SECURITY OF CELL PHONES AND PDAS

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

Our nation's workforce is highly mobile today, and very dependent on cell phones and personal digital assistants (PDAs) to carry out work-related functions while on the move. Cell phones and PDAs are small, relatively inexpensive, and convenient tools for many operations: voice calls, simple text messages, personal information management (PIM), such as phonebook, calendar, and notepad, and other functions that might normally be done at a desktop computer. It is possible to send and receive electronic mail, browse the Web, store and modify documents, deliver presentations, and access data remotely. Mobile handheld devices can carry out other useful functions if they are equipped with specialized built-in hardware, such as cameras, Global Positioning System (GPS) receivers, and reduced-size removable-media card slots. These devices use a variety of wireless interfaces, including infrared, Wireless Fidelity (Wi-Fi), Bluetooth, and several types of cellular interfaces.

The Information Technology Laboratory of the National Institute of Standards and Technology (NIST) recently issued a new publication that focuses on the security of cell phones and PDAs. The guide provides updated information to organizations about the issues they should consider in protecting the wireless handheld devices that their workers find indispensible.

NIST Special Publication (SP) 800-124, *Guidelines on Cell Phone and PDA Security: Recommendations of the National Institute of Standards and Technology*

NIST SP 800-124, *Guidelines on Cell Phone and PDA Security*, written by Wayne Jansen and Karen Scarfone of NIST, was issued in October 2008. The security of cell phones and PDAs had previously been discussed in NIST SP 800-48, *Wireless Network Security, 802.11, Bluetooth, and Handheld Devices*, which also covered security issues in wireless local area networks (WLANs) based on Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards, and in networks based on Bluetooth specifications. Bluetooth, which was developed by an industry consortium, is often used by cell phones, and provides three basic security services: authenticating the identity of communicating devices, protecting the confidentiality of information, and controlling access to resources by authorized devices.

The new guidelines discuss the technical and physical characteristics of cell phones and PDAs, the operating systems and network communications standards that they employ, and the applications that they support. A section of the publication describes the security threats to cell phones and PDAs. Another section of the guide deals with the safeguards that organizations can apply to reduce the risks.

NIST SP 800-124 contains an extensive list of references to both in-print and online sources of information about cell phone and PDA security. The appendices include a glossary of the technical terms employed in the publication and an acronym list. NIST SP 800-124 is available from the NIST Web site: http://csrc.nist.gov/publications/PubsSPs.html.

Cell Phones and PDAs: Capabilities and Operations

Cell phones are compact and highly mobile devices that contain a microprocessor, memory components, a radio module, a digital signal processor, and a microphone and speaker for voice communications. Many cell phones support a variety of applications including telephone calls, text messaging, a phone book, and calendar; newer devices often have the ability to synchronize data with a desktop computer, to connect to the Internet, and to access Web sites. They may also have enhanced capabilities such as a camera, applications for reviewing electronic documents, an expanded keyboard, and protocols for the exchange of graphics and audio data.

Different operating systems (OSs) and communications protocols are used for cell phone operations. Cell phone manufacturers may support several different OS platforms, including proprietary systems. Smart phones usually use one of the following: Palm OS, Windows Mobile (phone edition), Research in Motion (RIM) OS, Symbian OS, iPhone OS, and Linux. These advanced systems feature multitasking functions and support Java applications.

Cell phones communicate over cellular networks that divide a large geographical service area into smaller areas of coverage. Different standards are used in digital cellular networks in the United States, including Code Division Multiple Access (CDMA), Global System for Mobile (GSM) communications networks, 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), is used also. These different communications approaches are not compatible with each other.

PDAs are compact, mobile, battery-powered devices that are similar to handheld personal computers, but that store data in solid-state memory rather than on a hard disk. PDAs can synchronize data with a desktop computer, and reconcile and replicate data between the two devices. They contain a microprocessor, memory units, hardware keys and interfaces, and a touch-sensitive display screen. The latest PDAs contain slots that support memory cards and peripherals, such as a digital camera or wireless communications capabilities. Wireless communications, such as Infrared Data Association (IrDA), Bluetooth, and Wi-Fi, may also be built into the device.

The operating system (OS) of the PDA is held in Read Only Memory (ROM), including Flash ROM, which can be erased and reprogrammed electronically with OS updates or a different OS. Flash ROM may also be used to store critical user data and applications.

Random Access Memory (RAM), which normally contains user data, is kept active by batteries which can fail, causing all information to be lost. Devices may provide additional functionality through expansion capabilities such as input/output (I/O) and memory card slots, device expansion sleeves, and external hardware interfaces.

Two widely used families of PDA devices are Microsoft Windows Mobile (formerly Pocket PC) and Palm OS. Some Linux-based PDAs are also manufactured. All devices support a set of basic PIM applications, including contact information, calendar, email, and task management. Most PDAs can be used to communicate wirelessly, review electronic documents, and access Web sites. Third-party applications can be developed and installed using an available Software Development Kit (SDK) or Integrated Development Environment (IDE).

General Development Trends

Handheld devices have added features and functionality over the past few years. The screens of cell phones have been improved, and cameras are often built in. Available services include text messaging, chat messaging, multimedia messaging, instant messaging, and electronic mail. Continued development of handheld devices is expected to lead to capabilities for more powerful and higher-speed communications, similar to the power and functionality of a full desktop computer. These improvements will help to increase productivity, turning cell phones into extensive data reservoirs capable of holding a broad range of personal and organizational information.

Noncellular PDAs are becoming less popular as smart phones now provide the functionality of PDAs and deliver services at high communications speeds. Cell phones can access the Internet, allowing users to browse Web sites, send electronic mail, and engage in peer-to-peer services. Cell phones and PDA devices with built-in Wi-Fi communications may be able to use a nearby access point for Voice over Internet Protocol (VoIP) telephony, as either a backup to cellular service or a primary means of communication. Future communications are expected to be increasingly Internet-based and multimedia-oriented.

