TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones

William Enck (PSU), Peter Gilbert (Duke), Byung-Gon Chun (Intel), Landon P. Cox (Duke), Jaeyeon Jung (Intel), Patrick McDaniel (PSU), and Anmol N. Sheth (Intel)

Smartphone Security and Privacy

Smartphones allow users to download and run third-party applications from the Internet. Many of these applications provide valuable utility by using privacy sensitive information such as location to the user experience. However, once an application accesses information, it is very hard to know what it will do with that information, forcing users to blindly trust that their information will not be abused.

Privacy sensitive information on smartphones includes:

- Location
- Microphone
- Camera
- Phone identifiers (IMEI, IMSI, ICC-ID, Phone Number)

Goal: *Monitor app behavior to determine when privacy sensitive information leaves the phone.*

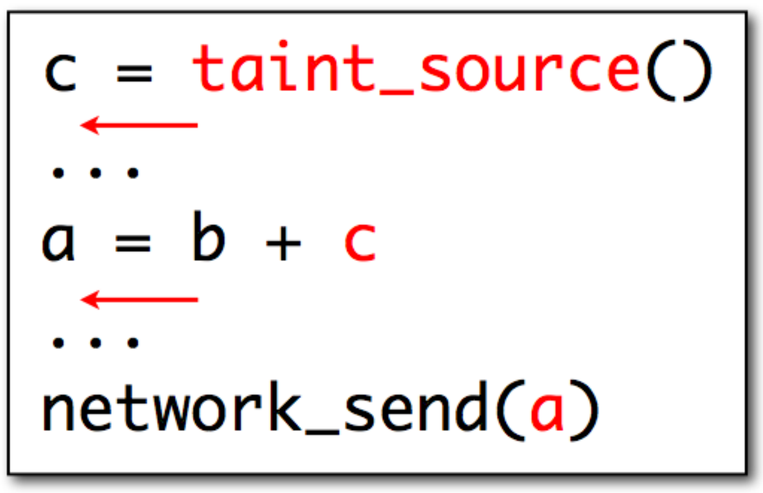
Challenges:

- Smartphones are resource constrained devices.
- Third-party applications are entrusted with several types of privacy sensitive information.
- Context-based privacy information is dynamic and can be difficult to identify even when sent in the clear.
- Applications can share information.

Taint Tracking

Dynamic taint analysis, also known as "taint tracking," is a technique that tracks information dependencies from an origin.

Conceptual Idea: *taint source*, *taint propagation*, *taint sink*

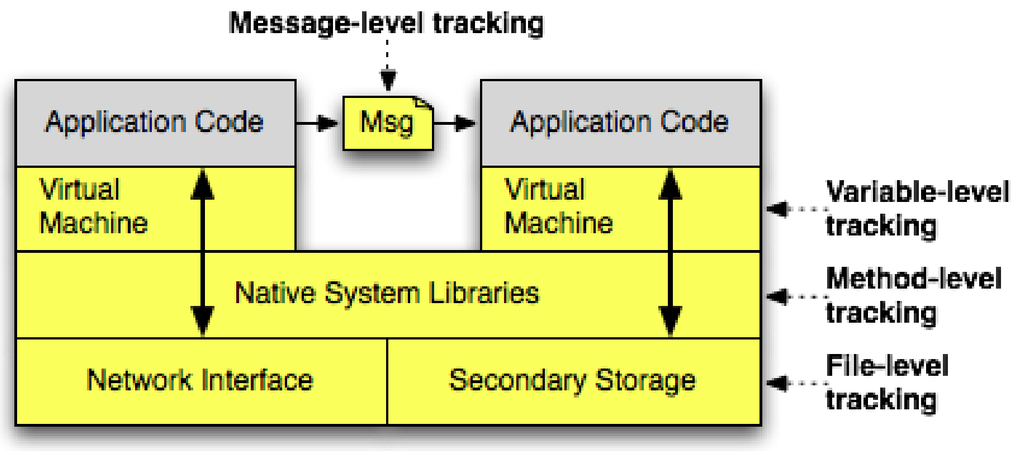


Limitations: performance and granularity tradeoffs

TaintDroid

TaintDroid is a system-wide integration of taint tracking for Android.

- Variable tracking throughout Dalvik VM environment
- Patches state after native method invocation
- Extends tracking between applications and to storage



Analysis Results

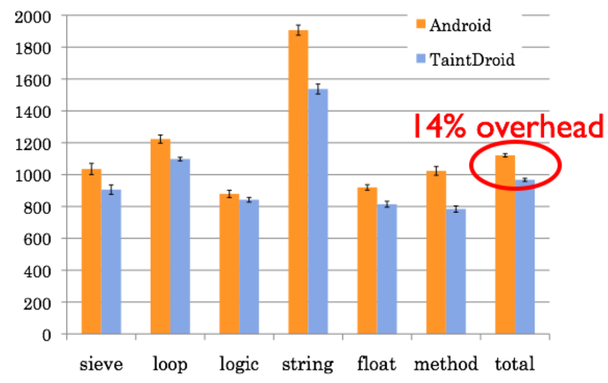
Randomly selected 30 applications with a bias on popularity and access to *Internet*, *location*, *microphone*, and *camera*.

applications	#	permissions
The Weather Channel, Cetos, Solitarie, Movies, Babble, Manga Browser	6	
Bump, Wertago, Antivirus, ABC --- Animals, Traffic Jam, Hearts, Blackjack, Horoscope, 3001 Wisdom Quotes Lite, Yellow Pages, Datelefonbuch, Astrid, BBC News Live Stream, Ringtones	14	
Layar, Knocking, Coupons, Trapster, Spongebot Slide, ProBasketBall	6	
MySpace, Barcode Scanner, ixMAT	3	
Evernote	1	

- 15 apps shared location with advertisement servers
- 7 apps shared IMEI with remote server without informing user
- 2 apps shared phone number, IMEI, ICC-ID with remote server

Performance

CaffeineMark 3.0 benchmark
(higher is better)



Memory overhead: 4.4%

IPC overhead: 27%

Macro-benchmarks:

- App load 3% (2ms)
- Address book: (<20ms) 5.5% create, 18% read
- Phone call: 10% (10ms)
- Take picture: 29% (0.5s)

Next Steps

TaintDroid provides a necessary component for achieving smartphone privacy by reporting how applications use information; however, it does not distinguish between desired use and abuse. Reported behavior may be shown to users, used by enforcement policies, or distributed by third-party security services evaluating app privacy. Each scenario has unique research challenges for investigation.

Supported by NSF and Intel Corp.