

Smart Phones as an Attack Vector

Problems and Practical Solutions

Tom Roberts

Technical Specialist

Mobile: 07730 530446

e-mail: tom.roberts@ngssecure.com

NGS Secure, Manchester Technology Centre, Oxford Road, Manchester M1 7EF www.ngssecure.com



Old vs. New

- Old phones were JUST phones
- New Smart phones are basically hand held computers.
- Ever increasing RAM, CPU speeds and Functionality.
- Open source means massive expansion in apps available for little or no cost.

Who would use these?

- Corporate espionage – Why innovate when you can appropriate?
- Disgruntled employees – Going e-postal
- Hacktivists – Their cause is your cause for concern
- Hackers/Crackers – See online EVE (mmorpg) to see how far they will go.
- Inadvertent – Because “smart phones” don’t have to have smart owners
- Journalists
- Organised Crime
- Disgruntled spouses
- Etc. Etc. Etc.

- Last but not least – Unknown “side effects” of installed applications

Corporate Espionage

- March 2010 report commissioned by Microsoft/RSA shows:
 - **Secrets comprise two-thirds of the value of firms' information portfolios. – “Secrets are targets for theft”**
 - **Compliance, not security, drives security budgets. – Missing the elephant in the room?**
 - **Firms focus on preventing accidents, but theft is where the money is. – “Hundreds of thousands vs. tens of thousands.”**
 - **The more valuable a firm's information, the more incidents it will have. – The bigger they are the harder they will be hit**
 - **CISOs do not know how effective their security controls actually are. – “Most enterprises do not actually know whether their data security programs work or not.”**

“Insider Theft Of Secrets And Other Unstructured Documents Was The Most Costly Type Of Incident”

See: http://www.rsa.com/products/DLP/ar/10844_5415_The_Value_of_Corporate_Secrets.pdf

Types of Attack

- Bugs
- Trackers
- Spycams
- Scanners
- Tethering
- Storage
- Injectors/Rootkits
- Purpose built devices
- Concept exploits

This list is just a sample!

Bugs

Bugs come in many varieties

- Remote listening
 - Listen to calls
 - Turn on microphone
- Get location of phone
- Remote camera operation

- Often sold as spouse detectors or child monitors

Example Bug Software - £1

- Available from the market
- Inexpensive
- Easy to use and deploy
- Can be installed on a phone in under 30 seconds



Bugs in Action

FBI taps cell phone mic as eavesdropping tool



cnet The FBI appears to have begun using a novel form of electronic surveillance in criminal investigations: remotely activating a mobile phone's microphone and using it to eavesdrop on nearby conversations.

The technique is called a "roving bug," and was approved by top U.S. Department of Justice officials for use against members of a New York organized crime family who were wary of conventional surveillance techniques such as tailing a suspect or wiretapping him.

Nextel cell phones owned by two alleged mobsters, John Ardito and his attorney Peter Peluso, were used by the FBI to listen in on nearby conversations. The FBI views Ardito as one of the most powerful men in the Genovese family, a major part of the national Mafia.

The surveillance technique came to light in [an opinion](#) published this week by U.S. District Judge Lewis Kaplan. He ruled that the "roving bug" was legal because federal [wiretapping law](#) is broad enough to permit eavesdropping even of conversations that take place near a suspect's cell phone.

Kaplan's opinion said that the eavesdropping technique "functioned whether the phone was powered on or off." Some handsets can't be fully powered down without removing the battery; for instance, some Nokia models will wake up when turned off if an alarm is set.

The U.S. Commerce Department's security office [warns](#) that "a cellular telephone can be turned into a microphone and transmitter for the purpose of listening to conversations in the vicinity of the phone." An [article](#) in the *Financial Times* last year said mobile providers can "remotely install a piece of software on to any handset, without the owner's knowledge, which will activate the microphone even when its owner is not making a call.

More...

p.s., "If a phone has in fact been modified to act as a bug, the only way to counteract that is to either have a bugsweeper follow you around 24-7, which is not practical, or to peel the battery off the phone," Atkinson said. Security-conscious corporate executives routinely remove the batteries from their cell phones, he added.

