Ethical Hacking and Countermeasures

Version 6

Module XXXVI

Hacking Mobile Phones, PDA and Handheld Devices

First iPhone Trojan in the wild

By Tom Espiner, ZDNetUK, News.com
Published on ZDNet News: Jan 08, 2008 11:26:18 AM

Tags: security, iPhone, Trojan, Apple iPhone, Trojan Horse, Erica, Spyware, Spyware, Adware & Malware, Viruses And Worms, Tom Espiner, ZDNetUK

The first warnings about the Trojan were posted on Saturday on the iPhone modification forum ModMyiFone.com, said security vendor F-Secure. When installed, the Trojan appeared to do nothing more than display the word "shoes", according to the ModMyiFone post.

However, when a user attempted to uninstall the malicious code, the application wiped files from the /bin directory, breaking "Erica's Utilities" such as sendfile. Erica's Utilities are a collection of command-line utilities for the iPhone, according to security vendor Symantec, which warned on Monday that the Trojan also overwrites OpenSSH, an open-source encryption protocol.

The Trojan, known as "iPhone firmware 1.1.3 prep", or "113 prep", is the first to be seen in the wild, according to Symantec researcher Orla Cox.

"This is technically the first Trojan horse seen for the iPhone; however, it does appear to be more of a prank than an actual threat," Cox wrote in a blog post. "The impact of uninstalling the 'Trojan' would appear to be an unintended side effect."

Affected users need to uninstall the Trojan and reinstall affected files, according to Symantec. The risk to users is minimal as they would have to choose to install the bogus package and the site which was hosting it has now been taken offline, wrote Cox.

Both Symantec and F-Secure warned that users should be cautious when installing third-party iPhone applications. Apple warned in September last year that its own updates could break unlocked iPhones running unofficial iPhone software.

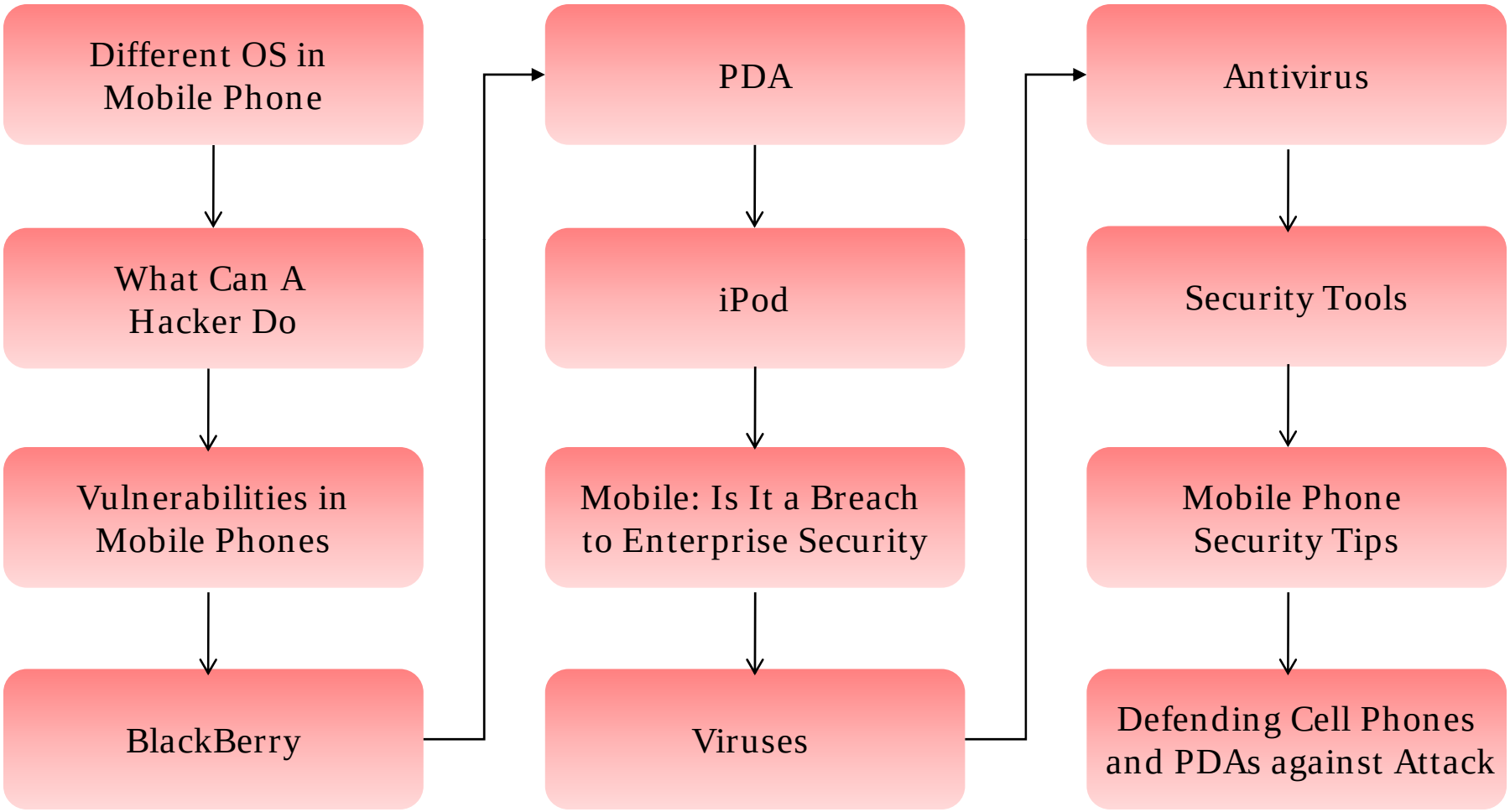
Source: *http://news.zdnet.com/*

Module Objective

This module will familiarize you with:

- Different OS in Mobile Phone
- What Can A Hacker Do
- Vulnerabilities in Mobile Phones
- BlackBerry
- PDA
- iPod
- Mobile: Is It a Breach to Enterprise Security
- Viruses
- Antivirus
- Security Tools
- Mobile Phone Security Tips
- Defending Cell Phones and PDAs against Attack

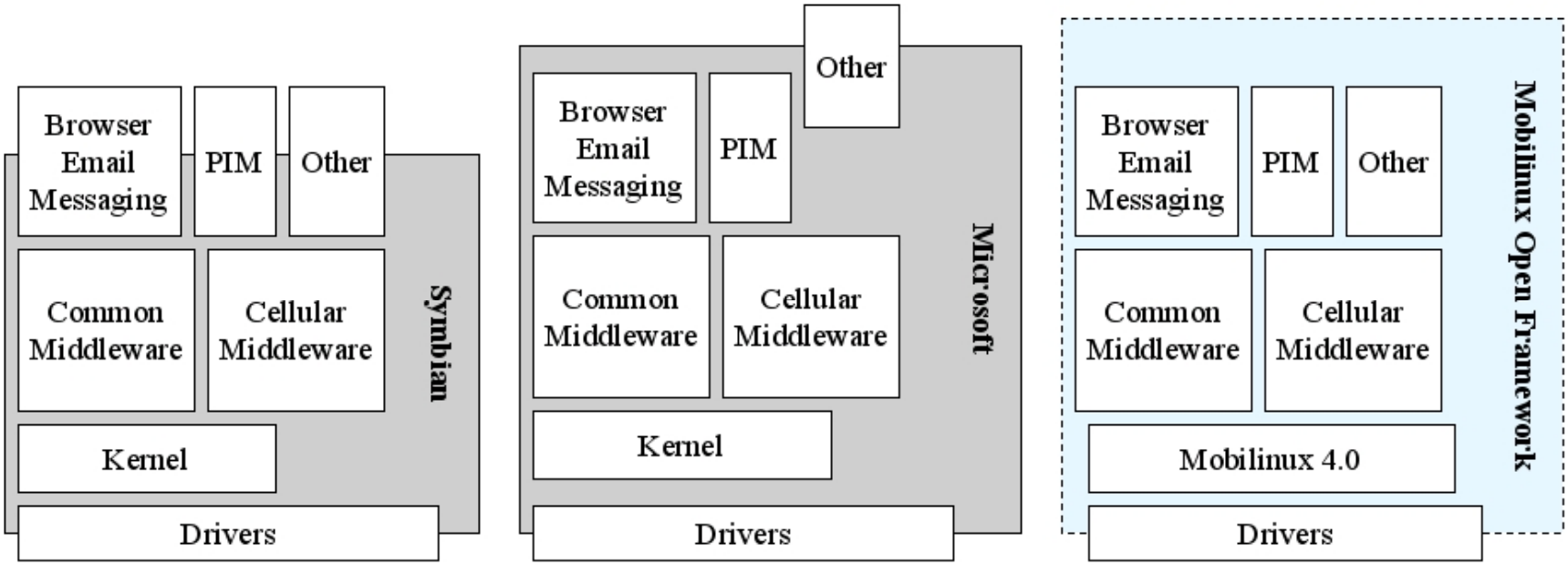
Module Flow



Different OS in Mobile Phone

- Palm OS
- Windows Mobile
- Symbian OS
- Linux

Different OS Structure in Mobile Phone



Evolution of Mobile Threat

Mobile phone operating systems consist of open APIs which may be vulnerable to attack

