Smartphone Hacks and Attacks:
A Demonstration of Current Threats to Mobile Devices

Daniel V. Hoffman, CISSP, CEH, CHFI
Chief Technology Officer

Global Threat Center

Exploit Research and Development

- Complete threat analysis against all exploit vectors
- Continual assessment of new devices and platforms
- Knowledge-share with worldwide device exploit network

Malware Operation Center

- Actively monitor SMobile customer Malware alerts, reporting and trending
- Monitor and scan publicly submitted Malware samples
- Scan partner feeds for discovered/ recent viruses, Spyware, etc.
- Continually monitor underground and public Malware bulletin boards, websites, newsgroups, etc.

Copyright 2008 SMobile Systems

Smartphone Platforms

- Symbian
- BlackBerry
- Windows Mobile
- iPhone
- Android

Copyright 2008 SMobile Systems

Why Does Smartphone Security Matter?

- Smartphones are rapidly replacing feature phones. Analyst predictions state that by 2012, 65% of all cell phone sales will be smartphones

- Cell phones are used for the same functions and have the same capabilities as PCs

- While most PCs have at least some security software in place, smartphones commonly do not have any security software installed

Copyright 2008 SMobile Systems

Why Does Smartphone Security Matter?

Would you conduct mobile banking and online purchases using a PC that didn't have antivirus software installed?

Are you willing to no longer require antivirus, firewall, encryption and VPN software on your enterprise workstations?

Copyright 2008 SMobile Systems

Why Does Smartphone Security Matter?

Smartphones are the new PCs for consumers

Smartphones are the new workstations for workers

Smartphones are susceptible to the exact same threats as PCs

Copyright 2008 SMobile Systems

Mobile Security Threat Environment

Threats to Mobility

- **Malware** – Viruses, Worms, Trojans, Spyware
- **Direct Attack** – Attacking device interfaces, browser exploits, etc.
- **Physical Compromise** – Accessing sensitive data
- **Data Communication Interception** – Sniffing data as it is transmitted and received
- **Authentication/Identity Spoofing and Sniffing** – Accessing resources with a user's identity or credentials
- **Exploitation and Misconduct** – Online predators, pornography, inappropriate communications

Copyright 2008 SMobile Systems

Mobile Security in the News

Mobile & Wireless

Google Scrambles to Patch Buffer Overrun Exploit in Android G1

By Clint Boulton
2008-10-27

Article Views: 10913
Article Rating: ★★★★☆ / 4

Table of Contents:

Google Scrambles to Patch Buffer Overrun Exploit in Android G1
(Page 1 of 2)

Security expert Charlie Miller leverages a flaw within an SDK component of Google's open-source Android operating system. The buffer overrun flaw lets hackers hijack the Web browser on a user's T-Mobile G1 smart phone, which is Google's first big entry into the mobile and wireless game to deliver users mobile Web services. Miller bought a G1 early from a T-Mobile employee on eBay to test his exploit. Google said it is working with T-Mobile on delivering a fix to the device.

The T-Mobile G1 smart phone has not even been on the market for one week, but a security expert has already found a significant flaw in the Google Android software that fuels it.

Rate This Article:

Poor ○ ○ ○ ○ ◉ Best
Rate

Add This Article To:

Digg this | Furl
Del.icio.us | Google
Slashdot | Simpy
Y! My Web | Spurl!
E-mail | PDF Version
Print

Copyright 2008 SMobile Systems

Mobile Security in the News

FOXNEWS.COM HOME > SCITECH

Experts: Zombie Cell-Phone Hack Attacks May Be Next

Thursday, October 16, 2008

Associated Press

E-Mail | Print

Share:

AP

Some of the most vicious Internet predators are hackers who infect thousands of PCs with special viruses and lash the machines together into "botnets" to pump out spam or attack other computers.

Now security researchers say cell phones, and not just PCs, are the next likely conscripts into the automated armies.

The mobile phone as zombie computer is one possibility envisioned by security researchers from Georgia Tech in a new report coming out Wednesday.

Copyright 2008 SMobile Systems

Mobile Security in the News

ITBUSINESSEDGE
YOUR TECHNOLOGY INTELLIGENCE AGENT

JUMP TO PRIORITY:
Choose your priority

:: Network Sentry ::

Securing your data and network, inside and outside the perimeter

Mobile Security: Still Crazy After All These Years

Posted by Carl Weinschenk on October 30, 2008 at 1:04 pm

The definition of insanity – at least in popular culture – is doing the same thing repeatedly and expecting a different result. By this definition, many business people and IT

"A quarter of lawyers put confidential documents on mobile devices ... the preferred device for storing data is the BlackBerry, followed by laptops, USB/memory sticks, smartphones, MP3/tablets or a combination of all of these"

SMOBILE SYSTEMS

Copyright 2008 SMobile Systems

Can You Name the Last 5 Widely Reported Global PC Viruses?

