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.
Smartphone Platforms

- Symbian
- BlackBerry
- Windows Mobile
- iPhone
- Android
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
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?
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
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
Mobile Security in the News

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:
1. Google Scrambles to Patch Buffer Overrun Exploit in Android G1
2. Android Flaw Is a Buffer Overrun

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 smartphone, 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 smartphone 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.
Experts: Zombie Cell-Phone Hack Attacks May Be Next

Thursday, October 16, 2008
Associated Press

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.
Mobile Security in the News

“Mobile Security: Still Crazy After All These Years

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
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.
And Malware isn’t the only way to exploit a mobile device
Let’s get specific as to what’s happening today
Threat: Malware
More than 400 known Malware to date in 30+ countries
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
Threat: Data Communication Interception
This is a sensitive message. Cubs are going to win the World Series!
Threat: Direct Attack
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.
Threat: Physical Compromise
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
Physical Compromise

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

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.
Threat: Exploitation and Misconduct
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
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.

It’s 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
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?
Threat: Authentication
Spoofing
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

[Image of a child holding a phone]
Symbian Virus Targets Mobile Banking Service

Anti-virus vendor, Kaspersky Lab says that it has detected a new malicious program capable of controlling a user’s mobile phone account. Last week, Kaspersky Lab experts detected the new malicious program for Symbian that targets customers of an Indonesian mobile phone operator.

The Trojan is written in Python, a script language, and sends SMS messages to a short number with instructions to transfer part of the money in the user’s account to another account, which belongs to the cybercriminals.

There are five known variants of Trojan. SMS Python Flocker, from a to e. The amounts transferred range from $0.45 to $6.90. Thus, if the cybercriminals behind the Trojan manage to infect a large number of phones, the amount transferred to their mobile phone account as a result could be quite substantial.
Curse of Silence Demo
### How to Address the Threats…

<table>
<thead>
<tr>
<th>Threat</th>
<th>SMobile Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware</td>
<td>Antivirus, Firewall, Application Revocation, Update OS</td>
</tr>
<tr>
<td>Direct Attack</td>
<td>Firewall, AntiVirus, Update OS</td>
</tr>
<tr>
<td>Physical Compromise</td>
<td>Encryption, Lock and Wipe</td>
</tr>
<tr>
<td>Data Communication Interception</td>
<td>VPN, SSL</td>
</tr>
<tr>
<td>Authentication Attacks</td>
<td>VPN, Antivirus, SSL, Firewall, Update OS</td>
</tr>
<tr>
<td>Exploit and Misconduct</td>
<td>Parental and Enterprise Controls, Application Revocation</td>
</tr>
</tbody>
</table>

* Treat the smartphone like a PC … because that’s essentially what it is
• 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!
Additional Resources:

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