Residual Network Data
on Android Devices

LT. Greg Cardwell and Prof. Rob Beverly
Consider Implications:
- Enemy use of COTS Smartphones
- US DoD Deployed COTS Smartphones

Intuitively, we believe this is insecure. For many reasons…

This work examines the extent to which current and residual network data can be retrieved from Smartphone Flash memory
Our Research:

- Conduct carefully controlled experiments using our own infrastructure to create known ground-truth Smartphone corpus
- Examine residual network data in corpus
- We limit our exploration to Android mobile OS
Nexus One Flash Partitions

- mtd0: "misc"
- mtd1: "recovery"
- mtd2: "boot"
- mtd3: "system"
- mtd4: "cache"
- mtd5: "userdata"

Source: Android Forensics: Hoog
Acquisition

• Rooting Tools
  - theunlockr.com
    • Adds superuser.apk to mtd3(system)
  - Gingerbreak.exe
  - superboot
• ssh / netcat / dd
• ADB Pull
• Nandroid
• Clean Android Smartphones
• Performed in Faraday Cage
• Communication. Run our own:
  - GSM BTS
  - 802.11 WiFi
  - Bluetooth
• Different experiments using different communication channels:
  - To our web server/content
• Per-experiment imaging
• Gives us known ground-truth corpus
Building the Corpus
Binary IP

Physical dump – 5 instances

Logical dump – 1 instance

Signature – 0x020106
DHCP ACK-Bootstrap Protocol
Message Type - 0x02
Hardware type - 0x01
Hardware Add len - 0x06
Hops - 0x00
Cellular Base Stations

User Data Partition – HTC Evo 4G

- **Android Location Package**
  - Installs cache.cell
  - DB records cell towers

- **Unallocated Instances**
## IP and MAC

### User Data Partition – Nexus One

<table>
<thead>
<tr>
<th>Count</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>3.0.0.5</td>
</tr>
<tr>
<td>8</td>
<td>193.113.200.195</td>
</tr>
<tr>
<td>8</td>
<td>192.168.192.192</td>
</tr>
<tr>
<td>8</td>
<td>192.168.77.1</td>
</tr>
<tr>
<td>4</td>
<td>1.8.8.1</td>
</tr>
<tr>
<td>4</td>
<td>1.4.0.1</td>
</tr>
<tr>
<td>3</td>
<td>192.168.251.150</td>
</tr>
<tr>
<td>3</td>
<td>200.142.130.104</td>
</tr>
<tr>
<td>3</td>
<td>2.6.32.9</td>
</tr>
<tr>
<td>3</td>
<td>139.7.24.1</td>
</tr>
<tr>
<td>2</td>
<td>213.158.194.226</td>
</tr>
<tr>
<td>2</td>
<td>210.241.199.199</td>
</tr>
<tr>
<td>2</td>
<td>194.182.251.158</td>
</tr>
<tr>
<td>2</td>
<td>212.53.51.143</td>
</tr>
<tr>
<td>2</td>
<td>200.192.230.142</td>
</tr>
<tr>
<td></td>
<td>149.254.201.135</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Count</th>
<th>MAC Address</th>
<th>Pre</th>
<th>Post</th>
</tr>
</thead>
<tbody>
<tr>
<td>1479</td>
<td>00:26:08:BC:D4:14</td>
<td>0x01</td>
<td>0x00</td>
</tr>
<tr>
<td>18</td>
<td>00:26:08:BC:D4:14</td>
<td>0xff</td>
<td>0x20</td>
</tr>
<tr>
<td>15</td>
<td>00:26:08:BC:D4:14</td>
<td>0x0a</td>
<td>0x23</td>
</tr>
<tr>
<td>12</td>
<td>90:21:55:2C:4D:67</td>
<td>0xff</td>
<td>0x00</td>
</tr>
<tr>
<td>11</td>
<td>00:26:08:BC:D4:14</td>
<td>0x5f</td>
<td>0x31</td>
</tr>
<tr>
<td>1</td>
<td>c0:c1:c0:40:cd:ac</td>
<td>0x11</td>
<td>0xff</td>
</tr>
<tr>
<td></td>
<td>00:11:95:39:13:d1</td>
<td>0x11</td>
<td>0xff</td>
</tr>
</tbody>
</table>

- cache.wifi
SSIDs

- Associated to a wireless access point
  - `wpa_supplicant.conf`
    - 3 Instances
    - 1 currently allocated
User Data Partition – Nexus One

- CheckInService.xml
  - 1 Currently Allocated

- Current IMSI

  - 29 - 9150500000000122
  - 01 - 9150500000000122
Bluetooth Data

User Data Partition – Nexus One

- Btopp.db
- Settings.db

- 1479 - 00:26:08:BC:D4:14 0x01 0x00
- 18 - 00:26:08:BC:D4:14 0xff 0x20
- 15 - 00:26:08:BC:D4:14 0x0a 0x23
- 11 - 00:26:08:BC:D4:14 0x5f0x31
Future Work

- MAC Address Database
- YAFFS Forensic Tools
- Mobile RAM Capture