Global Information Assurance Certification Paper

Mobile Devices Security Issues

by Marco Casazza
Submitted on January 14, 2004
GSEC Practical Assignment
Version 1.4b, Option 1

1. Abstract 3

2. Description of current situation 3
2.1 Availability of malicious code 4
2.2 Discovered vulnerabilities 5
2.3 Exploit scenario examples 6

3. Risk Analysis 7
3.1 Risks associated with PDAs 8
3.2 Risks associated with Smartphones 9

4. Countermeasures 10
4.1 Security Policy 10
4.2 Implementation of Security solutions 11

5. Conclusions 14

Sources and References 15

1. Abstract

In the last few years, the use of mobile devices (also referred as Handhelds) such as PDAs (Personal Digital Assistants) and Smartphones has dramatically increased, due to their ease of use and the considerable availability of new features.
This paper focuses on the description of the current security issues and the available countermeasures to protect the mobile device and the communication infrastructure (from a carrier point of view) from malicious code and inappropriate contents.

2. Description of current situation

The main characteristics of PDAs are represented by their reduced format and the availability of pre-installed operating systems and applications that allow to read and write documents, send and receive e-mails and to manage personal contacts.
Smartphones have additional features such as integrated cellular phone capabilities that allow access to advanced services such as Internet browsing, multimedia and Instant Messaging.
Wireless networks and mobile devices facilitate mobile workforces.
New device capabilities such as expanded memory, increased battery life, stronger computing power with access to wireless connections and Enterprise applications support are bringing down initial barriers to adoption of these new technologies.
Past the initial adoption phases, wireless and mobile devices will give way to more connected and more computerized workforces.
Increasingly, mobile workforces and individuals will change how information is accessed, secured, and managed.
Several analyst firms provided forecasts about the future of mobile devices:

- According to comScore Networks, the number of people in the U.S. who use personal digital assistants (PDAs) or mobile phones to access online services (Web based) is nearing 10 million[1];
- According to Cahners In-Stat/MDR, the market for PDAs should continue to experience double-digit growth over the next few years, peaking at 30 percent in 2004[2];
- According to Strategy Analytics, by 2007, 60 percent of the handheld devices sold will be wireless enabled[3];
  Strategy Analytics also found that PDAs with integrated cellular connectivity (mainly, via WiFi services) will account for 59 percent of total PDA sales in 2007.

The increased use and the business dependence on mobile devices is also confirmed by a recent PDA Usage survey[4] conducted by ZDNet UK on behalf of Pointsec Mobile Technologies.
The survey reported that the top ten uses for PDA devices in 2003 are most business related such as Business diary and Business names and addresses management.
This aspect, even if not strictly related to technological issues, puts in evidence the need to manage potential security issues concerning the use of mobile devices, especially when used as Network-enabled devices (Local Area Networks, Internet, Intranet).

[1] See http://www.comscore.com/press/release.asp?id=87
[2] See http://www.pcworld.com/news/article/0,a_id,84384,tk,dn021802X,00.asp
[3] See http://www.infosync.no/news/2002/n/2223.html
[4] See http://news.zdnet.co.uk/ hardware/mobile/0,39020360,2137153,00.htm

The technological strengths of mobile devices are also their main risk:
PDAs and Smartphones are lost at an high percentage and could easily become the target for ill-disposed.
Putting all the above together, it appears clear that the new technologies and features available with mobile devices are opening the road to new needs in the Security area.
The need to adopt mobility with confidence is driving the need to secure mobile devices.
Both "Home" and "Enterprise" customers have adopted mobile devices. The adoption of such technologies at an Enterprise level is following a course of slow, but constant growth.
Today, Enterprises are facing the impelling need to use mobile devices with a proactive approach to potential security implications.
Analyzing all the phases of adoption of such technologies, the security aspects constitute an extremely important element of the business strategies.
In the current situation, the Enterprises that decide to adopt a strategy of use of "mobile devices" have to face different aspects tied to the security:

- the need to guarantee the protection of the devices themselves and their data;
- the need to protect the network to which these devices connect to;
- the need to protect the flow of information in transit between the devices themselves and the network, with the same characteristics of protection adopted for computer desktops and laptops.

