Mobile Attacks Survey and Taxonomy

Wei Wang and Cristina Serban
AT&T Security Research Center - http://src.att.com

December 6, 2012
Outline

1. Objectives
2. Mobility trends
3. Attack attributes
4. Representative smartphone related attacks
5. Summary of attacks
6. General attack taxonomy
7. Using the attack taxonomy
7. Conclusions
Objectives

1. Survey and discussion of major security and privacy incidents related to smartphones reported in the general media
2. Summary of attacks by attack category, applicable platform, vulnerability, infection method, targets, impact and countermeasures
3. Mapping of these attacks to the proposed attack taxonomy
4. Demonstrate how the attack taxonomy is utilized to predict new potential attacks, possibly as an extension of existing attacks
What is a smartphone

- phone
- computer
- scanner
- sensor
- proxy
- access point
- ID card
- payment card

Future:

- centralized controller?
- personal monitoring device?
- your doctor’s assistant?
What is a smartphone

- phone
- computer
- scanner
- sensor
- proxy
- access point
- ID card
- payment card

Future:
- centralized controller?
- personal monitoring device?
- your doctor’s assistant?

High value

High complexity

And therefore a lot of possible threats...
Smartphone related statistics

Since Apple’s debut of the original iPhone in mid 2007 and the unveiling of open source Android OS in late 2007, the number of smartphone users has increased dramatically

Source: comScore - http://www.comscore.com/Insights/Blog/5_Years_Later_A_Look_Back_at_the_Rise_of_the_iPhone
Mobile malware statistics

Mobile malware took off as well, after a seemingly slow start

The number of new modifications of mobile threats by month, 2004–2011

The survey

- Looked at representative incidents / attacks related to smartphones reported in general media in 2006-2012
- Covering major types of attacks, but not attempting to be exhaustive
- Extracted attack attributes
- Summarized attacks
Attack related attributes

- Attack category
- Applicable platform
- Vulnerability
- Infection method
- Targets
- Behavior and Impact
- Countermeasures
## Representative smartphone related attack incidents