Posted by J.D. LeaSure, President / CEO ComSec LLC at 1:34 PM



Trackers

- No longer need GPS
- Can be installed on phone
- Remote sites allow service to track any number
- Accurate to 10 meters (best)
- Google's latitude a good example

- Often sold as anti theft software or "Find your phone" or used by "worried parents"

Sample Tracker Site

The screenshot shows a website for 'mobile Tracking' with a red and orange color scheme. At the top left is the logo, and at the top right are language options (English, Español, Italiano, Deutsch) and a login form with a 'Login' button. A navigation menu includes 'Home', 'Services', 'Downloads', 'About Us', and 'Contact Us'. A 'Join now!' link is also present. The main content area features the heading 'Track Your Mobile' and a list of target groups: 'Employees', 'Kids', and 'Mobile Work force'. A 'FREE DEMO!' button is prominently displayed. To the right is an image of a Nokia mobile phone showing a map with a red location pin. Below this are three columns: 'ABOUT US' (describing UK's leading software and SOS solutions), 'DOWNLOADS' (listing 'Footprint Lite' and 'Lifeassist Mobile Tracker'), and 'SERVICES' (describing standard mobile phone tracking). Each column has a 'more' link. The footer contains site navigation, copyright information (© 2009 Track And Locate), and the website designer's name (Web Design Sydney).

mobile Tracking

English | Español | Italiano | Deutsch

Login Id [Login](#)

[Home](#) [Services](#) [Downloads](#) [About Us](#) [Contact Us](#)

[Join now!](#) | Lost your password?

Track Your Mobile

- ▶ Employees
- ▶ Kids
- ▶ Mobile Work force

[FREE DEMO!](#)

ABOUT US

UK's leading MobileTracking software and SOS Man Down solutions.

- ▶ Emerging capability in spatial intelligence
- ▶ Globally competitive, locally operated.

[more](#)

DOWNLOADS

Download and install Mobile Tracker on your compatible GPS-enabled mobile device.

- ▶ Footprint Lite.
- ▶ Lifeassist Mobile Tracker.

[more](#)

SERVICES

Mobile Tracking has a standard Mobile Phone Tracking

- ▶ Footprint Lite.
- ▶ Lifeassist Mobile Tracker.

[more](#)

Home | Company | Contact Us | Services | Downloads | Sitemap | Privacy Policy

Website Designed by: Web Design Sydney

Copyright © 2009 Track And Locate. All Right Reserved. | SEO

Trackers (reverse lookup) Continued

International Phone Number Reversal

ANY COUNTRY

PayPal is the secure payment processor for your seller, Investigative Resources LLC
Cell Phone & Landline Phone Traces for the UK, *All international phone number reverse searches* USA & Canada fee is only 75\$ (see above)

100% guarantee again - no info - no fee.
Or you may order by check or money order to:
Investigative Resources
PO Box 1456
International Falls, MN 56649

Fee is \$250.00 US\$ 79.00 for USA and Canadian numbers (see above)

You Supply: The ENTIRE Phone Number (all pre-fixes, etc...) and the Country if you know it. It can be a Landline phone number or a Cellular Phone number

We Return: The Name, address, date service was established, account number as well as the ID info on file.

Click the button to pay:

Buy Now

Search Details: Cost of Search: \$250.00

Please allow up to 10 business days (normally 5 business days) to complete Search

Accuracy GUARANTEED

No hit - no fee..

- <http://www.unlisted-etcetera.com/?hop=mpndotcom.privateeye#international>

- Silent Cameras
 - Used by pin stealers and perverts.
 - High resolution means useful up to 10 feet away (or further)
- Motion Sensor cameras
 - Sold as security devices
 - Can send pictures remotely

Motion Detector Software

» Motion Detector



Rating: 4.0/5
(2 votes cast)

• **Summary:** Motion Detector is a program that allows you to use your Android device as an alarm, spycam or motion sensor.

• **Updated:** Mar 3, 2010 **Developer:** MVA

• **Tags:** [tools](#), [camera](#), [Motion Detector](#), [alarm](#), [spycam](#), [sensor](#)

• **Requirements:** Android Phone

Motion Detector is a program that allows you to use your Android device as an alarm, spycam or motion sensor. The program uses the built-in camera as a sensor and if it detects a movement in the surrounding area, it sends an email or a text message with a picture link to another cell phone.

