National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800-124

Guidelines on Cell Phone and PDA Security

Recommendations of the National Institute of Standards and Technology

Wayne Jansen
Karen Scarfone

NIST Special Publication 800-124

Guidelines on Cell Phone and PDA Security

Recommendations of the National Institute of Standards and Technology

Wayne Jansen
Karen Scarfone

C O M P U T E R S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

October 2008

U.S. Department of Commerce

Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology

Dr. Patrick D. Gallagher, Deputy Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 800-series reports on ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 800-124
Natl. Inst. Stand. Technol. Spec. Publ. 800-124, 51 pages (Oct. 2008)

Abstract

Cell phones and personal digital assistants (PDAs) have become indispensable tools for today's highly mobile workforce. Small and relatively inexpensive, these devices can be used for many functions, including sending and receiving electronic mail, storing documents, delivering presentations, and remotely accessing data. While these devices provide productivity benefits, they also pose new risks to organizations.

This document provides an overview of cell phone and PDA devices in use today and offers insights into making informed information technology security decisions on their treatment. The document gives details about the threats and technology risks associated with the use of these devices and the available safeguards to mitigate them. Organizations can use this information to enhance security and reduce incidents involving cell phone and PDA devices.

Acknowledgements

The authors, Wayne Jansen and Karen Scarfone, wish to thank their colleagues who reviewed drafts of this document and contributed to its technical content. Their appreciation also goes out to the individuals who reviewed the public-release draft of this document and provided comments during the review period. Improvements to the content would not have been possible without their feedback.

Table of Contents

Executive Summary

Cell phones and Personal Digital Assistants (PDAs) have become indispensable tools for today's highly mobile workforce. Small and relatively inexpensive, these devices can be used not only for voice calls, simple text messages, and Personal Information Management (PIM) (e.g., phonebook, calendar, and notepad), but also for many functions done at a desktop computer. The latter includes sending and receiving electronic mail, browsing the Web, storing and modifying documents, delivering presentations, and remotely accessing data. Mobile handheld devices may also have specialized built-in hardware, such as a camera, a Global Positioning System (GPS) receiver, and reduced-size removable-media card slots, and employ a range of wireless interfaces, including infrared, Wireless Fidelity (Wi-Fi), Bluetooth, and one or more types of cellular interfaces.

While these devices provide productivity benefits, they also pose new risks to an organization, including the following.

- Because of their small size and use outside the office, handheld devices can be easier to misplace or to have stolen than a laptop or notebook computer. If they do fall into the wrong hands, gaining access to the information they store or are able to access remotely can be relatively easy.
- Communications networks, desktop synchronization, and tainted storage media can be used to deliver malware to handheld devices. Malware is often disguised as a game, device patch, utility, or other useful third-party application available for download. Once installed, malware can initiate a wide range of attacks and spread itself onto other devices.
- Similar to desktop computers, cell phones and PDAs are subject to spam, but this can include text messages and voice mail, in addition to electronic mail. Besides the inconvenience of deleting spam, charges may apply for inbound activity. Spam can also be used for phishing attempts.
- Electronic eavesdropping on phone calls, messages, and other wirelessly transmitted information is possible through various techniques. Installing spy software on a device to collect and forward data elsewhere, including conversations captured via a built-in microphone, is perhaps the most direct means, but other components of a communications network, including the airwaves, are possible avenues for exploitation.
- Location tracking services allow the whereabouts of registered cell phones to be known and monitored. While it can be done openly for legitimate purposes, it may also take place surreptitiously.
- It is possible to create a clone of certain phones that can masquerade as the original. Once popular with analog phones, it is not as prevalent today with the rise of digital networks, but some early generation digital equipment has been shown to be vulnerable.
- Server-resident content, such as electronic mail maintained for a user by a network carrier as a convenience, may expose sensitive information through vulnerabilities that exist at the server.

To date, incidents from malware and other identified dangers that have occurred against handheld devices have been limited when compared with those against desktop and networked computers. One factor is that no single operating system dominates handheld devices to the same extent, fragmenting the number of potential homogeneous targets. Cellular network carriers have also favored a closed system approach in which they exerted control over devices and applications, as well as their networks. Nevertheless, an increasing amount of mobile malware has been reported over the past several years, which raises concerns

for the future, particularly when coupled with the recent trend towards establishing a more open system environment for cellular handheld devices. Such an open environment would not only facilitate application development and allow flexibility in choosing devices and applications from other sources, but it would also expedite malware development and potentially provide more attractive avenues of attack to exploit.

This document is intended to assist organizations in securing cell phones and PDAs. More specifically, this document describes in detail the threats faced by organizations that employ handheld devices and the measures that can be taken to counter those threats. The following key guidelines are recommended to Federal departments and agencies.

Organizations should plan and address the security aspects of organization-issued cell phones and PDAs.

Because security is much more difficult to address once deployment and implementation are underway, it should be considered from the beginning. Cell phones and PDAs are in many ways like desktop computers constructed in a more compact form; however, mobile handheld devices have important differences from them. For example, handheld devices are generally treated more as fixed appliances with a limited set of functions than as general-purpose desktop systems with the capability for expansion. Operating system upgrades and patches occur far less frequently than with desktop computers, and changes to firmware can be more daunting to carry out and have more serious consequences, such as irreversibility and inoperability. Augmenting a device with defenses against malware and other forms of attack is an important consideration in planning, as is centralizing device security management.

Organizations are more likely to make decisions about configuring mobile handheld devices securely and consistently when they develop and follow a well-designed plan for implementation. Developing such a plan helps identify critical issues and guides administrators in making tradeoff decisions between usability, performance, and risk. Existing system contingency, continuity of operations, and disaster recovery plans should also be extended to account for mobile handheld devices issued by the organization.

Organizations should employ appropriate security management practices and controls over handheld devices.

Appropriate management practices are essential to operating and maintaining a secure infrastructure that incorporates cell phones and PDAs. Security practices entail the identification of an organization's information system assets and the development, documentation, and implementation of policies, standards, procedures, and guidelines that help to ensure the confidentiality, integrity, and availability of information system resources. To ensure the security of the infrastructure, the following practices should be implemented for handheld devices:

- Organization-wide security policy for mobile handheld devices
- Risk assessment and management
- Security awareness and training
- Configuration control and management
- Certification and accreditation.

Organizations should ensure that handheld devices are deployed, configured, and managed to meet the organizations' security requirements and objectives.

Many security issues can be avoided if the devices are configured appropriately. The overarching principle is to institute only the required capabilities and services and to eliminate known vulnerabilities through patches, upgrades, and additional safeguards. Default system and application settings on a device may emphasize features, functions, and ease of use, at the expense of security. Administrators should configure devices in accordance with their organization's security requirements and reconfigure them as those requirements change. Security configuration guides or checklists, when they are available, can assist administrators in securing systems consistently and efficiently. Securing a cell phone or PDA would generally include the following steps:

- Apply available critical patches and upgrades to the operating system
- Eliminate or disable unnecessary services and applications
- Install and configure additional applications that are needed
- Configure user authentication and access controls
- Configure resource controls
- Install and configure additional security controls that are required, including content encryption, remote content erasure, firewall, antivirus, intrusion detection, antispam, and virtual private network (VPN) software
- Perform security testing.

Organizations should ensure an ongoing process of maintaining the security of handheld devices throughout their lifecycle.

Maintaining handheld device security requires constant effort, sufficient resources, and vigilance from an organization. Maintaining the security of a handheld device usually involves the following steps:

- Instruct users about procedures to follow and precautions to take, including the following items:
    - Maintaining physical control of the device
    - Reducing exposure of sensitive data
    - Backing up data frequently
    - Employing user authentication, content encryption, and other available security facilities
    - Enabling non-cellular wireless interfaces only when needed
    - Recognizing and avoiding actions that are questionable
    - Reporting and deactivating compromised devices
    - Minimizing functionality
    - Employing additional software to prevent and detect attacks.

- Enable, obtain, and analyze device log files for compliance
- Establish and follow procedures for recovering from compromise
- Test and apply critical patches and updates in a timely manner
- Evaluate device security periodically.

With organization-issued devices, centralized security management is often an important consideration, since it simplifies the configuration control and management processes needed to ensure compliance with the organization's security policy. A number of products provide centralized security management and oversight of cell phones and PDAs through the network infrastructure. The depth and breadth of capabilities that can be controlled vary among products. The following items are some common examples:

- Device registration
- Installation of client software, policy rules, and control settings
- Controls over password length and composition, number of entry attempts, etc.
- Remote password reset
- Remote erasure or locking of the device
- Controls to restrict application downloads, access, and use
- Controls over infrared, Bluetooth, Wi-Fi, and other means of communication
- Controls to restrict camera, microphone, and removable media use
- Controls over device content and removable media encryption
- Controls over VPN, firewall, antivirus, intrusion detection, and antispam components
- Remote update of client software, policy rules, and control settings
- Remote diagnostics and auditing
- Device compliance status reporting
- Denial of services to non-compliant or unregistered devices.

1. Introduction

The use of handheld devices has rapidly grown in recent years due to their convenience and inexpensiveness when compared to laptop or notebook computers. These devices are no longer viewed as coveted gadgets for early technology adopters; instead, they have become indispensable tools that provide competitive advantages for the mobile workforce and individual users [Mot08a]. Because of their pervasiveness in society, the security implications of these devices are a growing concern for many organizations and the impetus behind this document.

1.1 Authority

The National Institute of Standards and Technology (NIST) developed this document in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets; but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), "Securing Agency Information Systems," as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by Federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright, though attribution is desired.

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority, nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official.

1.2 Purpose and Scope

The purpose of this document is to provide an overview of cell phone and PDA devices in use today and offer insight into making informed information technology security decisions on their treatment. The discussion gives details about the threats, technology risks, and safeguards for these devices.

This document may be used by organizations interested in enhancing security to reduce related security incidents for current and future use of handheld devices. This document presents generic principles that apply to all such systems.

This guideline does not cover the following aspects relating to securing handheld devices:

- Ultra-Mobile Personal Computers (UMPC) that have the same characteristics as tablet or notebook computers, but in a very compact format
- MP3 players, cameras, calculators, and other handheld devices that are not typically used in organizational tasks or have limited textual information processing capabilities
- USB flash memory drives or pocket-size removable hard drives with USB, FireWire, or other high-speed interfaces

- Removable media, such as rewritable CDs, floppy drives, and zip drives not normally supported by handheld devices.

1.3 Audience

The intended audience for this document includes the following:

- Users of cell phones, PDAs, and other business-oriented handheld devices
- Security professionals, including security officers, security administrators, auditors, and others with information technology security responsibilities
- Information technology program managers concerned with system lifecycle security measures for handheld devices
- System and network administrators involved in supporting handheld devices,

This document, while technical in nature, provides background information to help readers understand the topics that are covered. The material presumes that readers have some minimal operating system and networking expertise and some experience using handheld devices. Because of the evolving nature of handheld device security issues, readers are expected to take advantage of other resources, including those listed in this document, for more current and detailed information.

1.4 Document Structure

The remainder of this document is organized into the following major sections:

- Section 2 presents an overview of handheld devices and discusses associated security problems.
- Section 3 discusses the security concerns associated with handheld devices.
- Section 4 discusses the safeguards available for mitigating the risks and threats discussed in previous sections.
- Section 5 contains a list of references.

The document also has appendices that contain supporting material. Appendix A contains a glossary of terms. A list of acronyms is found in Appendix B.

2. Device Overview

Handheld devices come in many different form factors, ranging from clamshell compacts to candy bar-shaped designs. Their capabilities can also differ widely, but at the core certain similarities abound. This section looks at those similarities and differences and provides background information to set a foundation for the discussion in the remaining sections of this guide.

2.1 Personal Digital Assistants

PDAs have their origins in simple digital organizers for telephone numbers. The first true PDA, the Newton from Apple, appeared in 1993 [CNI06]. Its main features were fax and email communications, built-in personal information management applications (e.g., contacts, calendar, notes), character recognition of pen-based input entered on a touch screen, and data synchronization with a desktop computer. These same characteristics can be seen in present-day PDA devices.

PDAs are in many ways like handheld personal computers; however, they have important differences. For example, PDAs are designed for mobility, hence compact in size and battery powered. They store user data in solid-state memory instead of a hard disk, and they hibernate to conserve battery power and avoid a time-consuming reboot when needed again. Because data retained in volatile memory is subject to loss and even data in non-volatile memory can be cleared if the device is reset, PDAs are also designed to synchronize data with a desktop computer and automatically reconcile and replicate data between the two devices.

Most types of PDAs have comparable features and capabilities. They house a microprocessor, Read Only Memory (ROM), Random Access Memory (RAM), a variety of hardware keys and interfaces, and a touch-sensitive display screen. The Operating System (OS) of the device is held in ROM. Several varieties of ROM are used, including Flash ROM, which can be erased and reprogrammed electronically with OS updates or an entirely different OS. Flash ROM may also be used to store critical user data and applications. RAM, which normally contains user data, is kept active by batteries whose failure or exhaustion causes all information to be lost.

The latest PDAs come equipped with system-level microprocessors that reduce the number of supporting chips required and include considerable memory capacity. Built-in Compact Flash (CF) and combination Secure Digital (SD)/MultiMedia Card (MMC) slots support memory cards and peripherals, such as a digital camera or wireless communications card. Wireless communication capabilities such as Infrared Data Association (IrDA), Bluetooth, and Wi-Fi may also be built in.

Different devices have different technical and physical characteristics (e.g., size, weight, processor speed, memory capacity). Devices may also use different types of expansion capabilities (e.g., I/O and memory card slots, device expansion sleeves, and external hardware interfaces) to provide additional functionality. PDA capabilities sometimes appear in other devices such as cell phones and GPS receivers. PDAs with cellular communications capabilities are generally considered to be smart phones, a class of cell phones discussed in more detail in Section 2.2.

The two most prominent families of PDA devices revolve around the operating systems used: Microsoft Windows Mobile (formerly Pocket PC) and Palm OS. Some Linux-based PDAs are also manufactured. Regardless of the PDA family, all devices support a set of basic PIM applications, which include contact, calendar, email, and task management. In addition, most PDAs provide the ability to communicate wirelessly, review electronic documents, and access Web sites. The ability to install third-party

applications or to develop them using an available Software Development Kit (SDK) or Integrated Development Environment (IDE) is also a common feature.