<table>
<thead>
<tr>
<th>Type: Root privilege and Data exfiltration</th>
<th>DroidDream Malware for Android</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time</strong></td>
<td>March 2011</td>
</tr>
<tr>
<td><strong>Category</strong></td>
<td>Trojan malware</td>
</tr>
<tr>
<td><strong>Platform</strong></td>
<td>Android</td>
</tr>
<tr>
<td><strong>Targets</strong></td>
<td>Any Android users</td>
</tr>
<tr>
<td><strong>Vulnerability</strong></td>
<td>Code exploit leads to root control over the phones</td>
</tr>
<tr>
<td><strong>Infection method</strong></td>
<td>Disguised as popular games</td>
</tr>
<tr>
<td><strong>Behavior and Impact</strong></td>
<td>The malware gains root access to the device and steals sensitive data from the phone, e.g., product ID, model, partner/provider, language, country and userID, can be stolen</td>
</tr>
<tr>
<td><strong>Countermeasure</strong></td>
<td>Google removed over 50 applications found to contain the malware from the Android Market, and activated an Android app kill switch that removed the malicious apps from user devices which have already downloaded the apps</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Type: Phishing, fraud, spam</strong></th>
<th><strong>SMS Phishing</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time</strong></td>
<td>June 2012</td>
</tr>
<tr>
<td><strong>Category</strong></td>
<td>Phishing</td>
</tr>
<tr>
<td><strong>Platform</strong></td>
<td>Any</td>
</tr>
<tr>
<td><strong>Targets</strong></td>
<td>Any smartphone user</td>
</tr>
<tr>
<td><strong>Vulnerability</strong></td>
<td>Phishing to human</td>
</tr>
<tr>
<td><strong>Infection method</strong></td>
<td>Victims receive a link in a SMS/MMS/email and are tricked to enter sensitive personal information on web; monetized by signing up premium services</td>
</tr>
<tr>
<td><strong>Behavior and Impact</strong></td>
<td>Spammers send SMS text messages saying “WON a FREE $1000 Giftcard! Enter &quot;405&quot; at <a href="http://www.****.com.***.biz">www.****.com.***.biz</a> to claim it and we can ship it to you immediately!”. After clicking the link, the web page asks the user to enter the code received in the SMS. The user then is redirected to another website to fill a form with sensitive personal information, email, home address, DOB, phone number, etc. Spammers can use this information for further attacks. Also, users are signed up for a premium service at $9.99/month.</td>
</tr>
<tr>
<td><strong>Countermeasure</strong></td>
<td>Beware of Phishing!</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th><strong>Type:</strong> Snooping/privacy</th>
<th><strong>Android Phone Snooping Vulnerability</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time</strong></td>
<td>May 2011</td>
</tr>
<tr>
<td><strong>Category</strong></td>
<td>Software flaw</td>
</tr>
<tr>
<td><strong>Platform</strong></td>
<td>Android</td>
</tr>
<tr>
<td><strong>Targets</strong></td>
<td>Android users using applications based on Google’s ClientLogin Protocol such as Google calendar and contacts synchronization service</td>
</tr>
<tr>
<td><strong>Vulnerability</strong></td>
<td>Google’s ClientLogin Protocol issues an authentication token which is valid for a maximum duration of 2 weeks, for any subsequent requests to the data service API</td>
</tr>
<tr>
<td><strong>Infection method</strong></td>
<td>Applicable to pre-2.3.4 Android smartphone versions and pre-3.0 Android tablet versions</td>
</tr>
<tr>
<td><strong>Behavior and Impact</strong></td>
<td>Attacker eavesdrops AuthToken (transmitted in clear text) and impersonates the user to access or modify user personal information in calendar, contacts, private web albums through Google services</td>
</tr>
<tr>
<td><strong>Countermeasure</strong></td>
<td>Limit the lifetime of AuthToken; mandate https for the services; switch to more secure authentication services. Google has fixed the problem in the latest Android releases, and delivered updates to old Android devices.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Type: Infrastructure</strong></th>
<th><strong>BBproxy Blackberry Trojan</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time</strong></td>
<td>August 2006</td>
</tr>
<tr>
<td><strong>Category</strong></td>
<td>Trojan malware</td>
</tr>
<tr>
<td><strong>Platform</strong></td>
<td>RIM/Blackberry</td>
</tr>
<tr>
<td><strong>Targets</strong></td>
<td>Enterprise internal network and data</td>
</tr>
<tr>
<td><strong>Vulnerability</strong></td>
<td>Exploits the trust relationship between a Blackberry and a company internal server to hijack a connection to the network. Since the data tunnel between the Blackberry and the server is encrypted, intrusion detection systems at the perimeter of the network cannot detect the attack.</td>
</tr>
<tr>
<td><strong>Infection method</strong></td>
<td>Embedded the malware into a game and downloaded to the Blackberry, or delivered through email</td>
</tr>
<tr>
<td><strong>Behavior and Impact</strong></td>
<td>Malware makes BlackBerry to open a communications channel between the attacker and the company's internal network. Attacker can get into the company's internal network and steal information or scan for more vulnerabilities.</td>
</tr>
<tr>
<td><strong>Countermeasure</strong></td>
<td>It is recommended that the Blackberry server is placed in a separate DMZ. The communication between Blackberry server and other internal network hosts should be very limited.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Type: Generic OS attacks</strong></th>
<th><strong>SSL Renegotiation DoS</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time</strong></td>
<td>March 2011</td>
</tr>
<tr>
<td><strong>Category</strong></td>
<td>DoS based on asymmetric processing</td>
</tr>
<tr>
<td><strong>Platform</strong></td>
<td>Any</td>
</tr>
<tr>
<td><strong>Targets</strong></td>
<td>SSL/TLS servers</td>
</tr>
<tr>
<td><strong>Vulnerability</strong></td>
<td>Basic TLS operations impose much more processing load on the server side than on the client side</td>
</tr>
<tr>
<td><strong>Infection method</strong></td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Behavior and Impact</strong></td>
<td>The client side can generate a lot of TLS renegotiation requests to exhaust the server resources</td>
</tr>
<tr>
<td><strong>Countermeasure</strong></td>
<td>Disable SSL/TLS renegotiation; rate-limit both incoming and renegotiation SSL/TLS requests; use SSL accelerator to offload processing. Existing DoS detection and mitigation methods do not work in this case because the initial SSL handshake is legitimate and renegotiations are done directly with the server.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type: Sensors</th>
<th>Spy Smartphone Software Tracks 'Every Move'</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>October 2011</td>
</tr>
<tr>
<td>Category</td>
<td>Spy software</td>
</tr>
<tr>
<td>Platform</td>
<td>Any</td>
</tr>
<tr>
<td>Targets</td>
<td>Any end users</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>Phishing to human</td>
</tr>
<tr>
<td>Infection method</td>
<td>The user opens a (personalized) email and a document, a picture, or pdf file. A program embedded in the attached document takes the hacked user's phone off to a secret website site which covertly downloads spying software onto the smartphone.</td>
</tr>
<tr>
<td>Behavior and Impact</td>
<td>Software designed to completely mine every secret on a smartphone can track its users, record their calls, copy their emails, read their text messages and bug the rooms the phones are sitting in. Sensors such as microphone and GPS are activated and used without user’s knowledge.</td>
</tr>
<tr>
<td>Countermeasure</td>
<td>Beware of phishing!</td>
</tr>
</tbody>
</table>


