Android Forensics: Automated Data Collection And Reporting From A Mobile Device

By

Justin Grover

Presented At

The Digital Forensic Research Conference

DFRWS 2013 USA Monterey, CA (Aug 4th - 7th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http:/dfrws.org

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

Justin Grover

DFRWS 2013

MITRE

Approved for Public Release

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

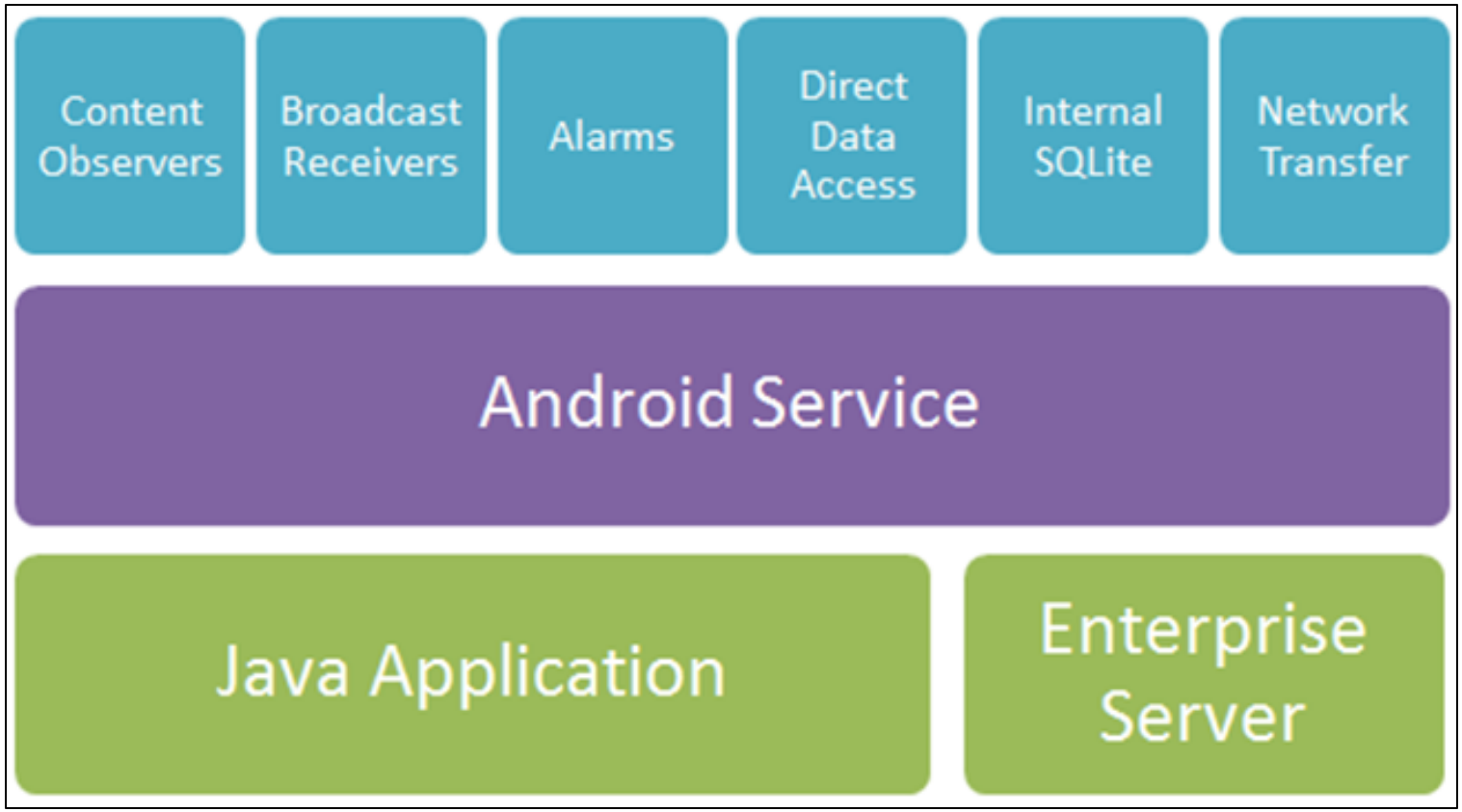
- **Mobile Device Management (MDM)**
  - Juniper Networks
- **Forensic Snapshots**
  - Encase Enterprise
  - AFLogical
- **Other Continuous Monitoring Systems**
  - Personal “Spy” Apps

