



Fall 2014
SEI Research Review
Behavior Based Analysis and
Detection of Mobile Malware

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Presenter: Joseph Yankel
Team: Dr. Jose Andre Morales
Hasan Yasar
Dr. John Cavazos UDel



Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE 01 OCT 2014		2. REPORT TYPE N/A		3. DATES COVERED -	
4. TITLE AND SUBTITLE Fall 2014 SEI Research Review Behavior Based Analysis and Detection of Mobile Malware				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Jose A. Morales				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited					
13. SUPPLEMENTARY NOTES The original document contains color images.					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT SAR	18. NUMBER OF PAGES 17	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution except as restricted below.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

DM-0001718



Project Description

Develop a fully automated behavior-based analysis approach capable of accurate suspicion assessment of software for mobile devices.

Expected Outcomes

- Behavior characteristics usable in assessing suspicion
- Efficient data collection techniques
- Automated app analysis with user interaction
- Suspicion assessment prototype for real devices

Impact for the DoD: identify potential malware early enough to avoid potential damage to the device. Provide fast accurate suspicion assessment of an app to an analyst



Behavior Characteristics

Identified various behaviors:

- Thread creation
- Accessing system data with potential PII
- Ingoing and outgoing SMS
- TCP connections
- Privilege escalation
- Device root

Most found in strace, logcat, and network data

Mostly occurs within a few seconds of main activity running



Analysis Methodology - Approach

- Strace Android APK
- Convert strace to graph
- Apply graph kernel for similarity computation
- Feed similarity to SVM for classification