Much of the media has been saying they haven't seen widespread evidence of smartphone infections without mentioning that most devices don't possess any mechanisms to track infections or to report attacks. They also don't mention that today's Malware is specifically written to be stealthy, financially motivated, undetectable and targeted – not widespread and obvious.

These critical omissions are used as a basis to downplay the need for smartphone antivirus.

Copyright 2008 SMobile Systems

And Malware isn't the only way to exploit a mobile device

Copyright 2008 SMobile Systems

Let’s get specific as to what’s happening today

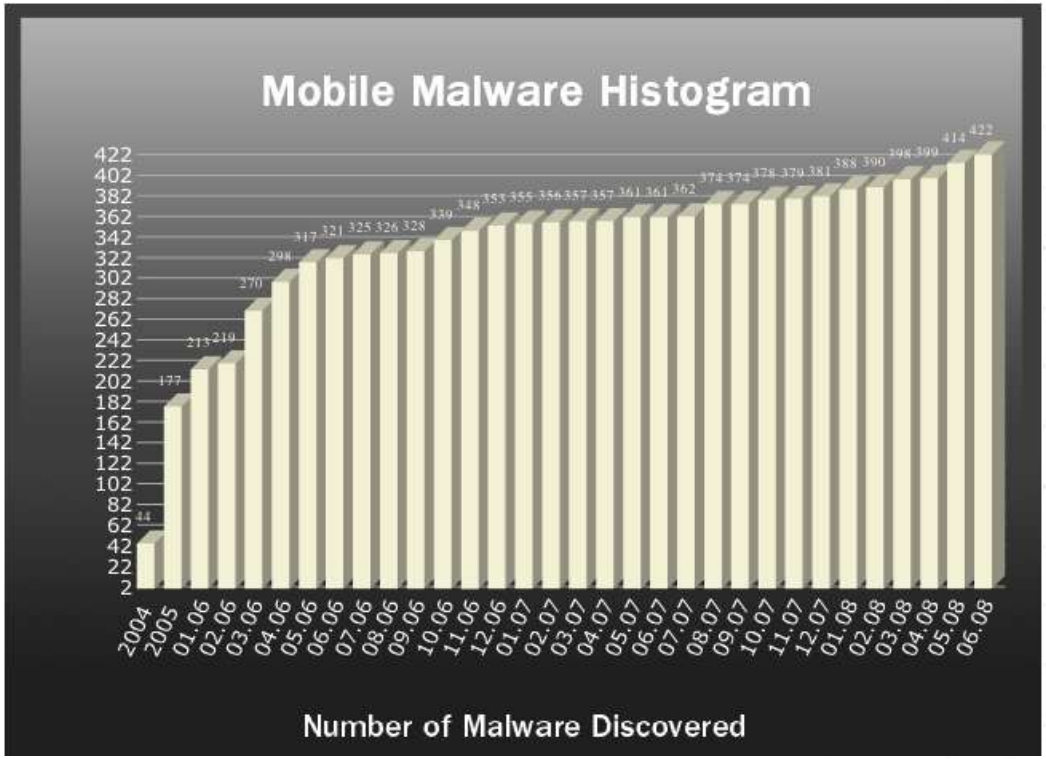
Copyright 2008 SMobile Systems

Threat: Malware

Copyright 2008 SMobile Systems

Current State of Mobile Malware

More than 400 known Malware to date in 30+ countries



Copyright 2008 SMobile Systems

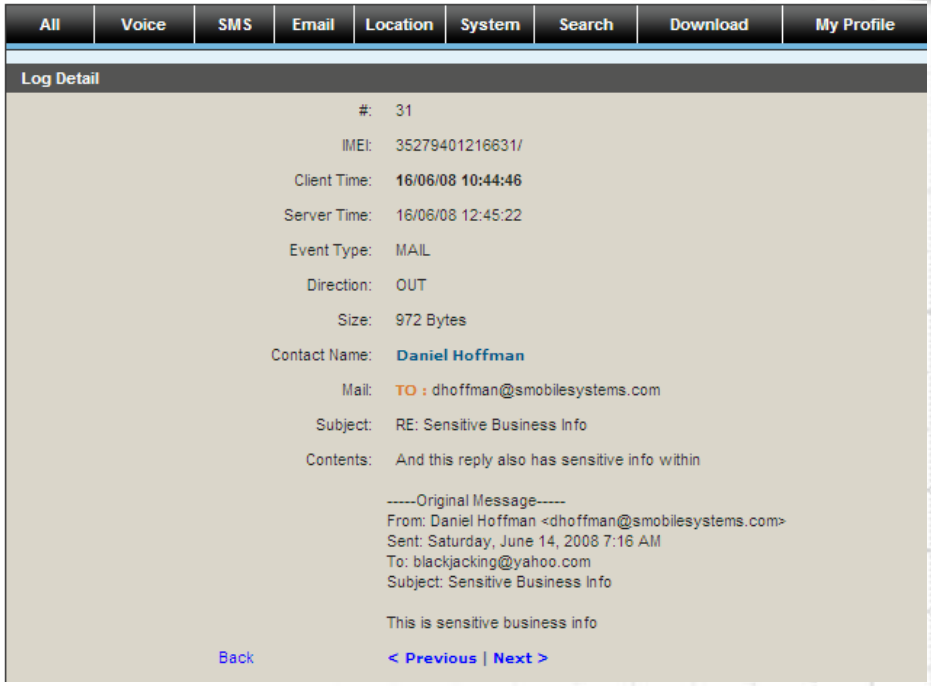
Spyware – The Hidden Threat to Mobile Devices

Spyware Properties:

- Silently runs on devices without the knowledge of the device user
- Easily installed via Trojans and other Malware
- 2 of the top 3 BlackBerry infectors are Spyware
- 4 of the top 5 Windows Mobile infectors are Spyware

Spyware Capabilities:

- Intercept and post to a website every SMS, MMS and e-mail (see image)
- Track every key typed by the device
- Remotely and silently turn on the phone to hear ambient conversations
- Track the position of the device