DroidWatch

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

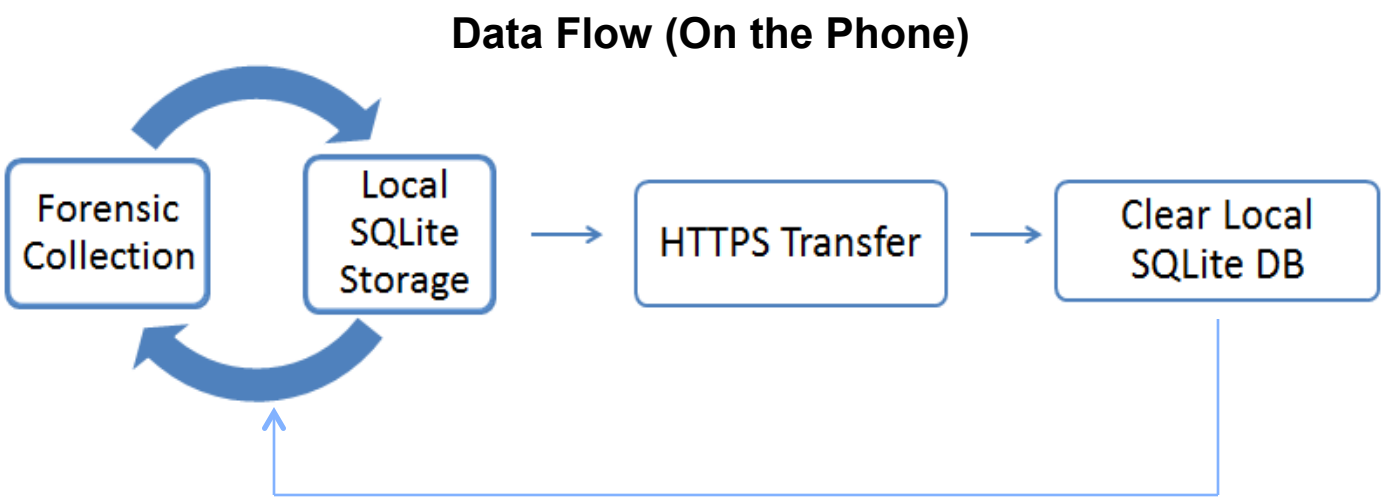
DroidWatch: Design

- **System Architecture**



DroidWatch: Design

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



DroidWatch: Design

- **Development Design Strategy**
  - Used to Prioritize Android App Components Useful for Monitoring
  - Implemented Throughout DroidWatch