Note: There are many tools for sale with similar features – a few examples include FlexiSpy, OmegaSpy, GMSSMSSpy, Spy Bubble, Spy Control, Spy Phone Tap, Mobile-Spy
## Summary of attack incidents

<table>
<thead>
<tr>
<th>Time reported</th>
<th>Fast increasing since 2006</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Software flaw, Trojan malware, botnet, access control flaw</td>
</tr>
<tr>
<td>Platform</td>
<td>All mobile platforms</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>1. Improper infrastructure placement and management (e.g., lack of domain isolation, extended trust-relationship between servers which do not need it)</td>
</tr>
<tr>
<td></td>
<td>2. Asymmetric processing load between client and server (e.g., TLS/SSL renegotiation)</td>
</tr>
<tr>
<td></td>
<td>3. Default root password exploitation, especially apps from untrusted sources</td>
</tr>
<tr>
<td></td>
<td>4. Inadequate app permission checking, especially for android apps</td>
</tr>
<tr>
<td></td>
<td>5. Software implementation flaw (e.g., buffer overflow, sensitive information not encrypted, lack of access control or authentication protocol defects, prolonged local and backup copy, certificate management flaw)</td>
</tr>
<tr>
<td></td>
<td>6. Physical signal property (e.g. power signal strength variation during cryptographic operations)</td>
</tr>
<tr>
<td></td>
<td>7. Physical exploitation of sensors on smartphone (e.g., start microphone or camera on smartphone without user’s knowledge; capture GPS location; etc)</td>
</tr>
</tbody>
</table>

© 2012 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.
### Infection method

1. Malware disguised as legitimate application for download  
2. Existing app with default root password, especially apps from untrusted sources  
3. Delivered through SMS/MMS/PUSH/email link or attachment  
4. Propagate through Bluetooth

### Targets

1. Enterprise IT infrastructure  
2. Mobility network  
3. Data from users and enterprises: contact book, user information, location, phone call, video of proximity  
4. Configuration data on the device, e.g., phone info/settings  
5. Physical components of phone (e.g., battery)

### Behavior and Impact

1. Data access: accessing existing data  
2. Data collection: voice, camera, location, keystroke  
3. Data exfiltration: e.g., through SMS or Email  
4. Billing fraud: Trojan malware sending SMS texts / redirecting calls to premium numbers, and incurring costs to victims  
5. Clone the smartphone to carry out various malicious activities  
6. Mobile botnets  
7. DoS/DDoS attacks
<table>
<thead>
<tr>
<th>Countermeasure</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Better practice in IT infrastructure placement and management</td>
</tr>
<tr>
<td>2. Software / protocol implementation bug fixes</td>
</tr>
<tr>
<td>3. Proper server resource planning/rate limiting (especially for asymmetric</td>
</tr>
<tr>
<td>processing operations) and anomaly response</td>
</tr>
<tr>
<td>4. Resource monitoring from end users’ perspective</td>
</tr>
<tr>
<td>5. Anti-virus / anti-malware for mobile apps</td>
</tr>
<tr>
<td>6. High caution (plus user awareness) for application download, especially</td>
</tr>
<tr>
<td>from untrusted sources</td>
</tr>
</tbody>
</table>
General attack taxonomy

Six categories in the taxonomy

- victim
- operation impact
- targets
- vulnerability
- attack vehicles
- protocol stacks

An attacker picks a **victim**, and **operation impact**, then explores **vulnerability** of the **targets** by **attack vehicles**.