2.1 Availability of malicious code

In general, any method that allows the introduction of executable code on mobile devices represents a potential vehicle of transmission of malicious code.
The first example of a malicious code that attacked mobile phones occurred in June 2000 when the Timofonica[5] virus hit thousands of Internet-enabled cellular phones customers of Telefonica, Spain's largest cell phone provider. This virus caused infected PCs to send text messages (SMS) to Telefonica mobile phone customers.
Another example occurred in Japan targeting the I-mode system developed and owned by Japan's largest cellular phone maker, NTT DoCoMo.
The I-mode system offers wireless device transactions, wireless Internet access and instant messaging services to both consumer and business markets.
In June 2000, a malicious code began to send a particular message to wireless users on the I-mode system. When the users received the message and clicked on a Hypertext link, the program dialed 110, the Japanese equivalent of 911 in North America, without the prior knowledge of the users .
This loading of emergency service lines with useless calls demonstrated the potential serious damage that malicious code spreading partially through mobile devices could inflict to critical key infrastructures.
The introduction of mobile devices-specific malicious code represents a threat not only limited to mobile devices: the additional risk is represented by the feasibility of wide infection of PCs, LANs and the Internet.
Since September 2000, several malicious code examples (viruses or trojan horses) for mobile devices (especially, targeting the Palm OS platform) appeared.

[5] See http://www.trendmicro.com/NR/rdonlyres/E173C2EB_-8C12-43FB-83E3-88DD8D6ED0ED/2772 /wirelessprotection022801.pdf

Until the middle of 2003, no malicious code specifically targeting the PocketPC has been seen.
Several joke programs were made available on PDAs running the EPOC Operating System. These programs proved to cause little damage (their main effects were sounding an alarm or flashing lights on the mobile device), but even not spreading from device to device, they demonstrate that malicious code can be written and can cause, at least, nuisance on mobile devices.
As reported by Symantec Corporation (source Symantec Security Response http://securityresponse.symantec.com) a very low number of malicious code with the ability to delete files exists for the Palm OS platform.

A couple of examples are reported below:
Palm.Liberty.A[6]
Pam.Liberty.A is the first Trojan horse program that infects handheld devices that run the Palm OS. It was discovered in August 2000. As of August 31, 2000, Symantec Security Response does not have any confirmed reports of users being affected by this Trojan horse. It is able to delete applications from Palm Pilot.
Palm.Phage.Dropper[7]
Palm.Phage.Dropper is the first virus to be discovered that infects handheld devices that run Palm OS. It was discovered on September 22, 2000. Symantec Security Response does not have any confirmed reports of users being affected by this virus, and it is considered a very low threat.
It is able to overwrite (delete) all applications on a Palm OS based device.

2.2 Discovered vulnerabilities
Mobile devices vulnerabilities could cause disruptions of services such as DoS (Denial of Service) attacks through mass messaging using SMS (Short Messaging Service) also known as mail bombing.
Usually, MMS (Multimedia Messaging Service) Clients use MIME (Multipurpose Internet Mail Extensions) decoding/encoding features to specify how messages must be formatted, so that they can be exchanged between different e-mail systems.
MIME is not secure by default; security is achieved by adding features such as S/MIME that guarantee authentication (using digital signatures) and privacy (using encryption).
New technologies included within the next generation mobile devices could be leveraged or exploited to develop malicious code.
A few examples of such technologies are:

- Over-The-Air (OTA) WAP (Wireless Application Protocol) extensions:
  standard supported by Nokia, SmartTrust and others for the transmission and reception of application-related information in a wireless communications system;
- WMLScript (Wireless Markup Language Script):
  light version of the JavaScript language and the scripting language used in WML pages;
- WTAI (Wireless Telephony Application Interface);
- WAP Push Method:

[6] See http://securityresponse.symantec.com/avcenter/venc/data/palm.liberty.a.html
[7] See http://securityresponse.symantec.com/avcenter/venc/data/palm.phage.dropper.html

based on open WAP standards, it delivers capabilities that enhance the richness and usability of applications (especially, push-enabled applications, such as real-time multi-user games and messaging).

