Global Information Assurance Certification Paper

Mobile Internet Connected Devices:
Our Next Big Achilles Heel
By Jeff Flynn
19 November 2000
GSEC Essay

Accurate estimations of future security environments bear directly on the effectiveness of resulting security systems and policies. Information security analysts frequently base these estimates on trends and the expectation that the future will be governed by a set of laws or empirical properties that remain somewhat constant. As one looks to our recent past, one can see the significant impact caused by the trend of moving from mainframes to internetworked PCs. So profound are these changes that the idea of cyberwarfare bringing death and destruction to the home front appears to be a real possibility. This was something that would have seemed like science fiction 20 years ago. While some information security analysts were sounding the alarm about PCs then, their voices were drowned out by the promise of greater utility, efficiency and cost effectiveness. As significant as this migration has been, another migration has begun that may dwarf it by comparison. This is the migration from geographically bound Internet connected computers to mobile Internet connected devices.

Mobile Internet connected devices are similar to mobile phones and possess some of the functionality we associate with our home computers and/or Personal Digital Assistants PDAs. They will be inexpensive. They will be ubiquitous, and they will perform an increasing number of functions. Initially, the functions will include those that are normally associated with portable devices. These may include voice communications, pager, to-do list, calendar, phone/address directory, clock, calculator, global positioning system receiver, MP3 players, CD players, digital camera and games. As time goes on, however, one can expect that these devices will provide the multi-functional capabilities associated with modern personal computers.

Already, devices like the Neopoint™ 2000, the Nokia 8260, the Qualcomm pdQ™ and the Handspring VisorPhone™ are appearing on the market. Each of these devices combines the functionality of cell phones and PDAs. Some of these also include wireless email and web browsing capabilities.

When examining Mobile Internet connected devices, it is important to remember that these devices are computers. Like computers, they possess inputs, outputs, processors, memory, operating systems and applications.

Interfaces are of particular interest to security analysts because they represent potential paths for attacking the device. Interfaces usually include a display and a keypad. The display may also be touch sensitive. Many PDA devices include an IrDA (infrared) interface that can be used for "beaming" information between devices and for synchronizing database entries with similarly equipped laptop machines. IrDA interfaces

are also currently available on various mobile phones used in Europe and Japan. On October 21st 2000, in a "Birds of a Feather" session at the SANS Monterey Conference, one attendee demonstrated how a Palm device could be used to download the address/phone number list from a Nokia mobile phone without the participation of the mobile phone's owner. Programs for Palm device have also been written that allow TVs and VCRs to be controlled by Palms. Consequently, TVs and VCRs might one day be maliciously programmed to intercept beamed messages.

A serial port is common on both PDAs and mobile phones. This interface can be used to synchronize the hand held device's database with a duplicate database stored on a PC. This interface can also be used to load new operating code into the device to change its behavior. Such software upgrades can be downloaded from the device vendors' web site. Many mobile phone service providers allow software to be upgraded using the RF interface. One would hope that digital signatures protect these upgrades. Still, illicit modification of device software is possible given sufficient expertise and physical access to the device.

RF interfaces to mobile devices can be particularly troublesome from a confidentiality perspective. For example, it has been possible to intercept analog mobile phone voice signals using easily obtained radio scanners. Newer digital systems have reduced the exposure to such threats, yet vulnerabilities are still being uncovered.

The microphone itself should not be overlooked as a potentially dangerous interface. Attacks may be possible where a mobile phone's microphone can be activated without the user's knowledge. This could convert the mobile phone into a sophisticated bugging device. Whether this is possible with current mobile devices may be questionable, but it is important to note that attacks like this have been successfully launched against networked PCs using Back Orifice and Netbus. As Mobile Internet connected devices advance in capability and complexity, attacks of this type may become quite commonplace.

As the industry matures, one should expect standardization in mobile device operating systems. Current options include PalmOS, WindowsCE, EPOC32 and various product specific operating systems such as that used with the Neopoint device. More commonly recognized operating systems like Windows95 through Windows2000 or the countless varieties of Unix are not considered optimal in the mobile device market. Long boot-up times, large memory requirements as well as other characteristics make these complex operating systems undesirable choices. Current devices use streamlined operating systems with minimal memory requirements. This reduces the cost of the mobile device, which is an important factor in gaining public acceptance. With respect to security, this fact may actually have a temporary benefit. Less available memory results in smaller and less complicated programs. This provides fewer opportunities for programmers to make mistakes that lead to security vulnerabilities. On the other hand, it also leaves little room for implementing security functions such as firewall, intrusion detection and anti-virus programs. Also, as time goes on, memory prices will decrease, and memory capacity will

increase. Increased memory capacity will lead to increased functionality and complexity, and the initial benefit of device simplicity will be lost.