"Users and enterprises who are waiting to experience an infection before implementing security software are placing themselves into the unsavory position of unknowingly becoming infected with Spyware and having absolutely no security software in place to address that infection."

– SMobile Global Threat Center

Copyright 2008 SMobile Systems

Threat: Data Communication Interception

Copyright 2008 SMobile Systems

iPhone E-mail Sniff

Follow TCP Stream

Stream Content

```
* OK IMAP4rev1 server ready (3.5.28)
1 CAPABILITY
* CAPABILITY IMAP4rev1 LOGIN-REFERRALS AUTH=XYMCOOKIE AUTH=XYMCOOKIEB64 AUTH=XYMPKI ID
1 OK CAPABILITY completed
2 AUTHENTICATE XYMPKI
+
2 OK AUTHENTICATE completed
[774 bytes missing in capture file]3 SELECT INBOX
* 209 EXISTS
* 0 RECENT
* OK [UNSEEN 11] Message 11 is first unseen
* OK [UIDVALIDITY 1] UIDs valid
* OK [UIDNEXT 526] Predicted next UID
* FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
* OK [PERMANENTFLAGS (\Answered \Flagged \Deleted \Seen \Draft)] Permanent flags
3 OK [READ-WRITE] SELECT  completed; now in selected state
4 UID FETCH 525 (BODY.PEEK[HEADER] BODY.PEEK[TEXT])
[1448 bytes missing in capture file]-Transfer-Encoding: quoted-printable
Content-Type: text/plain; charset="iso-8859-1"

This is a sensitive message.  Cubs are going to win the World Series=

--_D4FE9782-22CB-A85A-352B-4C80A2E42610_
Content-Transfer-Encoding: quoted-printable
Content-Type: text/html; charset="iso-8859-1"

<HTML><HEAD><M
=3Diso-8859-1'
ial; FONT-WEIG
in the world s

--_D4FE9782-22
```