OS has a number of connectivity mechanisms through which malware can spread

Malware propagates on the network by:

- Connectivity to mobile networks and the Internet
- Symbian installation files (SIS)
- SMS
- MMS
- Bluetooth
- Wireless
- USB
- Infrared

Threats

Mobile Malware Propagation:

- Malware propagates across the Internet and infects PCs
- Infected PC can infect a smartphone via:
  - IR
  - Bluetooth
- Infected smartphone can in turn propagate the malware through wireless LAN to other smartphones

DDoS Floods:

- Botnets on infected mobile devices wait for instructions from their owner
- After getting instruction to launch DDoS floods, the mobile provider's core infrastructure may be overwhelmed with a high volume of seemingly legitimate requests
- It results into denial of service, failure in connecting call as well as transmitting data

What Can A Hacker Do

Steal your information:

- Hackers can download addresses and other personal information from your phone

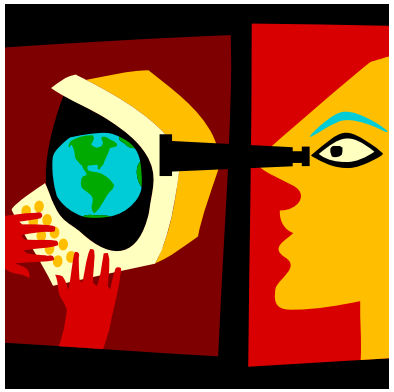
Rob Your Money

- Hacker can transfer money from your account to another account

Spying

Access your voice mails

Insert the virus



Vulnerabilities in Different Mobile Phones

A format string vulnerability in Research In Motion Ltd.'s BlackBerry 7270

- Allows a remote hacker to disable the phone's calling features

HTC HyTN using AGEPhone is vulnerable to malformed SIP messages sent over wireless LAN connections

- Active calls are disconnected

A buffer overflow vulnerability in Samsung SCH-i730 phones that run SJPhone SIP Clients

- Allows an attacker to disable the phone and slow down the operating system

A Dell Axim running SJPhone SIP soft phones is vulnerable to denial of service attacks

- It can freeze the phone and drain the battery

SDP parsing module of D-Link DPH-540 and DPH-541 Wi-Fi phones

- Allows remote attackers to disable the phone's calling features

Malware

Malware allows hackers to access critical and often confidential information which is stored on the device and on the network those devices connect to

Malware can steal contact information, address lists, message logs, and call logs

In some cases, the malware can also be used to issue commands from the device, so hacker can have total control of a smartphone or mobile phone to make calls and send messages

Malware will spread faster across the mobile network and it is difficult to detect because of complicated virus-writing techniques

Spyware

Hackers have created mobile spyware, which manipulates SMS messages and allows them to be read by others

Process:

- Hacker sends an SMS message to the target
- Target opens the message, installing the spyware onto the device
- That spyware, unknown to the victim, takes the SMS messages and forwards them on to the hacker

Spyware: SymbOS/Htool-SMSSender.A.intd

SymbOS/Htool-SMSSender.A.intd is a prototype spyware application that targets the Symbian OS

It sends copies of received SMS messages to the spyware author

SymbOS/Htool-SMSSender.A.intd is distributed as source code and in a SIS file named "XaSMS.SIS“

Both the source code and SIS file are included in a RAR archive file named "HackSMS.rar“

It copies the text of the last SMS message received, places it into a new SMS, and forwards the message to the spyware

Spyware: SymbOS/MultiDropper.CG

SymbOS/MultiDropper.CG is the spyware application that targets the Symbian operating system for mobile phones

The spyware application comes bundled with a variant of the MultiDropper mobile phone Trojan

It tracks text messages and copies log files with the phone number of incoming and outbound phone calls

Best Practices against Malware

Make sure all host systems that you sync your devices have the latest anti-virus protection

Activate Bluetooth when necessary and turn it off when not in use

Do not click on every attachment sent to your PC e-mail inbox, and check all unsolicited messages and software on PDAs and phones with suspicion

Blackberry

Serious BlackBerry hack attack exposed

Hacking program due to be released next week

Robert Jaques, vnunet.com 09 Aug 2006

Many enterprises that have issued staff with BlackBerry mobile email devices will be vulnerable to a serious hack attack when security researchers release exploit code, security experts warned today.

According to Secure Computing Corporation, any firm that has deployed a BlackBerry server behind its gateway could fall foul to the hacking code that is due to be published by IT security specialist Jesse D'Aguanno next week.

The soon-to-be-released hacking program, called BBProxy, can be installed on a BlackBerry or sent as an email attachment to an unsuspecting user. Once installed, BBProxy opens a back channel bypassing the organisation's gateway security mechanisms between the hacker and the inside of the victim's network, Secure Computing stated.

Since the communications channel between the BlackBerry server and handheld device is encrypted and cannot be properly inspected by typical security products, a tunnel is most often opened by the administrator to allow the encrypted communications channel to the BlackBerry server inside the organisation's network. A malicious person could potentially use this back channel to move around inside an organisation unabated and remove confidential information undetected or use the back channel to install malware on the network.

Paul Henry, vice president of Strategic Accounts for Secure Computing, warned that servers connecting to the public internet have an inherent risk: " Isolating these internet-facing servers reduces the risk of a compromised server providing access to other critical servers. Hence due diligence would require that any internet-facing server like a BlackBerry server should be isolated on its own demilitarised zone segment," said Henry.

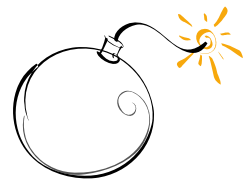
He also advised enterprises to ensure that their mail servers working with the BlackBerry server are also an internet-facing server and should also be isolated on their own separate DMZ.

Additional protection can be achieved by preventing internal users from opening arbitrary connections to either the BlackBerry server or mail server.