To connect to the Internet, mobile devices must employ some suite of communications protocols. Since the Internet runs on the TCP/IP protocol suite [1], TCP/IP would seem to be the obvious choice. In fact, another standard, Wireless Application Protocol™ [2], has garnered much support. Various arguments for a protocol suite other than TCP/IP have been offered. One argument is that TCP/IP requires too much software to be properly implemented on a handheld device. Another is that TCP/IP is not the best choice due to the bandwidth and bit error rate constraints of wireless networks. Arguments against alternative protocol suites suggest that carriers are selecting these protocols to exert more control over the market. Accordingly, in order for users to access the Internet, they must do so via gateways that convert from the environment controlled by the carrier to the open Internet. Connecting to the Internet in this manner allows the carrier to prevent communications between its customers and competing service providers. It's unclear at this time which standards will prevail.

WAP and TCP/IP have a great many similarities. Figure 1 compares the WAP stack to the TCP/IP stack.

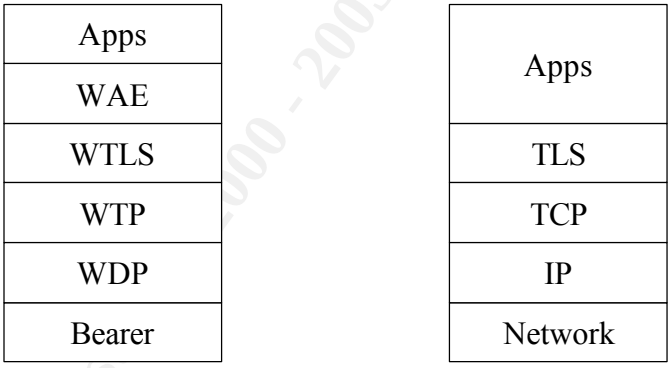

Figure 1. Comparing WAP™ to TCP/IP

Both stacks are designed to allow communication between dissimilar devices connected on dissimilar networks. There are several types of networks. These include Ethernet, tokenring and FDDI. Wireless networks are often called bearer networks and vary according to carrier and regional conventions. There are also many types of bearer networks. These include implementations using GSM SMS, CDMA SMS, IDEN SMS, IS-136 R-DATA, TETRA SDS, and GSM USSD/CELL BROADCAST. SMS represents Short Message Service, which is frequently used for transmitting WAP™ data over mobile networks.

The Internet Protocol (IP) contains the protocol ICMP (Internet Control Message Protocol). This protocol is used for sending management messages. The Wireless Datagram Protocol (WDP) contains a similar protocol called WCMP (Wireless Control

Message Protocol) [3]. Where ICMP may send a destination unreachable message because a packet can not be fragmented, WCMP may send a destination unreachable message or perhaps a Reassembly Failure message. Likewise, where ICMP includes ICMP echo requests and replies, WCMP includes echo requests and replies. Those familiar with various ICMP based network attacks should recognize that similar exploits may be possible using WCMP. In the TCP/IP world, for example, the ping of death, smurfing, ping flooding, source quench, and destination unreachable attacks all exploit various features of ICMP. The question lingers whether similar denials of service attacks based on WCMP features are also possible. The following types of WCMP messages should be of particularly concern:

- No route to destination
- Communication administratively prohibited
- Address unreachable
- Port unreachable
- Erroneous Header Field
- Message too big
- Reassembly time exceeded
- Buffer overflow
- Echo request
- Echo reply

One may also wonder if vulnerabilities like those that have been responsible for TCP (Transmission Control Protocol) based attacks are also to be found in WTP (Wireless Transaction Protocol). Exploits against TCP include syn flood, sequence number prediction, fin scanning and other attacks. Attacks have exploited features of most if not all protocols in the TCP/IP protocol suite. Consequently, it is likely that the WAP™ stack, will have it's own set of vulnerabilities. For example, many applications that run on top of TCP, have been found to contain buffer overflow vulnerabilities. Several of these have led to system administrator level compromises of both Unix and WindowsNT systems. Applications containing these vulnerabilities have included both of the most popular web browsers. One should expect that similar attacks will be identified for the new "mini-browsers" and other applications hosted on mobile devices.

Although many mobile phone service providers have selected WAP™, some have selected TCP/IP. PalmOS based systems include TCP/IP as part of the operating system [4]. Regardless of which protocol becomes the primary standard, vulnerabilities are likely to discovered and exploited.

The list of currently documented exploits against mobile devices is presently small compared to those against networked PCs. In August 2000, a report indicated that strange SMS messages were discovered by a Norwegian company [5]. These messages were being sent to mobile phones causing certain Nokia mobile phones to temporarily freeze. Insufficient information was provided to indicate whether these messages were

the result of a programming mistake or malicious intent. Last September, a Palm Virus was identified [6]. This virus (Palm Phage) can be transferred between Palm devices using the infrared or serial interfaces. When activated on a victim machine, it overwrites all other applications installed on the device. This virus was not widely distributed. Software vendors, however, are already distributing anti-virus packages for devices using PalmOS. Also in September, a trojan horse program (Palm_Lierty.A) for the palm was unleashed [7].