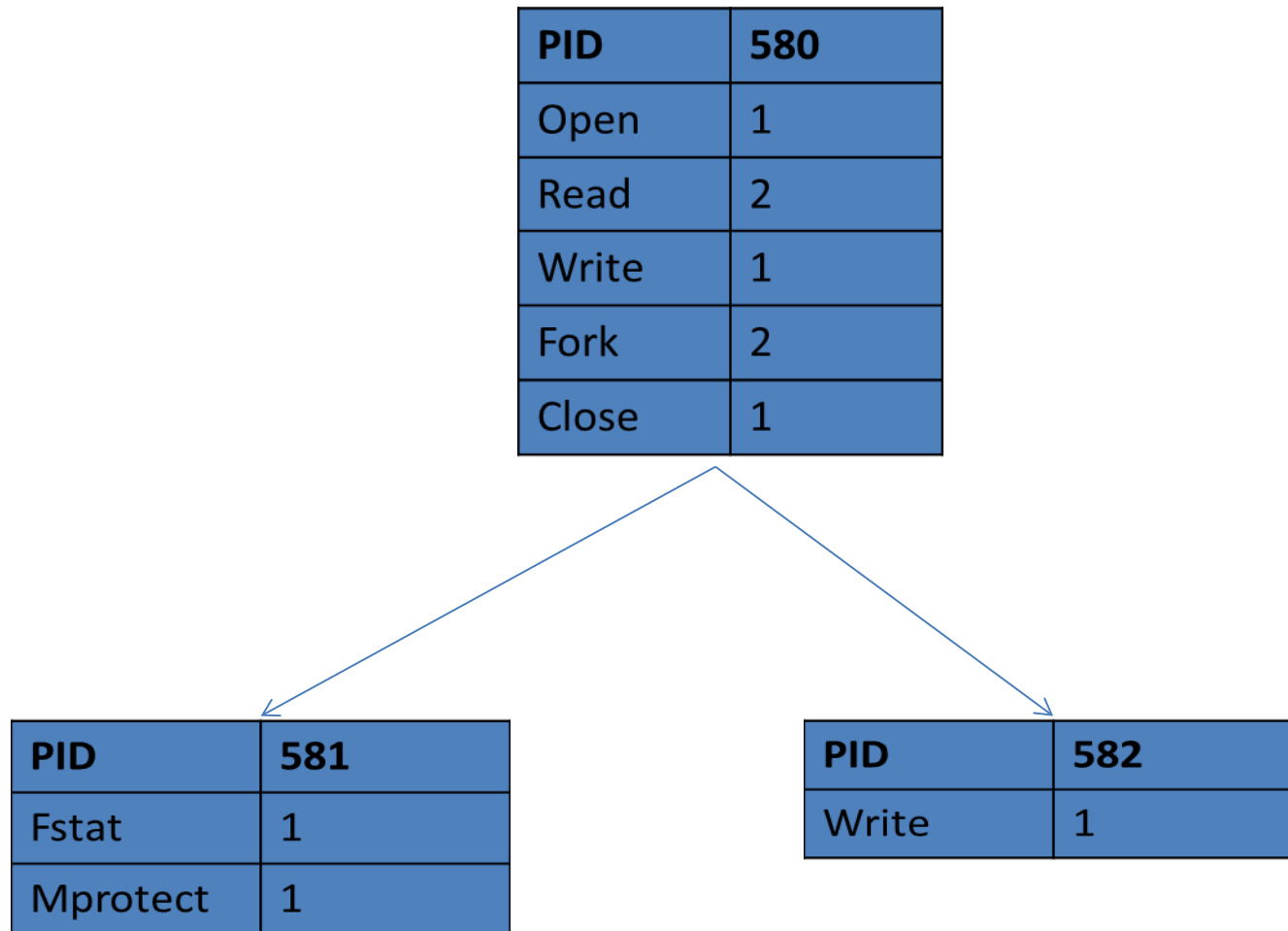


Analysis Methodology – Strace Sample

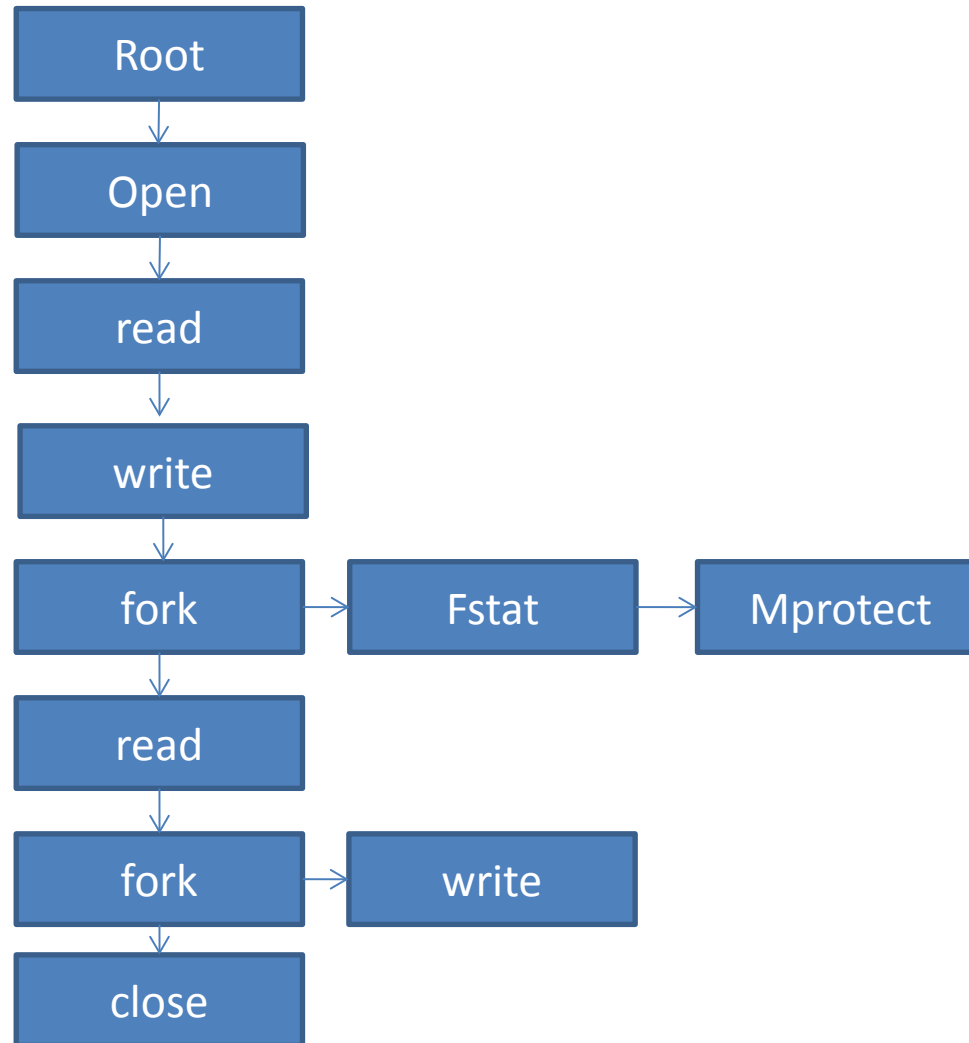
PID	System Call	Result
580	Open	1
580	Read	1
580	Write	1
580	Fork	581
581	Fstat	1
581	Mprotect	1
580	Read	1
580	Fork	582
582	Write	1
580	Close	1