Find | Save As | Print

```
0480  20 53 75 6e 2c 20 30 33  20 41 75 67 20 32 30 30   Sun, 03  Aug 200
0490  38 20 32 30 3a 30 39 3a  34 34 20 2d 30 37 30 30   8 20:09: 44 -0700
04a0  20 28 50 44 54 29 0d 0a  4d 49 4d 45 2d 56 65 72   (PDT).. MIME-Ver
04b0  73 69 6f 6e 3a 20 31 2e  30 0d 0a 63 6f 6e 74 65   sion: 1. 0..conte
04c0  6e 74 2d 63 6c 61 73 73  3a 20 0d 0a 46 72 6f 6d   nt-class : ..From
04d0  3a 20 22 44 61 6e 69 65  6c 20 56 2e 20 48 6f 66   : "Danie l V. Hof
04e0  66 6d 61 6e 22 20 3c 64  68 6f 66 66 6d 61 6e 40   fman" <d hoffman@
04f0  73 6d 6f 62 69 6c 65 73  79 73 74 65 6d 73 2e 63   smobiles ystems.c
0500  6f 6d 3e 0d 0a 53 75 62  6a 65 63 74 3a 20 53 65   om>..Sub ject: Se
0510  6e 73 69 74 69 76 65 20  4d 65 73 73 61 67 65 0d   nsitive  Message.
0520  0a 44 61 74 65 3a 20 53  75 6e 2c 20 33 20 41 75   .Date: S un, 3 Au
0530  67 20 32 30 30 38 20 32  32 3a 31 30 3a 32 30 20   g 2008 2 2:10:20
0540  2d 30 35 30 30 0d 0a 49  6d 70 6f 72 74 61 6e 63   -0500..I mportanc
```

Sniffed Packets
118 and 140

Copyright 2008 SMobile Systems

Threat: Direct Attack

Copyright 2008 SMobile Systems

iPhone Browser Exploit

independent security evaluators

Upon visiting a malicious website with an iPhone, the exploit code reads the log of SMS messages, the address book, the call history and the voicemail data. It then transmits all this information to the attacker. However, this code could be replaced with code that does anything that the iPhone can do. It could send the user's mail passwords to the attacker, send text messages that sign the user up for pay services, or record audio that could be relayed to the attacker.

Copyright 2008 SMobile Systems

Threat: Physical Compromise

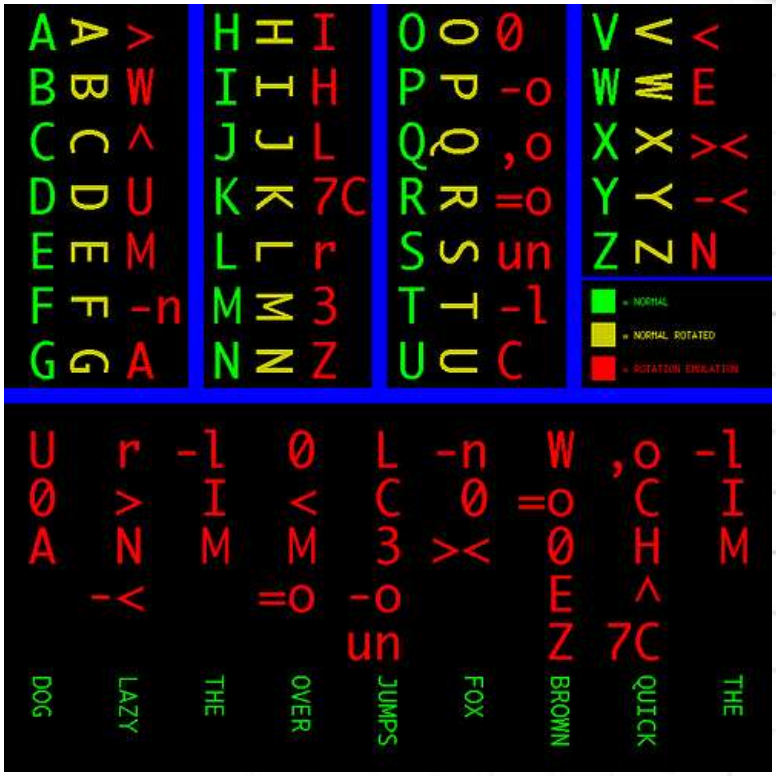
Copyright 2008 SMobile Systems

Physical Compromise

- Most smartphones do not offer encryption out of the box – the biggest reason iPhones aren't accepted in the enterprise

- User's don't always use PIN/passcodes to protect their devices

- Lock and wipe functionality doesn't exist for many platforms and not all BlackBerry devices utilize a BES Server



