetration into a company’s internal network. I provided a history of attacks against smartphones and wireless PDAs earlier in this paper. Like desktop and laptop systems, your handheld devices should run up-to-date antivirus software. In addition, you should strongly encourage your carrier to screen transmissions.

But no matter how up to date you keep your antivirus solution, there is always a delay between the time new malicious code is identified and when your software vendor provides an update. You can fill this gap with Host-based IPS.

Host-based IPS

There are two primary types of Intrusion Protection Systems (IPS)-Network and host. Network-based IPS systems protect the entire network or a network segment. Host-based IPS systems reside on and protect individual systems. In this model, we focus on host-based systems.

In an ideal environment, malicious code and unauthorized users are always denied access to handheld devices. In addition, the protections in an ideal environment prevent authorized users from destabilizing their systems as well as the network. But who works in an ideal environment?

Host-based IPS is a layer of protection that attempts to “catch” activities not blocked by the layers lower in the security model pyramid. These activities include, but are not limited to:

1. Deleting files
2. Moving files
3. Copying files
4. Installing executable files
5. Registry modifications
6. Denial of service processes

Version Management

An attacker can take advantage of one or more of the many publicly known vulnerabilities in the handheld device environment. Organizations that do not adequately update handheld OSs may face increasing costs associated with attacks that exploit these weaknesses.

Version management, as referenced in our model, is a set of policies, processes, and tools employed to ensure that all handheld devices are at the proper OS level. Processes include:

1. Checking vendor resources for new OS releases
2. Checking devices for current OS level
3. Applying OS updates as appropriate

These processes can be very time consuming and expensive if your carrier is not responsible for OS upgrades, leaving you to perform them manually. Most organizations are prime candidates for one of the many centralized mobile management

solutions available today. Attempting to manage the growing number of handheld devices across the enterprise without centralized control may result in costs higher than productivity gains.

Device Configuration

Training users to protect information on handheld devices is very important. However, companies must assist in this effort by locking down these devices through the use of centrally managed device policies. Device policies should be set in a system at the corporate office and automatically distributed and enforced. Policies managed in this way can include anything from forcing the use of passwords to controlling whether a device can connect at all. Policies you should strongly consider include:

1. Forcing the use of a password to access the device
2. Forcing the user to enter contact information so the device can be returned
3. Ensuring that all devices require end-user authentication.
4. Shutting down any service not required for proper operation, including Bluetooth capabilities
5. Controlling device configurations through the use of standard system settings that are locked to prevent modification.
6. Using the security features included in the operating system to restrict access to information, including encryption
7. Erasing all data on a handheld device when certain conditions are met
8. Automatic checking of each device to ensure it meets certain criteria, such as running antivirus software, before granting it access to the network
9. Requiring wireless access to the company network only through approved, secure paths

Putting It All Together

Each of the layers in this model supports the layer below it. It is the implementation of different safeguards at each layer that provides effective protection. Is it necessary to implement all the layers? Not necessarily. What to implement and how much to spend on implementation is a business decision; a business decision that should be based on the results of a risk assessment.

A risk assessment takes into account the potential threats to the device, the vulnerabilities of the device, and the business impact in dollars of a security incident directed at the device. The following formula defines the relationship between these risk elements:

Risk = Threats X Vulnerabilities X Business Impact

The resources applied to minimizing risk should be proportionate to the level of risk. Resources should be applied to reduce one or more of the risk factors as close to zero as possible. So what is the best approach to mitigating risk?

Another consideration is the impact of security controls on performance. Make sure there is a balance between securing company information and the ability of users to productively employ handheld devices.

Threats will always exist. Organizations have little control over this factor. Business impact is relatively static. There are, however, many opportunities to eliminate or mitigate vulnerabilities. The effective implementation of the layered model will result in reduced risk by eliminating or reducing end-user device vulnerabilities.

It is unreasonable to expect that any organization can completely eliminate losses related to wireless handheld devices. But the reasonable and appropriate application of a layered security model should help reduce risk to an acceptable level.

Works Cited

Dulaney, K., Hart, T. J., Basso, M., Fiering, L., Jones, N., Chapman, J., Simpson, R., & Redman, P. (2004). Predicts 2005: *mobile and wireless technologies*. Gartner document G00123537. Retrieved March 4, 2005 from <http://www.Gartner.com>

Missing in Action (2005, March). *Information Security*, 8(3), 22.

Noakes-Fry, K. & Diamond, T. (June, 2004). Personal firewalls: technology overview. Gartner document G00121188.
Retrieved December 19, 2004 from <http://www.Gartner.com>

Copyright 2005 Thomas W. Olzak. Tom Olzak, MBA, CISSP, MCSE, is President and CEO of Erudio Security, LLC. Tom can be reached at tom.olzak@erudiosecurity.com.