Smartphone Privacy & Security

USP Presentation
Sakshi Garg & Bin Liu
Outline:

- Privacy and Security threats in Smartphones
- Android Permissions
- Readings
- Blackphone
- Class Activity
- Urgent Challenges
  - Malware detection
  - Fine-grained access control of resources
Privacy and security threats in Smartphones:
Privacy and security threats in Smartphones:

- Malware
- Spyware
- Vulnerable applications
- Phishing attacks
- Browser exploits
- Wi-fi sniffing
- Network exploits
- Lost or stolen device
- Impersonation
- Reselling your phone
- The data available on phone
What data do smartphones have access to?
What data do smartphones have access to?

- Contact lists
- emails
- messages
- pictures
- Videos
- phone calls
- Calendar
- Notes

- Location
- Microphone
- Bluetooth
- Reminders
- facebook
- twitter
Spy Agencies Tap Data Streaming From Phone Apps!! (Jan 27 2014)

One of several undisclosed classified document provided by Snowden.
Spy Agencies Tap Data Streaming From Phone Apps!!

- The N.S.A. and Britain’s Government Communications Headquarters were working together on how to collect and store data from dozens of smartphone apps.
- The project was named “The mobile surge”.
- This include applications like Angry Birds, facebook, flicker, flixster.
- Just by updating the android software, users send more than 500 lines of data about phone’s history and use.
Android Permissions:

- Android permission system is intended to inform users about the risks of installing applications.
- Android users are provided with permission display that appears when users have selected an application to download.
- The display helps to understand that how the information is accessed and users can cancel the installation if permissions are excessive or objectionable.
Why permissions are useless in Android?

- Users have no choice but to accept permissions to install the application.
- In most of the cases users do not understand these permissions.
- Vague and confusing terms are used.
- Difficult for users to make informed decisions while installing applications.
- There are around 130 permissions.
Reading 1 !!

Android Permissions: User Attention, Comprehension, and Behaviour

Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner.
Reading Summary !!

- 2 usability studies:
  - Internet survey of 308 Android users
  - Interviewed and observed 25 Android users.
- 17% participants paid attention to permissions and 97% failed to answer comprehension questions.
- Low awareness of permission warning and comprehension.
Recommendations for improving usability of Permissions:

● Negative reviews from peer users should be provided.
● Re-organizing and re-naming categories.
● Category headings should be more relevant and convey the right purpose.
● Warnings should convey risks.
● More permissions should be classified as non-dangerous and hidden by default.
One of the biggest security risk!

Phones get lost or stolen.
How to ensure the security of your smartphone?
Mobile passwords:

PIN : Earlier versions of iphone 40% people do not use Pin in their phones

Unlock Pattern: Most of the Android Phones

Fingerprint Mechanism: iphone 5s
Blackphone
Blackphone: Privacy and Security focused Android smartphone

- Developed by Silent circle.
- To be released in June 2014.
- 4.7-inch HD IPS screen
- >2GHz quad core CPU
- 2 GB RAM
- 16 Gb storage
What is special about this phone?

- Lets you send peer-to-peer Encrypted texts, Phone Calls, Video Calls and File transfers.
- Silent Circle Apps: provides access to internet services bypassing the government surveillance.
- Provides internet access through VPN.
- Disconnect Secure Wireless.
## Android vs. PrivatOS

<table>
<thead>
<tr>
<th>Feature</th>
<th>Android Default</th>
<th>PrivatOS Enhancement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search</td>
<td>Trackable</td>
<td>Anonymous</td>
</tr>
<tr>
<td>Bundled Apps</td>
<td>Many, with privacy disabled by default</td>
<td>Few, and all privacy-enabled</td>
</tr>
<tr>
<td>Wi-Fi usage</td>
<td>Always on for geolocation and user tracking</td>
<td>Smart disabling of all Wi-Fi except trusted hotspots</td>
</tr>
<tr>
<td>App permissions</td>
<td>All-or-nothing</td>
<td>Fine-grained control in a single interface</td>
</tr>
<tr>
<td>Communications tools</td>
<td>Traceable dialer, SMS, MMS, browser. Vulnerable to spoofed cell networks and Wi-Fi.</td>
<td>Private calls, texting, video chat, file exchange up to 100MB, browsing, and conference calls</td>
</tr>
<tr>
<td>Updates</td>
<td>Supplied infrequently after carrier blessing</td>
<td>Frequent secure updates from Blackphone directly</td>
</tr>
<tr>
<td>Remote Wipe &amp; Anti Theft</td>
<td>Requires use of centralized cloud account</td>
<td>Anonymous</td>
</tr>
<tr>
<td>Business Model</td>
<td>Personal data mining for tracking and marketing</td>
<td>Delivering privacy as a premium, valued feature</td>
</tr>
</tbody>
</table>
Might not be that good of an idea!!