New features:

You can now start and stop the alarm remotely using text messages. Simply write "Alarm start" to start the alarm, and write "Alarm stop" to stop the alarm.

Motion Detector Screenshots



[Android Freeware on Facebook](#)

 **Do You develop for Android?**
[submit your free software here](#)

 **Hot Android Topics** rss
articles, reviews, tips & tricks

» **Popular Tags:** [tips](#), [reviews](#), [software](#), [games](#), [android](#), [HTC](#)

» **Recent Posts**

- [Skyfire Browser Heading to Android Smartphone Soon](#)
- [LG to Launch C710 Aloha Android Smartphone](#)
- [Motorola Titanium XT800 Android Phone Coming to Korea](#)
- [HTC Releases EVO 4G Video](#)
- [Firefox Mobile - Fennec available for download on Androids](#)
- [Motorola Milestone Gets the Android 2.1 Treatment](#)
- [Sony Ericsson Xperia X10 Plagued by Multitouch Issues?](#)
- [AT&T Not to Allow Unsigned Apps on the Dell Aero Android Smartphone](#)

» **Recent Software**

- [OnTrack Diabetes](#)
- [Gate Blaze](#)
- Nihroid

Spying made easy

FLEXISPY
Protect Your Children | Catch Cheating Spouses

Home | Features | Phones | Demo | Support | Community | Reseller | Affiliates | About Us | Cart

FlexiSPY America

Blackberry [Start here](#)
Nokia [Start here](#)
Win Mobile [Start here](#)
iPhone [Start here](#)
Android [Start here](#)

FLEXISPY - PRO-X

PRO-X | FULL DETAILS | Supported Phones

TOP OF THE RANGE SPYPHONE

- Listen to actual phone calls
- Use as a secret mobile gps tracker
- Includes all PRO features
- Change phones as often as you like
- Symbian, Windows Mobile & BlackBerry

ORDER NOW: €250.0 (per year)

[LEARN ABOUT SPYPHONE FEATURES HERE](#) [Buy Now](#)

FLEXISPY iPhone

iPhone | FULL DETAILS

Worlds Most powerful iPhone spy phone

- Secretly read SMS, Email, Call Logs
- Track location on map
- Make secret spy calls
- BASIC version from \$ 39.99

ORDER NOW: €250.0 (per year)

[Buy Now](#)

FlexiSPY Android Community Edition

FREE Android Spy Phone software lets you secretly read Call Records, SMS Messages and GPS locations

ready to get started?
FREE DOWNLOAD

Visit the new Flexispy Forum

TWITTER DO YOU FOLLOW ME?

FlexiSPY - PROX

- Top of the range spyphone
- Mobile Call Tapping, listen to actual phone calls
- Spyphone to bug a room or person
- Remote Listening
- Read all incoming and outgoing SMS
- Read all Call logs
- Know the location, Location tracking
- SIM Change SMS Notification
- 10 Day 100% money Back Guarantee
- AVAILABLE FOR THE PHONES BELOW

+ **symbian**

+ **symbian 9**

+ **Windows Mobile**

+ **BlackBerry**

Spying made easy

	Mobile-Spy	SpyBubble	E-Stealth	BIG daddy SPY
Data Monitoring				
SMS	✓	✓	✓	✓
Call History	✓	✓	✓	✓
Address Book	✗	✓	✓	✓
Email	✗	✓	✓	✓
Eavesdropping (found ONLY in Flyware)				
Call Interception	✗	✗	✗	✓
Remotely Activate Microphone	✗	✗	✗	✓
Location Tracking				
Location GPS	✓	✓	✗	✓
View On Map	✓	✓	✗	✓
Real-Time Tracking	✗	✓	✗	✓
Historical Tracking	✗	✓	✗	✓
Cell ID Tracking	✗	✓	✗	✓
Reporting				
Free Form Query	✗	✓	✗	✓
PDF	✓	✓	✗	✓
XML	✓	✓	✗	✓
RTF	✗	✓	✗	✓
CSV	✓	✗	✗	✓
Security				
Undetectable	✗	✗	✓	✓
SIM Change Alert	✗	✗	✗	✓
Works Even If SIM Changed	✗	✓	✓	✓
Password Change Notification	✗	✗	✗	✓
Install Direct From Internet	✓	✓	✗	✓
Remote Control				
Remote Control Utility	✗	✓	✓	✓
GUI setting screen	✗	✓	✓	✓
Remote Uninstall	✗	✓	✓	✓
Remote Stop/Start	✗	✓	✓	✓
SMS	✗	✗	✗	✓
GPRS	✓	✓	✓	✓
Email Relay	✗	✓	✓	✓
Compatible Platforms				
Symbian 8	✗	✓	✓	✓
Symbian 9	✓	✓	✓	✓
iPhone	✓	✓	✗	✓
Windows Mobile	✓	✓	✓	✓
Blackberry	✗	✓	✗	✓
Android	✓	✗	✗	✓

