INL/CON-06-11576
PREPRINT

# Nightmares with Mobile Devices are Just Around the Corner!

## IEEE Portable 2007

Kurt W. Derr

March 2007

The INL is a
U.S. Department of Energy
National Laboratory
operated by
Battelle Energy Alliance

# Nightmares with Mobile Devices are Just around the Corner!

Kurt W. Derr
*Idaho National Laboratory (INL)*
*Idaho Falls, Idaho 83415*

***Abstract***— *Mobile Computing Devices (MCDs) such as Personal Digital Assistants (PDAs), smart phones, handheld personal computers, and Tablet PCs, are proliferating in the marketplace. As MCDs become more powerful and commonplace with ubiquitous connectivity, the line that currently divides these handheld devices from typical network computers will become very unclear. Bluetooth, WiFi, and cellular technologies interconnect mobile devices with other computing devices and represent vectors into the device that may be exploited by malicious persons. A malicious person can theoretically take complete control of a mobile device via wireless and use it for all kinds of illicit purposes. While some malicious codes have been reported in the literature for these devices, it is only a matter of time before these codes become as common on mobile devices as they are on desktop computers. Most people have had an experience with a virus on their desktop PC, but have not had the same experience on their smart phone. This will change. The INL is conducting research into MCD vulnerabilities and countermeasures and has developed a web-based client server application for tracking this data. These efforts are described in this paper.*

## I. Introduction

Mobile devices have become integrated into the business processes of both government and commercial institutions. Cheap and ubiquitous mobile computing devices represent computing's fifth wave [1], bringing about new opportunities in the marketplace. MCDs are small, portable, and able to store large amounts of information. The breadth of communication options (infrared, radio frequency, or USB cable) for MCDs introduces many security risks. Some of the problems associated with MCDs are: easy to loose, misplace, or have stolen; potential loss/comprise of company data (user ids, passwords, contacts, digital certificates, sensitive documentation, credit card numbers), increases the opportunity for a backdoor into an enterprise's network, lack of authentication and limited logging capability. The use of these devices poses a risk to the security of an organization. Identifying wireless devices in a given air space is necessary to discover misconfigured devices or security holes or back doors into the corporate network.

Mobile phones are at the greatest risk due to their shear numbers in the marketplace [2] and the convergence of PDA like functionality and cellular technology into a single smart phone device [3]. There are currently more than 2.5 billion cellular connections worldwide [4]. The mobile malware count has already exceeded 200 so far this year [5].

Patching personal computer (PC) software to mitigate security vulnerabilities or upgrade applications is almost automatic today. However, patching mobile device firmware/software is a more difficult process, typically requiring connectivity with a PC. The likelihood that mobile device owners, who are mostly not security conscious, will perform these upgrades is highly improbable, increasing the possibility of spreading malware.

Information technology departments are allowing employees to procure mobile devices due to their low cost and ability to improve productivity. As such, a company or government entity has little control over corporate data leaving the organization on a mobile device. How the devices are used and the type of information that is stored on the devices will directly impact the overall risk to the organization. Organizations should perform risk assessments and develop security plans for MCDs to understand the value of data stored on these devices and the risk of compromising enterprise networks. MCD vulnerability tracking and research is essential to minimizing this risk.

## II. Threats To a Mobile Device

Threat modeling techniques are used to identify and prioritize the threats posed to a MCD. At a high level this process involves identifying the entry points into a device, assets on the device, how the device is used, modeling the system, identifying the threats, and determining if there are valid attack paths for the threats [6]. *Some* examples of potential threats, and corresponding assets, for smart phones are shown in Table 1.

**TABLE 1. POTENTIAL MOBILE DEVICE THREATS AND ASSETS**

| Threat | Asset |
|---|---|
| 1. Unauthorized local/long distance phone call | Access to cellular network |
| 2. Code execution | Ability to execute arbitrary code using a well-known process |
| 3. Unauthorized remote access | Mobile device configuration |
| 4. Unauthorized access to local network (LAN) | Data/processes on the LAN |
| 5. Spying on a conversation | Telephone conversation |
| 6. Deletion of meeting notices | Calendar |
| 7. Copying business/personal data | Database |
| 8. Deletion of contact list | Contact list |
| 9. Make cellular device useless | Mobile device battery |

**Threat 1.** An adversary that can place malicious code on the mobile device can potentially make long-distance phone calls

and disable the ringer. A user may not realize the unauthorized use of the phone until the monthly billing cycle.

