Android Forensics: Automated Data Collection and Reporting from a Mobile Device

Justin Grover

DFRWS 2013
Agenda

- Problem
- Solution
- Scope of Research
- Background
- Related Work
- DroidWatch
  - Design
  - Implementation
  - Analysis & Evaluation
  - Anti-Forensics
- Future Work
Problem

- **Android Smartphones Gaining Popularity**
  - In the U.S., as of May 2013
    - 141 Million People Owned a Smartphone
    - 52.4% of Smartphone Platforms ran Android

- **Enterprise Security is a Challenge**
  - Lack of Monitoring Technology for Enterprise Android Devices
  - Limited Data Availability for Internal Investigations
Solution

■ Android App
  – Continuous Monitoring of an Android Enterprise Device
    ■ Incorporates User Consent
    ■ Targeted for Internal Investigations

■ Contributions
  – 1st Open Source Android User Monitoring Solution of Its Kind
  – Design Strategy for Prioritizing Android App Components
  – Guide for Collecting Data Without Root Privileges
Scope of Research

- Test Device
  - Samsung Galaxy S II Epic 4G Touch (Unrooted)

- Investigators...
  - Incident Responders
  - Security Auditors
  - Forensic Investigators

- Investigating...
  - Policy Violations
  - Intellectual Property Theft
  - Misuse
  - Embezzlement
  - Sabotage
  - Espionage
Background

Android App Components

- Most Commonly Used
  - Activity - User Interface
  - Service - Long-Running Operation
  - Content Provider - Manages Access to Data
  - Broadcast Receiver - Handles Notifications

- Useful for Monitoring
  - Broadcast Receiver - Handles Notifications
  - Content Observer - Detects Changes
  - Alarm - Scheduled Operations
Background

■ Android Security Model
  – Apps & Users Are Sandboxed
  – Permissions Must Be Declared

■ Rooting Bypasses the Android Security Model
  – Legitimate Purposes
    ■ Forensics
    ■ Security Apps
    ■ Personal Use & Research
  – Nefarious Purposes
    ■ Tampering
    ■ Circumvent Enterprise Security
Related Work

- **Mobile Device Management (MDM)**
  - Juniper Networks

- **Forensic Snapshots**
  - Encase Enterprise
  - AFLogical

- **Other Continuous Monitoring Systems**
  - Personal “Spy” Apps
DroidWatch

- Design
- Implementation
- Analysis & Evaluation
- Anti-Forensics
DroidWatch: Design

- System Architecture

![System Architecture Diagram]

- Content Observers
- Broadcast Receivers
- Alarms
- Direct Data Access
- Internal SQLite
- Network Transfer

Android Service

Java Application

Enterprise Server
DroidWatch: Design

- Data Continuously Collected
- Data Periodically Transferred to an Enterprise Server

Data Flow (On the Phone)

Forensic Collection → Local SQLite Storage → HTTPS Transfer → Clear Local SQLite DB
Development Design Strategy

- Used to Prioritize Android App Components Useful for Monitoring
- Implemented Throughout DroidWatch
DroidWatch: Implementation

17 Data Sets Targeted for Collection
- Collected: 15
- Not Collected: 2

<table>
<thead>
<tr>
<th>Data Set</th>
<th>BroadcastReceiver</th>
<th>ContentObserver</th>
<th>Alarm</th>
</tr>
</thead>
<tbody>
<tr>
<td>App Installs / Removals</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Browser Navigation History</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Browser Searches</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Calendar Events</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Call Logs</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Contacts Added</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>GPS Location</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Location Settings</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MMS</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Pictures Added</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Screen Lock Status</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMS</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Third-Party App Logs</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
Typical Use Resulted in ~1MB Logs / Day
DroidWatch: Analysis & Evaluation

Detected Screen Unlock Actions (Splunk)
### Photo and MMS Search Results (Splunk)

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Time</th>
<th>Detector</th>
<th>Action</th>
<th>Additional Info</th>
<th>Host</th>
<th>Source</th>
<th>Source Type</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>12/22/2012</td>
<td>PhotoWatcher</td>
<td>Photo Added</td>
<td>dateOccurred=1356207652.000 description=20121222_152052.jpg</td>
<td>host=192.168.17</td>
<td>source=dbmon.kv</td>
<td>dbmon-kv</td>
<td>iPhoneWatcher Events/PhoneWatcher</td>
</tr>
<tr>
<td>2</td>
<td>12/22/2012</td>
<td>OutgoingMMSReceiver</td>
<td>MMS Sent</td>
<td>dateOccurred=1356207752.000 description=20121222_152052.jpg</td>
<td>host=192.168.17</td>
<td>source=dbmon.kv</td>
<td>dbmon-kv</td>
<td>iPhoneWatcher Events/PhoneWatcher</td>
</tr>
</tbody>
</table>
DroidWatch: Analysis & Evaluation

- Issues Noted:
  1. Last Known Locations Do Not Work Well
  2. Messages Sent to Multiple Contacts Only Listed a Single Recipient
  3. Incoming SMS Messages Do Not Contain Timezone
  4. No MMS Message Text
DroidWatch: Anti-Forensics

DroidWatch Susceptible To:
- Root
- Uninstallation
- Process Termination

Relies On:
- External protections
- Future Work
  - Anti-Tampering Mechanisms
  - Installation Within /system/app Directory
DroidWatch: Anti-Forensics

- **Destroying, Hiding, & Altering Evidence**
  - Alarms Susceptible
    - Possible to Tamper With Evidence Between Collections
  - Intent-Filter Priority
    - Apps With Max Intent-Filter Priority Values Can Override Broadcasts
      - Example: GoSMS

- **Counterfeiting Evidence**
  - No Verification of Real Data
  - Possible Denial of Service

- **Detecting Forensics Tools**
  - Automated Tools Could Turn Off Networking Before Data Transfers
Future Work

■ Additional Data Collections
  – USB Debugging
  – Voicemail Log
  – dumpsys / dumpstate / dmesg

■ Anti-Tampering Mechanisms
  – Database Encryption
  – Keep-Alive Logs
  – High Intent-Filter Priorities
  – Individual Event Checksums

■ Longer-Term Effort
  – Integrate into Mobile Device Management (MDM)
Conclusion

- DroidWatch Prototype Targeted for Internal Investigators
  - Source Code Available on GitHub

- Contact Info: jgrover@mitre.org

- Demo at tonight’s session!

------ Any Questions? ------