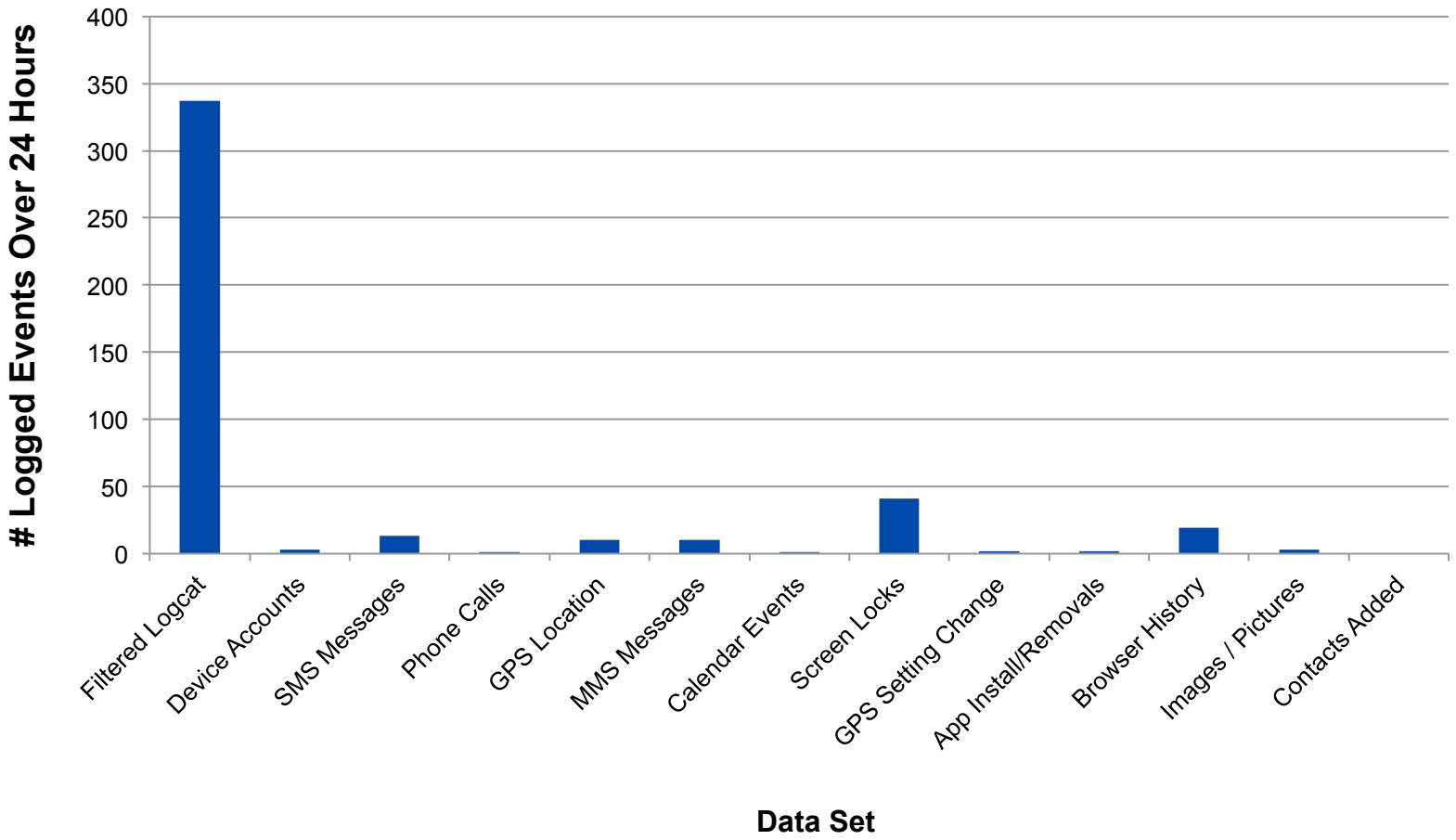
DroidWatch: Implementation

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

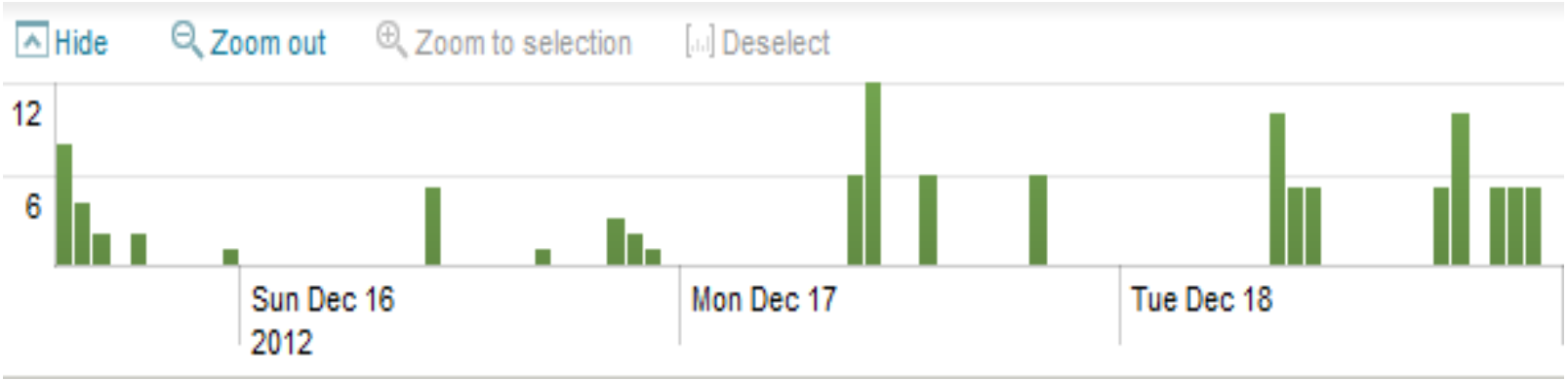
Data Set	Collection Component Used		
	BroadcastReceiver	ContentObserver	Alarm
App Installs / Removals	✓		
Browser Navigation History			✓
Browser Searches			✓
Calendar Events			✓
Call Logs		✓	
Contacts Added		✓	
GPS Location			✓
Location Settings	✓		
MMS	✓		✓
Pictures Added		✓	
Screen Lock Status	✓		
SMS	✓	✓	
Third-Party App Logs			✓

DroidWatch: Analysis & Evaluation

- **Typical Use Resulted in ~1MB Logs / Day**



DroidWatch: Analysis & Evaluation



Detected Screen Unlock Actions (Splunk)

DroidWatch: Analysis & Evaluation

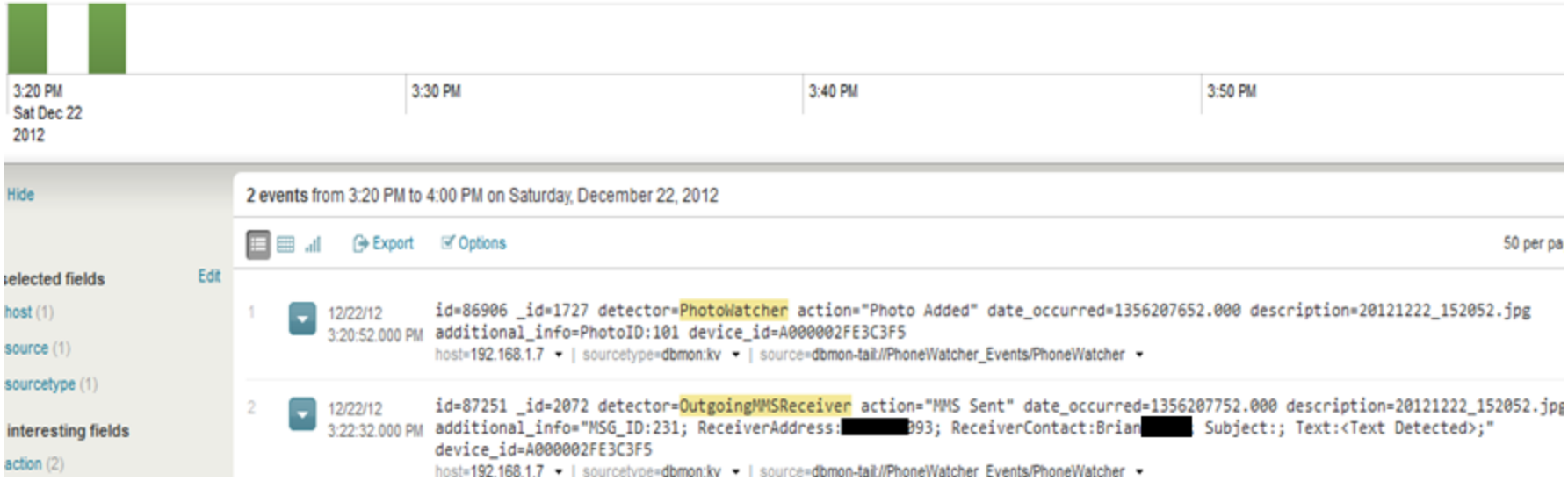


Photo and MMS Search Results (Splunk)

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? -------**

References

Azadegan, S., Yu, W., Liu, H., Sistani, M., & Acharya, S. (2012). Novel Anti-forensics Approaches for Smart Phones. *Hawaii International Conference on System Sciences* (pp. 5424-5431). Maui: IEEE.

comScore, Inc. (2013, June 28). *comScore Reports May 2013 U.S. Mobile Subscriber Market Share.* Retrieved from comScore:http://www.comscore.com/Insights/Press_Releases/2013/6/comScore_Reports_May_2013_U.S._Mobile_Subscriber_Market_Share

Distefano, A., Me, G., & Pace, F. (2010). Android anti-forensics through a local paradigm. Digital Forensics Research Workshop (pp. S95-S103). Portland, Oregon: Elsevier.

Hoog, A. (2010, March 1). *Open Source Android Digital Forensics Application*. Retrieved from Andrew Hoog SANS Blog: http://computer-forensics.sans.org/blog/2010/03/01/open-source-android-digital-forensics-application.

Shields, C., Frieder, O., & Maloof, M. (2011). A system for the proactive, continuous, and efficient collection of digital forensic evidence. *Digital Forensics Research Workshop* (pp. S3-S11). New Orleans, LA: Elsevier.