**Threat 2.** An adversary may be able to replace an existing well-known application with their own special version that enables them to execute code at will.

**Threat 3, 4.** An adversary who gains access to the device may modify the Bluetooth/WiFi configuration to require no authentication.

**Threat 5.** Special software placed on the device may allow others to listen in on conversations.

**Threat 6.** Unauthorized remote access would allow an adversary to read or modify entries in the calendar.

**Threat 7.** Databases do exist for mobile devices. Unauthorized access may enable an adversary to copy personal/business data.

**Threat 8.** Smart phones and PDAs contain contact lists. A contact list records email address, phone numbers, business address, and general notes on each contact. This information may be deleted or modified if an adversary has access to the device.

**Threat 9.** The battery is the lifeblood of a mobile device. Without power the cellular device is useless. An adversary may construct an attack that sends junk data to a smart phone, keeping the device continuously alive and draining the battery.

Some other possible threats include make long distance phone calls, gain access to contact information or meeting notes, connect to corporate systems (via Bluetooth, WiFi, or cradle) and exporting data, and sending email or SMS (Short Message Service) messages unbeknownst to the user. Threats that have valid attack paths are considered vulnerabilities; i.e., the vulnerability is a way of realizing the threat.

Software development kits (SDKs), with source code, are now available for MCDs. The source code provides the software developer with the ability to create distinctive devices, while also opening the door for malicious programmers to introduce additional threats.

## III. Mobile Device Vulnerabilities

The INL has categorized known vulnerabilities and attacks according to the type of network components and software elements that are susceptible. This provides a proof of principle on how an adversary might be able to exploit identified weaknesses in specific software elements in order to perform undesirable activities. Insecure or rogue wireless devices can compromise the infrastructure of an organization. Understanding the vulnerabilities, and the associated countermeasures, of MCDs is the key to mitigating the threat. The main objective of this effort is to enhance the security of MCDs and make them safer to use in corporate and government environments. Meeting this objective requires understanding the threats, and then providing guidance on how to mitigate those threats. This objective is met by performing vulnerability research and tracking mobile device vulnerabilities. Mobile device research requires an understanding of the continually evolving technologies deployed on MCDs.

A number of computer vulnerability databases are currently accessible over the Internet today. However there is no known equivalent to this in the mobile device world. The INL has developed a Web-based intelligent database application, MDVD (Mobile Device Vulnerability Database), that stores vulnerability and countermeasure information for MCDs. MDVD enables a user to query for technical information on a MCD, which accesses a vulnerability and countermeasure database, and produces a report detailing the known vulnerabilities and countermeasures. Vulnerability and countermeasure information is harvested from the Internet and then entered into MDVD. A variation of MDVD, based on a collaborative database model, will be hosted on the Internet in the near future. This will allow registered users to enter vulnerability and countermeasure data that will reviewed by moderators before being made available to all users.

The approach to understanding the security issues associated with mobile devices involves:

1. Vulnerability discovery,
2. Vulnerability testing,
3. Using tools to protect MCDs from vulnerabilities, and
4. Understand threats posed by the wireless landscape.

### *A. Vulnerability Discovery*

Viruses and other exploits are possible to develop for computing devices due to flaws, or vulnerabilities, in the software. Vulnerability verification requires the execution of exploits to establish the truth, accuracy, or efficacy of vulnerabilities on specific devices. Vulnerabilities for MCDs are found by:

- Searching the Internet for documented vulnerabilities and
- By first hand discovery using traditional vulnerability discovery techniques applied to mobile devices.

*Searching the Internet for Documented Vulnerabilities.* Information on computer and mobile device vulnerabilities come from several different sources on the Internet, but not limited to the following:

- Vulnerability databases,
- Alert services,
- Vulnerability tracking services,
- Advisory services, and
- General Web (blogs, Yahoo Answers, Google Answers, newsgroups, other)

Information is currently being manually gathered while exploring semi-automated information extraction techniques. Vulnerability information may be found on the Web in

generally an unstructured format. For example, "BlackBerry flaw highlights growing mobile device risks" is a news story that discusses an exploit that allows access to an enterprise network via the Blackberry (http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1211099,00.html). Vulnerability information is sometimes found in a semi-structured format where vulnerability title, reference, and ID are identified in an HTML table, such as http://www.qualys.com/research/rnd/top10/.

