EviHunter

Android App Forensic Analysis and Evidence Database

Chris Cheng, Brody Concannon, Chen Shi, Chenliang Xu, Zhen Xu, Neil Gong, and Yong Guan
Department of Electrical and Computer Engineering
Iowa State University

csafe Center for Statistics and Applications in Forensic Evidence

NIST National Institute of Standards and Technology U.S. Department of Commerce

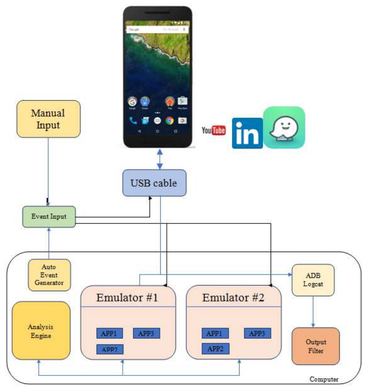
Project Rationale & Goals

>Nowadays mobile device forensics has become a critical and high-demand investigative capability desired by all law enforcement crime labs.

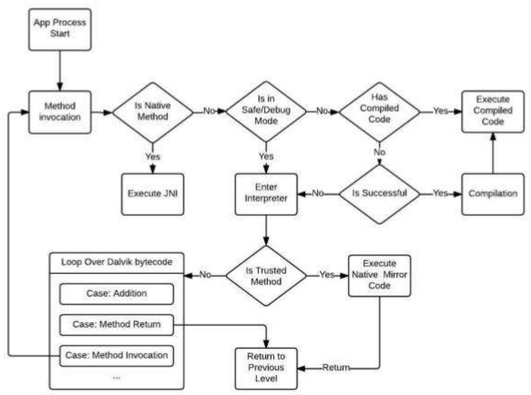
>Objective of this research: We aim at developing EviHunter to automatically analyze and discover possible evidential data from mobile devices, as a 1st step on Android devices, and are creating the largest app evidence database (AED) for law enforcement and security communities.

Design and Platform

EviHunter



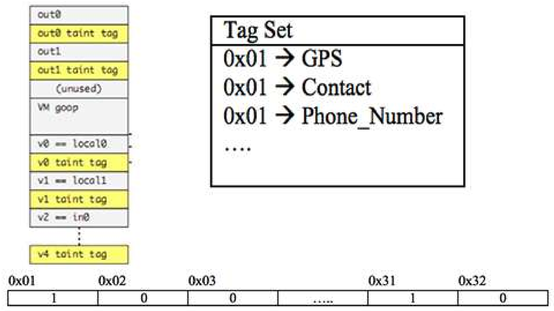
EviHunter System Setup



Simplified ART Platform

>We take Android app APK as input for Static EviHunter and report a list of evidence (types, locations, and syntax/formats). For our dynamic EviHunter, we modified Android ART platform to force the app going through the ART interpreter and bypass the checking of trusted mirror class such that all the java-based code are executed via the interpreter. Furthermore, the modified ART alters the interpreter instruction handling procedures such that our taint based analysis and propagation can be implemented, where our taint propagation rules are summarized in Table 1.