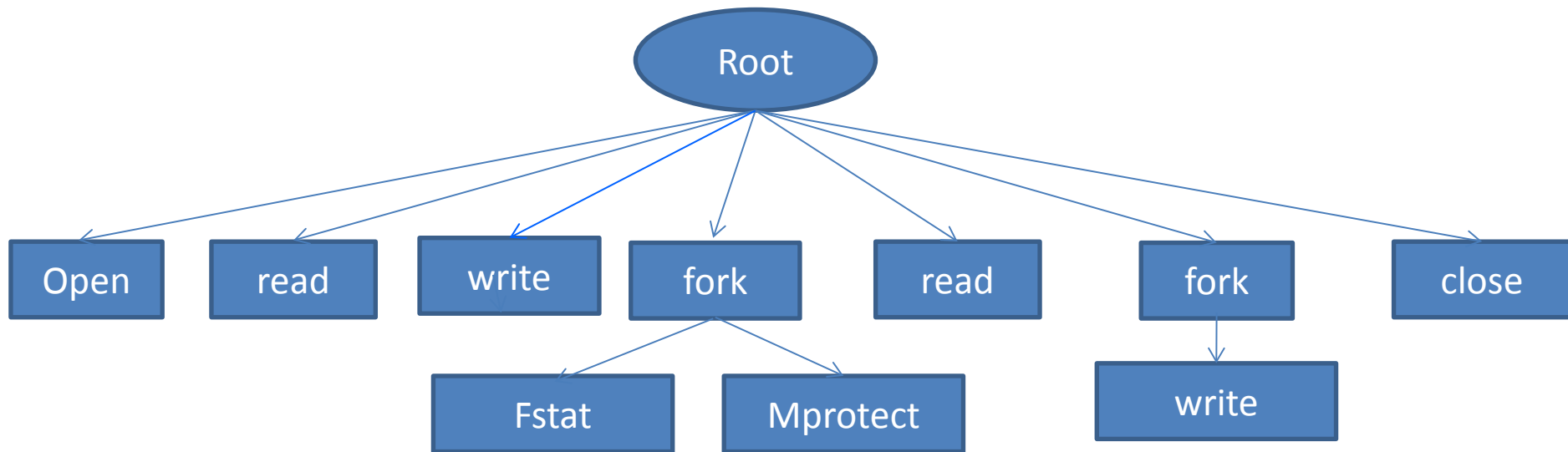
Analysis Methodology – Malware infection tree



Analysis Methodology – Ordered System Call Graph



Analysis Methodology – Unordered System Call Graph



Analysis Framework - 1

Two versions

1. analyze Android apps with interaction
2. and without interaction

Both run in Android SDK emulator on a linux VM.

Without interaction: runs the main activity of an app and collects the strace for 3 minutes

With interaction:

- leverage AppsPlayground (William Enck NCSU) for interaction
- attempt to run each app until all activities visited
- collect strace, logcat, network information, apk and signature data
- can run up to 30 minutes, average around 4 minutes to complete all activities



Analysis Framework - 2

- web based GUI created, accessible via website for public use.
- currently have 13K known malicious and 9K known benign android apps.
- all benign apps downloaded from Google Play
- Current analysis results are positive using malware infection trees.
 - with no interaction:
 - 11800 malicious and 7729 benign android app samples (2009-2014)
 - 27dimension feature vector per node using SVM
 - 94% detection accuracy, 6.97%FN, 7.57%FP
 - unordered neighboring combined with intersection kernel
- machine learning done by Dr. Cavazos's group in Udel.



Gangplank Upload Multi Reports Welcome, d1rdelmis Logout

Gangplank

Mobile Malware Analysis

Reports

File	Status	Date Completed	Analysis
com.classic.Pool.apk	SUCCESS	Oct. 6, 2014, 5:34 p.m.	View Report
com.surpau.ledflashlight.parete.apk	SUCCESS	Oct. 6, 2014, 5:35 p.m.	View Report



Gangplank Upload Multi Reports Welcome, distadmin Logout

Gangplank

Mobile Malware Analysis

- Analysis
- Logs
- Activities
- Services
- Permissions
- File Types
- Receivers
- Providers