Scanners

- Port scanners
 - TCP – easy
 - UDP – requires “root”
 - IP
 - URL
 - Code easy to download and modify
- Nmap already available for smartphones

Scanners – Examples



any use to you. Do you remember in the Matrix 2 when Trinity had to do some hacking to get into a building? She uses a port scanner to get started.

Port Scandroid is based on JMap by Tom Salmon.

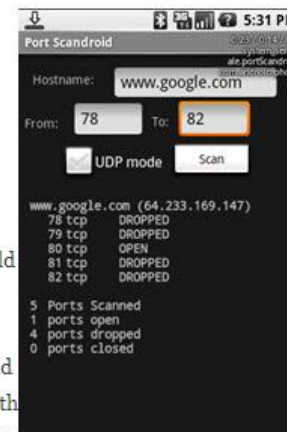
I learned some interesting stuff about programming for mobile devices and about 3G networks doing this project.

Lessons learned (in no particular order):

- **Check the quality of the code you are porting before you begin porting it.**

If I had to do this again, I wouldn't have ported JMap. It just isn't very high quality code. I should have *analyzed* the way the code solves the problem and rewritten it. That way, I could ensure that the code was high quality, and I could also have avoided all of the hackery involved with moving from pure Java to the android application space.

- **3G data networks aren't quite what they seem**



Tethering

- Allows internet “anywhere”
- Bypasses network firewalls
- Creates “backdoors” into networks
- Sold as “convenience device” or “free internet”

Tethering – How to

How to tether the iPhone

Updated: October 26, 2009

Page 1 of 3

[Discussion?](#)

Note: This will be the last ever update to this tutorial. Why? As of November 2009 I have cancelled my AT&T iPhone contract, because I can't afford it any more. I know it sounds ridiculous, but it's absolutely true. This decision will also affect other tutorials like this that are unique to having AT&T service.

Tethering is using your iPhone's EDGE or 3G Internet access to allow your computer to access the Internet when no Wi-Fi is available.

Be warned! This hack may violate your AT&T Terms of Service for your contract. Please check before attempting this procedure.

The question that arises when people hear about this hack is, how does AT&T know you are tethering? AT&T can tell by examining the packets transferred through the iPhone. They can determine how the header is assembled, and they also note sustained data transfers and connections to chat servers as dead giveaways.

There are three pages to this tutorial. Page 1 is for those on 3.1.2 firmware and who want to use a USB connection to tether with. [Page 2](#) is for those on 3.0.1 or lower firmware who want to use a USB connection to tether with. Page 3 is for everyone that wants to use BlueTooth to tether with.

Tethering – WiFi Access point

Use your Windows Mobile smartphone as a Wi-Fi access point

Date: February 9th, 2010

Author: Paul Mah

Category: Smartphones, Wi-Fi

Tags: Microsoft Windows Mobile, Mobile, Associated Press, Wi-Fi Access Point, Smart Phone, Microsoft Windows, Symbian Inc., Access Point, Paul Mah, WMWiFiRouter



Paul Mah explains how you can use the WMWiFiRouter application to turn your Windows Mobile smartphone into an Internet access point.

One method of accessing the Internet on-the-go is to make use of free or pre-paid Wi-Fi access points (APs), which you can find practically anywhere. Unfortunately, the access speeds at Wi-Fi APs can vary greatly, and it is not uncommon to come across Wi-Fi APs that do not work at all.