- The cost of the phone is $630 + $120 subscription yearly to use encrypted suite.
- To communicate using blackphone, the other person needs to have blackphone or use silent circle apps on their android or iPhone.
- New OS and hence higher scope of teething troubles and bugs.
Challenge: Malware

(Especially on Android)
Malicious Smartphone Application

Sensitive Information Exposure
Abuse of phone services (Phone, Message)

Root Exploitation
Package Repacking
Update Attack
Class Discussion

KNET: “Keep your Android device safe from malware”

Are these security measures enough?

Please find a possible attack in a security perspective.
Why so many malware apps?

Abuse of openness.

- Reduce Openness
  - Review process by human, restrict APIs (iOS)

- Maintaining order
  - Automatic detection (Google Bouncer)

- Tradeoff? Arms Race?
Google Bouncer

Analyzing Apps on Google Play

- External network available. (:-))
- Run the app in an QEMU emulator for 5 minutes
- Using a Google account with made-up name & email
- Simulate UI clicks (Predictable?)
- Dynamic analysis (Static analysis as well)

https://www.duosecurity.com/blog/duo-tech-talks-dissecting-the-android-bouncer
Analysis of Malware

- **Dynamic Analysis**
  - Run the app in simulator
  - Apply sufficient input (Measuring code coverage)
  - Create fake data / responses
  - => Slow, incomplete

- **Static Analysis**
  - Reverse Engineering
  - Examining unusual cases
  - Tracking data flow
  - => Weak against code obfuscation
Fighting against malware apps

Anti-malware apps

Especially for jailbroken / rooted devices

Sophisticated anti-malware analysis

Side channels, etc.

http://www.csc.ncsu.edu/faculty/jiang/
http://www.cs.ucdavis.edu/~hchen/

http://blog.malwarebytes.org/intelligence/2013/03/obfuscation-malwares-best-friend/
Challenge: Resource Control
Phone resource control

Fine-grained controls are needed
  “Google Map reads my contacts”
  “This game consume too much data traffic”

Existing Solutions
  iOS: Privacy Panel
  Android: Permissions, AppOps
  PDroid, LBE, XPrivacy, PMP
Users are overwhelmed with options!
Reduce Users’ Burden

Predictive
   Better default settings
   Labeling only for some of the apps

Abstraction & Aggregation
   Answering several questions only
Crowd-powered Smart Default

ProtectMyPrivacy (PMP)
Crowd-powered Smart Default

XPrivacy: [https://crowd.xprivacy.eu/](https://crowd.xprivacy.eu/)