PIM data residing on a PDA can be synchronized with a desktop computer or server using synchronization protocols such as Microsoft's ActiveSync protocol and Palm's HotSync protocol. Synchronization protocols can also be used to exchange other kinds of data (e.g., text files, images, and other media formats). A cable to link the PDA to a desktop computer is often supplied with the device to facilitate synchronization; it may also be possible to use a wireless interface for synchronization.

2.2 Cell Phones

Cell phones are somewhat similar to PDAs, but with an important difference—they support one or more radio interfaces to cellular telecommunications networks. They also have a different heritage. Early cell phones appeared in the U.S. in 1978 when AT&T conducted field trials authorized by the Federal Communications Commission in Chicago and Newark, New Jersey [ATT08]. The devices had the size and weight of a brick and were limited to voice communications. Since then, vast improvements have been made in the form factor of handsets, the communications capability of networks, and the services available.

Present-day cell phones are highly mobile communications devices that can also perform an array of other functions ranging from that of a simple digital organizer to that of a PDA. They are compact in size, battery powered, and lightweight, generally smaller and lighter than a PDA. Like a PDA, they house a microprocessor, various types of ROM, and RAM, but the display screen is usually not touch sensitive. Cell phones also include a radio module, a digital signal processor, and a microphone and speaker for voice communications. Flash ROM, a type of persistent memory, is normally used to store user data. The operating system of a cell phone is held in ROM.

As with PDAs, system-level microprocessors are used in cell phones to reduce the number of supporting chips required. Built-in Mini Secure Digital (MiniSD), MultiMedia Card Mobile (MMCmobile), or other types of reduced-size card slots may be included to support removable memory cards or specialized peripherals, such as an SD Input Output (SDIO) Wi-Fi card. Wireless communications such as infrared (e.g., IrDA) and Bluetooth are often built into the device. Other wireless communications, such as Wi-Fi, and Worldwide Interoperability for Microwave Access (WiMAX), may also be built in. Some phones partition certain capabilities into identity modules that can be removed from the handset; they are discussed further in Section 2.2.2.

Different devices have considerably different technical and physical characteristics (e.g., size, weight, processor speed, memory capacity), and devices may also use different types of expansion capabilities to provide additional functionality. Cell phones have steadily incorporated capabilities found in other handheld devices such as digital music players and cameras.

Bluetooth Communications: Bluetooth is a Personal Area Network (PAN) standard that enables wireless connections between electronic devices in the 2.4 GHz range over short distances, as an alternative to cables. Designed to be power efficient, Bluetooth has become a common feature in cell phones. Since wireless communications are inherently insecure, a number of basic security provisions have been defined for this standard to mitigate the risks involved. The three basic security services are defined by the Bluetooth specifications:

- Authentication - to verify the identity of communicating devices; only devices that properly authenticate can engage in communications.

- Confidentiality - to prevent information exposure from eavesdropping; only authorized devices can view data.
- Authorization - to control access to resources; only authorized devices can use a designated service.

The Bluetooth technical specifications have evolved over the years since their initial release. In mid-2007, version 2.1+Enhanced Data Rate (EDR) was issued, which included substantial improvements to security [Bak07]. In particular, a new security mode that uses Secure Simple Pairing (SSP) was defined as a service level enforced security mode, in which the three basic security services listed above may be instituted after connection establishment occurs.

Pairing is the process that allows two Bluetooth devices to associate themselves with one another by generating a shared link authentication key for use in future communications. SSP supports four association models, some of which can greatly simplify the user interaction required and protect against passive eavesdropping and man-in-the-middle attacks that were a source of concern with earlier versions of the specifications. With earlier versions, if the pairing and authentication exchanges were monitored and recorded, a brute force algorithm could be used to readily determine the link key [Sha05]. SSP uses the Elliptic Curve form of Diffie-Hellman public key cryptography to generate the link key, which imposes a significantly harder problem for an attacker to solve to derive the key than does the legacy pairing process.

Many existing cell phones and PDAs were produced before the current Bluetooth specifications and do not support the new SSP security mode. For these devices, three legacy security modes compliant with earlier versions of the specifications are relevant: non-secure mode, where no basic security services are enabled; service level enforced security mode, in which all three basic security services can be instituted after connection establishment occurs and access controls can be defined by policy; and link level enforced security mode, in which authentication (unidirectional or mutual) and encryption services can be instituted before connection establishment. Further details about the new and legacy security modes can be found in the current specifications [BTS07].

The introduction of SSP affects use of legacy security modes for version 2.1+EDR compliant devices. The new SSP mode is compulsory and the two legacy modes of no security and link level security are excluded for such devices. The remaining legacy mode of service level enforced security is conditional—to be used only for connecting to remote legacy devices that do not support SSP. Devices compliant with earlier versions of the specification must rely on the legacy security modes for communications among themselves. More comprehensive information from NIST about Bluetooth security is also available [Sca08].

Cell phones can be classified as basic phones that are primarily simple voice and messaging communication devices; advanced phones that offer additional capabilities and services for multimedia; and smart phones or high-end phones that merge the capabilities of an advanced phone with those of a PDA. This classification scheme is illustrative, since the features of actual devices do vary and can span more than one category. Over time, the trend has been for advanced features to appear in more basic phones as new features are added to high-end phones. Although the lines among this classification scheme are somewhat fuzzy and dynamic, it nevertheless serves as a general guide for discussion purposes.

Regardless of the type of cell phone, nearly all devices support voice calls and Short Message and Enhanced Messaging Service (SMS and EMS) text messaging not typically found in PDAs. Like PDAs, however, they also support basic PIM applications for phonebook and calendar, and often a means to synchronize PIM data with a desktop computer. Cell phones may also have the ability to synchronize data over-the-air with a server maintained by the cellular carrier, using the cellular network interface. More advanced devices provide capabilities to connect to the Internet and access Web sites, exchange electronic mail or multimedia messages, or chat using instant messaging. They may also provide enhanced PIM applications that work with specialized built-in hardware, such as a camera.

Smart phones add PDA-like capabilities for reviewing electronic documents (e.g., reports, briefing slides, and spreadsheets) and running a wide variety of general and special-purpose applications. Smart phones are typically larger than other phones, support a more substantial display with greater resolution (e.g., ¼ VGA and higher), and may have an integrated QWERTY keyboard or touch-sensitive screen. They also offer more extended expansion capabilities through peripheral card slots, other built-in wireless communications such as Bluetooth and Wi-Fi, and synchronization protocols to exchange other kinds of data beyond basic PIM data (e.g., graphics, audio, and archive file formats).

A cell phone manufacturer may support several different OS platforms in its product line (e.g., [Mot08b]). Basic and advanced cell phones typically use a company-proprietary operating system. Various real-time operating system solutions are also available for cell phone manufacturers from companies that specialize in embedded system software. Nearly all smart phones use one of the following operating systems: Palm OS, Windows Mobile (phone edition), Research in Motion (RIM) OS, Symbian OS, iPhone OS, and Linux. Unlike the more limited, real-time kernels in basic and advanced phones, these operating systems are multi-tasking and full featured, designed specifically to match the capabilities of high-end mobile devices. Besides an assortment of applications, they often come complete with a Java Virtual Machine and support for native applications through an SDK for C++ or another programming language.

It is important to note that the set of capabilities supported by a phone also requires matched support from the underlying communication services. For example, if data services have not been subscribed for the phone, advanced messaging, Web browsing, and other IP address-based Internet services cannot function.

2.2.1 Cellular Communications

The ability to communicate over cellular networks distinguishes cell phones from other types of handheld devices. As the name implies, cellular networks provide coverage based on dividing a large geographical service area into smaller areas of coverage called cells. Cells play an important role in reuse of radio frequencies in the limited radio spectrum available to allow more calls to occur than otherwise would be possible. As a mobile phone moves from one cell to another, a cellular arrangement requires active connections to be monitored and effectively passed along between cells to maintain the connection.

Within the U.S., different types of digital cellular networks abound that follow distinct, incongruous sets of standards. The two most dominant types of digital cellular networks in the U.S. are known as Code Division Multiple Access (CDMA) and Global System for Mobile Communications (GSM) networks. Other common cellular networks include Time Division Multiple Access (TDMA) and Integrated Digital Enhanced Network (iDEN). iDEN networks use a proprietary protocol designed by Motorola, while the others follow standardized open protocols. A digital version of the original analog standard for cellular telephone phone service, called Digital Advanced Mobile Phone Service (D-AMPS), also exists.

Cellular networks are also characterized by generation. First generation or 1G refers to analog technology on which cellular networks originated. Analog cellular networks are no longer supported by the major cellular carriers and perhaps only a few small carriers in rural areas continue to support them [Law08]. Second generation or 2G designates the original fully digital networks mentioned above that offered greater efficiency, performance, and services than 1G analog technology. Third generation or 3G network standards exist, which offer even higher data rates. Sometime fractional designations such as 2.5G are used to designate incremental improvements between two generations. Different generational digital cellular networks can be found across the U.S. as cellular carriers update equipment to support newer digital technologies.

CDMA refers to a technology designed by Qualcomm in the U.S., which employs spread spectrum communications for the radio link. Rather than sharing a channel, as many other network air interfaces do, CDMA spreads the digitized data over the entire bandwidth available, distinguishing multiple calls through a uniquely assigned sequence code. Successive versions of the IS-95 standard from the Telecommunications Industry Association (TIA) define CDMA conventions in the U.S., which is the reason why the term CDMA is often used to refer to IS-95 compliant cellular networks. IS-95 CDMA systems are sometimes referred to as cdmaOne. The next evolutionary step for CDMA towards 3G services is cdma2000, TIA/EIA/IS-2000 Series , Release A, based on the ITU IMT-2000 standard. Radio interfaces for cdma2000 include One times Radio Transmission Technology (1xRTT) and Evolution-Data Optimized (EV-DO), each offering increasing levels of performance over cdmaOne. Both Verizon and Sprint operate nationwide CDMA networks in the U.S.

GSM is a cellular system used worldwide that was designed in Europe, primarily by Ericsson and Nokia. Cingular and T-Mobile operate nationwide networks in the U.S. GSM uses a TDMA air interface. TDMA refers to a digital link technology whereby multiple phones share a single-carrier radio-frequency channel by taking turns—using the channel exclusively for an allocated time slice, then releasing it and waiting briefly while other phones use it. A packet switching protocol enhancement to GSM wireless networks called the General Packet Radio Service (GPRS) was standardized to improve the transmission of data. Enhanced Data rates for GSM Evolution (EDGE) is a later augmentation to GPRS that provides higher levels of performance. The 3G evolutionary step for GSM is known as Universal Mobile Telecommunications System (UMTS) and involves enhancing GSM networks with a Wideband CDMA (W-CDMA) air interface.

TDMA is also used to refer specifically to the standard covered by IS-136, which defines a specific type of cellular network. Using the term TDMA to refer to a general technique or a specific type of cellular network can be a source of confusion. For example, although GSM uses a TDMA air interface (i.e., the general technique), as does iDEN, neither of those systems is compatible with so-called TDMA cellular networks that follow IS-136.

Mobile phones work with certain subsets of the network types mentioned, typically those associated with the service provider providing the phone and from whom a service agreement was arranged. For example, a service provider or network operator for a GSM network that has some older TDMA network segments in operation might supply a phone with GSM voice and data capabilities and also TDMA capabilities. Such a phone would not be compatible with CDMA networks. Mobile phones with both GSM and CDMA capabilities exist. Mobile phones may also be acquired without service from a manufacturer, vendor, or other source, and be set up for service separately with a service provider or network operator, provided that the phone is compatible with the network. This sort of network portability is a common trait of phones that support identity modules.

Despite their differences in technology, cellular networks are organized similarly to one another. The main components are the radio transceiver equipment that communicates with mobile phones, the controller that manages the transceiver equipment and performs channel assignment, and the switching system for the cellular network. The technical names for these components are respectively the Base Transceiver Station (BTS), the Base Station Controller (BSC), and the Mobile Switching Center (MSC). The BSC and the BTS units it controls are sometimes collectively referred to as a Base Station Subsystem. The MSC uses several databases to perform its tasks, including a central repository system for subscriber data and service information.

2.2.2 Identity Modules

Subscriber Identity Modules are synonymous with certain mobile phones and devices that interoperate with GSM cellular networks. Under the GSM framework, a cellular phone is referred to as a Mobile Station and is partitioned into two distinct components: the Subscriber Identity Module (SIM) and the Mobile Equipment (ME). As the name implies, a SIM is a removable component that contains essential information about the subscriber, including the subscriber's assigned International Mobile Subscriber Identity (IMSI). The ME, the remaining radio handset portion, cannot function fully without one. The SIM's main function entails authenticating the cell phone to the network to gain access to subscribed services for the user. The SIM also provides storage for personal information, such as phone book entries and text messages, as well as service-related information.

The SIM-ME partitioning of a cell phone stipulated in the GSM standards has brought about a form of portability. Moving a SIM between compatible cell phones automatically transfers with it the subscriber's identity and the associated information and capabilities. In contrast, present-day CDMA phones do not employ a SIM. Analogous SIM functionality is instead directly incorporated within the device. While SIMs are most widely used in GSM systems, comparable modules are also used in iDEN phones and UMTS user equipment (i.e., a USIM). Because of the flexibility a SIM offers GSM phone users to port their identity, personal information, and service between devices, eventually all cellular phones are expected to include (U)SIM-like capability. For example, requirements for a Removable User Identity Module (R-UIM), as an extension of SIM capabilities, have been specified for cellular environments conforming to TIA/EIA/IS-95-A and -B specifications, which include Wideband Spread Spectrum based CDMA [3GP02].

At its core, a (U)SIM is a special type of smart card that typically contains a processor and between 16 to 128 KB of persistent Electronically Erasable, Programmable ROM (EEPROM). It also includes RAM for program execution and ROM for the operating system, user authentication and data encryption algorithms, and other applications. The (U)SIM's hierarchically organized file system resides in persistent memory and stores such things as names and phone number entries, text messages, and network service settings. Depending on the phone used, some information on the (U)SIM may coexist in the memory of the phone. Information may also reside entirely in the memory of the phone instead of available memory reserved for it in the file system of the (U)SIM [Wil05, Jan06].