Copyright 2008 SMobile Systems

Physical Compromise

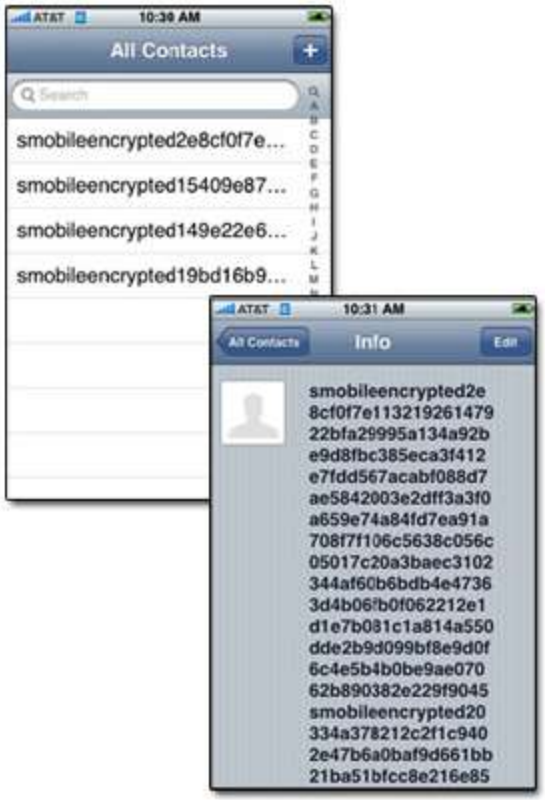
SMobile ContactCrypt Protects Against Newly Exposed iPhone Security Vulnerability

August 27, 2008

The Gizmodo Gadget Guide website recently published an article describing a very large security vulnerability in the iPhone. Because of this flaw, even passcode-protected devices can reveal sensitive personal information on the iPhone by easily pressing a few buttons. This vulnerability is possible because of two reasons:

1. The Emergency Call option can be exploited to expose sensitive information
2. Sensitive information on the iPhone is not encrypted.

To access sensitive information, a person stealing or finding an iPhone simply needs to select the Emergency Call option and press the Home Button twice. Doing so takes the user to the Favorites screen, where Contact information is clearly exposed. Because the sensitive Contact information is not encrypted, it can be easily viewed. Various Contact-related fields, such as URL's, can also be accessed via these contacts to provide access to the Safari browser and to e-mail.



- Even using a PIN/passcode doesn't guarantee protection
- Data is still unencrypted
- The authentication method can be bypassed

Copyright 2008 SMobile Systems

Threat: Exploitation and Misconduct

Copyright 2008 SMobile Systems

Exploitation and Misconduct

"For just about every category of mobile media activity, if you look at the 13- to 17-year-old bracket, they're doing more things with their phones than the average phone user … The same can be said for tweens – the 8- to 12-year-old crowd."

"47 percent of teenagers take photos with their mobile device – that's twice the industry average."

– Source: M:Metrics, Inc

Specific Threats

- Bullying
- Sexual exploitation
- Unsavory social situations

Copyright 2008 SMobile Systems

Exploitation and Misconduct

ABC 7 News > News > Local News
» leer el artículo en español

read | video | share | ABC 7 Talkback | email

text size: A | A | A

Sexting: New, Dangerous Teen Trend

posted 8:49 pm Thu May 15, 2008 -

tags: sexting • teen • cell • phone

A new, dangerous trend is growing among teenagers: text messaging explicit photos of themselves, also known as sexting. Students as young as 12 are exchanging salacious pictures and messages through their cellphones.

"A picture got out of somebody else's older sister and that kinda spread like wildfire through our school," said a tenth grader. The phenomenon is raging as wildly as their hormones. It's known as sexting or sex texting, sending lewd messages and pictures through a cellphone. "Nude body pictures, topless, bottomless, poses, inappropriate," said one tenth grader.

Its invaded middle schools as well. A seventh grader said, "It's not usually strangers. It's just somebody you've been talking to lately and they want to see more of you... literally."

Half of the 12 year old's ABC 7/NewsChannel 8's Julie Parker talked to had heard of this happening in their school. All the

SHARE | PRINT | EMAIL | RSS | AIM

share this story:
digg it | reddit | del.icio.us | technorati | newsvine

Copyright 2008 SMobile Systems

Exploitation and Misconduct

Enterprises:

•Where is your data going?

• What is your employee e-mailing, storing on their phone, texting?

• What websites are being visited with the company device? You control your PCs, why not your smartphones?