A more robust solution is make use of 3G wireless data or mobile broadband. Unless you already have a laptop that has this capability built-in, you'll need to get a data modem or make use of smartphone tethering. Another option is to use your smartphone as a dedicated Wi-Fi AP.

One key advantage of having a Wi-Fi AP is that more than one user can make use of the Internet at the same time. Implementing such functionality on the hardware front is the MiFi modem. But getting a MiFi personal hotspot entails purchasing the hardware and will likely require signing up for a separate mobile plan.

Fortunately, Windows Mobile and Symbian smartphone users have software options to

Sponsored Links

▶ [BlackBerry® Curve™ 8520](#)

Keep Up With What Is Important In Your Life With The BlackBerry Curve
www.blackberry.com

▶ [Vodafone™ Official Site](#)

Checkout Our Latest Range Of Smartphones. From Only £20/Month!
vodafone.co.uk

▶ [ACT for Mobile Devices](#)

ACT on Bberry or Pocket PC Synchronize or Wireless
www.camenoco.uk

ADVERTISEMENT

Microsoft Unified Communications

Check out how UC can help save businesses money.

Because it's everybody's business

White Papers, Webcasts, and Downloads

[Sanity Saves for IT Executives](#)
Five signs that you aren't cut out to be a CIO

[Five signs that you aren't cut out to be a CIO](#)



[Leadership vs. management; Understand the differences](#)



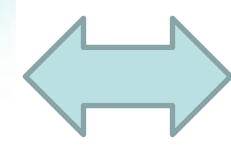
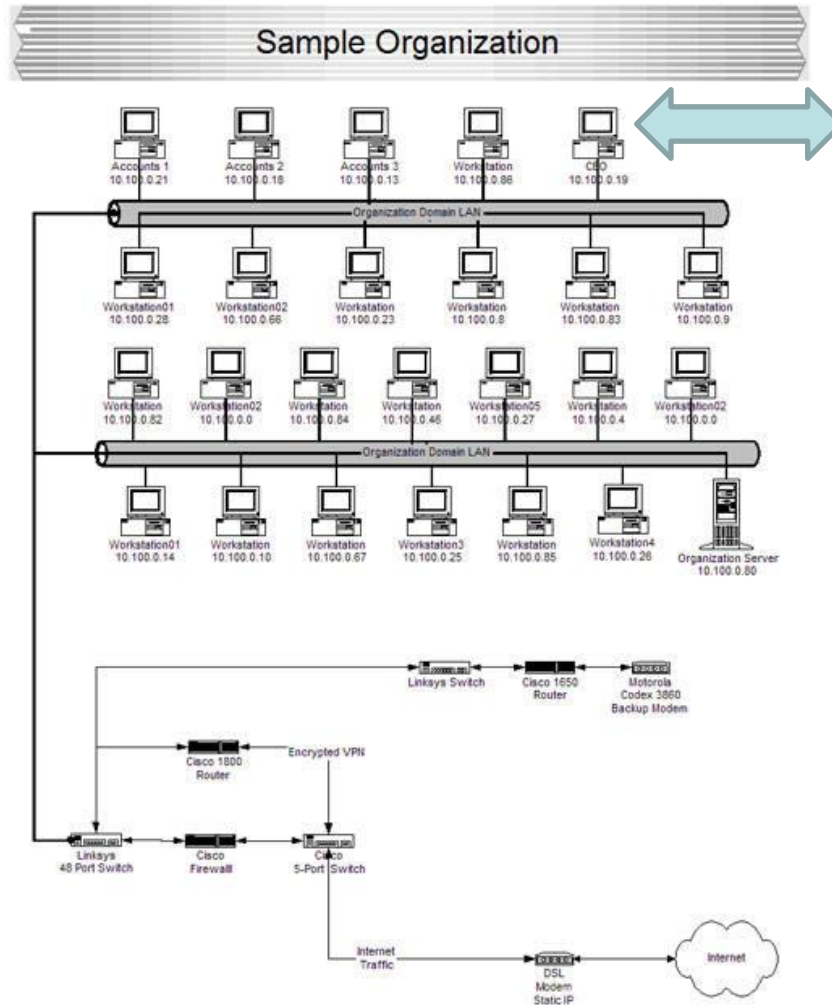
[Five ways to lead your team to peak performance](#)



[The five most lucrative certifications for IT leaders](#)



Tethering as a backdoor



Storage

- Phone storage now capable of 32GB
- 128GB available soon (Sandisk claim 2011 release)
- Can easily be converted/used as removable device
- Often overlooked for blacklisting
- Fast speeds make offload easy
- Small and virtually undetectable

Injectors/Rootkits

- Phone O/S may not be affected (Linux)
- Examples already found in the wild
- Phone security software may not detect
- Phones act as “carriers”
- Users may not be aware
- Can come as part of desired software
- Zombies, key loggers, password harvesters, the possibilities are endless.