There are no known databases dedicated strictly to MCD vulnerabilities. There are databases that contain information on features and capabilities of wireless and mobile devices (http://wurfl.sourceforge.net/) and a collection of data on the devices supported by each carrier in XML format (http://mobile.kaywa.com/). Some examples of vulnerability databases, which may include vulnerabilities for MCDs, are:

- OSVDB - http://www.osvdb.org/
- NVD - http://nvd.nist.gov/
- SFVD- http://www.securityfocus.com/vulnerabilities
- CERT – http://www.kb.cert.org/vuls/
- CERIAS - https://cirdb.cerias.purdue.edu/coopvdb
- Help Net Security - http://www.net-security.org
- LWN.net - http://lwn.net/Vulnerabilities/
- WVE - http://www.wirelessve.org/
- NISCC - http://www.niscc.gov.uk/

*First Hand Discovery of MCD Vulnerabilities.* Traditional vulnerability discovery techniques are applied to MCDs to find vulnerabilities. The vulnerabilities and countermeasures are part of the MDVD database. These vulnerability discovery techniques include source code review, protocol fuzzing [7], encryption analysis, and file version comparison. A detailed study of Bluetooth and WiFi protocol stacks on Linux, where source code is available, may generate ideas on possible attack vectors into a mobile device [8, 9, and 10] as well.

### B. *Vulnerability Testing*

The development of exploit code is one of the most difficult programming tasks when verifying computer vulnerabilities. The software may present a common programming error (e.g. buffer overflow), but writing an exploit that exercises that particular portion of the vulnerable software is often tricky. Not all programming errors are easily exploitable. Another challenge in writing exploit code is the hurdle of becoming familiar with unique mobile device architectures. Exploit code is often written in assembly instructions. The instruction set for a device depends upon the processor and available C libraries depend upon the operating system.

A vector analysis is performed using the previously discovered vulnerabilities in MDVD. The vector analysis produces attack vectors that represent the sequence of software steps that must be created to develop the exploits. The exploits are then run to verify the vulnerabilities in MDVD; i.e., make sure the vulnerabilities really represent weaknesses in the software that attackers could exploit.

### C. *Using Tools to Protect Mobile Devices from Vulnerabilities*

Protecting business organizations from MCDs with known vulnerabilities requires the ability to detect those devices and automatically identify vulnerabilities. Mobile computing devices continue to gain more capability, in terms of CPU power, data storage, battery life, and high-speed wireless communications. Many applications that run on desktop computers will be migrated to these devices as the capabilities increase. Commercial virus protection, firewalls, and intrusion detection systems provide a first line of defense. Data encryption, password protection, and sensible configuration management will also provide protection against mobile malware.

An INL toolkit is under development that identifies device vulnerabilities and provides an organization with countermeasure information that can be applied to mitigate those vulnerabilities. The toolkit additionally provides defensive software that may be deployed on a mobile device to mitigate the possibility of rogue code using the communications capability of the device to export information. The vulnerability is that communications channels may be subject to unauthorized use on a mobile device.

TABLE 1. POSSIBLE ENTRY POINTS INTO A MCD

| **General** | **Specific** |
|---|---|
| Wireless Communication Technology | Bluetooth, WiFi, Cellular, Infrared |
| Operating System | Linux, Windows, Palm, Symbian |
| Communication Protocol | HTTP, FTP, Telnet, SSH, TCP/IP |
| Application | Email, Browser, Office Software, Database, Games, Others |
| Software Code | VBScript, JavaScript, Applets, Active X Controls, batch files, shell scripts, macros, executables, Flash |

Mobile devices, like desktop computers, employ a variety of software technologies (see Table 2). Any of these technologies may provide potential attack vectors/entry points into a mobile device. For example, vulnerabilities in 802.11b/g, or an unsafe configuration, could enable a malicious user to gain unrestricted access to the device. Mobile device operating system (OS), communication protocol, application, or general software code that uses insecure functions and simply trusts input data makes the software vulnerable to buffer overruns, indexing errors, format string bugs, and Unicode/ANSI buffer size mismatches [11]. However, unlike desktop/laptop/server computers, mobile devices have one owner who is the "administrator" and "user" of the device. Additionally, access control lists, which are an important defensive mechanism for general computers, are non-existent on mobile devices.

### D. *Understanding Threats Posed By Wireless Landscape*

Understanding the potential methods of attack is important for implementing effective defensive strategies. Mobile devices use wireless communication technologies to connect to other devices and networks. The likelihood of malicious code being deployed on mobile devices will increase as mobile high-speed data networks become pervasive. A key element in safely using MCDs is to understand the threats posed by the wireless landscape, which consists of wireless transceivers used both in businesses and homes. MCDs move between work, home, and elsewhere, potentially making these devices susceptible to malicious code. Misconfigured devices, security holes, and back doors may be identified by collecting and analyzing data from the wireless landscape.