Apk General Information

com.classic.Pool.apk
 Path: /media/shere/93279bae-1110-4d5d-8061-85141b99363e

Logs

```
[11-05 01:48:38.254:1389:1699 W/ApiMonitor ]
PID 1389 (com.android.phone) invokes Intent.setAction(com.android.internal.telephony.gprs-data-stall) at 20131105_014838

[11-05 01:48:38.374:1389:1389 W/ApiMonitor ]
PID 1389 (com.android.phone) invokes Intent.setAction(com.android.internal.telephony.gprs-data-stall) at 20131105_014838

[11-05 01:48:38.414:1389:1389 W/ApiMonitor ]
PID 1389 (com.android.phone) invokes Intent.intent(com.android.internal.telephony.gprs-data-stall) at 20131105_014838

[11-05 01:48:38.484:1136:1292 W/ApiMonitor ]
PID 1136 (N/A) invokes Intent.setAction(com.android.internal.telephony.gprs-data-stall) at 20131105_014838

[11-05 01:49:38.565:1389:1700 W/ApiMonitor ]
PID 1389 (com.android.phone) invokes Intent.setAction(com.android.internal.telephony.gprs-data-stall) at 20131105_014938

[11-05 01:49:38.634:1389:1389 W/ApiMonitor ]
PID 1389 (com.android.phone) invokes Intent.setAction(com.android.internal.telephony.gprs-data-stall) at 20131105_014938

[11-05 01:49:38.654:1389:1389 W/ApiMonitor ]
PID 1389 (com.android.phone) invokes Intent.intent(com.android.internal.telephony.gprs-data-stall) at 20131105_014938

[11-05 01:49:38.684:1136:1312 W/ApiMonitor ]
PID 1136 (N/A) invokes Intent.setAction(com.android.internal.telephony.gprs-data-stall) at 20131105_014938

[11-05 01:50:13.063:1295:1295 W/ApiMonitor ]
PID 1295 (android.process.acore) invokes ContentResolver.acquireUnstableProvider(com.android.contacts) at 20131105_015013.
The return value: android.content.ContentProvider$Transport@410900e0

[11-05 01:50:14.614:1519:1656 W/ApiMonitor ]
PID 1519 (com.android.contacts) invokes AccountManager.getAuthenticatorTypes(void) at 20131105_015014

[11-05 01:50:14.614:1136:1353 W/ApiMonitor ]
PID 1136 (system) invokes AccountManagerService.getAuthenticatorTypes(void) at 20131105_015014

[11-05 01:50:14.644:1519:1656 W/ApiMonitor ]
PID 1519 (com.android.contacts) invokes AccountManager.getAccounts(void) at 20131105_015014

[11-05 01:50:20.234:2039:2039 V/MalwareAnalysisFramework ]
MalwareAnalysisFramework.onCreate() - @@@@com.gsu.b60.BigWinSlots.GS60_Android_Main@410502e8 @@@@

[11-05 01:50:20.674:2039:2039 W/ApiMonitor ]
PID 2039 (com.gsu.b60.BigWinSlots) invokes ContentResolver.acquireUnstableProvider(settings) at 20131105_015020. The
return value: android.content.ContentProviderProxy@41081100

[11-05 01:50:20.854:2039:2039 V/MalwareAnalysisFramework ]
MalwareAnalysisFramework.onResume() - @@@@com.gsu.b60.BigWinSlots.GS60_Android_Main@410502e8 @@@@
```



Gangplank Upload Multi Reports Welcome, dslalain Logout

isAvailable: false (wifi_p2p) - isConnected ? false

- Analysis
- Logs
- Activities
- Services
- Permissions
- File Types
- Receivers
- Providers

Activities

Total Activities

com.gosub60.BigWinSlots.GS60_Android_Main

Activities visited

Date: 2013-11-05 01:43:29.624
 Activity: com.gosub60.BigWinSlots.GS60_Android_Main
 Method: Launcher

Date: 2013-11-05 01:43:30.48
 Activity: com.gosub60.BigWinSlots.GS60_Android_Main
 Method: onCreate()

Date: 2013-11-05 01:43:31.108
 Activity: com.gosub60.BigWinSlots.GS60_Android_Main
 Method: onResume()

Date: 2013-11-05 01:44:03.012
 Activity: com.android.launcher2.Launcher
 Method: onResume()

Date: 2013-11-05 01:44:11.735
 Activity: com.gosub60.BigWinSlots.GS60_Android_Main
 Method: Launcher