Malware in the wild

CyberInsecure.com

Daily Cyber Threats And Internet Security News: Network Security, Online Safety And Latest Security Alerts

HOME ARCHIVES CONTACT ABOUT EMAIL SUBSCRIBE ADVERTISE

Search

March 9th, 2010

Vodafone Shipped Malware Infected HTC Magic Smartphones

Vodafone has been blamed for shipping Mariposa botnet malware and other nasties on a HTC Magic Android smartphones it supplied.

The mobile phone giant's Spanish arm supplied an HTC Magic smartphone preloaded with malware that attempted to establish a backdoor for stealing information on connected PCs during the synchronisation process. Vodafone acknowledged the problem but said that the incident was an isolated and local problem, which came to light because the customer affected works for Spanish anti-virus firm Panda Security.

The extra code was a strain of the Mariposa bot client that attempted to connect to systems not associated with the recent arrests of three suspected botmasters in Spain, according to an analysis of the attack by Panda Security researcher Pedro Bustamante.

"A quick analysis of the malware reveals that it is in fact a Mariposa bot client," Bustamante explained. "This one, unlike the one announced last week which was run by Spanish hacker group 'DDP Team', is run by some guy named 'tnls' as the botnet-control mechanism shows.

"Once infected you can see the malware 'phoning home' to receive further instructions, probably to steal all of the user's credentials and send them to the malware writer," he added.

The same mobile phone was also infected by Confiker and a Lineage password-stealing code, according to Panda. The incident came to light

Categories

- ▶ Adobe (25)
- ▶ Apple (48)
- ▶ BitTorrent (15)
- ▶ Botnets (36)
- ▶ Breaches And Incidents (188)
- ▶ Cryptography (8)
- ▶ Cybercrime (89)
- ▶ Data Theft (185)
- ▶ DDoS (26)
- ▶ Google (64)
- ▶ Hacked (130)
- ▶ Hardware (58)
- ▶ Malware (203)
- ▶ Mass Web Attacks (55)
- ▶ Microsoft (89)
- ▶ Mobile (35)
- ▶ Offline (15)
- ▶ Phishing (45)
- ▶ Privacy (185)
- ▶ Scams (76)
- ▶ Social Networks (34)
- ▶ Software (222)
- ▶ Spam (108)
- ▶ SQL Injections (33)

Red Mail 
Send us latest news and alerts

Internet Threat Level



Symantec ThreatCon
Threat Level Definitions

 Suspicious
Domain Check

 Free
Anti-virus tools
And Rescue CDs

Latest News Updates

emergency IE patch. The cumulative update (MS10-018) also fixes nine other security bugs and all versions of IE from 5.01 to 8.0 need patching.

Rootkits - Example

Researchers: Rootkits Work Nicely On Smartphones, Thank You

Rootkit-based exploits could include eavesdropping, user locator, Rutgers study finds

Feb 23, 2010 | 05:15 PM

By Tim Wilson
DarkReading

Computer scientists at Rutgers University this week are demonstrating ways that rootkits can attack new generations of smart mobile phones.

The researchers, [who are presenting their findings at a mobile computing workshop in Maryland](#), are showing how a rootkit could cause a smartphone to eavesdrop on a meeting, track its owner's travels, or rapidly drain its battery to render the phone useless -- all without the user's knowledge.

"Smartphones are essentially becoming regular computers," says Vinod Ganapathy, assistant professor of computer science in Rutgers' School of Arts and Sciences. "They run the same class of operating systems as desktop and laptop computers, so they are just as vulnerable to attack by [malware]."