Current models of phones can be precisely located through the Global Positioning System (GPS), Assisted-GPS (A-GPS), or other technologies for improving responses to 911 calls. This capability enables the delivery of information about location-based services to subscribers. Other long-term developments may involve the use of phones to hold credit card or other financial information needed for conducting electronic transactions, to authenticate the phone user for remote access to systems, and to provide information to the user about nearby buildings and historic sites.

Security Concerns

The widespread use of handheld devices creates new security risks for an organization. The devices and their memory cards may hold sensitive organizational and personal information, including information about 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. The remote resources accessed by a device through its wireless or wired communications capabilities may also be at risk, including cell phone services, voice mail and email repositories, and applications and data on corporate networks.

Attackers can achieve physical control of a device by overcoming the security mechanisms and gaining access to the contents of the device. Wireless interfaces such as cellular and Bluetooth provide additional avenues of exploitation. Financial losses can occur when subscription services that charge based on usage, such as number of text messages, toll numbers, and unit transmission charges, are used fraudulently. Attackers can use the devices to deliver malware through subscription services as well as through non-subscription wireless interfaces such as Bluetooth.

Security threats to mobile handheld devices include the following:

Loss or theft of cell phones and PDAs are issues because they are small and are often used outside the office. Handheld devices are easier to misplace or to be stolen than are laptop or notebook computers. With physical control, it is relatively easy for attackers to gain access to the information that the handheld devices store or are able to access remotely.

Unauthorized access to devices and their contents may be achieved by forging or guessing authentication credentials, such as a PIN or password, or bypassing the authentication mechanism entirely. Users often do not employ the security mechanisms built into a device, or they may apply settings that can be easily determined or bypassed.

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**, including text messages and voice mail, in addition to electronic mail. Besides the inconvenience of deleting spam, charges may apply for the unauthorized 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.

Electronic tracking services allow the location of registered cell phones to be known and monitored. This tracking can be done openly for legitimate purposes, but it may also take place surreptitiously.

It is possible to create a clone of certain phones that can masquerade as the original. Used in the past with analog phones, **cloning** is not as prevalent today with the rise of digital networks, but some early generation digital equipment has been shown to be vulnerable to cloning.

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 threats involving handheld devices have been limited when compared with those involving desktop computers. One factor is that there is no single dominant operating system for handheld devices, 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, especially when a more open system environment for cellular handheld devices is being established. An open environment would facilitate application development and allow flexibility in choosing devices and applications from many sources, but it would also expedite malware development and potentially provide more attractive targets to attack.

NIST Recommendations for Improving the Security of Cell Phones and PDAs

Many organizations and users have found that wireless communications devices are convenient, flexible, and easy to use. The security issues for these devices are significant, and many common safeguards available for desktop and networked computers are generally not readily available for handheld devices. Devices issued by the organization to staff members may be easier to administer than personally owned devices since the characteristics of the organization's devices are known, their configuration can be centrally managed, and controls can be installed to improve security and compel compliance with policy.

NIST recommends that organizations apply the following safeguards to protect their handheld devices:

Plan for and address the security aspects of organization-issued cell phones and PDAs.

Security issues are much more difficult to address when the deployment and implementation phases of systems are under way; security should be considered at the early stages of planning. While many of the security issues in protecting cell phones and PDAs are similar to protecting desktop computers, there are also significant differences.

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 are applied far less frequently than with desktop computers; changes to firmware can be more daunting to carry out and may 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; another consideration is the centralization of security management for mobile devices.

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 to identify critical issues and guides administrators in making trade-off decisions between usability, performance, and risk. Existing system contingency, continuity of operations, and disaster recovery plans should also be extended to include the mobile handheld devices that have been issued by the organization.

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. The following steps will help to ensure the security of the infrastructure:

* Develop an organization-wide **security policy** for mobile handheld devices.

* Analyze risks to identify vulnerabilities and threats, and assess their likelihood of success and potential damage. Then take steps to **manage assessed risks** by reducing them to an acceptable level and maintaining that level of risk.

* Conduct **security awareness and training** activities to assure that staff members are familiar with security policies and procedures.

* **Configuration control and management** should be applied to ensure that systems are protected against the introduction of improper modifications before, during, and after system deployment.

* Certify and accredit systems. Security **certification** of an information technology system involves an analysis of the system to determine how well it meets all of the organization's nontechnical and technical security requirements. The **accreditation** process involves management acceptance that the system meets the organization's security requirements.

Ensure that handheld devices are deployed, configured, and managed to meet the organization's security requirements and objectives.

Many security issues can be avoided if the devices are configured appropriately. Organizations should employ only the required capabilities and services on mobile devices and should eliminate known vulnerabilities through the application of patches, upgrades, and additional safeguards. The 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 the devices as those requirements change. Security configuration guides or checklists can assist administrators in securing systems consistently and efficiently. The following steps will bolster the security of cell phones and PDAs:

* 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.

Conduct an ongoing process to maintain the security of handheld devices throughout their life cycle.

Maintaining handheld device security requires constant effort, sufficient resources, and vigilance from an organization. To maintain the security of a handheld device, organizations should:

* 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 noncellular wireless interfaces only when needed;

Recognizing and avoiding actions that are questionable;
Reporting and deactivating compromised devices;
Minimizing functionality; and
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.

Centralized security management of organization-issued devices 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; and
Denial of services to noncompliant or unregistered devices.

More Information

For information about NIST standards and guidelines, as well as other security-related publications that help organizations protect their cell phones and PDAs, see NIST's Web page: http://csrc.nist.gov/publications/index.html.