Wireless transceivers may be cell towers, Bluetooth devices/access points, and WiFi devices/access points. Bluetooth technology is deployed in audio headsets, vehicles, mobile devices, printers, vending machines, parking meters, and others. WiFi technology is deployed as local area networks and in many laptop computers and mobile devices. As noted in Table 2, wireless devices and technologies represent potential vectors into mobile devices. To get an understanding of the wireless landscape, both Bluetooth and WiFi data were gathered in the same geographical area.

The collected Bluetooth data consists of Bluetooth device address, manufacturer, device type, signal strength, pairing and connection status, time, and services available. The Bluetooth services available may include voice gateway, dial-up networking, serial port, and file transfer. The Bluetooth Service Discovery Protocol (SDP) is a means for applications to discover which services are available and to determine the characteristics of those available services. The SDP is used by a Bluetooth client device to locate services that are available on or via devices in the client's air space. The WiFi data consists of MAC address, SSID (service set identifier), channel, speed, vendor name, encryption, managed or ad hoc, signal strength, signal to noise ratio (SNR), latitude and longitude, capability information, and beacon interval.

A three dimensional plot of normalized SNR, encryption, and channel WiFi data is shown in Figure 1. The data depicts the access points that would be easy for malicious users to target; i.e., no encryption and a high SNR. Figure 2 shows a plot of normalized access point manufacturer, encryption, and SNR WiFi data. A malicious person might target devices of a given manufacturer by simply trying the default SSID and password to gain administrative access to the device. An invalid MAC address (no denoted manufacturer) for some host may be an indication that the host is sniffing network traffic.

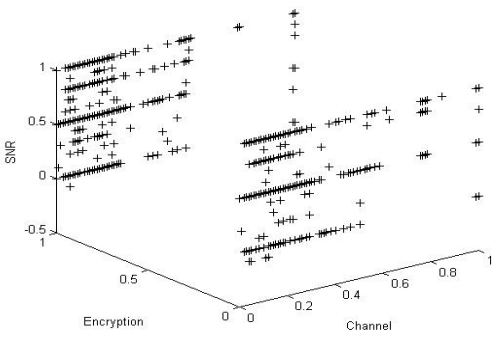


Figure 1. SNR, Encryption, and Channel Data

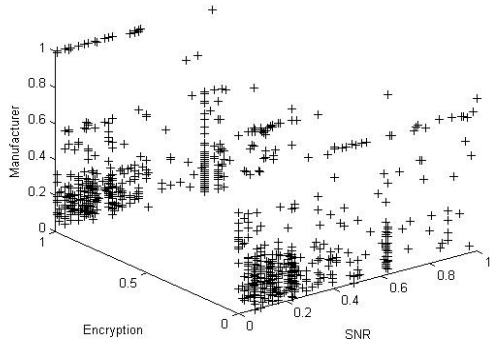


Figure 2. Manufacturer, Encryption, and SNR Data

One approach to detecting regularities and correlations in WiFi/Bluetooth discovery data is to group the data into classes or clusters. All of the objects in one cluster are highly similar to one another, and dissimilar to objects in other clusters. The data is represented as input vectors, where each input vector is for some WiFi/Bluetooth access point/device. Each element in a vector represents a WiFi/Bluetooth characteristic. One model-based approach to clustering data is a self-organizing neural network (NN) known as a Kohonen map [12, 13, 14]. Possible uses of the Kohonen map are for exploratory data analysis and novelty detection. As the network learns to recognize clusters of data the user also begins to understand the data and can refine the network and label the classes. Then the network can be used to perform classification of new data. If new data does not fit into the existing model, then these new data objects are called *outliers* and this indicates novelty. Novel manufacturer types, indicated by the first 6 digits of the MAC address, may represent spoofed MAC addresses.

Wireless landscape data was collected, while driving through a community, on observed wireless access points using both a high-gain directional antenna and a wireless PCMCIA card. WiFi data collection resulted in the discovery of over 800 access points and devices. The data shows that approximately 47% of detected access points have no authentication or encryption. In the wired world, this is analogous to finding Ethernet cables at various community locations that anyone can plug into and gain unrestricted access to the Internet with no authentication. Only 4% of the devices detected represented peer-to-peer connections.

