Mobile Device Security

Benjamin Halpert
Nova Southeastern University
bhalpert@nova.edu

ABSTRACT

Because of their small size, memory capability, and the ease with which information can be downloaded and removed from a facility, mobile devices pose a risk to organizations when used and transported outside physical boundaries. Mobile devices, including Personal Digital Assistants (PDAs), mobile phones, laptops, and smart phones can expose organizational data if not properly protected. This paper will cover areas of concern, different device types, and proposed solutions to mitigate the risks when using a mobile device.

Categories and Subject Descriptors

K.6.5 [**Security and Protection**]: *Authentication, Insurance, Invasive software (e.g., viruses, worms, Trojan horses), Physical security, Unauthorized access (e.g., hacking, phreaking)*

General Terms

Security, Management.

Keywords

Mobile, Security, Encryption, PDA, Laptop.

1. INTRODUCTION

Mobile device security is a major concern for organizations. Because of their small size, memory capability, and the ease with which information can be downloaded and removed from a facility, mobile devices pose a risk to organizations when used and transported outside physical boundaries. Mobile devices, including Personal Digital Assistants (PDAs), mobile phones, laptops, and smart phones can expose organizational data if not properly protected. This paper will cover different device types, areas of concern, and proposed solutions to mitigate the risks when using a mobile device. Wireless security issues are an integral part of assessing an organization's mobile device risk posture. However, discussion of wireless security is out of scope for this paper.

2. MOBILE DEVICE TYPES

Mobile devices come in many form factors. The majority of devices are classified as mobile include Personal Information Managers (PIMs), Personal Digital Assistants (PDAs), mobile phones, smart phones, camera phones, laptops, tablet personal computers (PCs), and removable storage media.

PIMs, PDAs, smart phones, and camera phones utilize operating systems such as Palm OS, Windows CE, Pocket PC, Smartphone 2002, Symbian, EPOC, and Linux. Laptop and Tablet PCs typically run more resource demanding operating systems to include Windows XP Professional, Mac OS X, and numerous Linux variants. Mobile devices are morphing into new form factors not traditionally associated with traditional PDAs. For example, Fossil has a product line called TECH. The TECH line has Wrist PDAs running the full PalmOne operating system and Wrist Net products from Microsoft [1, 2].

Removable media are also classified as mobile devices. Some examples of high density removable media include CompatFlash (CF), Secure Digital (SD), Memory Sticks, and removable USB drives, among others. One aspect that all mobile device types share is that they all lack adequate security mechanisms. As a result, third party security products will need to be evaluated and utilized to mitigate some of the risks of using mobile devices. The security ramifications of this fact will be explored further in subsequent sections.

3. AREAS OF CONCERN

Organizations are concerned about employee use of mobile device technologies for a multitude of reasons. First, the devices themselves are compact and have ever expanding internal memory capabilities. Beyond the device memory capabilities, most mobile devices can accommodate removable media that can store data, currently up to 1 Gigabyte, on SD cards that are roughly the size of a postage stamp. Both the combination of the portable device size and the additional removable memory capacity, create opportunities for sensitive and proprietary data to be removed from a facility and stored in an insecure fashion.

Mobile devices have become a target for individuals and groups involved in government espionage, corporate espionage, hacking, and device theft. As of the last report to congress, there are 75 known countries, both allies and enemies of the United States, that are actively pursuing US technologies [3]. From a device theft standpoint, mobile phones were targeted in roughly 28 percent of all robberies [4].

Not only do organizations need to be aware of espionage and theft related activities, but also employee forgetfulness and oversight must be addresses. Hurried travelers left 62,000 mobile phones, 2,900 laptops, and 1,300 PDAs in London taxi cabs over a six month period. That is an average of three phones per taxi [5].

4. RISK MITIGATION STRATEGIES

When analyzing risk mitigation techniques, organizations need to realize that 97 percent of the more than 3 million handheld

InfoSecCD Conference'04, October 8, 2004, Kennesaw, GA, USA.

devices deployed in the United States and used by employees are personally owned devices [6]. The ramifications of this fact are far reaching. Not only does an organization need to establish the proper processes, technologies, and awareness programs for the "approved" or "standard" device types, but they also must address the other 97 percent of devices that may be used within the organization.

4.1 General Protection Strategies

All mobile devices that may store, process, or transmit sensitive or proprietary data should utilize protection mechanisms that are commensurate with the mobile device capabilities. The device and the transmission to and from the device must be protected.

The following is a listing of precautions organizations should take to protect sensitive data on mobile devices:

- Utilize strong passwords consisting of alpha-numeric characters that are at least eight characters long and are unique.

- Install third party software protection mechanisms that can encrypt the contents of the mobile device, lock the device after a pre-specified time frame has passed, and wipe all the data from the device if the wrong password is entered more than the preset limit. An example product is PDA Defense [7]. For laptops and Tablet PCs, PC Guardian and PGP are product examples that can provide file based and full disk encryption [8, 9].

- Encrypt the device transmissions using an appropriate two-factor security mechanism, such as an RSA SecurID and a mobile VPN product, like the movianVPN from Certicom [10, 11].

- Install and update virus protection on all mobile devices. Many vendors produce anti-virus products for Tablet and Laptop PCs. The market for mobile anti-virus solutions is beginning to emerge. Currently, products are available from F-Secure and Trend Micro, among others. The most important aspect of mobile device anti-virus capability is to have the product do on-access scanning. Many of the current products only provide on-demand scanning, which is insufficient [12, 13].

- If a mobile device has wired or wireless network access capabilities, utilize a mobile firewall. An example product for PDA type devices is the Bluefire Mobile Firewall [14]. For laptops and tablet PCs, ZoneAlarm and Sygate Personal Firewall, among others, should be considered for deployment [15, 16].

- Most importantly, make sure that your organization has a mobile device policy that employees are familiar with. Create an awareness campaign to spread the word about mobile device security weakness and what employees can do to secure organizational, as well as personal, data on a mobile device. Hold Lunch and Learn sessions and present at organization events whenever possible. These are just some awareness suggestions.

4.2 Camera Phone Protection Strategies

In addition to the general risk mitigation techniques as described earlier, camera phones pose additional risks to organizational data and individual privacy. Many companies, including, BMW, DaimlerChrysler, and Samsung, prohibit camera phones from being brought onto company premises for fear that proprietary manufacturing methods and documentation may be photographed and removed from a facility. Additionally, many schools and health clubs have banned camera phones from locker rooms due to personal privacy issues [17].

4.3 USB Memory Device Protection Strategies

USB memory devices come in many form factors. Some look like normal writing pens while others fit on a key chain. Data can be removed easily from a facility if USB devices are allowed to be used. Even if prohibited, it may be hard to control the devices entering and exiting a facility.

Some techniques an organization can utilize to limit USB use are:

- Disable USB ports on servers and other systems containing sensitive data
- Disable auto-mounting features
- Prevent auto-installation of necessary drivers
- Restrict user access to existing devices

For securely transmitting data on a USB memory device, PGP can be used to encrypt the device contents or a secure USB product, such as the ClipDrive Bio, which provides data security via encryption and two-factor user authentication, password and finger-print biometric, for the USB memory device [9, 18].

5. CONCLUSION

Mobile device security is a major concern for organizations. Because of their small size, memory capability, and the ease with which information can be downloaded and removed from a facility, mobile devices pose a risk to organizations when used and transported outside physical boundaries. Familiarity with the different device types, areas of concern, and proposed solutions to mitigate the risks when using a mobile device are important for an organization to grasp prior to rolling out mobile devices to employees.

6. REFERENCES

[1] Palm: Wrist PDA http://www.fossil.com/jump.jsp?iMainCat=447&itemType=CATEGORY&itemID=448

[2] Microsoft: Wrist Net http://www.fossil.com/jump.jsp?iMainCat=450&itemType=CATEGORY&itemID=451.

[3] Annual Report to Congress on Foreign Economic Collection and Industrial Espionage—2002 (February 2003). http://www.ncix.gov/news/2003/may/Annual_Economic_Report_Version.pdf. Retrieved February 23, 2004

[4] Mobile phone crime prompts UK gov't to call for help. (January 8, 2002). *IT World.* Retrieved February 23, 2004, from http://www.itworld.com/Tech/2987/IDG020108phonetheft/pfindex.html

[5] Taxis a haven for forgotten goodies. (August 30, 2001). *BBC News.* Retrieved February 23, 2004, from http://news.bbc.co.uk/1/hi/uk/1518105.stm

[6] Walking Disasters. (April 24, 2000). *Computer World.* Retrieved February 23, 2004, from http://www.computerworld.com/news/2000/story/0,11280,46867,00.html.

[7] PDA Defense. http://www.pdadefense.com

[8] PC Guardian. http://www.pcguardiantechnologies.com/

[9] PGP. http://www.pgp.com

[10] RSA SecurID. http://www.rsasecurity.com/products/securid/

[11] Certicom movianVPN. http://www.certicom.com/index.php?action=product,mvpn

[12] F-Secure Anti-Virus™ for Pocket PC. http://www.f-secure.com/wireless/pocketpc/pocketpc-av.shtml

[13] Trend Micro PC –cillin for Wireless. http://www.trendmicro.com/en/products/desktop/pcc-wireless/evaluate/overview.htm

[14] Bluefire Security Technologies. http://www.bluefiresecurity.com

[15] Zone Labs ZoneAlarm. http://www.zonelabs.com/

[16] Sygate Personal Firewall. http://www.sygate.com/

[17] Camera phones don't click at work. (January 12, 2004). http://www.usatoday.com/money/workplace/2004-01-12-phones_x.htm

[18] Memory Experts International ClipDrive Bio. http://www.clip-drive.com/product_clipdrive_bio.htm