<table>
<thead>
<tr>
<th>Votes * deny/allow</th>
<th>Exceptions (yes/no)</th>
<th>CI95 ±% **</th>
<th>Restriction</th>
</tr>
</thead>
<tbody>
<tr>
<td>121 / 179 40%</td>
<td>7 / 293</td>
<td>5.5</td>
<td>accounts</td>
</tr>
<tr>
<td>171 / 125 58%</td>
<td>0 / 296</td>
<td>5.6</td>
<td>browser</td>
</tr>
<tr>
<td>177 / 119 60%</td>
<td>0 / 296</td>
<td>5.6</td>
<td>calendar</td>
</tr>
<tr>
<td>218 / 78 74%</td>
<td>0 / 296</td>
<td>5.0</td>
<td>calling</td>
</tr>
<tr>
<td>114 / 182 39%</td>
<td>0 / 296</td>
<td>5.5</td>
<td>clipboard</td>
</tr>
<tr>
<td>197 / 99 67%</td>
<td>0 / 296</td>
<td>5.3</td>
<td>contacts</td>
</tr>
<tr>
<td>156 / 140 53%</td>
<td>0 / 296</td>
<td>5.7</td>
<td>dictionary</td>
</tr>
<tr>
<td>174 / 122 59%</td>
<td>0 / 296</td>
<td>5.6</td>
<td>email</td>
</tr>
<tr>
<td>195 / 101 66%</td>
<td>0 / 296</td>
<td>5.4</td>
<td>identification</td>
</tr>
<tr>
<td>55 / 241 19%</td>
<td>0 / 296</td>
<td>4.4</td>
<td>internet</td>
</tr>
<tr>
<td>23 / 15 61%</td>
<td>0 / 38</td>
<td>14.9</td>
<td>ipc</td>
</tr>
<tr>
<td>240 / 56 81%</td>
<td>0 / 296</td>
<td>4.5</td>
<td>location</td>
</tr>
<tr>
<td>141 / 155 48%</td>
<td>0 / 296</td>
<td>5.7</td>
<td>media</td>
</tr>
<tr>
<td>192 / 104 65%</td>
<td>0 / 296</td>
<td>5.4</td>
<td>messages</td>
</tr>
<tr>
<td>173 / 123 58%</td>
<td>0 / 296</td>
<td>5.6</td>
<td>network</td>
</tr>
<tr>
<td>163 / 133 55%</td>
<td>0 / 296</td>
<td>5.6</td>
<td>nfc</td>
</tr>
<tr>
<td>116 / 180 39%</td>
<td>0 / 296</td>
<td>5.5</td>
<td>notifications</td>
</tr>
<tr>
<td>54 / 81 40%</td>
<td>0 / 135</td>
<td>8.2</td>
<td>overlay</td>
</tr>
<tr>
<td>227 / 69 77%</td>
<td>0 / 296</td>
<td>4.8</td>
<td>phone</td>
</tr>
<tr>
<td>96 / 70 58%</td>
<td>0 / 166</td>
<td>7.4</td>
<td>sensors</td>
</tr>
<tr>
<td>200 / 96 68%</td>
<td>0 / 296</td>
<td>5.3</td>
<td>shell</td>
</tr>
<tr>
<td>78 / 218 26%</td>
<td>0 / 296</td>
<td>5.0</td>
<td>storage</td>
</tr>
<tr>
<td>120 / 176 41%</td>
<td>0 / 296</td>
<td>5.6</td>
<td>system</td>
</tr>
<tr>
<td>97 / 199 33%</td>
<td>0 / 296</td>
<td>5.3</td>
<td>view</td>
</tr>
</tbody>
</table>
We need personalization

<table>
<thead>
<tr>
<th>Profile 1 (25.4%)</th>
<th>Profile 2 (15.8%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>✗ Call Log + ✓ Call Monitoring</td>
<td>✗ Positioning + ✓ Wi-Fi / 3G</td>
</tr>
<tr>
<td>✗ Call Log + ✓ Wi-Fi / 3G</td>
<td>✗ Positioning + ✓ ROOT</td>
</tr>
<tr>
<td>✗ Call Log + ✓ Phone State</td>
<td>✗ Call Log + ✓ Wi-Fi / 3G</td>
</tr>
<tr>
<td>✓ Call Log + ✓ ROOT</td>
<td>✗ Positioning + ✓ Phone State</td>
</tr>
<tr>
<td>✗ Call Log + ✓ Positioning</td>
<td>✓ Call Log + ✓ ROOT</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Profile 3 (17.8%)</th>
<th>Profile 4 (8.8%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>✗ Positioning + ✓ Wi-Fi / 3G</td>
<td>✓ Positioning + ✓ Wi-Fi / 3G</td>
</tr>
<tr>
<td>✓ Positioning</td>
<td>✗ Positioning + ✓ ROOT</td>
</tr>
<tr>
<td>✗ Positioning + ✓ SMS DB</td>
<td>✗ Positioning + ✓ Call Monitoring</td>
</tr>
<tr>
<td>✓ Positioning + ✓ ROOT</td>
<td>✗ Positioning + ✓ Phone State</td>
</tr>
<tr>
<td>✗ Positioning + ✓ Phone ID</td>
<td>✓ Wi-Fi Network</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Profile 5 (14.8%)</th>
<th>Profile 6 (17.2%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Positioning + ✓ ROOT</td>
<td>✓ Call Log + ✓ Call Monitoring</td>
</tr>
<tr>
<td>✓ Positioning + ✓ 3G / Wi-Fi</td>
<td>✓ Call Log + ✓ Wi-Fi / 3G</td>
</tr>
<tr>
<td>✓ Phone ID + ✓ ROOT</td>
<td>✓ Call Log + ✓ Phone State</td>
</tr>
<tr>
<td>✗ Phone ID + ✓ 3G / Wi-Fi</td>
<td>✓ Call Log + ✓ ROOT</td>
</tr>
<tr>
<td>✗ 3G / Wi-Fi + ✓ ROOT</td>
<td>✓ Call Log + ✓ Phone ID</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Smart Default

Intelligently predict users’ preferences
Minimum users’ burden
Transparent decision making process

First step of this (shamelessly): our paper! :)
Thanks!