Mobile devices are not highly secure. A number of devices are configured by default (Bluetooth and WiFi) to allow access to other computing resources with minimal security. Devices with Bluetooth technology fully enabled and ready to connect to others have easily been found in public places using a Bluetooth discovery tool such as BlueScanner.

A wireless intrusion detection system (WIDS) may help mitigate the threats posed to wireless local area networks (WLAN) and mobile devices via any wireless technology. A WLAN may be subject to TCP/IP and denial of service attacks, MAC address spoofing, and a wide variety of 802.11 specific threats [15].

## IV. Conclusions and Future Directions

Relatively inexpensive and powerful mobile devices using high-speed mobile data networks via WiFi, Bluetooth, and cellular technologies are the future. These devices are used in remote sensing, input [16], and control applications [17]. Mobile devices are not highly secure and, like desktop computers, need to have defensive software installed for protection. The Dick Tracy watch popularized in 1940s comics may be viable in the not too distant future as high-speed mobile networks become pervasive and mobile devices continue to increase in power and capability (http://www.pcmag.com/encyclopedia_term/0,2542,t=Dick+Tracy+watch&i=41250,00.asp).

Our future work involves further exploration of vulnerabilities in wireless technologies, developing additional mechanisms to both identify device vulnerabilities and to protect mobile devices from attack, and using mobile devices as remote sensors. Countermeasures may be developed for mobile device vulnerabilities when no commercial software exists.

A long-term goal is to perform semi-automatic collection of mobile device vulnerability data from the Internet and populate the MDVD. Clustering and classification of vulnerability and wireless data will be used in combination with active interrogation of a mobile device, as the device enters some area space, to identify potential threats to enterprise systems. This data will be used to help spot vulnerable devices and as input to a WIDS. The WIDS will use this information to detect both common and unique threats to the wireless landscape using neural networking techniques. Efficient clustering and classification techniques will be explored to gain a deeper understanding of regularities and correlations in mobile devices.

## References


[1] How to Ride the Fifth Wave, http://money.cnn.com/magazines/business2/business2_archive/2005/07/01/8265500/, July 1, 2005

[2] D. Dagon, T. Martin, and T. Starner, “Mobile Phones as Computing Devices: The Viruses are Coming!” IEEE Pervasive Computing, vol. 3, no. 4, pp. 11–15, 2004

[3] P. Zheng, L. Ni, The Rise of the Smart Phone, IEEE Distributed Systems Online, March 2006

[4] Newsgator, Geekzone, More Than 2.5 Billion Cellular Lines in the World, http://www.geekzone.co.nz/content.asp?contentid=6628

[5] F-Secure, F-Secure's Data Security Wrap-up for January to June 2006, http://www.f-secure.com/2006/1/

[6] F. Swiderski, W. Snyder, Threat Modeling, Microsoft Press, 2004

[7] Protocol Analysis, http://www.immunitysec.com/downloads/advantages_of_block_based_analysis.pdf

[8] A. Vladimirov, K. Gavrilenko, A. Mikhailovsky, Wi-Foo: The Secrets of Wireless Hacking, Pearson Education Inc. 2004

[9] R. Weeks, Linux Unwired, O'Reilly Media, 2004

[10] F. Zhu, M. Mutka, L. Ni, Service Discovery in Pervasive Computing Environments, IEEE Pervasive Computing, pp. 81–90, October 2005

[16] M. Howard, D. LeBlanc, Writing Secure Code, Microsoft Press, pp. 127-206, Appendix A, 2003

[11] K. Lam, D. LeBlanc, B. Smith, Assessing Network Security, Microsoft Press, pp. 308–311, 2004

[12] J. Lawrence, Introduction to Neural Networks, pp. 113-121, California Scientific Software Press, July 1994

[13] J. Han, M. Kamber, Data Mining, Concepts and Techniques, pp. 376–381, Morgan Laufmann Publishers, 2001

[14] T. Kohonen, The Self-Organizing Map, Proceedings of the IEEE, Vol 78 No 9, September 1990

[15] J. Farshchi, Wireless Intrusion Detection Systems, http://www.securityfocus.com/print/infocus/1742, November 2003

[16] R. Ballagas, J. Borchers, M. Rohs, J. Sheridan, The Smart Phone: A Ubiquitous Input Device, IEEE Pervasive Computing, pp. 70-77, January 2006

[17] J. Nichols, B. Myers, Controlling Home and Office Applications with Smart Phones, IEEE Pervasive Computing, pp. 60-67, July 2006