WMLScript, in particular, was designed to overcome some WML limitations, such as the ability to access the facilities of the mobile device.
For example, on a phone, WMLScript allows the programmer to make phone calls, send messages, add phone numbers to the address book and access the SIM card.
WMLScript provides programmable functionalities that can be used over narrowband communication links in clients with limited capabilities.
Symbian OS smartphones use m-route as synchronization protocol and for general communications.
m-route protocol is based on IP (Internet Protocol): once the smartphone establishes a connection, a few IP ports are opened and available.
These features obviously create more security issues.
Security portals such as SecurityFocus reported the discovery of vulnerabilities and the availability of proof of concept exploit code (when needed) that once executed could block the mobile device functionalities.

A couple of examples are reported below:
Siemens Mobile Phones %IMG_NAME Denial Of Service Vulnerability (Bugtraq ID 7507)[8]
Siemens Mobile Phones are prone to a denial of service when handling malformed image attachments in SMS messages. This is reportedly due to a boundary condition error.
A denial of service may occur when the malformed SMS is received, causing the phone to disconnect. It has also been reported that the user will not be able to access their Inbox. It should be noted that this condition could also occur if a user sends the malformed message from a vulnerable Siemens mobile phone.
This vulnerability was reported in Siemens *45 Series phones, but other phones may also be affected.
PalmOS vulnerable to an ICMP DoS attack (Bugtraq ID 7597)[9]
PalmOS is vulnerable to an ICMP DoS attack: this happens when an attacker continuously sends ICMP_ECHO packets to the device. This type of attack causes 100% CPU usage, and the device therefore comes to a total lockup. The Pilot is almost instantly rendered unusable, until the attacker stops sending packets, or the device is reset. The DoS attack often forces PalmOS to lose its network connections, due to the exhaustion of sending replies to the continuous hoard of ICMP_ECHO packets it is receiving.
Although unconfirmed, this attack may even cause the device to display the message "Fatal exception", and require resetting immediately.

2.3 Exploit scenario examples
Recently, in various security specialists briefings, several exploit techniques have been shown, such as SMS and MMS Spam/Spoofing and Virus propagation.
According to Job de Haas (ITSX Technical Director and presenter at the Black Hat Europe 2003 seminar)[10], several scenarios are possible:

[8] See http://www.securityfocus.com/bid/7507
[9] See http://www.securityfocus.com/bid/7597

Scenario 1

- User is CEO in board meeting.
- Attacker sends SMS/MMS with payload.
- Payload turns on GPRS and retrieves main payload.
- Main payload starts recording the conversation and sends it over the Net.
- Payload shuts down the display so the device appears turned off.

Scenario 2

- Corporate user runs infected application.
- Application stays dormant until ActiveSync.
- Application connects over GPRS to attacker.
- Backdoor path into corporate network is created.

Since it is just the beginning of a large scale adoption of mobile devices as business critical device, it is the time when Enterprises should start looking at ways to manage the security issues related to mobile devices.
Those issues are even more important if you think to the additional connectivity options and the combination with technologies such as WAP in the core of new generation phones (Smartphones).

3. Risk Analysis

The market of mobile devices is experiencing a notable transformation through the introduction of new devices with a number of functionality and ability never seen before, such as the possibilities to execute open operating systems and third party applications, guaranteeing Internet connectivity, e-mail and Instant Messaging services.
The use of Smartphones, particularly in EMEA and in Asia Pacific regions, continues to grow, nevertheless with a different dynamics to the growth of the PDAs.
Since most of the users of Smartphones are single individuals, the security solutions for Smartphones typically revert in the competence of Wireless Carrier Service Providers.
PDAs and Smartphones operating systems are by design mainly focused on low memory usage, small OS footprint and specific hardware support.
Malicious users are faced with the opportunity to challenge themselves on new sophisticated wireless devices running open operating systems, Java applications, additional features such as GSM phone, Internet access and always-on e-mail capabilities.
Basic security features have always been present, but only recently, operating systems and applications vendors seem to have focalized on security features offerings.
Generally speaking, the introduction of new sophisticated devices offers a new mode of transmission for malicious code to wireless and wired internal LANs and further propagation across the Internet.
The typical deployment strategy of mobile devices into an Enterprise does not allow the corporate IT managers more than little control over which wireless and handheld devices their users are connecting to the network.

[10] See http://www.blackhat.com/presentations/bh -europe-03/bh-europe-03-dehaas.pdf

Connecting a mobile device (such as a PDA) into a PC that is then connected to the internal network is similar to inserting a floppy disk• that has not been scanned for viruses• into a computer.
It also means that more systems are connecting to a critical business infrastructure through a hostile network, not represented by the private network, but, for instance, by a public hotspot, a cellular wireless data service or a partner's wireless network.
From a risk perspective, it is important to differentiate the risk analysis in relationship to the protection aspects of PDAs in comparison to Smartphones.

3.1 Risks associated with PDAs

Currently, at least for PDA devices, the data synchronization process through specific applications and procedures and the access to the Internet represent the greatest risks.
The data synchronization process constitutes the principal method through which applications and data are transferred on the mobile device.
For instance, Palm OS–based devices use the HotSynch technology (via Wireless LAN, Bluetooth or InfraRed port) to synchronize data residents on the computer desktop, to save the data on the computer desktop, to manage and to manipulate documents and to install new applications.
The network access through the PDAs represents another vehicle of possible transmission of malicious code: in general, the access to the Internet, to the electronic mail and to the other Internet standard protocols make it possible that the diffusion of malicious code is not limited by the programmability of the mobile device resident applications, but it could open doors that allows remote access, transmission of confidential data or receipt of virus.
The PDAs usually contain an IR (InfraRed) port that allows InfraRed communications (even though most devices use specific applications for the data transfer through the IR port, for instance, PalmOS Exchange manager).
The Risk Analysis related to the exploitation of these threats necessarily has to keep in mind several different factors:

- How the device resident applications can be programmed (the applications based on Palm OS can, for instance, exchange "launch codes" to allow the mutual access to its own data).
  Generally speaking, the PDAs operating systems don't provide the same scripting features as other operating systems or applications for computer desktops do.
- The File System Architecture, unlike the availability of functionalities of a common file system for computer desktops, typically control systems for data and applications access, such as Access Control Lists or Attributes, are not provided.
- Availability of open development environments and languages such as Networking APIs and File System APIs.

Concluding, on one end there are the prerequisites for the creation, the release and the diffusion of malicious code targeting PDAs, from the other end there are still different factors that limit a large scale diffusion of such code.
Since malicious code and vulnerability discovery always target the most popular communication methods and applications, we could expect a greater intensity of attacks trying to access PDAs in the future to gain access to Enterprise Networks and to confidential data.

3.2 Risks associated with Smartphones

Currently, for Smartphones, threats are typically represented by exploit of an operating system vulnerability (and relative implementation of the device vendor or a third party developer).
The adoption trend of generic wireless networking technology (and in this case, mobile phones with wireless capabilities) is following a track which sees home users and small businesses as early adopters.
These users are not always fully aware of the security implications and this aspect creates new security issues and new opportunities of malicious code diffusion.
New generation services like NTT DoCoMo I-mode offer multimedia contents and entertainment features via wireless connections and are generally considered both a more attractive subscription for consumer users and a more feasible target for malicious code writers to cause damage.
Unlike PDAs, Smartphones are usually seen as independent devices that don't rely on computer desktops for connectivity, but use their features to connect to the Wireless Carrier Service Provider.
An example of the potentialities of the Smartphones (and relative security implications) is given by Symbian OS, an open operating system, standard for data-enabled mobile phones.
Symbian OS is based on the EPOC codebase from Psion PDAs.
Symbian OS provides separate OS Core and User Interfaces; OS Core and UI's types are mixed and matched somewhat: Symbian controls OS Core while UI's are controlled by the owning company.
Symbian OS seems to be partially inspired by Microsoft in the use of a FAT filesystem and DLL usage.

Symbian was established as a private independent company and is currently owned by Nokia, Matsushita, Psion, Samsung Electronics, Siemens, LM Ericsson and Sony Ericsson.
Motorola one of the original founders with Nokia, Psion and LM Ericsson recently left.
Phone makers like Sony Ericsson, Matsushita, Nokia, Samsung, Siemens, Benq, Fujitsu, Sanyo and Mistubishi develop mobile phones based on Symbian OS.
Symbian established Symbian Platinum Partner program in order to enable the development of Symbian OS based applications: being part of the program enables access to OS source-code and to higher levels of support.
According to Craig Heath[11] (strategic product manager for Security at Symbian), phones with open operating systems that allow third party development are more vulnerable, because developers has access to the source code.

Currently, the main MS Windows Mobile-based phones makers are HTC Corporation, Mitac (both based in Taiwan) and Sendo (based in United Kingdom).
The income of Motorola as provider of Microsoft Windows Mobile-based phones will give remarkable push to their spreading.
Between the retailers of Motorola phones (using Microsoft technology) will also figure Orange, the French operator controlled by France Telecom: this is also good news after that T-Online had sent back the launch of its own MS Windows Mobile-based models because of technical problems.

[11] See http://www.pcworld.com/news/article/0,aid,110914,00.asp

Recently, security issues were also divulged about Microsoft solution for Smartphones based on MS Windows Powered Smartphone software[12].
The discovered security bug allowed users to disable security features enabled by default to prevent the installation of not certified applications.

The mobile devices market is evolving very quickly with the addition of new devices, peripherals, features and services: companies like NTT DoCoMo and Motorola recently announced[13] the future availability of mobile devices based on open-source operating systems (Linux) equipped with Sun Microsystem's Java programming language.
This will change ulteriorly the scenario in terms of security issues.

4. Countermeasures

Based on the analysis previously conducted, the real challenge now is trying to define a "secure" approach in establishing a PDA/Smartphone deployment strategy in the Enterprise.
A multi layered protection approach[14] should consist of:

- Definition of security and usage policies;
- Increase the awareness of the potential threat involving corporate IT managers, service providers, operating system and application developers and end users;
- Device registration and Change and Control Management procedures;
- Definition of an "Employee Termination" procedure;
- Deployment of Security and Management solutions which include Antivirus protection, File encryption, Device Firewall and VPN software, Device Integrity, Theft Protection, Device Authentication, Device Management, Desktop Synchronization tools.

4.1 Security Policy

The first phase, as always, is based on sound and well known (by users) integrative Security Standards that regulate the use of mobile devices within the Enterprise.
Typically, the Security Policy should describe the:

- Scope of the Security Policy itself.
  The Security Standards should be related to Enterprise-owned devices. Only on those devices should be stored sensitive information. This would limit the employee to use personal mobile device to synchronize data from Corporate tools.
- Mobile device hardware supported by the internal IT infrastructure.
  A list of supported devices (vendor and model) and eventual expansion slots should be provided.

[12] See http://www.pcworld.com/news/article/0,aid,108834,0_0.asp
[13] See http://www.internetnews.com/wireless/article.php/3172841
[14] See http://www.sans.org/score/handheldsche_cklist.php

Also, placed in evidence that eventual existing PDAs and Smartphones need to be replaced if they don't meet the security requirements.
Limited support could be provided in the meantime.

- Standard Security
  PDAs and Smartphones should be required to adhere to the same security standards already required for laptops, because of their similar mobility.
  Minimum Security requirements could include Antivirus and Data encryption software.
- Software and operating systems supported by the internal IT infrastructure.
  Every mobile device should have personal productivity tools such as, to name a couple, document reader/writer, synchronization software with minimum or mandatory required version.
  Eventually, system management software could be deployed to allow centralized asset management, software delivery, remote backup capabilities.
- Available services.
  Allowed services should be listed; for instance, e-mail service may not be allowed unless additional security measures (such as SSL VPN) are implemented, specific types of network connections could be disallowed such as GPRS or Bluetooth.
- Security Policy Enforcement.
  Statement about the impossibility of using PDAs or Smartphones not adhering to such standards.
- Insurance regulations.
- Which additional PDA/Smarthone Standards will be considered in the future.

Once communicated, the Security Policy should be periodically reviewed, so that any change (from a technological point of view or not) could be properly addressed.

4.2 Implementation of Security solutions

Several tools working at the device level and/or at the operator level are available in order to make the mobile devices more secure.
These solutions tipically include features such as malicious code protection (antivirus), inappropriate contents protection (content and spam filtering), data and traffic encryption and help to overwhelm gaps in terms of security within the mobile devices themselves.

Malicious code protection from viruses, worms and trojan horses is generally achieved through Antivirus solutions that can identify, repair or block malicious code. Several Antivirus providers such as Symantec[15], Network Associates McAfee[16] and Trend Micro[17] already offer Antivirus solutions specialized for mobile devices (minimal footprint and capability to recognize only mobile devices specific threats): these solutions are "desktop assisted" with the antivirus application periodically synchronized with a PC Desktop in order to receive configuration and antivirus definitions updates.

[15] See http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=237&EID=0
[16] See http://www.networkassociates.com/us/products/mcafee/antivirus/remote_user/vs_pda.htm
[17] See http://www.trendmicro.com/en/products/desktop/pcc-wireless/evaluate/overview.htm

Alternately, a wireless-based feature may allow the antivirus application to retrieve the updates from the Internet.

Wireless capabilities within mobile devices constitute another potential threat; the presence of a local personal firewall and the secure encrypted remote access to the private network through the public Internet offer an additional layer of protection. Device resident Personal Firewall[18] and Virtual Private Network solutions (both IPSec and SSL based) are available in order to guarantee the protection of the device during network communications.

One of the main risks associated with mobile devices is their loss or theft: only few seconds are needed to synchronize information from a mobile device to a PC if the access to the PDA is not password protected or the password is weak or the information are not encrypted.
Ability to get into a private network or access to confidential information (imagine a case of identity theft) could be realized.
Data Encryption tools are available and allow to set an additional security layer: tools such as PDA Defense (from Asynchrony Solutions[19]) provide several advanced features to protect the access to the mobile device connectivity features and stored data.

For large Enterprises, the cost of controlling mobile devices is tremendous, due to the number of workers using a variety of devices. Theft and security are huge concerns, but Enterprises also worry about the cost of application updates. According to Ronni Colville, a network and systems management analyst at Gartner Inc:[20]
"Enterprises of all sizes are looking for one-stop shopping for managing their desktops, laptops and, more often now, their wireless devices".
At an Enterprise level, there is an increasing need of security solutions that integrate with Mobile Device Management frameworks, such as Novell ZENWorks[21] for Handhelds or Mobile Automation Handheld Management[22] solutions.
Mobile Device Management frameworks include asset management, software delivery, remote backup features that help to manage the mobile devices from a central console with a single view on both mobile devices, computers and network infrastructure.

From a Wireless Carrier Service Providers point of view, the main next business target is represented by Enterprise customers, rolling out more and better data and services from their wireless networks. While this drives growth for these wireless carriers, it also raises security risks. Also, in Europe where the mobile phone market has reached a saturation point, operators are looking for other ways to get more revenue. Security may be an added service that Enterprises (and then, end users) will pay for.
The main threats are the increased availability of third generation mobile phones based on Symbian OS, the characteristics of the MMS (Multimedia Messaging

[18] See http://www.bluefiresecurity.com/mobile_firewall_plus.php
[19] See http://www.asolutions.com/products -pdadefense.asp
[20] See http://www.computerworld.com/networkingtopics/networking/manageme_nt/story/0,10801,73767,00.html
[21] See http://www.novell.com/products/zenworks/handh_elds/quicklook.htm l
[22] See http://www.mobileautomation.com/ma.asp?cat=solutions&page=handheld_mgmt

Services – based on technical specification TS 23.140 of the Generation Partnership Project – 3GPP) platform and the vulnerability of the communication infrastructure.
A typical Carrier infrastructure is based on systems acting as WAP Gateways and routing messages to MMS (Multimedia Messaging Services) Relay Servers.
The communication between the WAP Gateways and the MMS Relay Server is HTTP based.
Mobile operators are increasingly demanding for IP Multimedia System (IMS) platforms that offer advanced services such as SMS, MMS, Instant Messaging, Chat and others.
There is an increased need for security solutions working at the operator level that support protocols such as SIP (Session Initiation Protocol, commonly used for multimedia presentations across the Internet and Internet telephony applications) and are able to filter malicious code or unwanted content (spam).
Several operators became aware of the availability of special forged MMS messages which could block the normal behaviour of third generation mobile phones.
Security solutions at the Carrier level (thus working at the gateway level) should allow the detection of malicious code or spam using wireless Internet protocols (for instance, Compact HTML – CHTML and the Wireless Markup Language – WML) as transport vectors.
New solutions such as Content Guardian from Telcotec[23] help to provide protection to both operators and mobile subscribers from adult, inappropriate, unsolicited or damaging content originating from mobile devices, e-mails, external applications and the Internet.

[23] See http://www.telcotec.com/products.html

5. Conclusions

Although malicious code targeting the mobile device platforms has yet to cause serious damage, such code seen in the lab and, in some cases, in the real world, has indicated that there is the potential for serious damage.

Since the difference between cellular phones (and in some instances, computer desktops and laptops) and mobile phones is rapidly disappearing, the new functionalities of the mobile devices represent a new potential target for hackers (and even disgruntled or careless employees) — in much the same way that each new technology emerged in the last two decades has been.

The threat from malicious code targeting mobile devices is currently in its infancy.

But, we have seen that it is possible to develop Trojan Horses since executable programs could be created and perform malicious actions unknown to the user.

It is possible to have virus since it is possible to find files and write to them.

It is possible to have a worm since the mobile devices can be connected to a network, can copy over that network and damage to existing users can be caused.

Until today, in fact, malicious code has yet to negatively impacted mobile device users.

But this will probably soon change: probably, the attackers will get more and more interest as soon as these new technologies are largely deployed, a standardization process begins and exchange of data increases due to additional network connectivity (Bluetooth and 3G/UMTS services).

It's not possible to anticipate how threats will appear, or when, but what it's sure is what technologies are expected in the next 12 to 24 months: these technologies could drive threats very fast (Bluetooth, 3G/UMTS).

Unfortunately, it doesn't exist a "digital device" that is 100% secure.

Tipically, wireless security threats should be viewed as an extension of wired security threats. The strategy is to build upon currently implemented product and services, adding specific solutions for wireless devices and networks where needed.

And as mobile devices technologies and applications expand and evolve, careful attention must be made to maintain those security measures.

The deployment phase of mobile devices should include the implementation of security measures from the start.

The alternative to waiting until the threat materializes in the wild could cause remarkable costs in terms of reduced productivity, loss of confidential information and consumer confidence.

Sources and References

1.– Graham Mudd (comScore Networks)
"**Ten Million Internet U sers Go Online Via A Cell Phon e Or PD A, Reports comScore Media Metrix** ", 27 Aug 2002
URL: http://www.comscore.com/press/release.asp?id=87

2. – Tom Krazit (IDG News Service)
"**PDA Popularity Grows, but More Slowly** ", 18 Feb 2002
URL: http://www.pcworld.com/ news/article/0,aid,84384,tk,dn021802X,00.asp

3. – Jørgen Sundgot (infoSync)
"**2002 PDA shipments going up** ", 26 Aug 2002
URL: http://www.infosync.no/news/2002/n/2223.html

4. – Munir Kotadia (ZDNet UK)
"**Careless PDA users threaten corporate security** ", 8 Jul 2003
URL: http://news.zdnet.co.uk/hardware/mobile/0,39020360 ,2137153,00.htm

5. – Trend Micro
"**Virus and Malicious Code protection for Wireless Devices** " Feb 2001
URL: http://www.trendmic ro.com/NR/rdonlyres/E173C2EB -8C12-43FB-83E3-88DD8D6ED0ED/2772/wirelessprotection022801.pdf

6. – Motoaki Yamamura (Symantec Security Response)
"**Palm.Liberty.A** " Aug 2000
URL: http://securityresponse.symantec.com/avcenter/venc/data/palm.liberty.a.html

7. – Motoaki Yamamura (Symantec Security Response)
"**Palm.Phage.Dropper** ", Sep 2000
URL: http://securityresponse.symantec.com/avcenter/v enc/data/palm.phage.dropper.html

8. – r2subj3 ct@dwclan.org
"**Siemens Mobile Phones %IMG_NAME Denial Of Service Vulnerability** ", 6 May 2003
URL: http://www.securityfocus.com/bid/7507

9. – Shaun Moore
"**PalmOS vulnerable to an ICMP DoS attack** ", 14 May 2003
URL: http://www.securityfocus.com/bid/7597

10. – Job de Haas (Technical Director, ITSX)
"**Pocket PC Phone Security** ", 15 May 2003
URL: http://www.blackhat.com/presentations/bh -europe-03/bh-europe-03-dehaas.pdf

11. – Gillian Law (IDG News Service)
"**Do PDAs Pose a Security Risk?** ", 02 June 2003
URL: http://www.pcworld.com/news/article/0,aid,110914,00.asp

12. – Joris Evers (IDG News Service)
"**Security Flaw Found in Smartphone Software"** , 16 Jan 2003
URL: http://www.pcworld.com/news/article/0,aid,108834,00.asp

13. – Mark Ber niker (internetnews.com)
"**NTT DoCoMo Backs Linux, Symbian** ", 4 Dec 2003
URL: http://www.internetnews.com/wireless/article.php/3172841

14. – Eric Maiwald and his PDA team (SANS Institute – Bluefiresecurity)
"**Handheld Security Checklist** " ,12 Aug 2003
URL: http://www.sans.org/score/handheldschecklist.php

15. – Symantec Corporation
Symantec Antivirus for Handhelds Corporate Edition
URL: http://enterprisesecurity. symantec.com/products/products.cfm?ProductID=237&EID=0

16. – Network Associates Inc.
McAfee VirusScan PDA Enterprise
URL: http://www.networkassociates. com/us/products/mcafee/antivirus/remote_user/vs_pda.htm

17. – Trend Micro
Trend Micro PC -cillin for Wireless
URL: http://www.trendmicro.com/en/products/des ktop/pcc-wireless/evaluate/overview.htm

18. – Bluefiresecurity
Bluefire Mobile Firewall Plus
URL: http://www.bluefiresecurity.com/mobile_firewall_plus.php

19. – Asynchrony So lutions
PDA Defense
URL: http://www.asolutions.com/products -pdadefense.asp

20. – Matt Hamblen (Computerw orld)
"**Tool Integrates Desktop, Mobile Device Management** ", 26 Aug 2002
URL: http://www.computerworld.com/networkingtopics/networking/management/story/0,10801,73767,00.html

21. – Novell
Novell ZENWorks for Handhelds
URL: http://www.novell.com/products/zenworks/handhelds /quicklook. html

22. – Mobile Automation
Mobile Automation Handheld Management solutions
URL: http://www.mobileautomation.com/ma.asp?cat=solutions&page=handheld_mgmt

23 – Telcotec
Telcotec Content Guardian
http:// www.telcotec.com/products .html

Last Updated: July 28th, 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
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
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 Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	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
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
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event