The (U)SIM operating system controls access to elements of the file system [3GP05a]. Actions such as reading or updating can be permitted or denied unconditionally, or allowed conditionally with certain access rights. Rights are assigned to a subscriber through four to eight digit Personal Identification Number (PIN) codes. PINs protect core (U)SIM subscriber-related data and certain optional data. PIN codes can be modified by the subscriber and their function disabled or enabled. A preset number of attempts, usually three, are allowed for providing the correct PIN code to the (U)SIM before further attempts are blocked completely, rendering communications inoperative. Only by providing a correct PIN Unblocking Key (PUK) can the value of a PIN and its attempt counter be reset on the (U)SIM. If the number of attempts to enter the correct PUK value exceeds a set limit, normally ten attempts, the card becomes blocked permanently. The PUK for a PIN can be obtained from the service provider or network operator by providing the identifier of the SIM (i.e., its Integrated Circuit Chip Identifier or ICCID). The ICCID is normally imprinted on the (U)SIM, but can also be read from an element of the file system.

(U)SIMs have a width of 25 mm, a height of 15 mm, and a thickness of 0.76 mm, which is roughly the footprint of a postage stamp. Though similar in dimension to MiniSD or MMCmobile removable memory cards supported by some cell phones, (U)SIMs follow a different set of specifications with vastly different characteristics. For example, their pin connectors are not aligned along a bottom edge as with removable media cards, but instead form a circular contact pad integral to the smart card chip, which is

embedded in a plastic frame. (U)SIMs also employ a broad range of tamper-resistance techniques to protect the information they contain.

The slot for the (U)SIM card is normally not accessible from the exterior of the phone to facilitate frequent insertion and removal, as with a memory card. Instead, it typically is found in the battery compartment under the battery. When a (U)SIM is inserted into a phone handset and pin contact is made, a serial interface is used for communicating between them. A (U)SIM can be removed from a phone and read using a specialized (U)SIM reader and software through the same interface. Standard-size smart card adapters are also available for (U)SIMs, which allows them to be inserted into and read with a conventional smart card reader.

Authenticating a device to a network securely is a vital function performed via the SIM. Cryptographic key information and algorithms within the tamper-resistant module provide the means for the device to participate in a challenge-response dialogue with the network and respond correctly, without exposing key material and other information that could be used to clone the SIM and gain access to a subscriber's services. Cryptographic key information in the SIM also supports stream cipher encryption to protect against eavesdropping on the air interface [Ved93, Wil03].

2.3 Software Applications

With the exception of low-end cell phones, most cell phones and PDAs can be extended with application software to perform additional tasks. Application software can range from simple games used for recreation to special-purpose programs developed for enterprise use. However, software applications are highly dependent on the computational resources and capabilities of the device in question. Since the hardware and software environment can vary widely among handheld devices, it often becomes a factor when selecting or developing software applications as well as selecting compatible peripheral equipment that may be needed for an application.

Applications tend to be available for certain classes of devices within a device manufacturer's product line, or between different manufacturers' product lines. Application coverage can be more widespread if common middleware such as Java or Brew is present on devices from different device manufacturers, or if a common manufacturer-independent operating system such as Symbian or Windows Mobile is used across the devices. Application software product manufacturers sometimes implement their application on more than one popular operating system or middleware platform to support a larger market.

Organizations are often interested in software solutions that can be deployed across a range of supported handheld devices and are compatible with network infrastructure services. Therefore, devices purchased for organizational use may be limited to certain families of devices. The push mail service offered through RIM's backend BlackBerry Enterprise Server for corporate electronic mail synchronization with BlackBerry and other compatible devices is one example.

The availability of an SDK for certain types of platforms is another motivation for limiting device selection by organizations that develop in-house applications for handheld devices or plan to do so in the future. Different device manufacturers offer distinct SDKs for their devices and may target only a subset of those devices. For example, Nokia offers individual Java SDKs for its series 40 and series 60 devices and an additional C++ SDK for its series 60 devices. No SDK exists for its series 30 devices. The series 30 and series 40 devices use the proprietary Nokia OS, while the series 60 devices use Symbian.

Specialized applications may also be provisioned via handhelds, particularly cell phones, by government municipalities or organizations for their citizens. Micro payment applications used to pay fees for public transport or public parking spaces are a common example. Organizations are also adopting mobility to

drive more effective and efficient operations in areas such as health care. Through deployment of mobile devices, field activities previously done manually are being automated as extensions to existing critical systems in enterprise resource planning integration. In these environments, the mobile device is the user's main computing platform and more of a vital tool than a peripheral facility. Some application manufacturers offer mobile extensions to their application suites, providing a convenient means of extending the functionality to the mobile worker. Third-party middleware also exists to provide needed functionality if an application manufacturer does not provide such extensions or does not support certain platforms.

2.4 General Trends

Over recent years handheld devices have gained considerably more features and functionality. Cell phones in particular have seen features at one time available only in high-end units gradually appear in advanced and basic phones. For example, LCD screens have gone from monochrome to grayscale to color display technologies, and built-in cameras, which at one time were a rarity, are now commonplace. Similarly, simple text messaging (i.e., Simple Message Service) has led to chat messaging, multimedia messaging (i.e., the Multimedia Messaging Service, MMS), instant messaging, and electronic mail. Mobile devices are expected to continue to become more powerful and communicate at higher speeds, eventually giving people the power and functionality of a full desktop. Besides increasing productivity, such improvements are rapidly turning cell phones into extensive data reservoirs capable of holding a broad range of personal and organizational information. Some handheld devices are even capable of functioning as a removable USB drive, when set into the proper mode, to facilitate use of their available storage.

While non-cellular PDAs are still produced, their popularity is overshadowed by that of smart phones. The convenience of ubiquitous cellular connectivity coupled with PDA functionality is too strong an attraction for many, particularly in organizational use. With most cellular networks transitioning from current second-generation communications capabilities into the third generation, smart phones are better able to take advantage of available high-speed data communications to deliver services.

High-speed cellular data communications capabilities have endowed cell phones with Internet capabilities. Any service that can be provisioned via an IP address is potentially available to a cell phone user. This includes not only the ability to browse the Web and send electronic mail, but also to engage in peer-to-peer services. Other wireless capabilities also allow other types of services to be delivered. For example, cell phones and PDA devices with built-in Wi-Fi communications may be able to take advantage of the availability of a nearby access point for Voice over IP (VoIP) telephony, as either a backup to cellular service or a primary means of communication. Communications are expected to be increasingly Internet based and multimedia oriented.

Current models of phones are able to be precisely located through GPS, Assisted-GPS (A-GPS), or other technologies for improving 911 responses. A side effect of that capability is the opportunity for delivery of location-based services to subscribers. For example, it is possible for a subscriber to register a phone for continuous monitoring and location tracking, which is viewable via a Web interface. Other types of location-based services envisioned in the near term include the following:

- Finding relevant information, such as a restaurant or pharmacy, based on current location
- Receiving advertisement and coupons based on proximity
- Displaying maps showing a route from the current location to the desired destination

- Tracking location and behavior, such as a lengthy stay at one spot
- Obtaining a self-guided tour of a city.

Handheld devices have also reached a point where they can be used as electronic wallets to hold credit card or other financial information needed to conduct electronic transactions. Purchasing small-value items, such as tickets or permits for public transport and parking or vending machine goods, is already a reality in some areas of the world. Related standards for Near Field Communications (NFC), a short-range point-to-point wireless communication technology, have been issued and devices are starting to appear with capabilities that allow them to function as a connectionless identity card for credit and debit transactions and other purposes, such as interacting with NFC-enabled advertisements [Seg07, Bar08].

Handheld devices are being used for higher-value transactions and mobile banking as well. For example, GCASH service in the Philippines allows users to send and receive cash and to make payments and online purchases via SMS text messages [Tbn08]. Asian countries, particularly Japan and South Korea, are also active in mobile financial transactions. Japan's largest phone carrier, NTT DoCoMo, offers a credit card application, and BitWallet offers a product called Edy, an electronic money system usable in more than 71,000 convenience stores [Wil08]. In the U.S. both AT&T and Verizon are planning to begin preloading electronic wallet software on handsets to facilitate mobile banking. Differences in payment instruments and payment protocols used by various service providers and concerns about security have so far limited widespread adoption of any one scheme.

Mobile phones are increasingly being used as a second factor in two-factor authentication schemes used for remote access [Mcm07, Rap07]. The handset is used essentially as a security token registered to the user. Verifying that the user concurs with the action is typically done via a phone call or SMS text message. Additional software may also be installed on the phone to facilitate the process.

As the capabilities of mobile devices continue to expand, more advanced applications are envisioned. For example, someday a person may be able to take a photo or video of an object such as a building and retrieve historical or other information about it. Some cities are already facilitating such forms of information retrieval by placing signs with two-dimensional bar codes on buildings and in other public areas, which are able to be scanned by properly equipped cell phones [Gor08, Mar07, Vas06]. Existing one-dimensional bar codes on products can also be handled the same way. Similarly, one might be able to interact with specially-equipped buildings using a handheld device to post personal information electronically (e.g., photos and comments) to share with others or to retrieve and render information already posted there.

3. Security Concerns

While handheld devices provide many productivity benefits, they also pose new risks to an organization's security. Over time, significant amounts of sensitive organizational and personal information can accumulate on a handheld device, including removable memory cards and SIMs. For example, mobile email on a device may discuss sensitive topics such as product announcements, financial statements, or litigation issues. Information such as calendar and phonebook entries, passwords for online accounts, electronic documents, and audio and video media are also potential items of interest to an attacker. As the memory capacity of these devices increases, so too does the amount of information and associated risk. In addition, remote resources directly accessible by a device through its wireless or wired communications capabilities may also form a potential target. This includes cell phone services, voice mail and email repositories, and also applications and data on accessible corporate networks.

Mobile handheld devices typically lack a number of important security features commonly found on desktop computers. They also lie at the periphery of an organization's infrastructure, which can make them difficult to administer centrally [Jan04a]. Concerned individuals and organizations aware of the potential risks involved can often mitigate many of the associated threats with add-on security mechanisms and other safeguards, once the threats are understood.

3.1 Threats

A simple way to consider threats to handheld devices is to compare them with those for desktop computers, which are more familiar to everyone and documented elsewhere. Essentially, the threat profile for handheld devices is a superset of the profile for desktop computers. The additional threats for cellular handheld devices stem mainly from two sources:

- Their size and portability
- Their available wireless interfaces and associated services.

Size and portability can result in the loss of physical control of a device. With enough time and effort and with physical control, many types of security mechanisms can be overcome or circumvented to gain access to the contents of a device or prepare the device for reuse or resale. Wireless interfaces such as cellular and Bluetooth provide additional avenues of exploitation. Services that require subscription (e.g., cellular voice and text messaging) and accumulate charges based on usage (e.g., number of text messages, toll numbers, and unit transmission charges) can be a means of fraud or otherwise cause financial damage. They can also be used to deliver malware, the same as with non-subscription wireless interfaces such as Bluetooth. Security threats to mobile handheld devices include the following items, which are discussed in more detail below:

- Loss, theft, or disposal
- Unauthorized access
- Malware
- Spam
- Electronic eavesdropping
- Electronic tracking

- Cloning
- Server-resident data.

Application Development: Organizations developing their own mobile device applications face many of the same threats as those listed above. While the development of secure applications for mobile handheld devices is outside the scope of this publication, some of the issues are discussed here to raise awareness of the range of security concerns involved.

Several aspects of mobile devices make software development for them more difficult than for desktop computers [Jos07]. The diversity of hardware architectures (e.g., network interfaces, input mechanisms, and display capabilities), operating system and software capabilities (e.g., supported security features and content rendering on a small screen), and development support (e.g., SDK availability and quality) make the development and testing of applications and any associated content a complex, time consuming, and error prone process. Any resulting errors can in turn lead to exploitable vulnerabilities.

Typically, cross platform development and testing is used for production, which entails compiling applications on a platform different from the target system, and testing and debugging them in an emulated environment. The results are then packaged and loaded onto one or more actual target devices for further testing and validation. Any needed changes are addressed back on the development system and the process is repeated. Packaging tools may obfuscate the code to discourage reverse engineering, apply a digital signature to ensure the integrity of the code and the identity of the signer can be checked, or perform other security-related operations to meet operational requirements. Even if obfuscated, applications may still be reverse engineered to gather information that could be used to facilitate an attack, such as details concerning the authentication mechanism [Fog06]. Code signing, while useful in protecting the integrity of the code and identifying the source, does not preclude reverse engineering.

Mobile wallet applications developed for financial transactions or mobile banking have to be examined thoroughly for threat scenarios involving spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privileges. Protecting sensitive information stored on the device, such as account numbers or authentication data (e.g., passwords or PINs), is also a concern [Fog06, Jos07]. Sensitive data should be encrypted during data transmission and when stored on the device or in external memory cards. Available isolation techniques should also be applied to ensure that trusted applications and content are protected from other applications on the device.

Mobile devices have a broad attack surface including Bluetooth, Wi-Fi, and cellular communications interfaces as well as protocols for Web transactions, electronic mail, instant messaging, and SMS, EMS, and MMS messaging. For example, many applications use SMS text messages for short transactions. Cellular channel encryption, which ends at the radio interface, may not be adequate to meet the end-to-end confidentiality requirements of an organization, requiring application-level encryption to be used over the network [He08]. Other threats also exist, since SMS does not guarantee integrity of the message content or authentication of the source. Applications may need to protect transactions by providing security controls, such as digital signatures to validate the source and protect the message integrity, and encryption to provide confidentiality.

3.1.1 Loss, Theft, or Disposal

Because of their small size, handheld devices have a propensity to become lost or misplaced. They are also an easy target for theft. If proper measures are not in place and activated, gaining access can be straightforward, potentially exposing sensitive data that resides on the device or is accessible from it. Correct disposal of older model phones is a related issue. Manually resetting a device is a common step taken to clear out data and restore its original settings before selling or donating a device. Although from a logical perspective the data is gone, from a physical perspective it is retained, marked as unused space.

[Nak06, Lei08]. Software and hardware products are available that can be used to recover erased data from the flash memory present in most present-day cell phones [Bre06, Bre07].

Hundreds of thousands of cell phones and PDAs are lost each year. The Gartner Group estimated that, for 2001, 250,000 cell phones and handheld devices would be lost in airports, and less than 30 percent of them would be recovered [Ben03]. A survey of taxi companies in Australia, Denmark, Finland, France, Germany, Norway, Sweden, Great Britain, and the U.S. indicates tens of thousands of digital devices were left behind inadvertently [CP05]. An estimated 85,619 mobile phones and 21,460 PDAs were left behind in one Chicago taxi firm's vehicles during the six-month period of the study, compared with only 4,425 laptops. One estimate given for the year 2007 was that approximately eight million phones would be lost [Hoa07]. An informal study by Readers Digest in 2007 in over 32 large cities worldwide suggests that about 32% of lost phones would not be recovered by their owners [Sha07].

Besides the compromise of its logical and physical data, a cell phone with active service could be used indiscriminately to place toll and international calls and accumulate charges for the subscriber. In addition, the device itself may have significant value and may be able to be restored to its original settings manually and reused easily, even if the contents of user data are wiped away in the process. Phone flasher units capable of rewriting and restoring the memory of different types of cell phones are available for purchase from many sources on the Internet [Alz07]. Flashers can also be used to dump physical memory for recovery of deleted objects [Bre07].

3.1.2 Unauthorized Access

Even if security measures are utilized, access to the device and its contents may be gained by forging or guessing authentication credentials (e.g., a PIN or password) or bypassing the authentication mechanism entirely. Anecdotal information indicates that most cell phone and PDA users seldom employ security mechanisms built into a device, and if employing them, often apply settings that can be easily determined or bypassed. For example, before turning to other means with locked cell phones, forensic investigators often attempt commonly used PIN codes, such as 1234 or 0000, as two of the three permissible attempts allowed before the device is completely locked down [Kni02]. Cell phones can also be vulnerable if configured incorrectly. For example, certain Motorola phones provide a two-level access mechanism that can be enabled on the handset: a phone lock needed to gain access to the device and a security code needed to reset the phone lock in case it is forgotten. A user may set the phone lock, but not change the security code from its default value, allowing anyone to gain access by using the default security code value to reset or disable the phone lock [Jan07a].

Weaknesses in the authentication method are another avenue that can be exploited. For example, some devices may have a reserve password or master password built into the authentication mechanism, which allows unfettered access when entered, bypassing the phone lock set by the user [Kni02, Smi06]. On certain handsets, the master security code for overriding the phone lock mechanism can be calculated directly from the equipment identifier [Jan07a]. Occasionally a backdoor can be found to bypass all or part of the control mechanism [Wit08]. Forensic tools and procedures also exist that can be used to bypass built-in security mechanisms and recover the contents of a device [Aye07, Bre07, Lawr08]. Both software and hardware-based methods are available for data recovery, including those that exploit existing vulnerabilities [Jan07a]. A number of GSM mobile phones allow acquisition with a forensic tool, if a PIN-enabled (U)SIM is missing or removed from the device. It is also possible to create substitute (U)SIMs for certain models of phones that fools them into treating the (U)SIM as the original, and allowing access.

Manufacturers often incorporate built-in test facilities or other backdoors into a device that an examiner can exploit to obtain information. For example, some software tools are able to acquire the memory of

certain phones directly through a diagnostic/debugging protocol that bypasses the authentication mechanism. Scanning the memory contents can reveal authentication information such as passwords or phone locks. Some mobile phones also have active hardware test points on the circuit board that can be used to probe the device. Many manufacturers now support the JTAG standard, which defines a common test interface for processor, memory, and other semiconductor chips, on their devices [Int96]. Test equipment can be used to communicate with a JTAG-compliant component via existing test points and to image the contents of memory of a locked device [Wil05, Bre06]. An experienced technician can also dismantle a phone by heating the circuit board sufficiently to desolder its memory chips and access the contents using a memory chip reader [Wil05, Bre07].

3.1.3 Malware

Mobile malware is typically targeted more toward handheld devices for which an SDK is available than those without one, since code development is easier to perform. SDKs are more prevalent for smart phones and PDAs than for other handheld devices, and to date those environments have experienced the most attacks [Fse08].

Communications networks can be used to deliver viruses and other forms of malware to handheld devices. Malware may also be received during synchronization with desktop computers and via tainted storage media. Malware can be spread in a variety of ways, including the following common ones:

- Internet Downloads – A user may download an infected file via an Internet connection. The file could be disguised as a game, security patch, utility, or other useful application posted somewhere as a free or shareware download. Even downloads of legitimate applications may pose problems if they contain vulnerabilities that can be exploited by malware.
- Messaging Services – Malware attachments can be appended to electronic mail and MMS messages delivered to a device. Instant Messaging (IM) services supported on many phones are another means of malware delivery. The user must choose to open the attachment and then install it for the malware to infect the phone.
- Bluetooth Communications – Bluetooth technology is a convenient way to connect devices and send messages or move files between them. Bluetooth device communications can be placed in different modes: discoverable, which allows the device to be seen by other Bluetooth-enabled devices; connectable, which allows the device to respond to messages from connected devices; or completely off. Malware can be delivered by engaging the available connectivity services supported by a device left in discoverable mode.

With all of these delivery methods, the user usually has to give consent for the malware to install and execute. Malware writers use social engineering techniques to get users to carry out the necessary actions.

The range of malware behaviors and subsequent consequences is broad. Malware may potentially eavesdrop on user input or otherwise steal sensitive information, destroy stored information, or disable a device. Malware may also accumulate wireless communications fees against a subscriber, for example, by sending SMS messages or initiating calls to chargeable toll numbers [Mcm06]. Propagation onto other handheld devices or even desktop computers may also be attempted by malware to broaden its effect or to perturb the entire communications network. The following distinct high-level categories of malware attacks have been identified [Oco07]:

- Spoofing – Malware is able to provide phony information to the user to trigger a decision or action that impacts the security of the device.
- Data Interception or Access – Malware residing on the device is able to intercept or access data.
- Data Theft – Resident malware is able to collect and send data out of the device.
- Backdoor – Malware resident on the device is able to offer functionality that allows an attacker to gain access at will.
- Service Abuse – Resident malware is able to perform actions that cause higher than expected service provider costs for the user.
- Availability – Malware resident on the device is able to impact the availability or integrity of either the device or the data held upon it.
- Network Access – Malware resident on the device is able to use the device for one or more unauthorized network activities, including port scanning or using the device as a proxy for network communications.
- Wormable – Resident malware is able to use available technology to propagate itself in a semi-autonomous fashion.

While the range of misbehavior that malware can exhibit is extensive, outbreaks experienced to date on mobile handheld devices have been mild compared with those encountered by networked desktop, laptop, and notebook computers. However, incidents have been increasing steadily and are expected to continue to expand [Nar06].

Example Malware: Instances of previous attacks launched by malware against mobile handheld devices are discussed below. They are intended to illustrate the ways in which malware has manifested itself in the past and to gain insight about the potential security risks involved. The examples are not exhaustive; documentation of many other instances can be found on the Web sites of anti-malware vendors.

Fraud – The protection feature of a game developed for Symbian smartphones offered an early example of how subscriber fraud could be perpetuated through cell phone calling charges [Mcc04]. If the game was obtained from a different region than the phone service, an SMS message would be sent to a premium rate toll number before the game would be unlocked. The ill-fated arrangement affected subscribers who bought legitimate copies of the game outside the service area, as well as those with copies obtained illicitly, and eventually removed. However, copies remained and continued to spread. More recently, the threat was realized as a Trojan (Viver) targeting the Series 60 version of Nokia's Symbian operating system. The Trojan software appeared on file-sharing sites for mobile phone content, advertised as a photo editor, video codec, or other utility, enticing users to download and install it. Once downloaded and installed, the malware sends SMS messages to premium-rate numbers in Russia to accrue fees [Bro07].

Denial of Service – Denial of service on Symbian Series 60 (S60) phones was perpetuated by another Trojan (Fontal-A) spread though file sharing. Once installed, the Trojan causes the phone to fail when it is rebooted [Ley05a]. The Trojan also disables the application manager, which prevents any existing application, including itself, from being uninstalled, or new applications from being installed. A hard reset to reformat the phone and reinitialize its original settings resolves the problem, but at the expense of wiping out all user data. Besides Nokia, other phones from other manufacturers employ S60, including those from Samsung, Panasonic, and Siemens. A different type of denial of service exploit, involving buffer overflow vulnerabilities in MMS implementations, was demonstrated on Windows Mobile devices [Ley07]. Sending a long MMS message with a malware payload appended causes targeted devices to crash when the malware is deposited into memory. Denial of service attacks may also be targeted at certain features of a handheld device. For example, a battery exhaustion attack maximizes power consumption in various ways, such as performing unneeded but valid energy-consuming tasks repeatedly to drain the battery prematurely [Mar04].

Virus Propagation – In 2005, a mobile phone virus (Commwarrior-B) begin appearing on Symbian Series 60 phones [Law05]. The virus replicated itself by way of MMS message attachments and Bluetooth. MMS recipients are queried as to whether they want to open the attachment, while Bluetooth recipients are queried as to whether to accept the file and, subsequently, whether to run it. Once the virus is installed, it starts to look for other nearby Bluetooth phones to infect. At the same time, it sends an enticing MMS message to phone numbers listed in the address book, attaching a copy of itself as a disguised .exe file. This virus illustrates how multiple methods of replication can be used for propagation. Another virus (Mabir.A) works similarly, but responds with an infected reply to any message that arrives at the device, instead of using address book entries [Ley05b].

Remote Access – A classic Trojan (Brador) targeting Windows Mobile 2003 ARM-based PDA devices creates a file in the Startup folder on the device, which allows it to gain control each time the device is started [Lan04]. It sends the attacker an email message containing the IP address of the device as notification that the backdoor on the infected device is active. The attacker can then make a connection to the device, view and download files, or even upload more malicious code. The Bluetooth implementations of certain Nokia and Sony Ericsson phone models have also be shown to be vulnerable to something termed Bluesnarfing, whereby the address book, calendar, IMEI number, and other data can be extracted over the wireless interface [Bet04]. Certain device models were shown to be vulnerable even when Bluetooth was set in non-discoverable mode, and no prompts, messages, or other indications appear on the phones' display during the exploit.

3.1.4 Spam

Unwanted SMS text messages, email, and voice messages from advertisers have begun to appear on mobile phones [Mil05, BBC08]. Besides the inconvenience of removing them, charges may apply for inbound activity, such as a per-message charge on each SMS message received or charges for those messages above the monthly limit of a service plan. Data downloads may also cost extra, with each image attachment further escalating costs. Mobile spam may also be used fraudulently to persuade users to call or send text messages to chargeable service numbers using social engineering techniques. Spam can also be used for phishing attempts that entice users into revealing passwords, financial details, or other private data via Web pages, email, or text messages, or to download malware attached to the message or via a Web page [Esp06].

Instant messaging and multimedia messages are other possible means for malware delivery through spamming. Denial of service is also a possibility using spam techniques. For example, repeated attempts to establish Bluetooth pairing with a phone block the user from being able to initiate a call until the prompt is acknowledged. Also, sending a specially-crafted vCard to a certain model of Nokia handset was demonstrated to be capable of exploiting a vulnerability that denied service temporarily to the phone until it was rebooted [Gra03].

3.1.5 Electronic Eavesdropping

Most users understand the need to control the surrounding physical space when discussing sensitive topics to avoid someone listening to their phone conversation. Similarly, attempts to access and eavesdrop on transmitted information are another possible threat to avoid. The most direct way of electronic eavesdropping is for spy software to be installed onto a device to collect and forward information onto another phone or server [Mag08, Ver08]. Such applications exist for certain phone models and are commonly advertised as a means to monitor a spouse or child's activities. The capability to remotely turn on the microphone and listen or record conversations in the area is also a feature for some of these tools. Phones with vulnerabilities could allow the spy software to be loaded over an active communications interface.

More indirect techniques are also available. Configuring a notebook computer to impersonate a legitimate access point for a public wireless hot spot, such as a coffee shop or an airport first-class lounge, allows client connections to be attracted and sensitive data captured from unsuspected patrons [Bib05, Shm08]. The computer may route traffic onto the legitimate access point while continuing to monitor communications. Since it provides gateway services and DNS settings to connecting clients, mapping authentic domain name of certain Web sites, such as a bank or financial institution, to the IP number of a malicious Web site is also a possibility. In a similar fashion, it is also possible, although more difficult, to set up a cellular base station to pose as a legitimate one [Mey04].

While communications between a mobile phone handset and cell tower were designed with security in mind, apparent weaknesses exist that can be exploited. Researchers in Korea assembled equipment that was used to monitor a CDMA system [Hyu06], while researchers in Israel and the U.S. have found effective ways to crack the encoding system for GSM cell phone networks to enable eavesdropping [Bar03, Kir08, Nar08]. Specialized intercept equipment for law enforcement surveillance of cell phone traffic also exists [Bea07]. In a more targeted approach on the network fabric, cell phone switches have been surreptitiously modified to allow eavesdropping on the conversations of subscribers [Pre07].

3.1.6 Electronic Tracking

While cellular carriers have had for some time the ability to track device location with varying degrees of accuracy for internal use, other companies now offer location tracking services for registered cell phones to allow the whereabouts of the user to be known by friends and family [PBS07, She08]. The services are also touted as a means to track employees' whereabouts [Fol03, Reu06]. Registration can take place quickly, making temporary misplaced devices or unattended devices a possible target [Gol06]. Some tracking services periodically send the phone a notification for the user that monitoring is taking place, and may give the user the option to terminate the service. Other services provide no notification or indication of monitoring to the user, once registration is complete. Radio isolation bags exist, which contain metallic fibers that essentially create a Faraday cage to block radio frequencies and prevent tracking. However, they completely prevent normal use of the phone (e.g., incoming calls) and cause the battery to drain rapidly, since the phone boosts its signal in an attempt to register with a tower.

At least one early tracking service was shown to be vulnerable to the possibility of surreptitiously registering someone else's phone for tracking without having possession of the device [Pam05]. For example, if the scheme to complete the registration of a phone requires a positive acknowledgement from the device as confirmation, such as an SMS message reply with an authenticator code, but uses a code value that is predictable or not unique, another means such as an online SMS gateway could be used to forge the response needed to complete registration.