Source: *http://www.vnunet.com/*

Blackberry Attacks

"BlackBerry Attack Toolkit" along with "BBProxy" software exploits the vulnerability of any company's website



- BBProxy is a security assessment tool that runs on blackberry devices and allows the device to be used as a proxy between the Internet and the Internal network

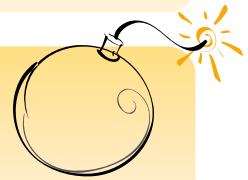
"Attack vector" links and tricks the users by downloading the malicious software

Blackjacking or Hijacking attacks exploit legal users' BlackBerry devices and replaces them on network with harmful devices

Blackberry Attacks: Blackjacking

Blackjacking : *Using the BlackBerry environment to circumvent perimeter defenses and directly attacking hosts on a enterprise networks*

BBProxy tool is used to conduct the Blackjacking



Attacker installs BBProxy on user's blackberry or sends it in email attachment to the targets

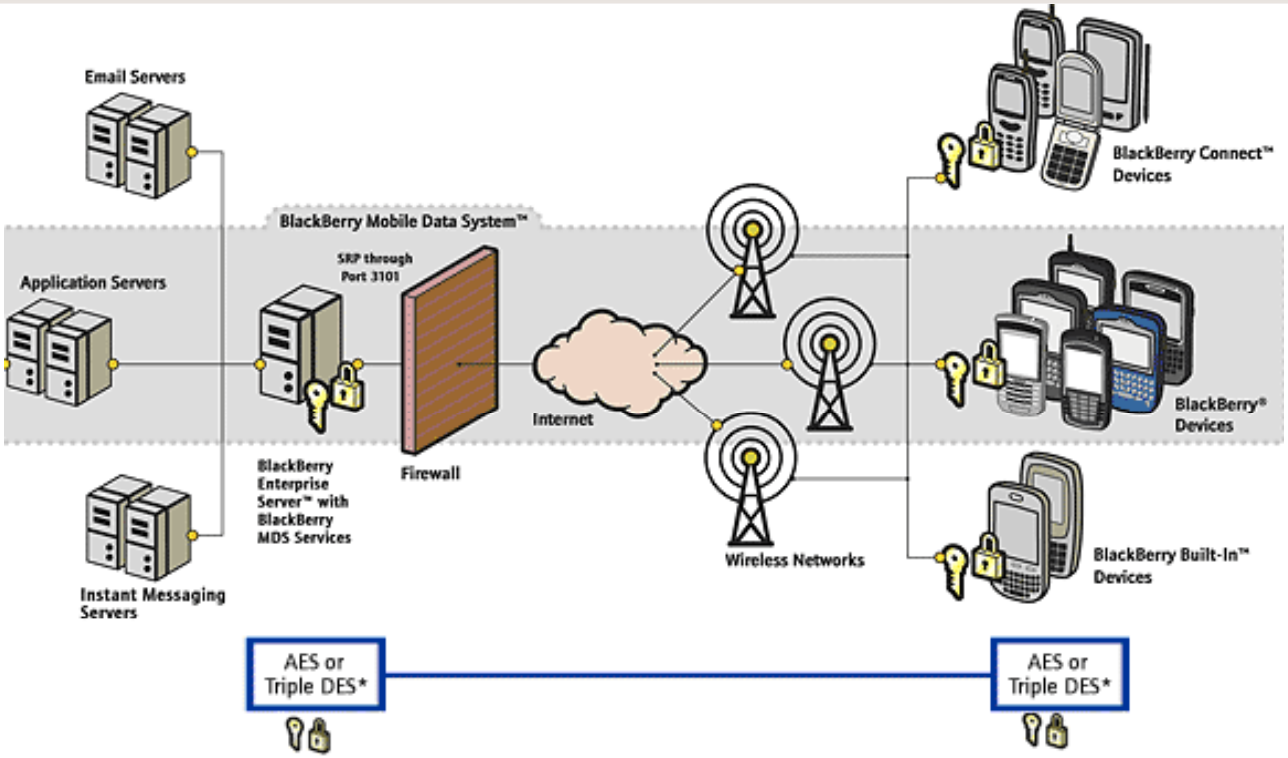
Once this tool is activated, it opens a covert channel between hackers and compromised hosts on improperly secured enterprise networks

This channel between the BlackBerry server and handheld device is encrypted and cannot be properly inspected by typical security products

BlackBerry Wireless Security

The BlackBerry Enterprise Solution uses Advanced Encryption Standard (AES) or Data Encryption Standard (Triple-DES) encryption methods to encrypt data in transit

The BlackBerry Enterprise Solution is designed so that data remains encrypted during transit and is not decrypted between the BlackBerry Enterprise Server and the handheld devices



BlackBerry Signing Authority Tool

It helps the developers by protecting the data and intellectual property

It enables the developers to handle access to their sensitive APIs (Application Program Interfaces) and data by using public and private signature keys

It uses asymmetric private/ public key cryptography to validate the authenticity of signature request

It allows external developers to request, receive, and verify the signatures for accessing specified API and data in a secure environment

Countermeasures

- Clean the BlackBerry device memory
- Protect stored messages on the messaging server
- Encrypt application password and storage on the BlackBerry device
- Protect storage of user data on a locked Blackberry device
- Limit the Password authentication to ten attempts
- Use AES (Advanced Encryption Standard) technology to secure the storage of password keeper and password entries on BlackBerry device (e.g. banking passwords and PINs)

Personal Digital Assistant (PDA)

PDA Security Issues

Six different security issues related to PDA:

- Password theft
- Viruses and data corruption
- Data theft through line sniffing
- Theft of the PDA itself
- Mobile code vulnerabilities
- Wireless vulnerabilities

ActiveSync Attacks

Windows Mobile Pocket PC and Smartphone are vulnerable to ActiveSync attacks

ActiveSync handheld is connected to a desktop PC via its cradle

ActiveSync requires a password to be entered

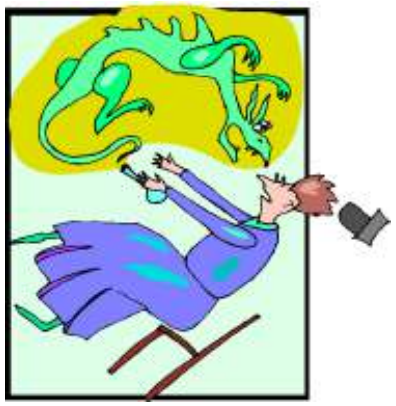
Attacker can access the password through password sniffing or brute force dictionary attacks

If an unauthorized user gains access to the desktop, they will have access to the ActiveSync password

After accessing the password, attacker can steal private information or unleash the malicious code

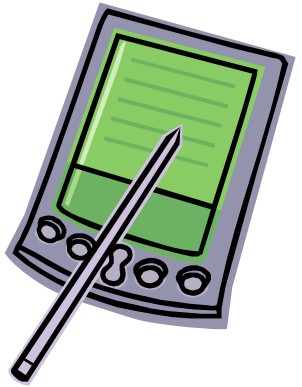
HotSync Attack

HotSync is the process of synchronizing information between your Palm handheld device and your desktop PC



Palm devices can be vulnerable because of HotSync features

When HotSync enables to synchronize elements, the Palm OS opens TCP ports 14237 and 14238 as well as UDP port 14237



Attacker can open connections to these ports and access private information or unleash the malicious code

PDA Virus: Brador

Brador is the first known backdoor for the Pocket PC hand-held devices

When run, the backdoor copies itself to startup folder, mails the IP address of the PDA to the backdoor author, and starts listening commands on a TCP port

The hacker can then connect back to the PDA via TCP port and control the PDA through the backdoor

It runs on ARM-based Pocket PC devices that have Windows Mobile 2003 (Windows CE 4.2) or later

PDA Security Tools: TigerSuite PDA

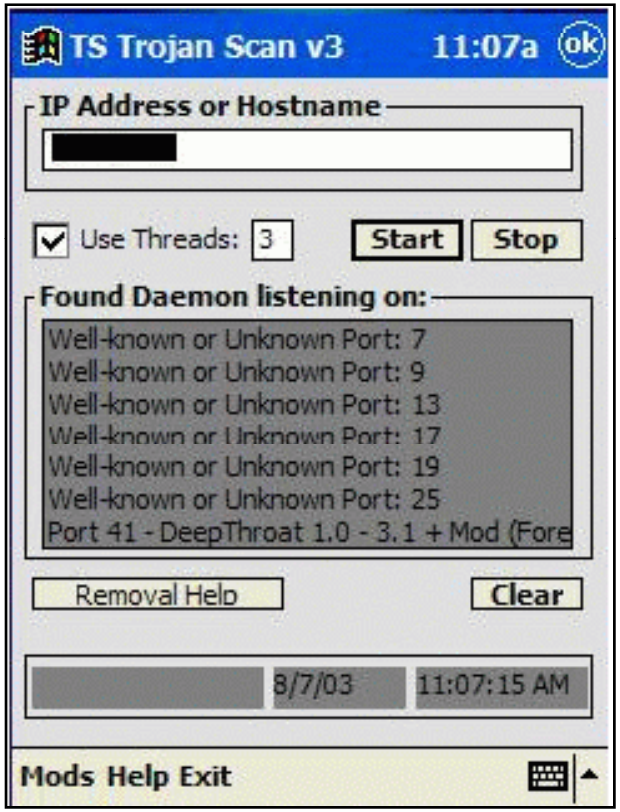
TigerSuite PDA includes remote scanning, service detection, penetration testing, and network and file tools such a hex editor, IP subnetter, host collaboration, and remote Trojan scanner