Other attacks are being postulated. One interesting postulated attack involves tricking mobile phones into turning off their encryption function [8]. Because it is illegal to export or use certain types of encryption in various countries, some mobile phones will automatically disable their encryption when they are used in these countries. It appears that it is possible for an attacker to jam the signals from a legitimate cell site. An impersonated site can then indicate that the mobile phone is located in a country where encryption is not allowed. The mobile phone responds to this information and disables encryption. This would allows communications with the mobile phone to be intercepted in the clear. As difficult as this attack may sound, it is probably not outside the resources of organized crime. Before recent technologies (since 1997) were developed to counter the problem, some criminal groups assembled fake cell sites in order to capture the ESNs of passing mobile phones. These stolen ESNs were then used to clone mobile phones in order to steal long distance services.

Use of mobile devices to access the Internet is still a new phenomenon. Widespread public acceptance has not yet been established. To understand why, one only needs to try out the new technology. It simply does not have the utility of modern PC based web browsers connected via high capacity data links. The user interface is mostly textual, and it's slow. Expect this to change. Expect the bandwidths to increase, and the clarity and richness of the displays to improve. When they do, more and more customers will be lured to this technology. The promise of having the right information when and where it is needed will cause this market to improve and to grow. As it grows, we will become more and more dependent upon it. Eventually, we will come to rely on it like we do on our cars or our electric utilities. Businesses, governments and educational institutions will also come to rely on it. Mobile Internet connected devices will quickly become a critical component of our infrastructure. The situation now is quite similar to the situation we faced when networked microcomputers were first starting to become popular. Only this time, things could change faster. Mobile Internet connected devices are being designed for the masses. The cost to purchase such a device will be less than $100, and competition between service providers for the massive market will make the cost of the service quite reasonable. As service providers and device manufactures fight it out to gain initial market share, time to market will become the overriding consideration. This rush to achieve product release dates will motivate companies to cut corners in the area of security. Few companies will expend the resources or time required to properly implement appropriate security measures. Fewer companies will publicly disclose their design information so that security analysts may independently validate the strengths and weaknesses of the security functions. Still fewer companies will expend the time and

money necessary to have their products validated against the lowest levels of assurance defined in government standards such as FIPS140-1 [9] or Common Criteria [10].

As we consider the trends toward mobile Internet connected devices, the result is predictable. System crackers will find and exploit the vulnerabilities. Viruses, trojan horses, worms and other sorts of malware for these devices will become more and more common. And once again, we will find ourselves struggling in an environment not governed by the ideals of freedom and justice, but one governed by the desires of those most powerful, those most clever and those most willing to take unfair advantage.

[1] Comer, Douglas E., Internetworking with TCP/IP, Volume 1, Principles, Protocols, and Architecture, 3rd Edition, 1995, Prentice Hall, ISBN 0-13-216987-8

[2] Wireless Application Forum Ltd., WAP™ Datagram Layer Implementation Guidelines, Version 24-Aug-1999, URL: http://www.wapforum.org/what/technical.htm (11/19/00)

[3] Wireless Application Forum Ltd., WAP™ WCMP, Wireless Control Message Protocol Specification, Approved version 19-Feb-2000, WAP-202-WCMP, URL: http://www.wapforum.org/what/technical.htm (11/19/00)

[4] Rhodes, Neil & McKeehan, Julie, Palm Programming: The Developer's Guide, 1st Edition, December 1998, O'Reilly, ISBN 1-56592-525-4

[5] Batista, Elisa, "Wireless Phone Hack Attack?", 31 August 2000, URL: http://www.wirednews.com/news/technology/0,1282,38557,00.html (11/1/00)

[6] Boulton, Clint, "A Palm Virus Is Born", 22 September 2000, URL: http://www.internetnews.com/wd-news.com/wd-news/article/0,,10_467241,00.html (11/6/00)

[7] Sones, Benjamin, "The Palm That Cried 'Horse?'", 5 September 2000, URL: http://www.hhcmag.com/newsworthy/shownews.asp?article=57 (11/19/00)

[8] Robinson, Sara, "Cell Phone Flaw Opens Security Hole", 18 September, 2000 URL: http://www.zdnet.com/intweek/stories/news/0,4164,2628754,00.html (11/19/00)

[9] NIST Computer Security Division, FIPS 140-1: Security Requirements for Cryptographic Modules, URL: http://csrc.ncsl.nist.gov/cryptval/ (11/19/00)

[10] The Common Criteria Implementation Board (CCIB), The Common Criteria for Information Technology Security Evaluation (CC) version 2.1, URL: http://csrc.ncsl.nist.gov/cc/ (11/19/00)

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor