ProfileDroid: Multi-layer Profiling of Android Applications

Xuetao Wei
Lorenzo Gomez
Iulian Neamtiu
Michalis Faloutsos

How do we know what is occuring in an app? Description, connections, services?

>550 000 apps on 

Goal - Complete app profile given limited:

-Time
-User Effort
-Cost

Comprehensive profile:

-resource use(sys calls/network traffic)
-device resources & permissions(camera, microphone, sensors)
-entities app communicates(cloud/third party)

Potential Users:

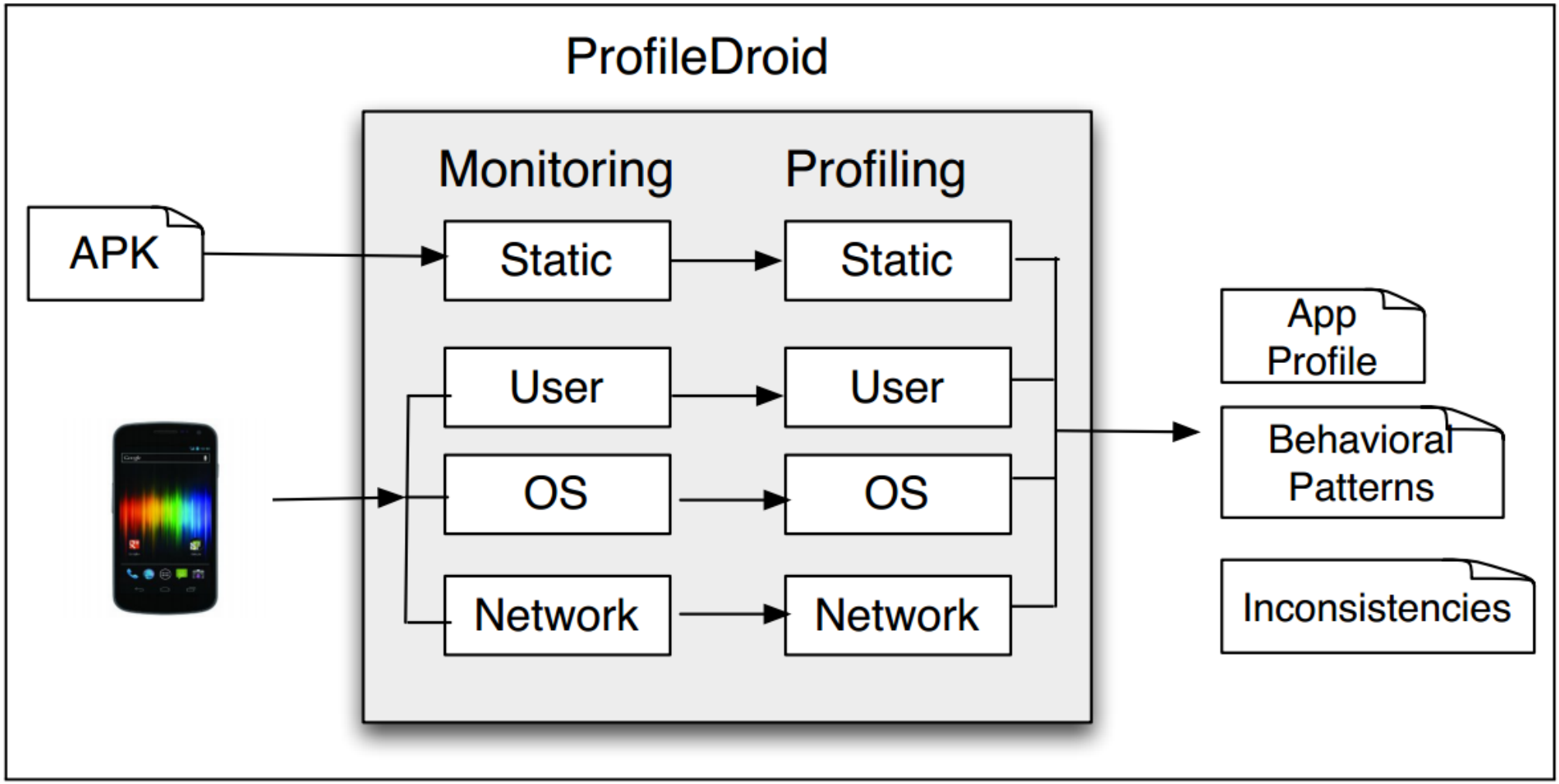
-app developers
-system administrators
-owner Android app market
-end user

Profile Uses:

-enhance user control
-improve user experience
-assess performance & security
-facilitate troubleshooting

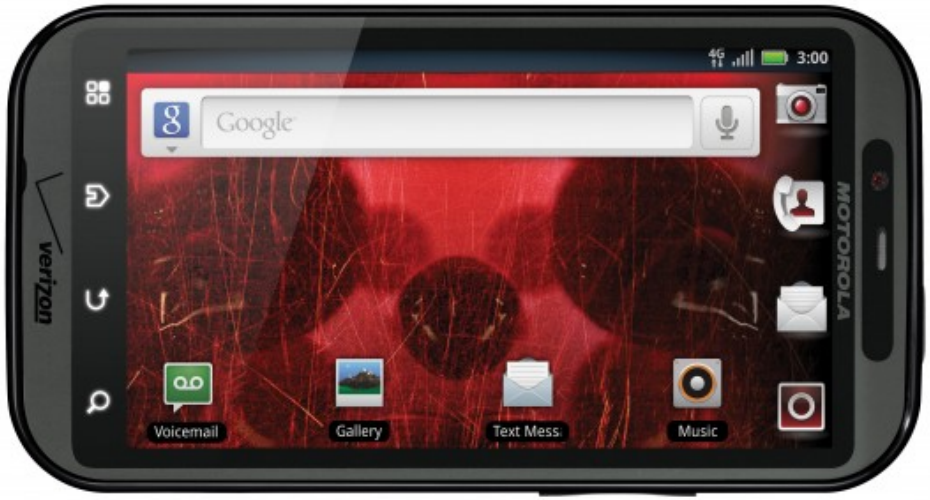
Proposed Solution → **ProfileDroid**

Comprehensive, systematic app profile spanning 4 layers



Testing Method

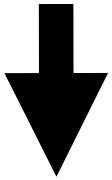
-Motorola Droid Bionic phone
-Android 2.3.4
-Linux Kernel 2.6.35
-Profile 27 Apps
-19 Free
-8 Paid Counterparts
-30 runs/app



ProfileDroid Overview

Each layer composed of monitoring & profiling

Monitor running app on device



Information fed into computer and profiled

Layer Implementation I

Static Layer

-examine apk using *apktool*
-Manifest.xml
-/smali bytecode

User Layer

-user generated events
-touchscreen, sensors
-system debug & log msg output using *adb*

Layer Implementation II

OS Layer

-system calls using *strace*
- 4 classifications (filesys, network,VM/IPC, misc)

Network Layer

-data packets using *tcpdump*
-parse, domain-resolve & classify traffic

Apps

App name	Category
Dictionary.com, Dictionary.com-$$	Reference
Tiny Flashlight	Tools
Zedge	Personalization
Weather Bug, Weather Bug-$$	Weather
Advanced Task Killer, Advanced Task Killer-$$	Productivity
Flixster	Entertainment
Picsay, Picsay-$$	Photography
ESPN	Sports
Gasbuddy	Travel
Pandora	Music & Audio
Shazam, Shazam-$$	Music & Audio
Youtube	Media & Video
Amazon	Shopping
Facebook	Social
Dolphin, Dolphin-$$	Communication (Browsers)
Angry Birds, Angry Birds-$$	Games
Craigslist	Business
CNN	News & Magazines
Instant Heart Rate, Instant Heart Rate-$$	Health & Fitness

>1 000 000 downloads
Top 130 free apps

Many Categories
-entertainment
-productivity
-tools

Experiment Conditions

-no other apps running

-Wifi strong signal

-install one app at a time

-3 users x 10 runs/app x 5 minutes/run

Layer Analysis: Static

App	Internet	GPS	Camera	Microphne	Bluetooth	Telephony
Dictionary.com	✓			I		I
Dictionary.com-$$	✓			I		I
Tiny Flashlight	✓		✓			
Zedge	✓					
Weather Bug	✓	✓				
Weather Bug-$$	✓	✓				
Advanced Task Killer	✓					
Advanced Task Killer-$$	✓					
Flixster	✓	✓				
Picsay	✓					
Picsay-$$	✓					
ESPN	✓					
Gasbuddy	✓	✓				
Pandora	✓				✓	
Shazam	✓	✓		✓		
Shazam-$$	✓	✓		✓		
YouTube	✓					
Amazon	✓		✓			
Facebook	✓	✓	I			✓
Dolphin	✓	✓				
Dolphin-$$	✓	✓				
Angry Birds	✓					
Angry Birds-$$	✓					
Craigslist	✓					
CNN	✓		✓			
Instant Heart Rate	✓		✓		I	I
Instant Heart Rate-$$	✓		✓		I	I

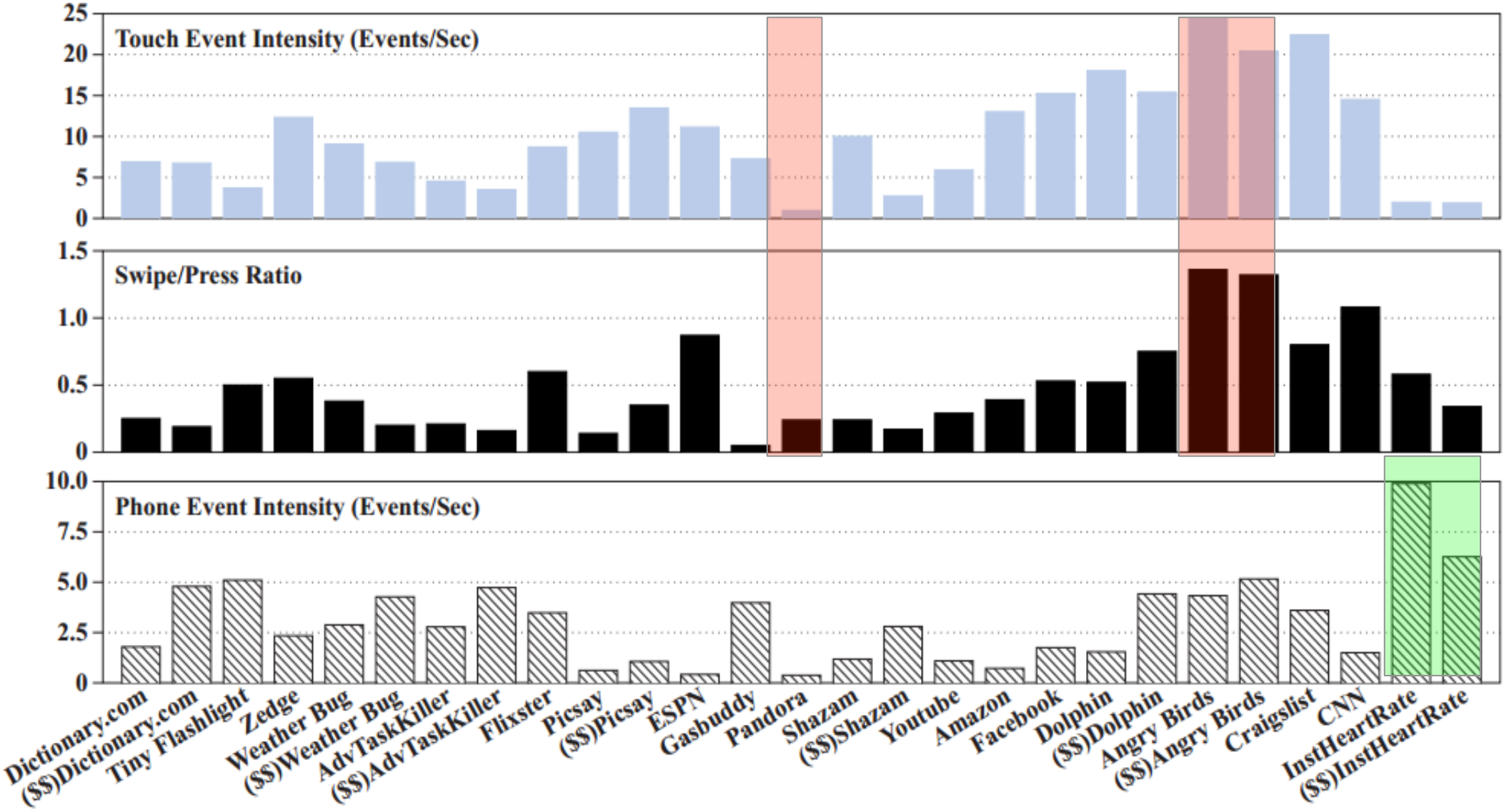
Analyze app without running it (apk/ manifest)

Functionality

Intent

Layer Analysis: User

Input events from user interaction → presses/swipes
Phone events → generated by phone (sensor readings)



Layer Analysis: OS

App	Syscall intensity (calls/sec.)	FS (%)	NET (%)	VM& IPC (%)	MISC (%)
Dictionary.com	1025.64	3.54	1.88	67.52	27.06
Dictionary.com-$$	492.90	7.81	4.91	69.48	17.80
Tiny Flashlight	435.61	1.23	0.32	77.30	21.15
Zedge	668.46	4.17	2.25	75.54	18.04
Weather Bug	1728.13	2.19	0.98	67.94	28.89
Weather Bug-$$	492.17	1.07	1.78	75.58	21.57
AdvTaskKiller	75.06	3.30	0.01	65.95	30.74
AdvTaskKiller-$$	30.46	7.19	0.00	63.77	29.04
Flixster	325.34	2.66	3.20	71.37	22.77
Picsay	319.45	2.06	0.01	75.12	22.81
Picsay-$$	346.93	2.43	0.16	74.37	23.04
ESPN	1030.16	2.49	2.07	87.09	8.35
Gasbuddy	1216.74	1.12	0.32	74.48	24.08
Pandora	286.67	2.92	2.25	70.31	24.52
Shazam	769.54	6.44	2.64	72.16	18.76
Shazam-$$	525.47	6.28	1.40	74.31	18.01
YouTube	246.78	0.80	0.58	77.90	20.72
Amazon	692.83	0.42	6.33	76.80	16.45
Facebook	1030.74	3.99	2.98	72.02	21.01
Dolphin	850.94	5.20	1.70	71.91	21.19
Dolphin-$$	605.63	9.05	3.44	68.45	19.07
Angry Birds	1047.19	0.74	0.36	82.21	16.69
Angry Birds-$$	741.28	0.14	0.04	85.60	14.22
Craigslist	827.86	5.00	2.47	73.81	18.72
CNN	418.26	7.68	5.55	71.47	15.30
InstHeartRate	944.27	7.70	1.73	75.48	15.09
InstHeartRate-$$	919.18	12.25	0.14	72.52	15.09

System Call Intensity

System Call class
-File System
-Network
-VM&IPC
-Misc

49 system calls used of possible 370

Layer Analysis: Network

Data communication via Wifi or 3G/4G

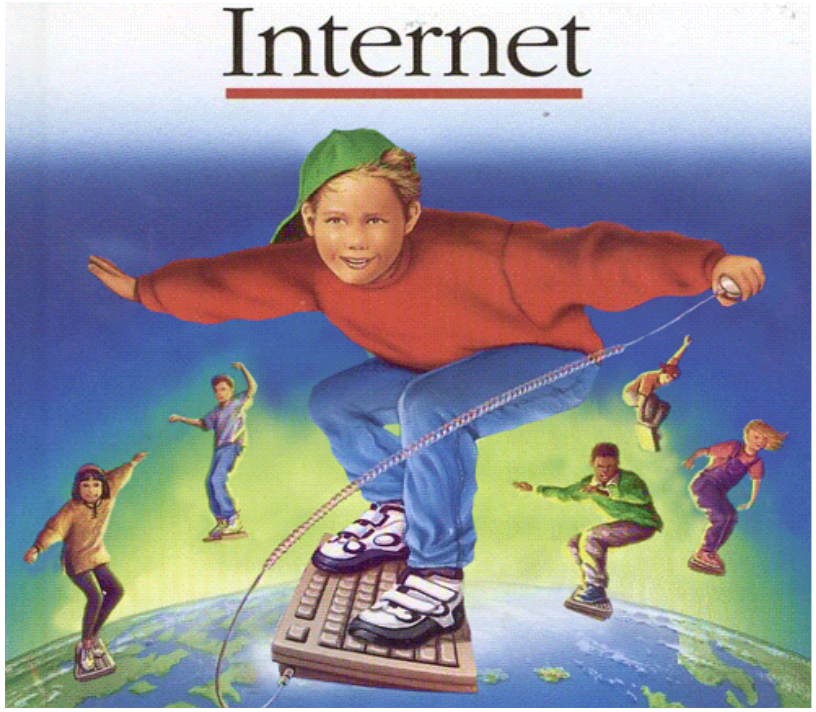
Traffic intensity

CDN+Cloud traffic

Traffic origin

Third party traffic

Google traffic



Incoming/Outgoing traffic ratio

distinct traffic sources

Percentage of traffic HTTP or HTTPS

Layer Analysis: Network

App	Traffic intensity (bytes/sec.)	Traffic In/Out (ratio)	Origin (%)	CDN+Cloud (%)	Google (%)	Third party (%)	Traffic sources	HTTP/HTTPS split (%)
Dictionary.com	1450.07	1.94	–	35.36	64.64	–	8	100/–
Dictionary.com-$$	488.73	1.97	0.02	1.78	98.20	–	3	100/–
Tiny Flashlight	134.26	2.49	–	–	99.79	0.21	4	100/–
Zedge	15424.08	10.68	–	96.84	3.16	–	4	100/–
Weather Bug	3808.08	5.05	–	75.82	16.12	8.06	13	100/–
Weather Bug-$$	2420.46	8.28	–	82.77	6.13	11.10	5	100/–
AdvTaskKiller	25.74	0.94	–	–	100.00	–	1	91.96/8.04
AdvTaskKiller-$$	–	–	–	–	–	–	0	–/–
Flixster	23507.39	20.60	2.34	96.90	0.54	0.22	10	100/–
Picsay	4.80	0.34	–	48.93	51.07	–	2	100/–
Picsay-$$	320.48	11.80	–	99.85	0.15	–	2	100/–
ESPN	4120.74	4.65	–	47.96	10.09	41.95	5	100/–
Gasbuddy	5504.78	10.44	6.17	11.23	81.37	1.23	6	100/–
Pandora	24393.31	28.07	97.56	0.91	1.51	0.02	11	99.85/0.15
Shazam	4091.29	3.71	32.77	38.12	15.77	13.34	13	100/–
Shazam-$$	1506.19	3.09	44.60	55.36	0.04	–	4	100/–
YouTube	109655.23	34.44	96.47	–	3.53	–	2	100/–
Amazon	7757.60	8.17	95.02	4.98	–	–	4	99.34/0.66
Facebook	4606.34	1.45	67.55	32.45	–	–	3	22.74/77.26
Dolphin	7486.28	5.92	44.55	0.05	8.60	46.80	22	99.86/0.14
Dolphin-$$	3692.73	6.05	80.30	1.10	5.80	12.80	9	99.89/0.11
Angry Birds	501.57	0.78	–	73.31	10.61	16.08	8	100/–
Angry Birds-$$	36.07	1.10	–	88.72	5.79	5.49	4	100/–
Craigslist	7657.10	9.64	99.97	–	–	0.03	10	100/–
CNN	2992.76	5.66	65.25	34.75	–	–	2	100/–
InstHeartRate	573.51	2.29	–	4.18	85.97	9.85	3	86.27/13.73
InstHeartRate-$$	6.09	0.31	–	8.82	90.00	1.18	2	20.11/79.89