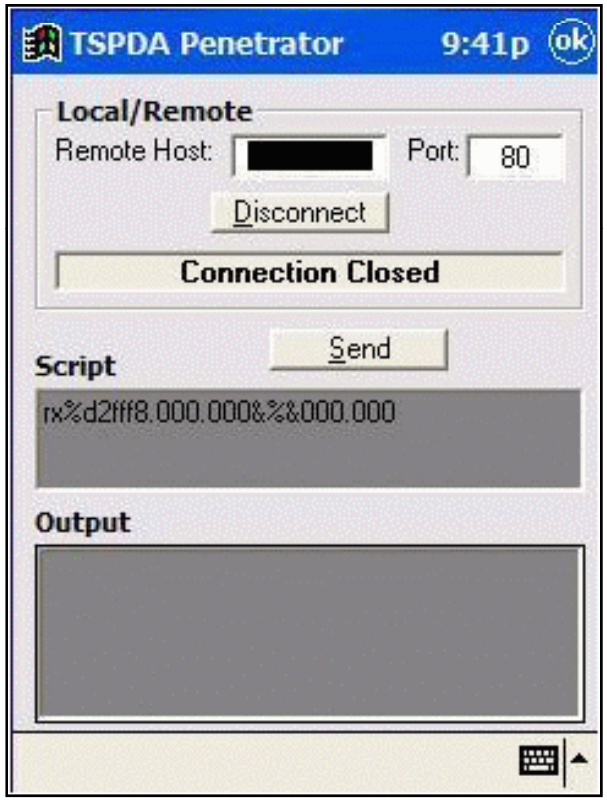
Suite operates from Main Memory or Storage Card, and is compatible with wireless, IR and LAN Internet and/or network connections

Features:

- Hex Editor--File Hack
- IP Subnetter
- Remote Trojan Scanner
- Host Collaboration
- Stealth Scanning
- Port FIN Scanner
- Session Sniffers
- Service Recognition and Verification
- TigerSim Virtual Server Simulators
- WLAN Scanning with RC Site Query

TigerSuite PDA: Screenshot





Security Policies for PDAs

Organizations generally create security policies to protect sensitive data residing on PDAs

End-user behavior policy states that PDAs should not be used for receipt or sending of e-mails with private and sensitive information

By creating end-user behavior security policies, organizations can hold the end-users accountable for security violations

Users can create a policy that requires the synchronization capability (hotsync) to be turned off

iPod

iPod

The iPod refers to a class of portable digital audio players designed and marketed by Apple Computer

Devices in the iPod family offer a simple user interface designed around a central scroll wheel

The iPod can play MP3, M4A/ AAC, Protected AAC, AIFF, WAV, Audible audiobook, and Apple Lossless audio file formats

iTunes is a media player for playing and organizing digital music, video files, and purchasing digital music files in the FairPlay digital rights management format

The iTunes Music Store (also sometimes referred as "iTunes" or "iTMS") is the component of iTunes through which you can purchase digital music files from within iTunes

Misuse of iPod

iPod's large capacity and ability to connect easily to a computer and transfer data rapidly via USB, makes it potentially more useful in information theft

iPod devices can be used to spread viruses or child pornography, or maintain records for criminal organizations

- Criminals use iPod and all its features in a variety of ways
- Calendar entries may contain dates of crime or other events that are related to crime
- Contact information of conspirators or victims along with photos or other documentation are transferred and stored on iPod

Jailbreaking

Jailbreaking is the process used to unlock the iPhone and iPod touch devices to allow the installation of third-party applications

It can add ringtones or change wallpaper on your iPhone

It opens up your iPhone's file system so that it can be accessed from your computer

Tool for jailbreaking: iDemocracy

iDemocracy is the iPhone jailbreak and third-party app installation solution for the Windows platform

It installs Installer.app (for 3rd party apps/ games), custom ringtones, and SIM unlock

It has new features like free ringtones on firmwares , as well as File Browsing

iDemocracy: Screenshot

Tool for jailbreaking: iActivator

iActivator is a Cocoa-based application for the Mac

iActivator is a graphical interface providing iPhone activation/deactivation tools, and methods for breaking/restoring the jail

iActivator: Screenshot

Tool for jailbreaking: iNdependence

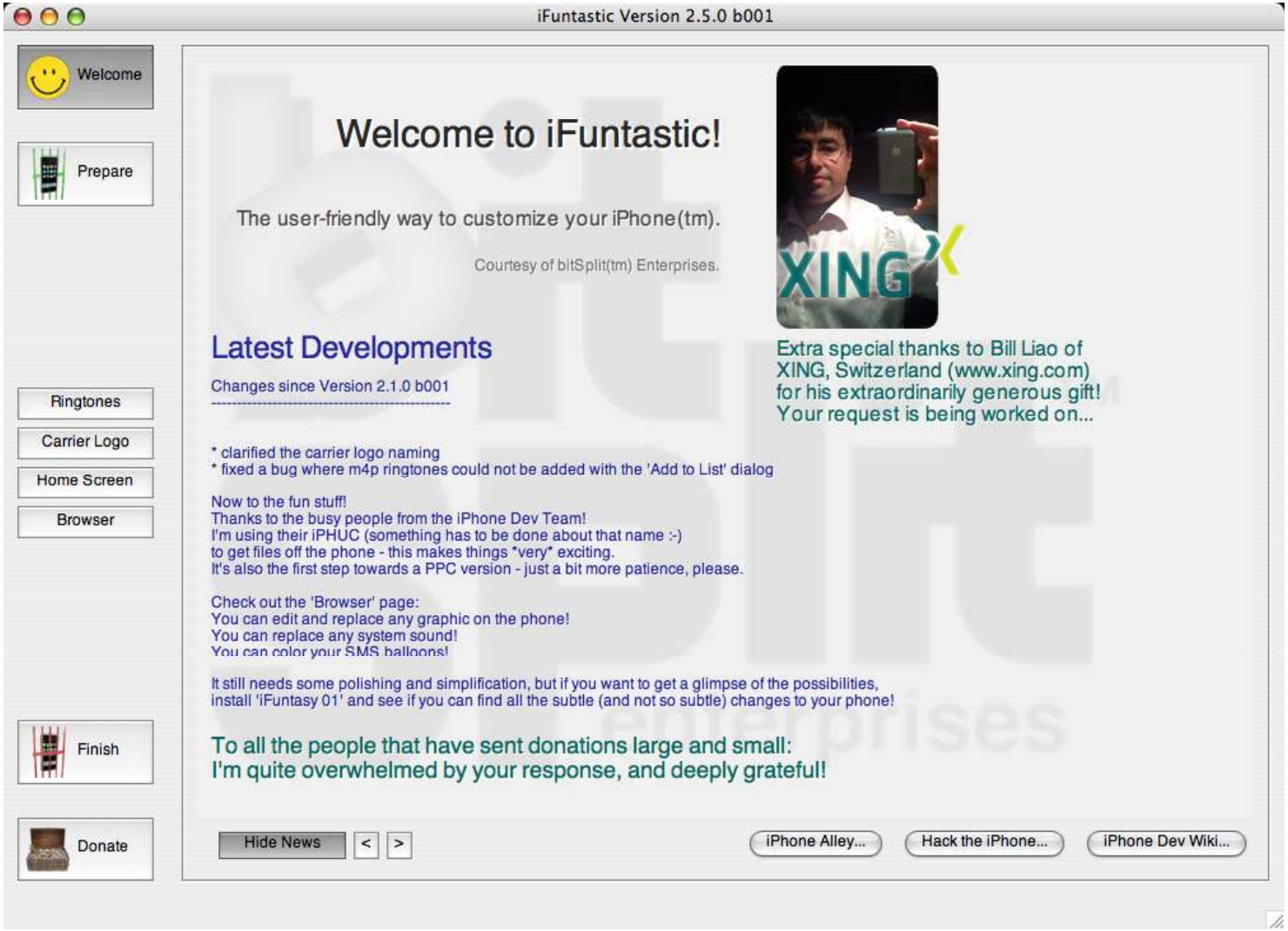
iNdependence is a Cocoa-based application for Mac OS X which provides an easy-to-use interface for jailbreak, activation, SSH installation, and ringtone

It allows unauthorized third-party application installation on your iPhone

Tool for jailbreaking: iFuntastic

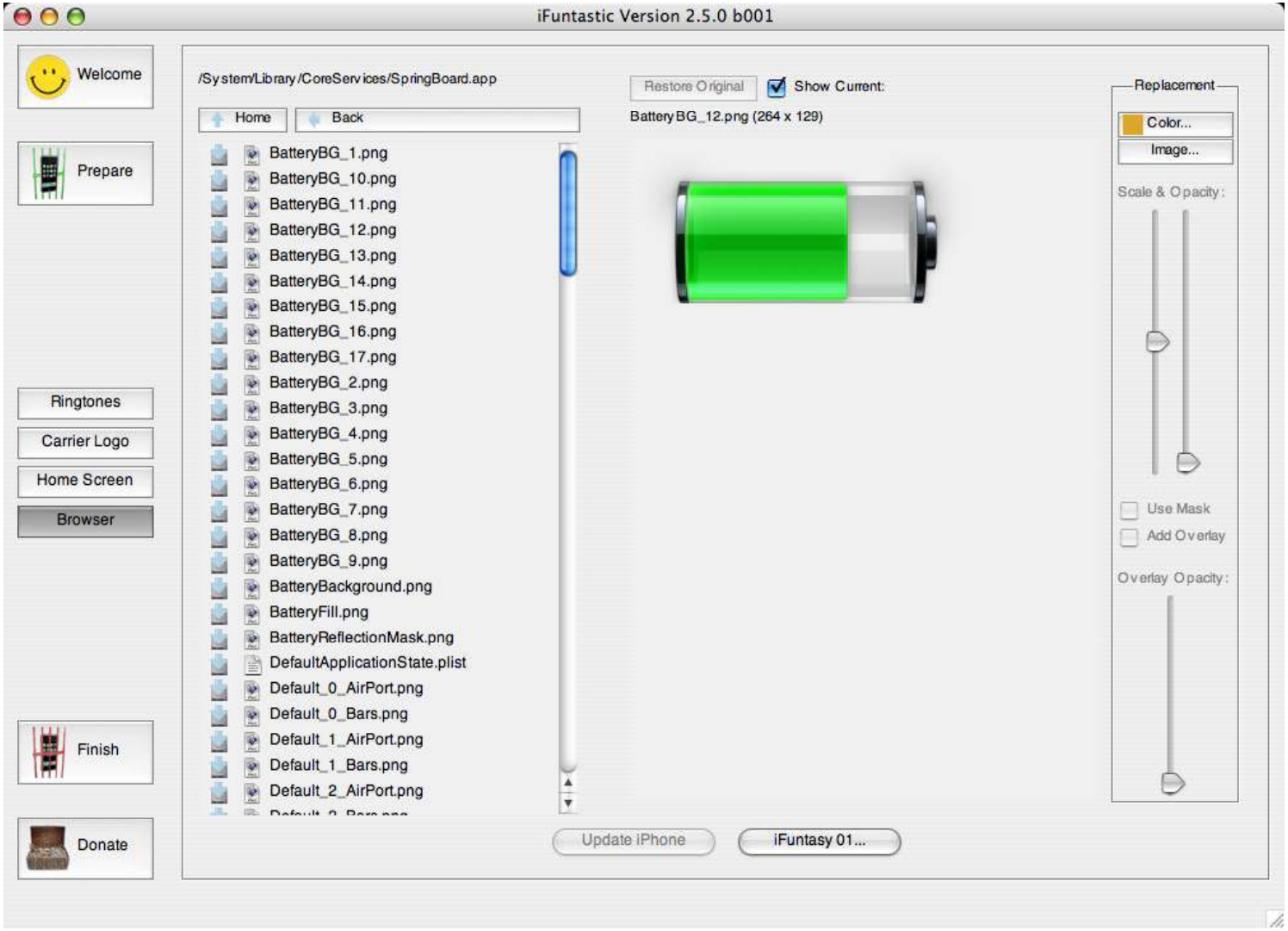
- iFuntastic is an iPhone hacking and modification tool
- It can dig into your iPhone, edit images, and logos
- It can replace any system sounds and color iChat SMS balloons
- It has full file browser feature, which simply browses the iPhone's internal file system, and edit UI images

iFuntastic: Screenshot 1



iFuntastic: Screenshot 2

iFuntastic: Screenshot 3



Prerequisite for iPhone Hacking

An Intel Mac

The iPhone Hacking Kit

Your Mac and iPhone need to be connected to the same Wi-Fi network

Step by Step iPhone Hacking using iFuntastic

Install iFuntastic in your Applications folder, which is present in the iPhone Hacking Kit

After installing do the following steps:

Reboot your Mac safely. You don't want iFuntastic crashing during this process

↓

Make sure your iPhone is on, then plug it into your Mac using the usual cable

↓

After iTunes launches, quit it

↓

Launch iFuntastic

↓

Press Prepare button, present on the left side of the iFuntastic window

↓

Click the Jailbreak button at the bottom of the window

↓

On the next page of the window, there are six steps, follow them

↓

You will see the window as on next slide

Step by Step iPhone Hacking

AppSnapp

AppSnapp is a process for jailbreaking and allowing the installation of non-sanctioned third-party applications to the iPhone

The process will jailbreak the iPhone or iPod Touch and then push Installer.app to the device, which contains a catalog of native applications that can be installed directly over a WiFi or EDGE connection

It automates the process on iPhones running software/ firmware

It can be completed using the iPhone without interacting with a Mac or Windows computer

Steps for AppSnapp

Navigate to http://www.jailbreakme.com on your iPhone or iPod Touch, to automatically jailbreak and put Installer.app on the device

Click the "Install AppSnap" button at the bottom of the page, you will see the "Slide to Unlock" screen

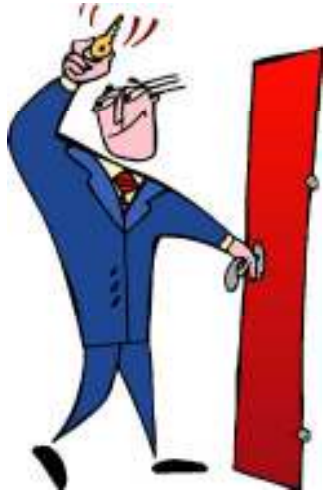
After sliding to unlock, you will have the "Installer" icon on your screen, tap the "Installer" icon, then tap "Sources", and install the "Community Sources" package

Install the BSD Subsystem and OpenSSH under "System"

Now your iPhone is primed to receive and make use of third-party binaries

Tool to Unlock iPhone: iPhoneSimFree

- iPhoneSimFree is used to unlock the iPhone
- iPhoneSimFree Unlock works on all versions of iPhone
- iPhoneSimFree Unlocked phones can be updated from any version to 1.1.1 safely without bricking your radio and GSM functions
- iPhoneSimFree Unlock is restore and update resistant