Copyright 2008 SMobile Systems

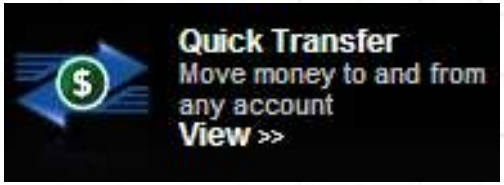
Threat: Authentication Spoofing

Copyright 2008 SMobile Systems

Mobile Banking is on the Rise

One million mark achieved by Bank of America in active mobile banking customers

Thu. June 12, 2008; Posted: 01:07 PM



Copyright 2008 SMobile Systems

Mobile Banking Trojan – January 21, 2009

cellular-news

Google™ Custom Search | Search

Recent News | News Categories | Phones Database | Recruitment | Resources | Conferences | About Us

Home >> More Handsets news >> This Article

Daily News Headlines

Get a *free* email of the news articles

Your e-mail a | Go

Click for sample copy
Our privacy policy

Symbian Virus Targets Mobile Banking Service

Advertise Here

Top Lists over 7 Days

Reads | E-mails | Jobs

Sony Ericsson Denied Playstation Brand - Expects Full Year Loss in 2009

US Patent Firms Seeks Ban on Imports of Nokia, HTC Mobile Phones

SMOBILE SYSTEMS

Copyright 2008 SMobile Systems

Curse of Silence Demo

Copyright 2008 SMobile Systems

How to Address the Threats …

Threat	SMobile Product
Malware	Antivirus, Firewall, Application Revocation, Update OS
Direct Attack	Firewall, AntiVirus, Update OS
Physical Compromise	Encryption, Lock and Wipe
Data Communication Interception	VPN, SSL
Authentication Attacks	VPN, Antivirus, SSL, Firewall, Update OS
Exploit and Misconduct	Parental and Enterprise Controls, Application Revocation

*** Treat the smartphone like a PC … because that's essentially what it is**

Copyright 2008 SMobile Systems

Conclusion

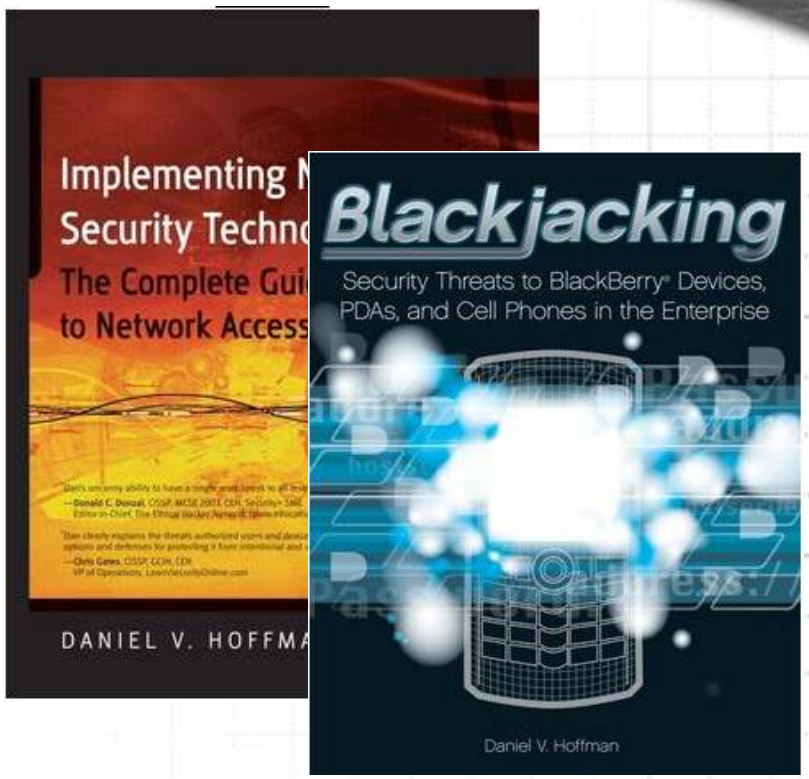
- Threats to smartphones do exist and devices are being exploited. This is an undeniable fact and the data supports it
- Smartphones are the new PCs and need to be protected with the same security technologies
- Physical compromise is currently the easiest means of exploitation
- Smartphone Malware does exist and has infected devices
- Malware is now being written to be stealthy, undetectable and for financial gain – infection and exploitation can occur without the knowledge of the device user/owner
- Not all smartphone security products significantly drain the battery!

Copyright 2008 SMobile Systems

Thank You

Additional Resources:

- Smobilesystems.com
- Ethicalhacker.net
- BlackJacking Book
- Complete Guide to NAC Book



Copyright 2008 SMobile Systems