3.1.7 Cloning

If certain unique device identifiers built into a cell phone are reprogrammed into a second cell phone, a clone is created that can masquerade as the original. For example, monitoring the radio wave transmissions of analog cell phones allowed the factory-set Electronic Serial Number (ESN) and Mobile Identification Number (MIN) from those devices to be obtained easily and used to create clones [FCC05]. Though not as prevalent today with the rise of digital networks, analog networks may still exist in some rural areas. Technology used in digital cell phone networks improved security during device authentication by using cryptography to thwart device identifiers from being recovered. However, with physical access to a device, cloning of some early generation equipment is possible [Rao02, Bea07].

3.1.8 Server-Resident Data

Applications or content hosted on servers maintained by another party pose the risk of exposing sensitive information. Electronic mail and other communications solutions that keep content on a server operated by the network carrier is a common example [Ben03, Lei08]. Downloadable add-on applications may also provide services this way. The most obvious threats are from rogue employees administrating the server or vulnerabilities in the server's defenses exploited by an attacker. A well-publicized incident involving the T-Mobile account of a celebrity's Sidekick device illustrates the problem [Mcw05, Rob05]. The address book, photos, electronic mail, and voice mail of the device were maintained on a T-Mobile server for access through a Web portal. The server was able to be accessed by unauthorized users who gained access to the information and posted it elsewhere for public viewing.

Third-party data resident on servers other than those of network carriers may also be a concern. For example, unauthorized access to the data maintained at Web servers operated by cell phone tracking companies would expose the current and past whereabouts of an individual.

3.2 Outlook

Expectations on future threats and threat levels are highly speculative at best. Nevertheless, based on general trends and the history of other computing platforms, a general perspective on the near- and mid-term possibilities can be offered.

3.2.1 Near-Term

To date, incidents from malware and other identified dangers that have occurred against handheld devices have not been as widespread as with their larger counterparts. One likely reason is that no single operating system dominates mobile phones, as in the case of desktop and networked computers. An estimated thirty to forty different operating systems exist for cell phones [Say08]. Compatibility between versions of an operating system is not ensured, nor is compatibility across different hardware. The lack of a sizeable monoculture complicates things for attackers. The developer community for mobile devices is smaller than for desktop and networked computers and further segmented by the target platform family. This situation also makes it difficult to implement common security solutions over a significant range of devices.

Cellular network operators also take measures to protect their networks, which helps to reduce incidents. Besides using conventional security mechanisms to handle common attacks that also occur in wired traffic, such as viruses and denial-of-service attacks, mobile carriers monitor their networks for specific wireless concerns, such as abnormal use, and raise alerts for immediate action when limits are exceeded. Mobile carriers also employ security measures to prevent spamming [Mil05]. Specific cellular-oriented attacks, such as repeated pinging of a cell phone to keep it active and drain its battery prematurely, can also be detected and blocked.

Another reason for relatively few incidents in the wild also appears to be the lack of incentive for malware writers and attackers. Desktop computer users conduct banking and shopping transactions more readily than cell phone users, providing more opportunity. The range of targets is also richer due to a broader range of popular applications, plug-ins, and media formats for business, education, and entertainment, which frequently contain vulnerabilities that go unpatched. These factors have kept attacks and malware development for mobile handheld devices more in the hobbyist stage where notoriety is the incentive, than in the criminal stage where profit is the motivation. As long as these factors remain relatively constant, so too should the near-term threat levels.

3.2.2 Mid-Term

Trends towards open development platforms, such as Google's open Android system within the Open Handset Alliance (OHA), may alter the situation in the future. While common APIs and SDKs across a range of devices would facilitate application development, they would also provide malware developers the same advantage. U.S. cellular network carriers also appear to be moving away from a closed system approach in which the devices and applications are controlled by the service provider, to a more open environment that would allow flexibility in choosing devices and applications from other sources [Lawt08].

Perhaps the most worrisome trends in mobile device security are the rising amount of mobile malware reported each year and the progressive incorporation of advanced Web capabilities in devices [Sin08]. The former indicates a growing malware development community, while the latter an increasing source of potential attack vectors. The Mobile Web embraces cell phone-based activities, such as social networking posts, location-based socialization services, and multi-user gaming, which can be characterized as having potentially many connected users and sources of content [Sac08]. However, many handheld device browsers currently lack support for some of the technologies and standards required, including JavaScript, Document Object Model (DOM) and Cascaded Style Sheets (CSS) used with Asynchronous JavaScript and XML (AJAX) [Jeo07, Bri08]. As the Web capabilities of mobile devices improve, a tipping point may occur that impels malware incidents and movement from the hobbyist stage toward the criminal.

Another complicating factor is that handheld devices are regarded more as fixed appliances that provide a predefined set of functions than are desktop and networked computers that are designed for general purpose computing. Operating system upgrades and patches occur far less frequently and changes to firmware can be more daunting to carry out, creating a somewhat static target for malware. Difficulties that may occur include the loss of data and installed applications, the inability to roll back to the previous version should the changes create problems, and the state of the device made inoperable should processing fail for some reason (e.g., battery not fully charged).

The Trusted Computing Group industry association has recognized the potential problems involved and proposed a solution. Its Mobile Phone Work Group has developed a standard for a hardware component called the Mobile Trusted Module (MTM), for enabling trust in future mobile devices by establishing a trusted computing base [Sch08]. Similar to the Trusted Platform Module defined for desktop and networked computers, the MTM functions as a tamper-resistant trusted engine, able to store information securely. Several trust engines can operate independently on behalf of different sets of stakeholders. The operation of the engine ensures the operating system, applications, and data have not been corrupted and remain trustworthy.

4. Safeguards

It should be clear from the previous section that mobile handheld devices provide productivity benefits, but also pose new risks to an organization's security. However, because their adoption often takes place informally and piecemeal, organizations may not recognize mobile devices as part of an organization's infrastructure nor treat them accordingly. One of the key issues facing an organization is distinguishing between employee-owned equipment versus organization-issued equipment. Initially, allowing employee-owned cell phones and PDAs to be used for business purposes may seem to be a cost-effective approach for an organization. However, the ability to control and manage the devices is difficult to accomplish, fueling the security risks involved. In addition, provisioning any needed security solutions is much more difficult to do when the devices are not restricted to approved platforms.

The security issues for cell phones and PDAs range beyond those of other computer equipment. Moreover, many common safeguards available for desktop and networked computers are generally not as readily available across a broad spectrum of handheld device types. Organization-issued devices are normally easier to administer since the characteristics of the devices are known, their configuration can be centrally managed, and controls can be installed to improve security and compel compliance with policy. These same characteristics also allow organizational applications developed for desktop computers to be more easily extended to the mobile platform.

The remainder of this section reviews a variety of safeguards for cell phones and PDAs that can be applied to reduce associated risks to organizations. More comprehensive guidelines are also available from NIST about selecting and specifying minimum management, operational, and technical security controls for information systems [Ros07].

4.1 User-Oriented Measures

Maintaining the security of a handheld device involves the active participation of the user. Users should be instructed about procedures to follow and precautions to take when using organization devices. For example, handheld devices have a number of built-in configuration settings and security features that often go unused. Understanding and taking full advantage of the facilities afforded by a cell phone or PDA is an important step towards establishing a comprehensive set of security safeguards. The remainder of this section outlines such user-oriented measures.

4.1.1 Maintain Physical Control

Maintaining oversight of a mobile handheld device is important. Its use should be treated similarly to a credit card, maintaining control at all times and storing it securely if left unattended. Besides the cost of the device itself, the loss or theft of a handheld device places the confidentiality of the device's contents at risk, as well as the contents of computational resources reachable by it.

Lending a mobile phone to another person at a minimum offers an opportunity for misuse, and in the worst case, risks installation of malware or activation of unwanted services, such as device tracking. Unexpected costs due to toll calls placed or services used could be incurred and sensitive data on the phone stolen. A threatening call or message placed from a phone would likely be attributed to the user by authorities. The security settings of the device could also be changed, making the phone vulnerable to other forms of threat that could go unnoticed because of the changes.

4.1.2 Enable User Authentication

User authentication mechanisms generally available on most devices are PINs and passwords. While such knowledge-based authentication mechanisms are not foolproof, they are the first barrier toward deterring unauthorized access to cell phones and PDAs. Reading and understanding the documentation covering the entire set of features and options for authentications is crucial to making correct and safe choices to employ. For example, password recovery or other features may involve master-level passwords whose default settings can provide an avenue to compromise the authentication mechanism.

Organization policy regarding the length and composition of passwords and PINs for cell phones and PDAs should be followed. Using the same password for a handheld device that is used for network access or access to other devices and applications should be avoided. Different techniques exist to recover the password from various handheld devices, which in turn could possibly compromise access to the network or other devices. Some authentication mechanisms include a timeout feature that locks the device automatically after reaching a preset inactivity threshold, much like a screen saver. While it can sometimes be annoying, it can also help protect a lost, stolen, or misplaced device until the owner regains control over it.

Modes of Authentication: Verifying an individual's claimed identity through user authentication is the first line of defense against unauthorized use of a mobile handheld device. Three types of techniques commonly used for authentication are proof by knowledge (e.g., passwords), proof by possession (e.g., tokens, such as smart cards), and proof by property (e.g., fingerprints). Using multiple modes of authentication, in which two or more authentication techniques are encountered successively, is also possible and generally affords greater protection. Implementing authentication solutions on handheld devices can be problematic, however [Jan03]. For example, hardware tokens can drain battery power away from the device more quickly and can be troublesome to interface to a device. On-device processing needed for certain authentication techniques, such as voice authentication or fingerprint verification, may also go beyond the computational limits of some devices. While handheld devices offer extraordinary challenges compared with desktop computers, some interesting ways to authenticate users do exist and are discussed below.

Passwords are the oldest and most popular form of proof-by-knowledge technique in use today and remain a common solution for handheld devices. Some drawbacks, such as the inability for users to recall a complex string mandated by most of today's password policies, beleaguer their usage. Indications that human memory is well suited to certain visual and cognitive tasks involving the processing of images has stimulated the development of visual login techniques, also known as graphical or picture passwords. Two main categories have emerged: those that require the user to recall and select a sequence of displayed images, and those that require the user to draw a series of lines over a grid or image template. The former category has been implemented in a number of commercial security products for handheld devices; both categories remain active areas of research [Jan04b].

Smart card authentication is perhaps the best-known proof-by-possession mechanism. Smart cards are credit-card-size security tokens that hold an embedded computer chip containing an operating system, programs, and data. Some organizational security infrastructures already incorporate smart cards, and extending them to handheld devices potentially offers benefits. For example, smart cards could convey user security credentials and policy rules to a device to govern user permissions and allowed behavior. Smart cards are not very amenable to handheld devices, however, because of the comparatively large size of the card itself and the need to incorporate or connect with a card reader of similar size. Common means to accommodate smart cards are device expansion sleeves that contain a reader, or separate readers that connect wirelessly to the device. Perhaps the most promising development with full-size smart cards involves wireless smart cards that incorporate a radio frequency chip; eventually high-end mobile devices could include the capability to communicate with them.

Some manufacturers offer smart cards in alternative formats that are more compatible with handheld devices, namely, removable media cards [Jan07b]. Removable-media smart cards are typically dual-function, providing

significant amounts of storage in addition to smart card functionality. The latter could be used for user authentication and other purposes. As mentioned in an earlier section, (U)SIMs are fundamentally smart cards in reduced size that are used in certain types of cell phones. Because (U)SIMs are typically under the control of the network carrier and not normally readily accessible (i.e., removable of the battery from the handset is typically required), they are not a good option for user authentication with a device. Smart cards have also been packed within a plastic housing with a USB connector at one end. However, very few handheld devices support host USB ports, which are needed to interface to these peripherals.

Fingerprints are the oldest proof-by-property technique involving biometrics. The fundamental operation of a biometric system is comparing newly captured measures of some biometric characteristic (i.e., physiological and behavioral) against a previously enrolled template derived from registered measures taken earlier [Jan03]. Only a few handheld devices have incorporated fingerprint authentication technology. Signature dynamics, involving measurements of speed, acceleration, direction, pressure, stroke length and pattern, and time and distance the writing stylus is lifted, is a more common biometric, targeted toward mobile devices that have a touch-sensitive screen and are able to capture such signature characteristics. A number of commercial security products for handheld devices incorporate signature verification technology.

4.1.3 Backup Data

Using a handheld device as the sole repository for important information is an invitation for disaster. Not only can the device be lost or stolen, but it can also be accidentally damaged. To preserve valuable data residing on a handheld device, a restorable backup of the contents should be done regularly. Data may be synched with a desktop computer as a primary means of backup and also for possible dual use. Data includes personal information management data, electronic documents, photos, music, software applications, and network settings.

Backing up data on the memory card is an alternative means of backup, but is effective only if the card is kept separately away from the device. Otherwise, the device and card could be lost or stolen together, narrowing the benefits mainly to situations where the device fails. Contact data such as phone numbers and addresses can also be printed out and kept in a day planner as a form of physical backup.

4.1.4 Reduce Data Exposure

Avoid keeping sensitive information, such as personal and financial account information, on a handheld device. As mentioned earlier, authentication mechanisms can be bypassed or broken and even deleted information can often be recovered from memory. Although they might be convenient for authenticating to online accounts or to other devices, maintaining PINs, passwords, user IDs, and account numbers on a handheld device should also be avoided. Sensitive data could also be maintained on removable memory cards, kept separately from the device until needed. Issues with labeling and tracking sensitive data held on this type of media may arise.

If the presence of sensitive data is not avoidable, the data should be kept in a suitable encrypted form until required. Some devices do support built-in encryption capabilities. For example, certain Symbian devices provide a “wallet” to store personal information, such as credit card numbers, contacts, user names, and passwords, in an encrypted form. The wallet opens when the password is entered and closes automatically after a period of inactivity. Any products and procedures of this type should be checked for compliance with organizational encryption policies. A significant number of commercially available encryption tools also exist, particularly for smart phones and PDAs, which typically have more capable processors needed to perform cryptographic calculations quickly. Some products also encrypt memory card contents in addition to encrypting device contents.

Protecting sensitive data on a device with encryption is an effective measure, especially appropriate for devices used for organizational purposes. The Advanced Encryption Standard was developed for Federal departments and agencies to encrypt and decrypt such information [FIPS01]. Encryption, while effective, has its limitations, however, since a malicious application could gain access to decrypted contents when the device is in use.

Current memory cards that follow the multimedia card security standards include a password locking capability that some handheld devices utilize. For example, a number of Symbian OS devices take advantage of this capability. A case-sensitive password up to 8 characters long can be entered for a memory card. Once enabled, the password is required again whenever the memory card is reinserted into the device. If the memory card is inserted into another card locking-compatible device, a prompt for the password appears. Other devices without this feature, including desktop computers with card readers, fail to recognize the card. This feature can be a useful means to secure sensitive data kept separately from the device, particularly when encryption is also employed. One drawback that can occur is if the device fails and the user forgets the password needed to unlock the card.

Communication protocols usually include authentication and encryption features that protect data in transit. Configuration settings should take full advantage of those features and normally enable them as the default setting. Being aware of the operating environment of the device can also be of benefit, since different environments pose different communications risks (e.g., public wireless hotspot versus office access point), and more sensitive operations can be deferred until the device is located in a safer physical environment.

At the end of service or the reissuance of the device to someone else, the memory of a device containing sensitive data should be erased by completely overwriting it or expunging all data to keep the contents from being recovered and analyzed. Memory erasure products exist for some mobile devices and manually performing a hard reset clears memory for others. Any procedure used should be verified. If no procedure can be determined, the alternative is to physically destroy the memory (e.g., passing the entire device through an industrial-grade shredder for destruction).

4.1.5 Shun Questionable Actions

Malicious programs are spread to mobile phones mainly through communications channels such as multimedia messages or Bluetooth connections. Any messages or contacts received on a mobile phone from an unknown number or device should be treated with suspicion. Messages should be destroyed without opening and connections denied. Even content received from a friend or acquaintance should be suspect, since malware can take advantage of address book entries and message exchange capabilities to propagate themselves, often in the guise of an interesting attachment or link. For example, an MMS message or electronic mail message from a familiar number or address, which contains an installable program as an attachment, could be produced by a malicious program as well as by the presumed originator.

Most malware requires user interaction to take effect, making the option of taking no action when solicited a viable means of prevention. To date, instances of malware-infecting mobile devices rely on the user accepting the installation of infected files or connections from other devices. For example, malware attempting to propagate via a Bluetooth connection cannot install itself without user approval. Any request from a mobile phone to accept the installation of an unknown program whose installation was not initiated by the user should not be accepted. Similarly, incoming connections of any type should not be accepted unless they are expected.

A program that repeatedly tries to download malware via a Bluetooth connection may effectively prevent the user from using the phone or disabling Bluetooth. In such situations, simply moving out of range of the other device can quash its reattempts to connect. It is also important to keep the device configured to deliver notifications for user approval when connection and download attempts occur.

Media may seem harmless, but it should be treated cautiously, since it can be a means to launch malware. For example, Windows Mobile devices are able to detect when a storage card is inserted and to automatically load and execute an application from it, similar to the way in which the autorun feature in Windows desktop systems works with removable media, such as CD and USB drives [Fog04, MS06]. Social engineering is one way that users are induced into taking such actions or into allowing someone else to take them on their devices. Because of its effectiveness, forensic tools have been developed to exploit the autorun feature to recover data from handheld devices.

Software download from sites that seem suspicious or are not known should also be avoided. Organizations should have policy in place about software downloads and may prefer to establish an internal procedure for centrally managing software distribution and installation. Some devices have application security features that prevent the installation of third-party applications unless they are digitally signed. As an alternative, many reputable and reliable sources for software, media, and other types of download exist and should be used to obtain content. Never install anything whose origin is unknown or suspect. Ideally, only programs that are from reputable manufacturers and have verified digital signatures should be installed.

4.1.6 Curb Wireless Interfaces

A simple defense against many forms of malware is to turn off Bluetooth, Wi-Fi, infrared, and other wireless interfaces until they are needed. This is particularly important for Bluetooth devices due to the increased risk of encountering mobile malware in crowded settings, such as an airport, sports event, or concert, which offer a target-rich environment for an attack. Being invisible prevents the device from being scanned and located, and its wireless interface used as an avenue of attack. Disabling a wireless interface also has the benefit of extending the battery life of the device.

Automatic connections to cellular data services, such as GPRS or EDGE, should be turned off when not in use. Staying offline avoids malware infections and may also prevent an infected device from sending data from the phone to other parties. A phone automatically connecting to data services may also be an indication that the phone is infected with malware attempting to spread itself.

If needed for some purpose, the Bluetooth wireless interface should be set in discoverable mode only temporarily, until pairing with another device is completed. This measure helps to avoid discovery attempts by malware attempting to spread itself, although brute force techniques can deduce and query the address in some implementations. Where possible, Bluetooth settings should be configured to notify the user of incoming connection requests and to receive confirmation before proceeding. Certain mobile phones also offer the ability to control Bluetooth functionality selectively by enabling only the supported profiles needed to interoperate with another device. Device pairing should be performed outside of public places, preferably in areas that are radio isolated, to prevent monitoring and recording exchanges over the air and using them to regenerate security keys needed to eavesdrop. Using a long random PIN is also advised to complicate the calculations required in certain attacks.

Since Bluetooth keys normally reside on paired devices, those devices should be password protected to defend against lost, stolen, or compromised units. As an added measure, defining a list of known trustworthy devices with which the device can connect via Bluetooth should be possible. If achievable,

configure Bluetooth to use the lowest power setting needed for the connection. Adjusting power lower helps reduce the likelihood of an attack from long range.

4.1.7 Deactivate Compromised Devices

If a device is lost or stolen, disabling service, locking it, or completely erasing its contents are useful actions to take remotely. Contacting the cellular carrier to report a lost or stolen cell phone and discontinue service is always an option available to subscribers. GSM carriers in many countries can also go a step further and register the identifier of the phone (i.e., the International Mobile Equipment Identity or IMEI) in a global database to prevent it being used elsewhere [GSM08]. Knowing the reporting procedure in advance of an incident and what information to provide is essential, since stolen phones can accrue significant charges for which the subscriber may be responsible up until the time it was reported stolen. A copy of a filed police report may also be required to have the charges waived. To expedite the process and minimize the consequences, organizations should establish and inform users of procedures for reporting lost or stolen organization-issued handheld mobile devices.

Certain devices, such as Blackberry devices and some cell phones, have the capability to lock a device or erase its contents remotely through a built-in mechanism. Memory cards may also be affected in the same way. Locked devices and memory cards can be unlocked subsequently by the user, if they are recovered. Products are also available for some devices to add in this capability. When evaluating such products, care should be taken to ensure that the locking feature is not able to be bypassed and that the erasure process completely overwrites or expunges data from memory.

The remote protection mechanism is typically triggered through the receipt of a message containing a pre-registered activation code. Therefore, for the mechanism to function, the device must be able to receive communications via the cellular network (e.g., not radio isolated). To enable the mechanism, the device owner specifies the activation code and selects an option for the type of action to take. A range of options from a device lock to a full content erasure may be available, or merely a single choice, depending on the implementation. Notification of the user's identity module being replaced with another identity module (e.g., that of a thief) is sometimes a supported option.

A device that is compromised through a remote attack, but still in the user's possession, can be deactivated through the means above. However, other, simpler actions can be taken more quickly to contain the problem until it can be fully resolved. A compromised device may continue to operate and cause harm when service with a cellular carrier is discontinued or even when the device has been turned off. Although some devices have a built-in backup battery to maintain power temporarily, removing the battery eventually eliminates the ability of the device to function. If the battery is not removable, placing the device in a radio isolation bag blocks radio frequencies and prevents communication, eventually draining the battery completely. The device's ability to authenticate and communicate with the cellular network while operating on the backup battery can also be disabled by removing any identity module present, but removal does not affect other wireless interfaces. Organizations should establish and inform users of procedures for handling and reporting the compromise of organization-issued handheld mobile devices.

4.1.8 Minimize Functionality

Increased functions, features, and capabilities typically give rise to insecurities. Reducing them to only those required can have the opposite effect. Disabling wireless interfaces until needed, as discussed earlier, provides a good example of the benefits. Any unneeded features should be disabled through configuration settings. In some situations, it may be possible instead to remove a feature from a device

completely to avoid it being reactivated. Similar consideration should be given to minimizing the use of add-on applications and plug-ins. Once installed, these applications are able to access user content and device programming interfaces, and they may also contain vulnerabilities [Fog06]. Their benefits should be carefully evaluated against risks before installation, since such add-on functionality may provide new avenues for attack.

Cellular service agreements and service settings are another way to reduce functionality. For example, eliminating data service and subscribing to only voice service prevents full access to the Internet, which may not be required. It may also be possible to have the carrier restrict access to international destinations that are not used or bar other services. For example, many cellular carriers allow the subscriber to block text messages that originate from the Internet, which is the main source of wireless spam [Pog08].

4.1.9 Add Prevention and Detection Software

The operating system and built-in applications on a handheld device are more difficult to update than those on a desktop computer, making additional security controls that prevent and detect attacks against the device a necessity. Prevention and detection software to defend against malware and other forms of attack is an important addition. A wide range of these products exist for various handheld devices, particularly smart phone and PDAs, which can be used to augment the security mechanisms already present in a device. Keep in mind that add-on security software may contain or introduce weaknesses and should be properly evaluated before use [Fog06]. Products typically include one or more of the following capabilities:

- User authentication alternatives, including biometric and token-based mechanisms
- Device content and memory card encryption
- Firewall
- Antivirus
- Intrusion detection
- Antispam
- Device content and memory card erasure
- Virtual private networking.

With organization-issued devices, centralized security management is often an important consideration, since it simplifies the configuration control and management processes needed to ensure compliance with the organization's mobile device security policy. A number of products provide centralized security management and oversight of cell phones and PDAs through the network infrastructure. Solutions typically require augmenting the infrastructure with the addition or expansion of enterprise servers and the use of Lightweight Directory Access Protocol (LDAP), Active Directory, or other similar directory services. Periodic communications with managed devices take place to ensure security and other configuration settings are correct and in compliance with policy, as well as to perform updates to security credentials, downloads of log files, configuration updates, and other related functions. The depth and breadth of capabilities that can be controlled vary among products. The following items are some common examples:

- Device registration

- Installation of client software, policy rules, and control settings
- Controls over password length and composition, number of entry attempts, etc.
- Remote password reset
- Remote erasure or locking of the device
- Controls to restrict application downloads, access, and use
- Controls over infrared, Bluetooth, Wi-Fi, and other means of communication
- Controls to restrict camera, microphone, and removable media use
- Controls over device content and removable media encryption
- Controls over VPN, firewall, antivirus, intrusion detection, and antispam components
- Remote update of client software, policy rules, and control settings
- Remote diagnostics and auditing
- Reporting of device compliance status
- Denial of services to non-compliant or unregistered devices

4.2 Organizational-Oriented Measures

Handheld devices have the potential to create a security hole in an organization's security infrastructure, if not addressed properly. For example, employees who buy their own units may attempt to synchronize them with an office workstation or use their workstation connectivity to access the organization's intranet. A device with wireless capabilities could potentially create an unauthorized side channel to the Internet. The storage capacity of these devices has grown to the point where they contain sufficient memory to hold a significant amount of an organization's data for working away from the office while on travel or at home, and this data needs to be protected.

As an extended component of an organization's infrastructure, handheld devices need to be secured appropriately. Organizations should expand their security management practices and controls over handheld devices, if this has not yet been done.

4.2.1 Establish a Mobile Device Security Policy

Organizations should have a security policy in place for mobile handheld devices. A security policy defines the rules, principles, and practices that determine how an organization treats these computational resources, whether they are issued by the organization or owned by individuals. Individuals could also expect to benefit from taking similar considerations with personally owned handheld devices.

The security policy should reflect an organization's view on required safeguards, based on a consideration of the assets involved, the impact of loss or compromise, and the threat environment. The policy should cover the full life cycle of a device from its issuance to the user to its retrieval after dismissal, transfer, or similar event, and comply with relevant regulations and legislation. Restrictions on use for personal communications on organization-issued devices or storing personal information on them, such as contacts, photos, and music, should be clearly stated, as well as the implications if a device containing personal information is lost, stolen, damaged, or remotely erased. Information security in any

organization is largely dependent on the quality of the security policy and its implementation and enforcement. Technology alone cannot overcome a poorly planned or nonexistent security policy.

4.2.2 Prepare Deployment and Operational Plans

Addressing security issues of cell phones and PDAs once deployment and implementation are underway is difficult; instead, security should be considered from the beginning. Required device characteristics are often associated with available safeguards and can affect procurement decisions. Organizations are more likely to make decisions about configuring mobile handheld devices securely and consistently when they develop and follow a well-designed plan.

Plans should address methods for protecting data, authenticating users, accessing organizational networks and resources, and handling lost or stolen devices [Gau07]. The handling of compromised devices to limit exposure and contain the problem is also an important consideration. Device issuance, backup and recovery, and content erasure before disposal or reissuing are other aspects to address when preparing the plans, as is centralized device security management. Planning should take into account any required business applications to be used with the devices and any required controls over the installation of third-party applications by employees, and address any anticipated security issues that relate to those applications from an organization-wide perspective.

Developing such plans helps to identify critical issues and guides administrators in making tradeoff decisions between usability, performance, and risk. For similar reasons, existing system contingency, continuity of operations, and disaster recovery plans should also be extended to account for mobile handheld devices issued by the organization.

4.2.3 Perform Risk Assessment and Management

Security involves continually analyzing and managing risks. As seen in earlier sections, mobile devices have their share of risks and must also contend with a dynamically changing environment. A risk analysis identifies vulnerabilities and threats, enumerates potential attacks, assesses their likelihood of success, and estimates the potential damage from successful attacks. Risk management involves taking steps to reduce assessed risk to an acceptable level and maintain that level of risk. Ongoing risk analysis and management is an important organizational activity that is increasingly being mandated by law and regulation.

4.2.4 Instill Security Awareness through Training

User awareness of the organizational security policy and procedures for handheld devices is a prerequisite to their successful implementation. If the workforce is not familiar with the policy and procedures instituted and the ramifications for violating them, compliance will likely be happenstance. Even organization-controlled devices can create security issues if not used properly. In addition to making employees aware of the policy and the consequences for noncompliance, actively monitoring and dealing with compliance issues that arise helps to eliminate risky behavior.

4.2.5 Perform Configuration Control and Management

Configuration control and management ensures that the system is protected against the introduction of improper modifications before, during, and after system deployment. Configuration control leads to consistency with the organization's security policy for mobile devices. Changes to a configuration should be vetted and tested before deploying to the production environment.

Considerations to take when preparing standardized software configurations to satisfy the security policy include the following items:

- Available patches and upgrades to the operating system that affect security
- Unnecessary services and applications that can be eliminated or disabled
- Necessary applications that require installation and proper configuration
- User authentication and access controls available on the device
- Other security-related control settings available on the device (e.g., notifications and alarms, inactivity timer lock, logging options, memory allocation)
- Additional security controls, described in Section 4.1.9, that require installation and proper configuration
- Certify and accredit handheld devices.

The security certification of an information technology system requires that the system is analyzed to determine how well it meets all of the non-technical and technical security requirements of the organization. Accreditation occurs when the organization's management accepts that the system meets the organization's security requirements. Both processes are a prerequisite to deploying handheld devices, particularly if other components of the network infrastructure are involved. Such network infrastructure components typically involve enterprise servers used to interact with devices to deliver services and provide oversight.

5. References

[Alz07] Marwan Al-Zarouni, Introduction to Mobile Phone Flasher Devices and Considerations for Their Use in Mobile Phone Forensics, 5th Australian Digital Forensics Conference, December 2007, http://scissec.scis.ecu.edu.au/conference_proceedings/2007/forensics/15_Al-Zarouni%20-%20Introduction%20to%20Mobile%20Phone%20Flasher%20Devices%20and%20Considerations%20for%20their%20Use%20in%20Mobile%20Phone%20Forensics.pdf

[Att08] Technology Timeline, 1946: First Mobile Telephone Call, AT&T, http://www.corp.att.com/attlabs/reputation/timeline/46mobile.html

[Aye07] Rick Ayers, Wayne Jansen, Ludovic Moenner, Aurelien Delaitre, Cell Phone Forensic Tools: An Overview and Analysis Update, NIST Interagency Report (IR) 7387, March 2007, http://csrc.nist.gov/publications/nistir/nistir-7387.pdf

[Bak07] Anindya Bakshi, Bluetooth Secure Simple Pairing, Wireless Design and Development Magazine, December 2007, http://www.wirelessdesignmag.com/PDFs/2007/1207/wd712_coverstory.pdf

[Bar03] Elad Barkan, Eli Biham, Nathan Keller, Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication, Proceedings of Crypto 2003, http://www.cs.technion.ac.il/users/wwwb/cgi-bin/tr-get.cgi/2003/CS/CS-2003-05.pdf

[Bar08] BART Trial First to Use Mobile Phones to Pay for Fares, Food, Bay Area Rapid Transit, January 30, 2008, http://www.bart.gov/news/articles/2008/news20080130.aspx

[BBC08] Beijing Investigates Spam Attack, BBC News, March 24, 2008, http://news.bbc.co.uk/2/hi/business/7311242.stm

[Bea07] Christopher Beam, How Do You Intercept a Text Message?, Slate Magazine, March 7, 2007, http://www.slate.com/id/2161402/

[Ben03] Chris Bennett, Challenges of Mobile Security, SearchCIO.com, TechTarget, December 17, 2003, http://searchcio.techtarget.com/tip/0,289483,sid182_gci952382,00.html

[Bet04] Bryan Betts, Bluetooth Holes Could Put You the Wrong Side of the Law, Techworld, February 23, 2004, http://www.techworld.com/features/index.cfm?fuseaction=displayfeature&FeatureID=357

[Bib05] Erin Biba, Does Your Wi-Fi Hotspot Have an Evil Twin?, PC World, Medill News Service, March 15, 2005, http://www.pcworld.com/article/id,120054-page,1/article.html

[Bre06] Marcel Breeuwsma, Forensic Imaging of Embedded Systems Using JTAG (Boundary-Scan), Digital Investigation, Volume 3, Issue 1, 2006, pp. 32-42

[Bre07] Marcel Breeuwsma et al., Forensic Data Recovery From Flash Memory, Small Scale Digital Device Forensics Journal, Vol. 1, No. 1, June 2007, http://www.ssddfj.org/papers/SSDDFJ_V1_1_Breeuwsma_et_al.pdf

[Bri08] Peter Bright, Microsoft Casting About for Viable Mobile Browser Strategy, Ars Technica, October 07, 2008, http://arstechnica.com/news.ars/post/20081007-microsoft-casting-about-for-viable-mobile-browser-strategy.html

[Bro07] Matthew Broersma, Smartphone Trojans Discover Profit Motive, Techworld, 22 May 2007, http://www.techworld.com/security/news/index.cfm?newsid=8889

[BTS07] Bluetooth Core Specifications, Version 2.1 + EDR, Volumes 0 to 4, Bluetooth SIG, Inc., July 26, 2007, http://www.bluetooth.com/NR/rdonlyres/F8E8276A-3898-4EC6-B7DA-E5535258B056/6545/Core_V21__EDR.zip

[Che07] Zhu Cheng, Mobile Malware: Threats and Prevention, McAfee, Inc., September 5, 2007, http://www.mcafee.com/us/local_content/white_papers/threat_center/wp__malware_r2_en.pdf

[CNI06] Ten-Year-Old Apple Newton Beats Latest Windows UMPC, CNET Networks, Inc., July 27, 2006, http://crave.cnet.co.uk/handhelds/0,39029444,49282366,00.htm

[CP05] Taxis Hailed as Black Hole for Lost Cell Phones and PDAs, as Confidential Data Gets Taken for a Ride, Check Point, January 24, 2005, http://www.checkpoint.com/press/pointsec/2005/01-24a.html

[Esp06] Tom Espiner, Phone Phishing Attack Hits US, ZDNet.co.uk, June 23, 2006, http://news.zdnet.co.uk/security/0,1000000189,39277240,00.htm

[FCC05] Cell Phone Fraud, FCC Consumer Advisory, Federal Communications Commission, Consumer & Governmental Affairs Bureau, September 26, 2005, http://www.fcc.gov/cgb/consumerfacts/cellphonefraud.html

[FIPS01] Announcing the Advanced Encryption Standard (AES), NIST, Federal Information Processing Standards (FIPS) Publication 197, November 26, 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[Fog04] Seth Fogie, Security Reference Guide: Windows Mobile Autorun, informIT, November 25, 2004, http://www.informit.com/guides/content.aspx?g=security&seqNum=91

[Fog06] Seth Fogie, Airscanner Vulnerability Summary: Windows Mobile Security Software Fails the Test, informIT, September 1, 2006, http://www.informit.com/articles/article.aspx?p=607375

[Fol03] FollowUs to a Smarter Method of Locating Your Mobile Workers, FollowUS, 2003, http://www.followus.co.uk/Mobile.pdf

[Fse08] Résumé des Menaces Mobiles pour 2007, F-Secure, April 8, 2008, http://www.f-secure.fr/news/fs_news_20080330_01_fra.html

[Gau07] Nalneesh Gaur, Bob Kiep, Managing Mobile Menaces, Information Week, May 1, 2007, http://www.informationweek.com/news/showArticle.jhtml?articleID=199100696

[Gol06] Ben Goldacre, How I Stalked my Girlfriend, The Guardian, February 1, 2006, http://www.guardian.co.uk/technology/2006/feb/01/news.g2

[Gor08] David Gorn, Bar Code Hopping in San Francisco, NPR, April 1, 2008, http://www.npr.org/templates/story/story.php?storyId=89271743

[Gra03] Patrick Gray, Mobile Phone Vulnerable to DoS Attack, ZDNet Australia, February 26, 2003, http://news.zdnet.co.uk/hardware/0,1000000091,2131098,00.htm

[GSM08] IMEI Database, The GSM Association, 2008, http://www.gsmworld.com/using/security/index.shtml

[He08] Rongyu He, Zheng Qin, Xi Qin, A Secured Mobile Access Scheme for SMS Message, Information Technology Journal, Volume 7, No. 2: 2008, pp. 261-268, http://www.ansijournals.com/itj/2008/261-268.pdf

[Hoa07] Bruce Hoard, 8M Cell Phones Will Be Lost in '07 -- how to back yours up, Computerworld, July 13, 2007, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9026944

[Hor03] Hadar Horesh, Technion Team Cracks GSM Cellular Phone Encryption, of Haaretz Newspaper, online edition, September 3, 2003, http://www.cs.technion.ac.il/~barkan/GSM-Media/HaaretzInternetEnglish.pdf

[Hyp06] Mikko Hypponen, Malware Goes Mobile, Scientific American, November 2006, http://www.sciam.com/article.cfm?id=malware-goes-mobile

[Hyu06] Dae Hyun Ryu, Seung Ju Jang, A Security Weakness of the CDMA (Code Division Multiple Access) Cellular Service, International Journal of Computer Science and Network Security, Vol. 6, No. 5, May 2006, pp. 218-227, http://paper.ijcsns.org/07_book/200605/200605C11.pdf

[Int96] Designing for On-Board Programming Using the IEEE 1149.1 (JTAG) Access Port, Intel, Application Note, AP-630, November 1996, http://www.intel.com/design/flcomp/applnots/29218602.PDF

[Jan03] Wayne Jansen, Authenticating Users on Handheld Devices, Proceedings of the Canadian Information Technology Security Symposium, May 2003, http://csrc.nist.gov/groups/SNS/mobile_security/documents/mobile_devices/PP-AuthenticatingUsersOnPDAs.pdf

[Jan04a] Wayne Jansen, Vlad Korolev, Serban Gavrila, Thomas Heute, Clément Séveillac, A Unified Framework for Mobile Device Security, The 2004 International Conference on Security and Management (SAM'04), June 2004, http://csrc.nist.gov/groups/SNS/mobile_security/documents/mobile_devices/PP-UNIsecFramework-fin.pdf

[Jan04b] Wayne Jansen, Authenticating Mobile Device Users Through Image Selection, First International Conference on The Internet Society, May 2004, http://csrc.nist.gov/groups/SNS/mobile_security/documents/mobile_devices/PP-VisualAuthentication-rev-DS04.pdf

[Jan07a] Wayne Jansen, Rick Ayers, Guidelines on Cell Phone Forensics, NIST, Special Publication 800-101, May 2007, http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf

[Jan07b] Wayne Jansen, Serban Gavrila, Thomas Heute, Clément Séveillac, Smart Cards for Mobile Devices, International Journal of Information and Computer Security, Vol. 1, No. 4, 2007, http://portal.acm.org/citation.cfm?id=1359375.1359379&coll=GUIDE&dl=GUIDE

[Jeo07] Jonathan Jeon, Seungyun Lee, Position Paper: Toward a Mobile Rich Web Application – Mobile AJAX, W3C/OpenAjax Workshop on Mobile Ajax, September 2007, http://www.w3.org/2007/06/mobile-ajax/papers/etri.jeon.MobileAJAX-PositionPaper-r5.pdf

[Jos07] Lourdhu Hoseph, Alagan Anpalagan, Trends and Challenges in Handheld Wireless Application Development, IEEE Canadian Review, No. 55, October 2007

[Kir08] Jeremy Kirk, Common Mobile Security Doesn't Cut It, Hackers Say, IDG News Service, March 30, 2008, http://www.pcworld.com/article/id,143969-c,hackers/article.html

[Kni02] Ronald van der Knijff, Chapter 11: Embedded Systems Analysis, Handbook of Computer Crime Investigation, Edited by Eoghan Casey, Academic Press, 2002

[Lan04] Mary Landesman, Brador Trojan infects Pocket PC, About, Inc., August 5, 2004, http://antivirus.about.com/od/wirelessthreats/a/brador.htm

[Law05] Stephen Lawson, Phone Virus Spreads Through Scandinavian Company, Computerworld, September 1, 2005, http://www.computerworld.com/securitytopics/security/story/0,10801,104300,00.html

[Law08] Stephen Lawson, Most Analog Cellular to Fade Away Next Week, PC World, February 14, 2008, http://www.pcworld.com/article/id,142511/article.html

[Lawr08] Troy Lawrence, Apple iPhone Passcode Work-Around, Digital Forensic Lab, Fort Worth Police Department, February 26, 2008, http://mobileforensics.files.wordpress.com/2008/02/iphone_passcode_workaround.pdf

[Lawt08] George Lawton, U.S. Cell Phone Industry Faces an Open Future, Industry Trends, Computer Magazine, IEEE Computer Society, Vol. 41, No. 2, February 2008

[Lei08] Jacob Leibenluft, Do Text Messages Live Forever?, Slate Magazine, May 1, 2008, http://www.slate.com/id/2190382/

[Ley05a] John Leyden, Mobile Trojan Kills Smart Phones, Channel Register, April 6, 2005, http://www.channelregister.co.uk/2005/04/06/mobile_killer_trojan/

[Ley05b] John Leyden, Text Me and I'll Reply with a Virus, The Register, April 4, 2005, http://www.theregister.co.uk/2005/04/04/mabir_mobile_worm/

[Ley07] John Leyden, How to Crash a Windows Mobile Using MMS, The Register, January 2, 2007, http://www.theregister.co.uk/2007/01/02/windows_mms_vuln/

[Mag08] Spyphone Software Guide, Magic SpySuite, http://www.magicspysuite.com/img/MagicSpySuite_symbian_0s_9.pdf

[Mar04] T. Martin et al., Denial-of-Service Attacks on Battery-Powered Mobile Computers, IEEE Int'l Conf. Pervasive Computing and Communications, IEEE CS Press, March 2004, pp. 309–318, http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?tp=&arnumber=1276868&isnumber=28556

[Mar07] Laura Marriott, 2D Codes: Coming to a Phone Near You, The ClickZ Network, April 19, 2007, http://www.clickz.com/showPage.html?page=3625619

[Mcc04] Andy McCue, Smartphone 'Trojan' Found to Be Code Flaw, CNET Networks, August 12, 2004, http://news.zdnet.co.uk/security/0,1000000189,39163271,00.htm

[Mcm06] Robert McMillan, New RedBrowser Trojan First to Target J2ME, Computerworld, February 26, 2006, http://www.computerworld.com/securitytopics/security/story/0,10801,109083,00.html?source=x73