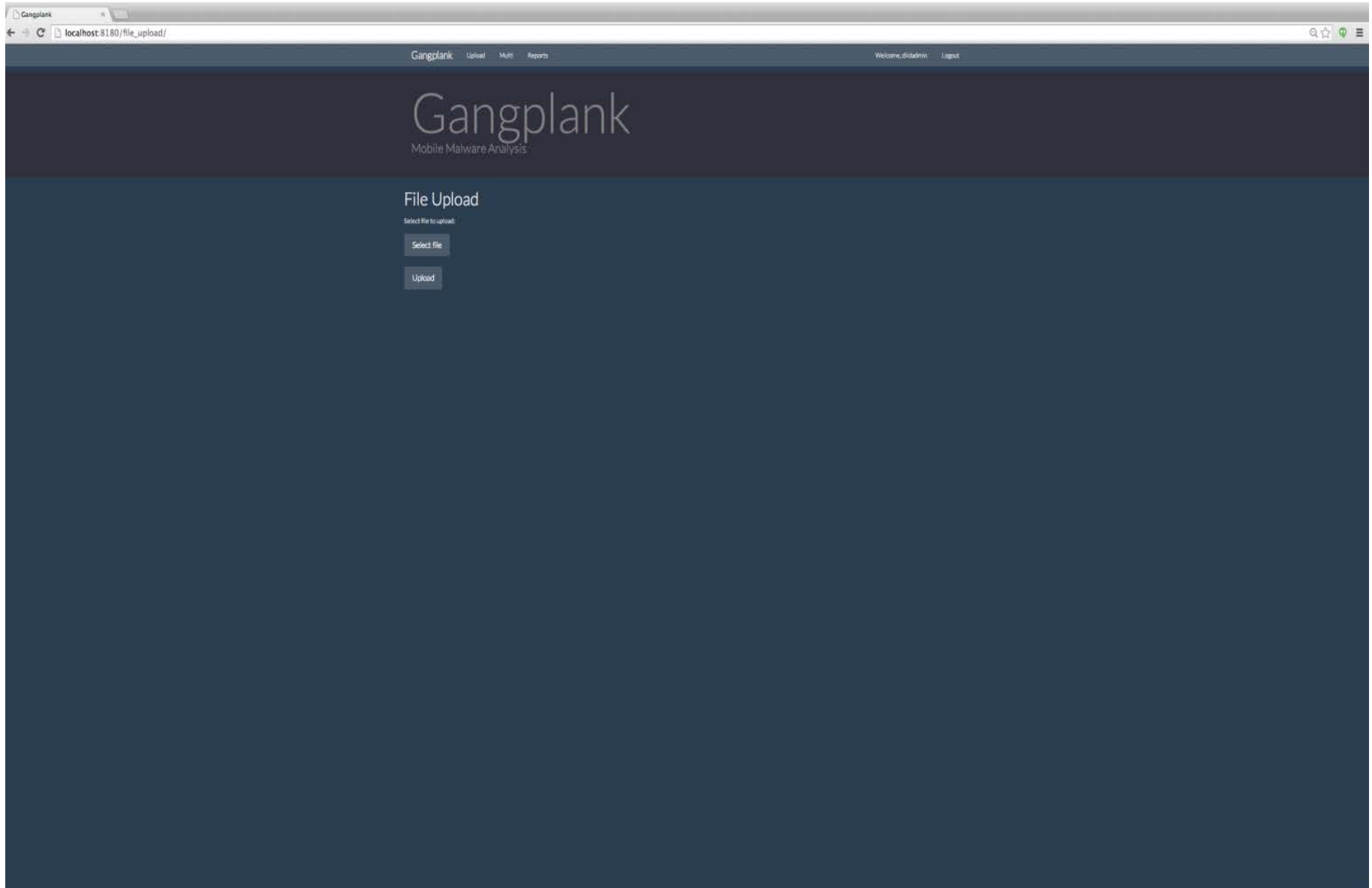
Date: 2013-11-05 01:44:13.093
 Activity: com.gosub60.BigWinSlots.GS60_Android_Main
 Method: onCreate()

Date: 2013-11-05 01:44:13.421
 Activity: com.gosub60.BigWinSlots.GS60_Android_Main
 Method: onResume()

Services

com.gosub60.BigWinSlots.GS60_Android_MicrotransactionMgr_BillingService





Final Thoughts

- Analysis framework accessible via web gui
- 94% detection accuracy based on strace file analysis
- better detection than most major anti-malware engines
- Our accuracy is far better than other anti-malware with newer samples
- Majority of malicious activity occurs in first 2 seconds of execution
- Should continue to improve features to reduce FN and FP
- Paper being submitted to IEEE Security and Privacy

Interested in knowing more???

- Jose Andre Morales, Ph.D.
- jamorales@cert.org



Contact Information

Presenter / Point of Contact

Dr. Jose A. Morales

SEI: CERT

Email: jamorale@sei.cmu.edu

Joseph Yankel

SEI: CERT

Email: jdyanke@cert.org

U.S. Mail

Software Engineering Institute

Customer Relations

4500 Fifth Avenue

Pittsburgh, PA 15213-2612

USA

Customer Relations

Email: info@sei.cmu.edu

Telephone: +1 412-268-5800

SEI Phone: +1 412-268-5800

SEI Fax: +1 412-268-6257