Ganapathy and computer science professor Liviu Iftode worked with three students to study the use of rootkits in smartphone operating systems. They note that while many PCs carry virtual machine monitors to help detect rootkits, most smartphones cannot support a VM monitor.

Rootkit attacks on smartphones -- or upcoming tablet computers -- could be more devastating because smartphone owners tend to carry their phones with them all of the time, the researchers say. This creates opportunities for potential attackers to eavesdrop, extract personal information from phone directories, or just pinpoint a user's whereabouts by querying the phone's GPS receiver.

Purpose built devices

- New devices mean phones can be crafted to any purpose
- Open source allows rapid development
- New CPU and internal memory makes these (in effect) hand held computers
- Backtrack already ported to one of these devices
- Hardware specialists no longer required
- Examples available on YouTube

Purpose built devices - Example



Unleash Yourself

Introducing the Neo FreeRunner

- Free and Open Source Code
- Free and Open Wifi
- Unleash Your Creativity

[BUY IT NOW](#)

DBoard



Open It Up. Get access to the

Accessories



Not enough? Get Spares Pack

Purpose built devices – Anything is possible

- Gumstix + Flow = whatever you want.



Concept exploits – the future or already here?

- Phones come equipped with ability to read RFID signals
 - Could be used to clone and replay ID cards – hidden scanner?
 - Contactless smart card readers?
 - Warbumping or contactless pick pocketing
- Smart Phone Botnets (Photnets) – Already Proven
 - With almost no adequate prevention spread could be rapid.
- Phones now already equipped with biometric scanners
 - Biometrics recorders?

Prevention

- Awareness/Policy
 - “Time and Place” usage on both corporate AND personal phones
 - Consistency of phone type usage across deployment
 - Clear and unambiguous statements on allowed downloads and usage
- Outright ban
 - Harsh – but in some environments your only course
 - Corporate = yes, personal = no
 - Alternative to deploy “anti signal” devices
- Audit
 - Software – good for corporate solutions
 - Legal ambiguity about ability to audit personal devices

5 Ways To Detect Mobile Phone Surveillance Software

- **#1) Has someone recently asked to borrow your cell phone?** Much of the cell phone surveillance software that is purchased online requires a person to get physical access to your cell phone. Common tricks people will do in order to gain access to your cell phone in order to install mobile eavesdropping software is to ask if they can borrow your phone to download a game or ringtone for you, use your phone because their "battery" is out, and to play a favorite game on your phone. All of these activities will enable them to get access to your web browser which is all they need to download mobile eavesdropping software and install it on your phone.
- **#2) Have you noticed an unusual increase in your data plan charges?** Another sign that you might have mobile phone surveillance software installed is if you notice an unusual spike in your data usage fees. Mobile phone surveillance software such as [Flexispy](#) & [MobiStealth](#) use 3G, GPRS, or EDGE to transfer the data collected from your cell phone, which means if you are not the type who uses your cell phone to browse the web or download apps, an unusual spike in data traffic is a good indicator that you have mobile phone surveillance software on your phone.
- **#3) How long does your battery last?** Is your BlackBerry's battery life suddenly a lot shorter than the usual amount of hours? Depending on the type of cell phone surveillance software installed, your cell phone might experience a considerable amount of abnormal battery drain. This is because the spy app runs continuously in the background, thus requiring more than usual battery use.
- **#4) Do You See Quick Flashes?** Does your cell phone 'lights up' for no reason but doesn't ring. Mobile eavesdropping software that have remote monitoring features (spy call) enable someone to secretly listen to your cell phone and listen to your immediate surroundings. When a spy call is made, the cell phone may briefly light up for a split second. This doesn't happen all the time, but it does happen on certain handsets.
- **#5) Do You Hear An Echo?** When mobile phone surveillance software is installed on your phone, you might occasionally hear a very small noise or click when someone is attempting to tap into your call and listen in on your conversation. Sometimes it's hard to tell with background noise in general, but if you do notice an occasional clicking noise when calling a certain number, it probably means you have surveillance software on your phone.

Thank You – Questions?

“Technology makes it possible for people to gain control over everything except over technology.”

John Tudor

“Technology is so much fun but we can drown in our technology. The fog of information can drive out knowledge.”

Daniel J Boorstin

“Security without awareness, is useless.”

Tom Roberts