Detailed Methodology and Results

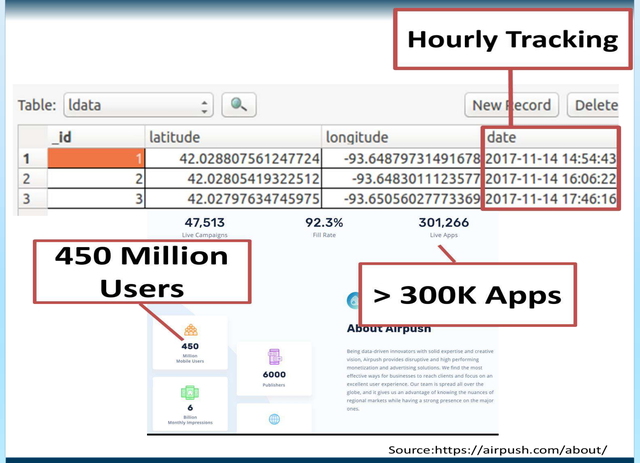


Taint Tag Format

Operations		Propagation Rules: Bit-wise mode	Tag-id mode
Unary Operation: $V_1 = V_2$ move, move-return, …		$T(V_1) \leftarrow T(V_2)$	$T(V_1) \leftarrow T(V_2)$
Binary Operation: $V_1 = V_2 \otimes V_3$ Add, Shift, Xor, …		$T(V_1) \leftarrow T(V_2)$ or $T(V_3)$	$T(V_1) \leftarrow T(V_2) \cup T(V_3)$
Array	aget V_1, V_2, V_3 $V_1 = V_2[V_3]$	$T(V_1) \leftarrow T(V_2[V_3])$ or $T(V_2)$	$T(V_1) \leftarrow T(V_2[V_3]) \cup T(V_2)$
	aput V_1, V_2, V_3 $V_2[V_3] = V_1$	$T(V_2) \leftarrow T(V_2)$ or $T(V_3)$	$T(V_2) \leftarrow T(V_2) \cup T(V_3)$
Static Field	sget V_1, f $V_1 = f$	$T(V_1) \leftarrow T(f)$	$T(V_1) \leftarrow T(f)$
	sput V_1, f $f = V_1$	$T(f) \leftarrow T(V_1)$	$T(f) \leftarrow T(V_1)$
Instance Field	iget V_1, V_2, f $V_1 = V_2.f$	$T(V_1) \leftarrow T(V_2.f)$	$T(V_1) \leftarrow T(V_2.f)$
	iput V_1, V_2, f $V_2.f = V_1$	$T(V_2.f) \leftarrow T(V_1)$	$T(V_2.f) \leftarrow T(V_1)$

Table 1 Taint Propagation Rules

Case Studies: Airpush Advertisement



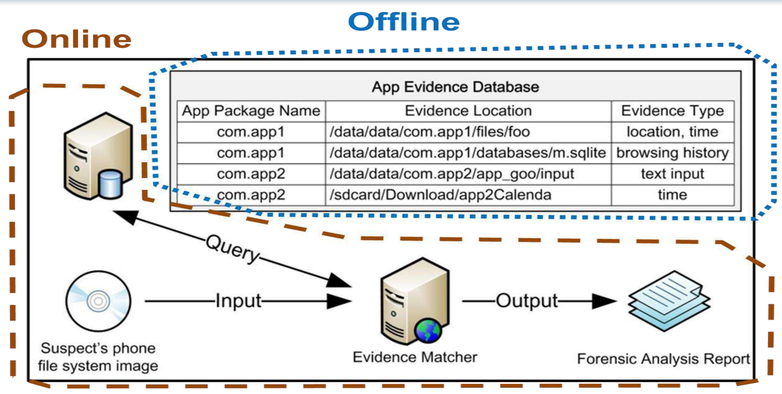
Source:https://airpush.com/about/

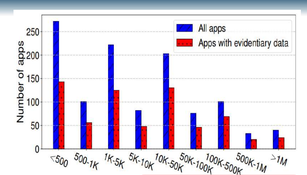
Summary and Future Directions

We have prototyped EviHUnter tools. Some initial success has been demonstrated in accurately discovering evidentiary data from apps. We are building (likely the largest) App Evidence Database (expected over 8 millions of apps) via active large app collections from over 50 app stores across the world. Selected publications include:

1. Chris Chao-Chun Cheng, Chen Shi, Neil Zhenqiang Gong, and Yong Guan, "EviHunter: Identifying Digital Evidence in the Permanent Storage of Android Devices via Static Analysis," in Proceedings of the 25th ACM Conference on Computer and Communications Security (ACM CCS 2018), Toronto, Canada, October 15-19, 2018
2. Zhen Xu, Chen Shi, Chris Cheng, Neil Gong and Yong Guan, "A Dynamic Taint Analysis Tool for Android App Forensics," in *Proceedings of the 12th International Workshop on Systematic Approaches to Digital Forensics Engineering (SADFE 2018)*, Held in Conjunction with the 39th IEEE Symposium on Security and Privacy (SP 2018), San Francisco, CA, USA, May 24, 2018 (Best Paper Award)

App Evidence Database (AED) and Evaluation Results





Evidence Type	SQLite DB	SharedPreferences	Ordinary File
Location	145	195	151
Time	343	1129	435
Visited URL	20	25	19
Text Input	166	411	186

The material presented here is based upon work supported by the National Institute of Science and Technology under Award No. 70NANB15H176. The Center for Statistics and Applications in Forensic Evidence (CSAFE) team works to build a statistically sound and scientifically solid foundation for the analysis and interpretation of forensic evidence to grow competence in the forensic sciences and legal communities, and bring together forensic practitioners and other stakeholders through educational and training opportunities.