*Protocol stacks* define where the attack can be detected or mitigated.
General attack taxonomy

Classified by Victim
- Company
- Business Partners
- Business Customers
- Governments
- Consumers
- Others

Classified by Operational Impact
- Misuse of resources
  - Network
  - Denial of Service
  - Bandwidth Depletion
  - Resource Consumption
  - Connection Consumption
  - Service compromise
  - Content compromise
- Data Extortion
  - Intellectual Property
  - Customer Information
  - Database
  - Policies
  - Business strategy
- Host compromise
  - Data Breach
  - Privacy exposure
  - Battery consumption
  - Location leakage
  - Root compromise
- Fraud
- Brand

Classified by Targets
- Network
  - Bandwidth
  - Connectivity
  - Spectrum
- Hardware
  - Battery
  - Camera
  - GPS
  - Sensors
  - Memory Card
- OS
  - Software
  - End user
  - Data
  - Privacy
- Services on servers
  - Email
  - Web
  - DNS
  - SMS/MMS
  - CDN
- HLR, BTS
- Data
  - Intellectual Property
  - Customer
  - Database
  - Policies
  - Business strategy

Classified by Vulnerabilities
- Standards Flaws
  - 3GPP, 3GPP2
  - Control channel limit
  - Control/voice shared channel
  - GSM, GPRS
  - Asymmetric authentication
- Hardware Flaws
  - Chip
  - SIM
  - Plug-in devices
- OS Flaws
  - Buffer Overflow
  - Stack
  - Heap
- Software Flaws
  - BIOS
  - Firmware
  - Application
- Design Flaws
  - Policy
  - Insecure Input Validation
- Human
  - Social Engineering
  - Ignorance
  - Access Control
  - Misconfiguration
  - Incorrect Permission
  - Supply Chain
  - Device Modification
  - Default password

Classified by Attack Vehicle
- Reconnaissance Tools
  - Scanning
  - Sniffing
- Malformed Packets
- Normal Packets for Flooding
- SMS/MMS
  - Spam
  - Phishing
- Email
  - Phishing
- Malware
  - Virus
  - Spyware
  - Worm
  - Trojan
  - Injected scripts
  - Rootkit
  - Key logger
  - Adware
  - Man-in-the-Browser
- Social Engineering
  - IM
  - Blogs
  - Communities
  - Google website
  - P2P content sharing
- BotNet
  - IRC
  - P2P

Classified by Stacks
- Physical
  - USB
- MAC/physical
  - NFC, Bluetooth
- Physical Channel
  - RF jamming
  - RACH, SDCCH
  - Paging channel consumption
  - IMSI spoofing
- Transport Layer
  - TCP
  - UDP
- Internet Layer
  - Port scanning
  - IP scanning
  - IP spoofing
  - Control message flooding
- Application
  - Web
  - SIP
  - Signaling
  - Registration hijacking
  - Amplification attack
  - RTP
  - DNS
  - Email/MMS/MMS
  - Spam
  - Phishing
  - Peer-2-Peer
  - Index poisoning
  - Content poisoning
  - SSH/ftp/telnet
  - DHCP
  - Other Application Gateways
  - Human
Using the attack taxonomy: Looking at APTs

Advanced Persistent Threats (APT) –
• Fast growing
• Difficult to prevent / detect / remediate
• Causing significant losses

APT goals:
• Steal intellectual property (IP) from the targeted organization
• Gain access to sensitive data or strategic business information
• Blackmail, embarrassment, data poisoning, illegal insider trading
• Disrupt organization’s business
Conclusions

The case study is focused on mobile attacks, and the taxonomy includes attacks that are specific to mobility, and not found in general cyber security attacks – such as SMS/MMS-based attacks.

The taxonomy is especially helpful for reasoning about attacks and threats, to identify all potential vulnerabilities and design countermeasures in the new area of mobile security.
Thank you!

AT&T Security Research Center

http://src.att.com