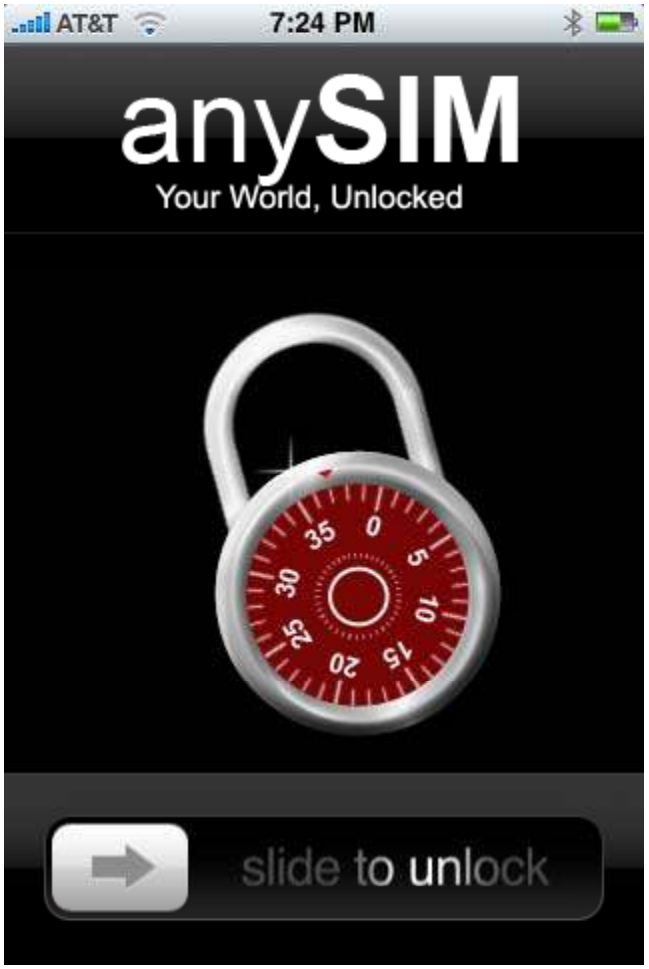
iPhoneSimFree: Screenshot

Tool to Unlock iPhone: anySIM

anySIM is a GUI-based SIM unlocking solution for iPhone

This is for iPhones working recently with OS v1.1.1 running on it or iPhones that were upgraded from 1.0.2 to 1.1.1

It is described as fully automatic, requiring only to be copied to a "jailbroken" iPhone and launched from the Springboard interface



Steps for Unlocking your iPhone using AnySIM

Jailbreak your iPhone with software

Set it up to install third-party applications

Use the following steps to put AnySIM on it:

1. Download AnySIM and expand the ZIP file
2. Drag the resulting file "anySIM" (full name, anySIM.app) to your /Applications Folder
3. Open Terminal (located in /Applications/Utilities) and type the following:

   ```
   scp -r /Applications/anySIM.app root@IPADDRESS:/Applications/
   ```

   - Replace the IPADDRESS with the IP address of your iPhone (you can determine your iPhone's IP Address by tapping Settings, then "Wi-Fi," —tap the arrow next to the name of the Wi-Fi network to which your iPhone and look at the IP Address)
4. Restart your iPhone
5. Run the AnySIM application to unlock your iPhone

Activate the Voicemail Button on your Unlocked iPhone

Get your carrier's voicemail number

Click on your iPhone's phone button

Then click on the Keypad tab

Add the following code: *5005*86***xxx**#

Here **xxx** would be your voicemail number

After entering the code you tap call

This results in the code being set

Tap now on the voicemail button and it should automatically call your usual voicemail service

Podloso Virus

Podloso virus is a file which can be launched and run on an iPod

It should be stressed that for the virus to function, Linux has to be installed on the iPod

After installing this virus in iPod, it installs itself to the folder which contains program demo versions

Once launched, the virus scans the device's hard disk and infects all executable .elf format files

Security Tool: Icon Lock-iT XP

Icon Lock-iT XP works with iTunes to lock and encrypt your AAC music files

Icon Lock-iT XP will work on any type of portable storage device including the 20gb hd and 40 gb hd apple ipods

Icon Lock-iT series combines compatibility with portable data storage devices and new encryption algorithms

Features:

- Lock and encrypt files and folders
- Conforms to new Advanced Encryption Standard (AES)
- iPod and Flash Drive compatibility
- Autorun feature
- Decryption functionality

Mobile: Is It a Breach to Enterprise Security?

Threats to Organizations Due to Mobile Devices

- Loss of general company data and files from these increasingly memory-laden devices
- Key sales contacts could go to a competitor

- The employee's time to recover from the loss
- The time the network administration team needs to replace the device and handle the loss
- Use of such devices as means of stealing company information. The "inside job" on data theft can be pulled off using a wide variety of mobile devices

Threats to Organizations Due to Mobile Devices (cont'd)

A lost or stolen portable device can provide hackers with multiple means to compromise internal networks and can lead to loss of market share and identity theft

Phone fraud of various types -- e.g., employees making unauthorized long-distance personal calls

Security Actions by Organizations

- Develop a comprehensive, strategic plan for mobile devices that incorporates security policies
- Companies need to define which mobile devices are allowed and under what conditions
- Companies should place limits on network and application access, and on business data storage and transfer
- Create acceptable usage policies for mobile device and proactively educate users about them
- Apply technologies that make it impossible for users or devices to break company policy
- Audit and monitor mobile device activity among employees to prove security policy compliance

Trojans and Viruses

Skulls: Trojan

- Skulls is a malicious SIS file trojan that will replace the system applications with non-functional versions
- If Skulls is installed, it will cause all application icons to be replaced with picture of skull and cross bones
- The icons do not refer to the actual applications any more, so none of the Phone System applications will start
- If Skulls is installed, only the function of calling and receiving works
- All functions which need some system application, such as SMS and MMS messaging, web browsing, and camera no longer works

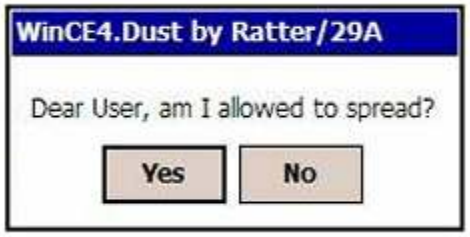
Duts: Virus

Duts is a parasitic file infector virus for the PocketPC platform

Duts is a 1520 bytes long program, hand written in assembly for the ARM processor

Duts attempts to infect all EXE files in the current directory

Duts only infects files that are bigger than 4096 bytes and have not been infected yet



Source: *http://www.f-secure.com/*

Doomboot.A: Trojan

Doomboot.A is a malicious SIS file trojan that drops corrupted system binaries and Commwarrior.B into the infected device

The Commwarrior.B dropped by Doomboot starts automatically and spreads

The system files dropped by Doomboot.A cause the device to fail in the next reboot

Bluetooth spreading of the Commwarrior.B causes battery drain

Antivirus

Kaspersky Antivirus Mobile

Kaspersky Anti-Virus Mobile protects smartphones from malicious programs that target mobile platforms

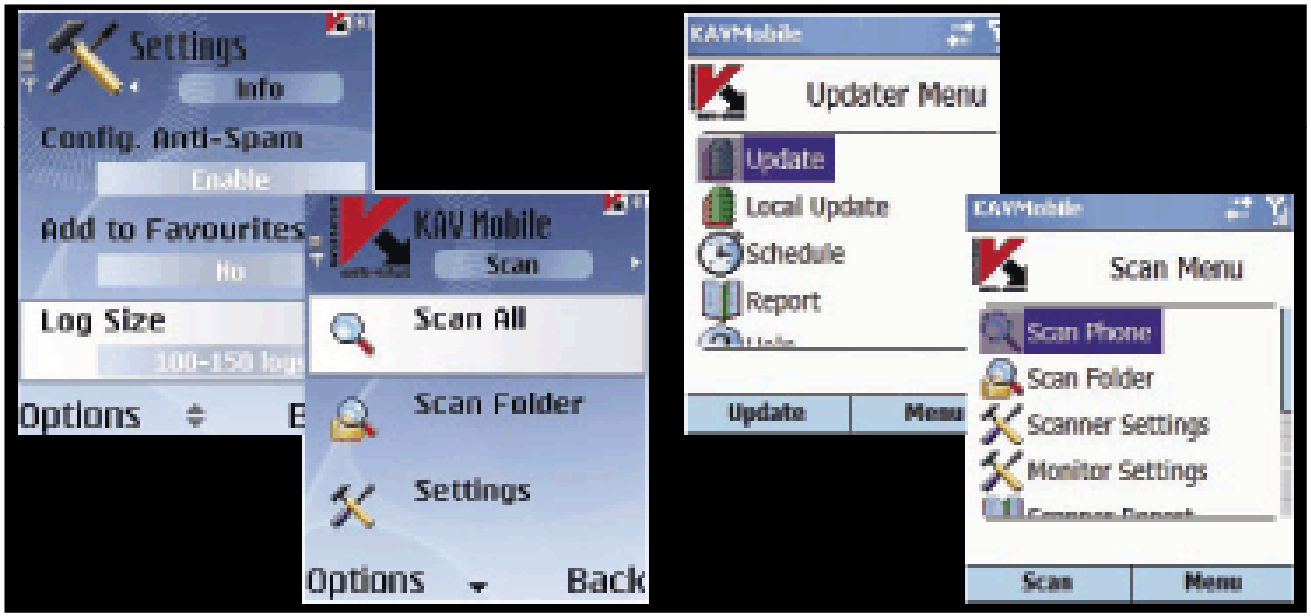
Features:

- Antivirus scanning of the smartphone's internal memory and extension cards
- Automatic scanning of all incoming or modified SMS, MMS, email items, and executable files
- On-schedule scanning

Advantages:

- Real-time antivirus scanning
- Anti-spam for SMS/EMS/MMS
- Fast and discreet performance
- Automatic database updates

Kaspersky Antivirus Mobile: Screenshot



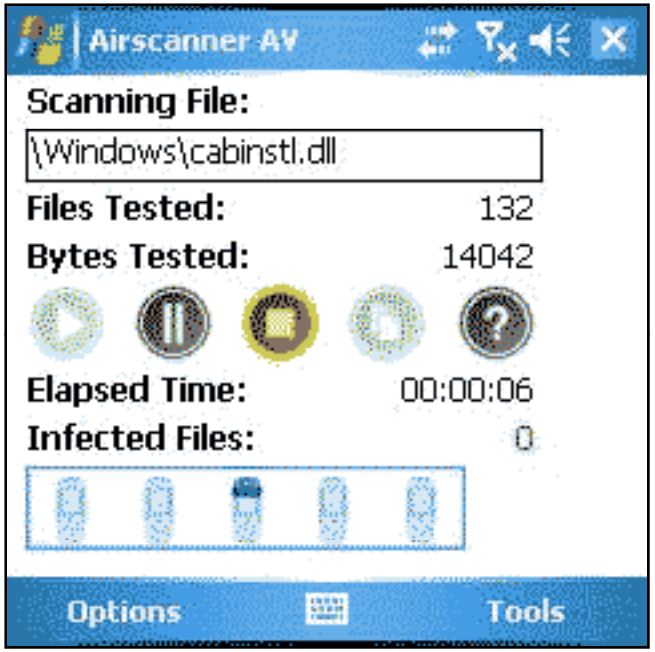
Airscanner

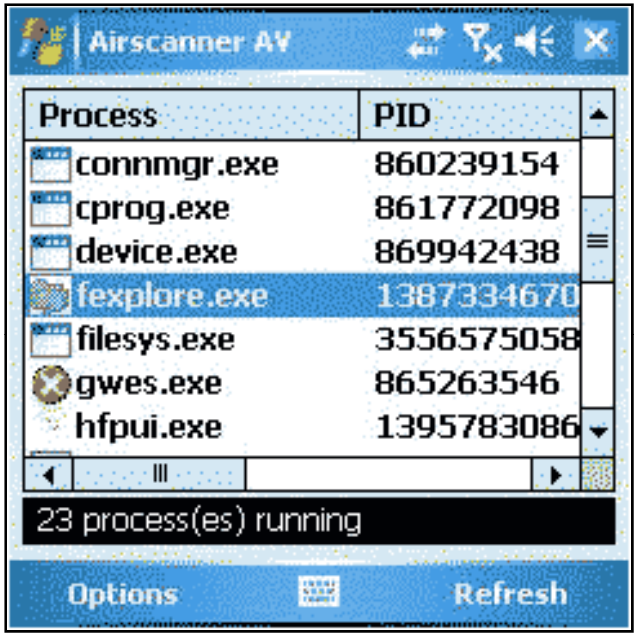
Airscanner protects your mobile device from harmful malware

Features:

- Automatic, online updates of virus signatures and scanning engine
- Fast, optimized scanning speed based on patent pending technology
- Support for Windows Mobile and Smartphone and Pocket PC

Airscanner: Screenshot





BitDefender Mobile Security

BitDefender Mobile Security provides antivirus protection for mobile devices running Symbian or Microsoft Windows Mobile

Features:

- Permanent Antivirus Protection
- On-Demand Virus Scan
- Fast updates through GPRS or via PC

BitDefender Mobile Security: Screenshot

SMobile VirusGuard

SMobile VirusGuard protects mobile devices against malware delivered via email, SMS, MMS, direct download, Bluetooth, or infrared transmission

It secures mobile devices by scanning for malicious content on-demand and on-access

Once harmful content is detected, it alerts the user and offers the option to delete the data or save it

Features:

- Fully protects your device from the latest mobile threats
- Real-time Monitor scans any file received via SMS, MMS, Bluetooth, WiFi, infrared, or desktop sync
- On-demand scans of internal memory, memory card, and/or full device
- Alerts you when infected file is auto-detected and deleted

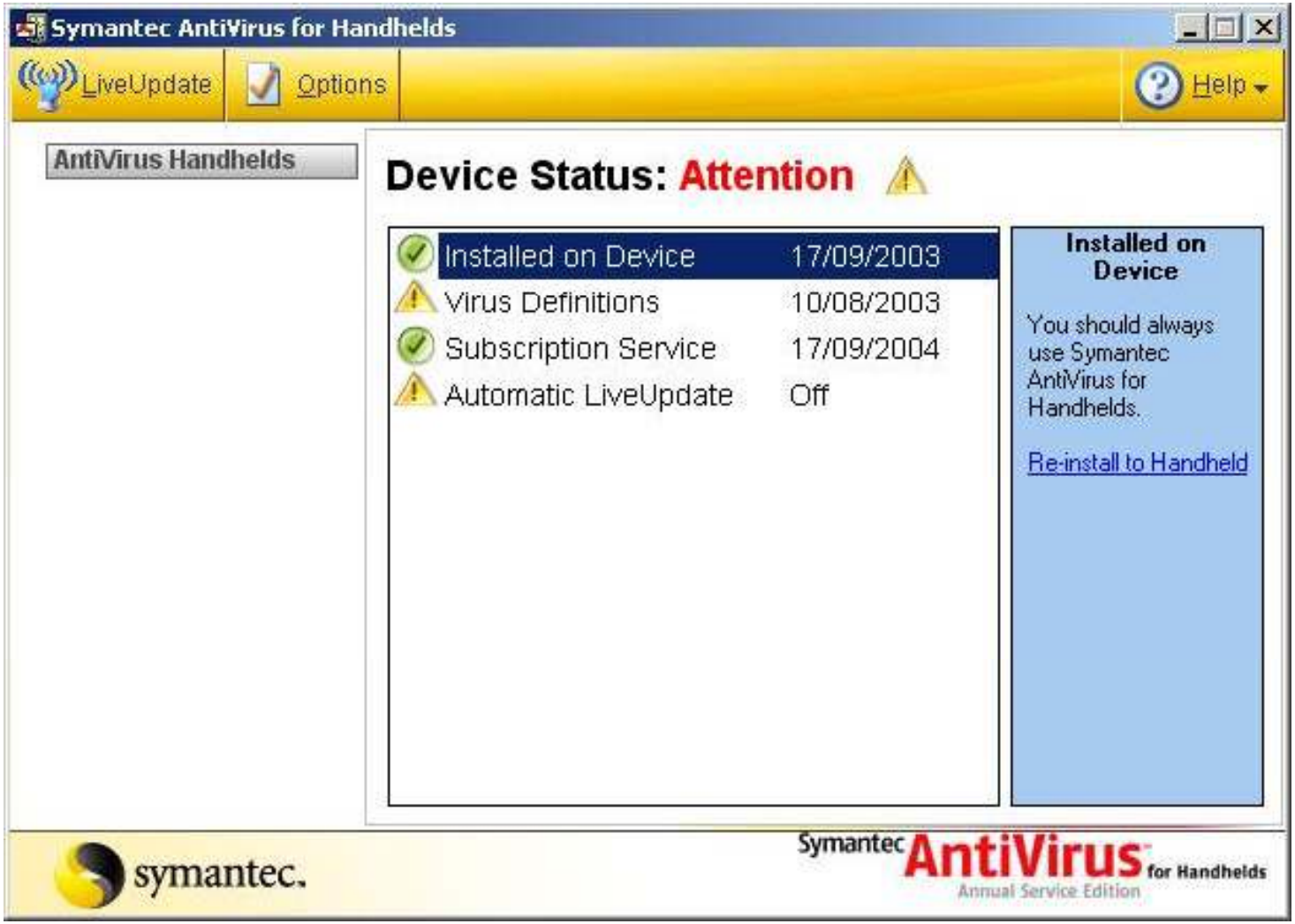
Symantec AntiVirus

Symantec AntiVirus for Handheld devices provides both real-time and on-demand scanning