[Mcm07] Robert McMillan, Mobile Phones Help Secure Bank of America Transactions, IDG News Service, October 05, 2007, http://www.cio.com/article/144106/Mobile_Phones_Help_Secure_Bank_of_America_Transactions

[Mcw05] Brian McWilliams, How Paris Got Hacked?, O'Reilly Network, February 22, 2005, http://www.oreillynet.com/pub/a/mac/2005/01/01/paris.html

[Mey04] Ulrike Meyer, Susanne Wetze1, On the Impact of GSM Encryption and Man-in-the-Middle Attacks on the Security of Interoperating GSM/UMTS Networks, IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), 2004, pp. 2876-2883, http://www.cs.stevens.edu/~swetzel/publications/gsm.pdf

[Mil05]] Christa Miller, Mobile Spam: Coming to Your Mobile Phone?, Law Enforcement Technology, August 2005, http://www.officer.com/print/Law-Enforcement-Technology/Mobile-Spam--Coming-to-Your-Mobile-Phone/1$26241

[Mot08a] Judy Mottl, My Cellphone, My Everything..., internetnews.com, Jupitermedia Corporation, March 14, 2008, http://www.internetnews.com/mobility/article.php/3734366

[Mot08b] Judy Mottl, What's Motorola's Android Plan?, internetnews.com, Jupitermedia Corporation, September 30, 2008, http://www.internetnews.com/mobility/article.php/3774911

[MS06] Managing Applications on Storage Cards with Autorun.exe, Windows Mobile Development Center, Microsoft Corporation, 2006, http://msdn.microsoft.com/en-us/library/aa454179.aspx

[Nak06] Ellen Nakashima, Used Cellphones Hold Trove of Secrets That Can Be Hard to Erase, Washington Post, October 21, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/10/20/AR2006102001647_pf.html

[Nar08] Ryan Naraine, Low-Cost Attack on GSM Encryption Demoed, eWeek, February 20, 2008, http://www.eweek.com/c/a/Security/LowCost-Attack-on-GSM-Encrytion-Demoed-at-Black-Hat/

[Oco07] James O'Connor, Attack Surface Analysis of BlackBerry Devices, Symantec Security Response, Ireland, April 2007, http://www.symantec.com/avcenter/reference/attack.surface.analysis.of.blackberry.devices.pdf

[Pam05] Jonathan Pamplin, How to Track Any UK GSM Mobile Phone, 2600 Magazine, Vol. 22, No. 4, 2005

[PBS07] GPS Technology Helps Parents Track Teens, PBS, February 19, 2007, http://www-tc.pbs.org/newshour/extra/features/jan-june07/gps_2-19.pdf

[Pog08] David Pogue, How to Block Cellphone Spam, Circuits, The New York Times, June 12, 2008, http://www.nytimes.com/2008/06/12/technology/personaltech/12pogue-email.html?_r=1&8cir&emc=cira1&oref=slogin

[Pre07] Vassilis Prevelakis and Diomidis Spinellis, The Athens Affair, IEEE Spectrum, July 2007, http://spectrum.ieee.org/print/5280

[Rao02] Josyula R. Rao et al., Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards, IEEE Symposium on Security and Privacy, Oakland, CA, May 2002, http://www.research.ibm.com/intsec/gsm.ps

[Rap07] Jim Rapoza, Free 2-Factor Authentication Is Calling, Ziff Davis Enterprise, Inc., September 06, 2007, http://etech.eweek.com/content/security/free_twofactor_authentication_is_calling.html

[Reu06] Using Cell Phones to Track Employees, Reuters Limited, 2006, http://news.zdnet.com/2100-1035_22-6035317.html

[Rob05] Paul Roberts, Paris Hilton: Victim of T-Mobile's Web Flaws? IDG News Service, March 01, 2005, http://www.pcworld.com/article/id,119851-page,1/article.html

[Ros07] Ron Ross, Stu Katzke, Arnold Johnson, Marianne Swanson, Gary Stoneburner, George Rogers, Recommended Security Controls for Federal Information Systems, Special Publication 800-53 Revision 2, NIST, December 2007, http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf

[Sac08] Al Sacco, Mobile Web 2.0: Gen Y Embraces Mobile Social Networks, CIO Magazine, May 28, 2008, http://www.cio.com/article/371714/

[Say08] Peter Sayer, Vodafone CEO Calls for Mobile OS Consolidation, PC World, IDG News Service, February 12, 2008, http://www.pcworld.com/article/id,142392/article.html

[Sca08] Karen Scarfone, John Padgette, Guide to Bluetooth Security, Special Publication 800-121, NIST, September 2008, http://csrc.nist.gov/publications/nistpubs/800-121/SP800-121.pdf

[Sch08] Andreas U. Schmidt, Nicolai Kuntze, Michael Kasper, On the deployment of Mobile Trusted Modules, Fraunhofer Institute for Secure Information Technology SIT, 2008, https://www.trustedcomputinggroup.org/groups/mobile/MTM_deployment_paper.pdf

[Seg07] Sascha Segan, Nokia Intros NFC Phone That Doubles As Credit Card, PC Magazine, January 07, 2007, http://www.pcmag.com/article2/0,2817,2079922,00.asp

[Sha05] Yaniv Shaked, Avishai Wool, Cracking the Bluetooth PIN, 3rd International Conference on Mobile Systems, Applications, and Services (MobiSys 2005), June 2005

[Sha07] Ed Shanahan, Excuse Me, Is This Your Phone?, Reader's Digest, July 2007, http://www.rd.com/national-interest/special-reports-and-surveys/excuse-me-is-this-your-phone/article.html

[She08] Adam Sherwin, The Facebook Tool Which Turns Your Mobile into a Snoop, The Times, April 1, 2008, http://technology.timesonline.co.uk/tol/news/tech_and_web/article3656103.ece

[Shm08] Airsnarf - A Rogue AP Setup Utility, Version 0.2, The Shmoo Group, Retrieved on 6/16/2008 from: http://airsnarf.shmoo.com/

[Sin08] Michael Singer, Web 2.0: Firefox Key to Open Mobile Web, InformationWeek, April 24, 2008, http://www.informationweek.com/news/internet/browsers/showArticle.jhtml?articleID=207401960

[Tbn08] Using Globe G-CASH, TxtBuff News, July 30, 2008, http://news.txtbuff.com/using-globe-g-cash/

[Vas06] Jessica E. Vascellaro, The Bar Code Gets a Hip New Life, The Pittsburgh Post-Gazette, May 24, 2006, http://www.post-gazette.com/pg/06144/692714-96.stm

[Ver08] FlexiSPY PRO-X - Top Level Symbian Spyphone, Vervata, Retrieved on 6/16/2008 from: http://www.flexispy.com/spyphone-call-interceptor-gps-tracker-symbian.htm

[Wil05] Svein Willassen, Forensic Analysis of Mobile Phone Internal Memory, IFIP WG 11.9 International Conference on Digital Forensics, National Center for Forensic Science, Orlando, Florida, February 13-16, 2005, in Advances in Digital Forensics, Vol. 194, Pollitt, M.; Shenoi, S. (Eds.), XVIII, 313 p., 2006

[Wil08] Martyn Williams, Only in Japan: The Best Technologies You Can't Buy, IT World, February 11, 2008, http://www.itworld.com/tech-you-cant-buy-080211

[Wit08] Stephen Withers, Whoops! iPhone Passcode Bypass a Cinch, August 28, 2008, http://www.itwire.com/content/view/20273/53/

Appendix A—Glossary

Assisted GPS (A-GPS) – A technology for providing more accurate location fixes for 911 dispatching when poor signal conditions exist.

Authentication Mechanism – A hardware or software-based mechanism that forces users to prove their identity before accessing data on a device.

Bluetooth – A wireless protocol developed as a cable replacement to allow equipped devices to communicate with each other within a short distance.

Brute Force Password Attack – A method of accessing an obstructed device by attempting multiple combinations of numeric/alphanumeric passwords.

Buffer Overflow Attack – A method of overloading a predefined amount of space in a buffer, which can potentially overwrite and corrupt memory in data.

Code Division Multiple Access (CDMA) – A spread spectrum technology for cellular networks based on the Interim Standard-95 (IS-95) from the Telecommunications Industry Association (TIA).

Cradle – A docking station, which creates an interface between a user's PC and PDA, and enables communication and battery recharging.

Deleted File – A file that has been logically, but not necessarily physically, erased from the operating system. Deleting files does not necessarily eliminate the possibility of recovering all or part of the original data.

Desktop Computer – Any personal computer or workstation used exclusively in a work environment at home or in the office, running a popular operating system, including Windows, Mac OS, and Linux.

Electronic Serial Number (ESN) – A unique 32-bit number programmed into CDMA phones when they are manufactured.

Encryption – Any procedure used in cryptography to convert plaintext into ciphertext to prevent anyone but the intended recipient from reading that data.

Enhanced Data for GSM Evolution (EDGE) – An upgrade to GPRS to provide higher data rates by joining multiple time slots.

Enhanced Messaging Service (EMS) – An improved message system for GSM mobile phones allowing picture, sound, animation and text elements to be conveyed through one or more concatenated SMS messages.

File System – A software mechanism that defines the way that files are named, stored, organized, and accessed on logical volumes of partitioned memory.

Flash ROM – Non-volatile memory that is writable.

General Packet Radio Service (GPRS) – A packet switching enhancement to GSM and TDMA wireless networks to increase data transmission speeds.

Global Positioning System (GPS) – A system for determining position by comparing radio signals from several satellites.

Global System for Mobile Communications (GSM) – A set of standards for second generation cellular networks currently maintained by the 3rd Generation Partnership Project (3GPP).

Image – An exact bit-stream copy of all electronic data on a device, performed in a manner that ensures the information is not altered.

Infrared Data Association (IrDA) – A standard for line-of-sight infrared communication between devices over short distances.

Integrated Circuit Card ID (ICCID) – The unique serial number assigned to, maintained within, and usually imprinted on the (U)SIM.

Integrated Digital Enhanced Network (iDEN) – A proprietary mobile communications technology developed by Motorola that combines the capabilities of a digital cellular telephone with two-way radio.

International Mobile Equipment Identity (IMEI) – A unique identification number programmed into GSM and UMTS mobile phones.

International Mobile Subscriber Identity (IMSI) – A unique number associated with every GSM mobile phone subscriber, which is maintained on a (U)SIM.

Multimedia Messaging Service (MMS) – An accepted standard for messaging that lets users send and receive messages formatted with text, graphics, photographs, audio, and video clips.

Password Protected – The ability to protect the contents of a file or device from being accessed until the correct password is entered.

Personal Digital Assistant (PDA) – A handheld computer that serves as a tool for reading and conveying documents, electronic mail, and other electronic media over a communications link, and for organizing personal information, such as a name-and-address database, a to-do list, and an appointment calendar.

Personal Information Management (PIM) Applications – A core set of applications that provide the electronic equivalents of such items as an agenda, address book, notepad, and reminder list.

Personal Information Management (PIM) Data – The set of data types such as contacts, calendar entries, phonebook entries, notes, memos, and reminders maintained on a device, which may be synchronized with a desktop computer.

Short Message Service (SMS) – A cellular network facility that allows users to send and receive text messages of up to 160 alphanumeric characters on their handset.

SMS Chat – A facility for exchanging messages in real-time using SMS text messaging that allows previously exchanged messages to be viewed.

Subscriber Identity Module (SIM) – A smart card chip specialized for use in GSM equipment.

Synchronization Protocols – Protocols that allow users to view, modify, and transfer/update data between a cell phone and desktop computer.

UMTS Subscriber Identity Module (USIM) – A module similar to the SIM in GSM/GPRS networks, but with additional capabilities suited to 3G networks.

Universal Mobile Telecommunications System (UMTS) – A third-generation (3G) mobile phone technology standardized by the 3GPP as the successor to GSM.

Universal Serial Bus (USB) – A hardware interface for low-speed peripherals such as the keyboard, mouse, joystick, scanner, printer, and telephony devices.

Volatile Memory – Memory that loses its content when power is turned off or lost.

Wireless Fidelity (Wi-Fi) – A term describing a wireless local area network that observes the IEEE 802.11 protocol.

Appendix B—Acronyms

1xRTT	One Times Radio Transmission Technology
A-GPS	Assisted Global Positioning System
AJAX	Asynchronous JavaScript and XML
BSC	Base Station Controller
BTS	Base Transceiver Station
CDMA	Code Division Multiple Access
CF	Compact Flash
CSS	Cascaded Style Sheets
D-AMPS	Digital Advanced Mobile Phone Service
DOM	Document Object Model
EDGE	Enhanced Data rates for GSM Evolution
EDR	Enhanced Data Rate
EEPROM	Electronically Erasable, Programmable Read Only Memory
ESN	Electronic Serial Number
EV-DO	Evolution-Data Optimized
FISMA	Federal Information Security Management Act
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
ICCID	Integrated Circuit Chip Identifier
IDE	Integrated Development Environment
iDEN	Integrated Digital Enhanced Network
IM	Instant Messaging
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IrDA	Infrared Data Association
ITL	Information Technology Laboratory
LDAP	Lightweight Directory Access Protocol
ME	Mobile Equipment
MIN	Mobile Identification Number
MiniSD	Mini Secure Digital
MMC	MultiMedia Card
MMCmobile	MultiMedia Card Mobile
MMS	Multimedia Messaging Service
MSC	Mobile Switching Center
MTM	Mobile Trusted Module

NFC	Near Field Communications
NIST	National Institute of Standards and Technology
OHA	Open Handset Alliance
OMB	Office of Management and Budget
OS	Operating System
PAN	Personal Area Network
PDA	Personal Digital Assistant
PIM	Personal Information Management
PIN	Personal Identification Number
PUK	PIN Unblocking Key
RAM	Random Access Memory
ROM	Read Only Memory
R-UIM	Removable User Identity Module
S60	Symbian Series 60
SD	Secure Digital
SDIO	Secure Digital Input Output
SDK	Software Development Kit
SIM	Subscriber Identity Module
SMS	Short Message Service
SSP	Secure Simple Pairing
TDMA	Time Division Multiple Access
TIA	Telecommunications Industry Association
UMPC	Ultra-Mobile Personal Computer
UMTS	Universal Mobile Telecommunications System
USIM	UMTS Subscriber Identity Module
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
W-CDMA	Wideband Code Division Multiple Access
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access