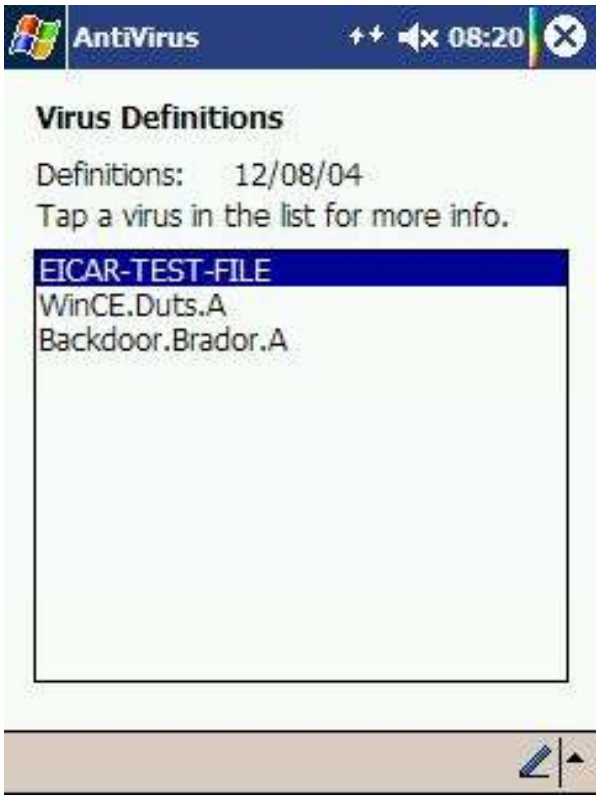
Symantec AntiVirus for Handhelds protects these handheld devices from viruses, worms, and other malicious threats

Auto-Protect scans for viruses when files are downloaded and when email attachments are received

Symantec AntiVirus: Screenshot 1



Symantec AntiVirus: Screenshot 2



F-Secure Antivirus for Palm OS

F-Secure Anti-Virus for Palm OS provides strong protection against any known malware for the Palm platform

It offers on-device protection with a continuous, fully automatic update service, and technical support

F-Secure Anti-Virus for Palm OS consists of three main components:

- The PC client is used for the automatic distribution of Anti-Virus database updates
- The anti-virus medium transfers updates from the host PC to the handheld
- The scanning application runs on the Palm OS handheld

F-Secure Antivirus for Palm OS: Screenshot

BullGuard Mobile Antivirus

http://www.bullguard.com

BullGuard protects Pocket PCs and smartphones from malicious programs that target mobile platforms

Features:

- On-Demand Scanning
- On-Access Scanning

BullGuard Mobile Antivirus: Screenshots

Security Tools

Sprite Terminator

Sprite Terminator locates and protects your mobile device information from unauthorized access in the event of theft or loss

Features:

- Locates your phone using GPS
- Lost or Stolen Phone - Remotely Lock or Wipe it
- Remote Delete – Send an SMS message to initiate thewipe operation including all external storage cards
- Remote Lock-Down – Send an SMS message to lock all functionality or re-set the device master password
- SIM Change Alert – Receive a notification SMS message if the SIM card has been changed

Sprite Terminator: Screenshot

Mobile Security Tools: Virus Scan Mobile

VirusScan Mobile is designed from the ground-up for mobile protection

It provides the protection against viruses, worms, dialers, Trojans, and battery-sapping malware

It protects against the threats originating from e-mail, instant messaging, and internet downloads

Features:

- Scans and cleans files, e-mails, Internet downloads, text messages, and attachments
- Identifies and removes viruses, Trojans, worms, and other malicious applications without interrupting your connections
- Inline cleaning automatically cleans infections when viruses, worms, Trojans, or other threats are found

Virus Scan Mobile: Screenshot

Defending Cell Phones and PDAs Against Attack

Mobile phones and PDAs are becoming more technologically advanced; attackers are finding new ways to target victims

By using text messaging or email, an attacker could lure you to a malicious site or convince you to install malicious code on your portable device

Different ways to defend cell phones and PDAs against attack:

- Take precautions to secure your cell phone and PDA
- Be careful aboutposting your cell phone number and email address
- Do not follow links sent in email or text messages
- Be wary of downloadable software
- Evaluate your security settings

Mobile Phone Security Tips

- Keep your mobile anti-virus updated
- When entering a crowded zone, make sure your Bluetooth is switched off
- Do not open untrustworthy applications
- Do not pair your device with unknown devices
- Never leave your phone unattended in public or at home
- Register 15-digit IMEI (international mobile equipment identification) number of your GSM mobile phone handset which makes it easier to deactivate the phone if it is stolen
- Lock your GSM phone to your SIM card
- Protect your mobile phone by setting up a Personal Identification Number (PIN) code

Summary

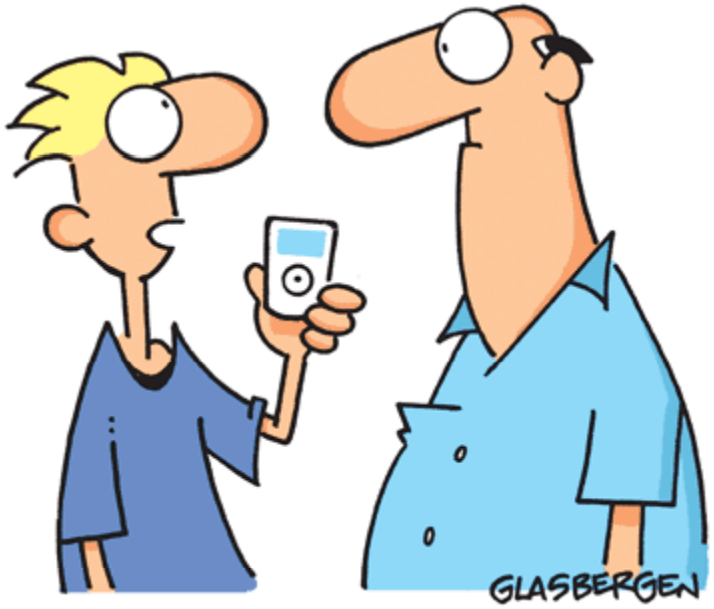
With mobile hacking, hackers can steal your information, rob your money and insert malicious code

Blackjacking means use the BlackBerry environment to circumvent perimeter defenses and attack hosts on enterprise networks

iPod's large capacity and ability to connect easily to a computer and transfer data rapidly via USB makes it potentially more useful in information theft

AppSnapp is a process for jailbreaking and allowing the installation of non-sanctioned third-party applications to the iPhone

Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as PDA and mobile phones



"THERE'S NOTHING WRONG WITH YOUR IPOD, DAD. IT'S JUST TOO EMBARRASSED TO PLAY THE KIND OF MUSIC YOU LIKE!"

"It's just like a Blackberry, but a lot cheaper. It's a Dingleberry!"

"You're allowed up to 5 cell phones on your family calling plan. Where's mine?"

"Originally, P.D.A. stood for 'pretty darned amazing' ...but that didn't sound high-tech enough."