Results Analysis – Multi-layer Intensity

Tuple consisting of (static, user, OS, network) intensity

App	Static (# of func.)	User (events/ sec.)	OS (syscall/ sec.)	Network (bytes/ sec.)
Dictionary.com	L	M	H	M
Dictionary.com-$$	L	M	M	M
Tiny Flashlight	M	L	M	L
Zedge	L	M	M	H
Weather Bug	M	M	H	M
Weather Bug-$$	M	M	M	M
AdvTaskKiller	L	M	L	L
AdvTaskKiller-$$	L	M	L	L
Flixster	M	M	L	H
Picsay	L	M	L	L
Picsay-$$	L	M	M	M
ESPN	L	M	H	M
Gasbuddy	M	M	H	M
Pandora	M	L	L	H
Shazam	H	L	M	M
Shazam-$$	H	L	H	M
YouTube	L	M	M	H
Amazon	M	M	M	H
Facebook	H	H	H	M
Dolphin	M	H	M	H
Dolphin-$$	M	H	M	M
Angry Birds	L	H	M	M
Angry Birds-$$	L	H	H	L
Craigslist	L	H	H	H
CNN	M	M	M	M
InstHeartRate	M	L	H	M
InstHeartRate-$$	M	L	H	L

Layer	Min	Q1	Med	Q3	Max
Static	1	1	2	2	3
User	0.57	3.27	7.57	13.62	24.42
OS	30.46	336.14	605.63	885.06	1728.13
Net	0	227.37	2992.76	6495.53	109655.23

Min < L < Q1

Q1 < M < Q3

Q3 < H < Max

Easy method to classify apps into coarse behavioural categories

Results Analysis – Cross-layer Intensity

Behaviour across layers

-identify potential discrepancies

-further characterization when one layer insufficient

Network Traffic Disambiguation
-cross check user & network layers, distinguish advertisement and expected traffic

Application Disambiguation
-behavioural fingerprinting,
eg file manager vs database

Results Analysis – Free/Paid Apps

Static Layer
-no difference

User Layer
-similar behaviour, same GUI between versions

OS Layer
-free app system call significantly higher (50-100%)
-lower performance, higher energy consumption

Network Layer
-majority of paid apps show reduced net traffic, fewers ads/analytics
-paid apps communicate to fewer sources

Results Analysis – VM&IPC Security/ Performance trade-off

Apps isolated from hardware via VM

Apps isolated from each other on seperate VM copies

Isolation provides security and reliability advantages

Disadvantage is high overhead from running bytecode
on top of VM and significant IPC

VM & IPC account for 63-87% of total system calls

Results Analysis – Network Encryption

Android apps communicate sensitive data (GPS, contacts, account info)

Network analysis reveals most apps don't use HTTPS, only HTTP

¼ of Facebook traffic uses HTTP

HTTPS deployment is lagging on Android, undesirable security implications

App	HTTP/HTTPS split (%)
Dictionary.com	100/–
Dictionary.com-$$	100/–
Tiny Flashlight	100/–
Zedge	100/–
Weather Bug	100/–
Weather Bug-$$	100/–
AdvTaskKiller	91.96/8.04
AdvTaskKiller-$$	–/–
Flixster	100/–
Picsay	100/–
Picsay-$$	100/–
ESPN	100/–
Gasbuddy	100/–
Pandora	99.85/0.15
Shazam	100/–
Shazam-$$	100/–
YouTube	100/–
Amazon	99.34/0.66
Facebook	22.74/77.26
Dolphin	99.86/0.14
Dolphin-$$	99.89/0.11
Angry Birds	100/–
Angry Birds-$$	100/–
Craigslist	100/–
CNN	100/–
InstHeartRate	86.27/13.73
InstHeartRate-$$	20.11/79.89

Results Analysis – Traffic Sources/ Google

Once app receives Internet permission, user blind to communication sources

Most apps communicate with 2 sources

Some apps communicate with 10 or more sources

Paid apps have fewer traffic sources than free apps

Android a Google platform, interesting to note how apps differ in communicating with Google

App	CDN+ Cloud	Google	Third party	Google In/Out
Dictionary.com	3	1	4	2.42
Dictionary.com-$$	2	1	0	1.92
Tiny Flashlight	0	1	3	2.13
Zedge	2	1	1	2.06
Weather Bug	5	1	7	4.93
Weather Bug-$$	3	1	1	13.20
AdvTaskKiller	0	1	0	0.94
AdvTaskKiller-$$	0	0	0	–
Flixster	4	1	4	0.90
Picsay	1	1	0	0.93
Picsay-$$	1	1	0	0.94
ESPN	1	1	3	3.84
Gasbuddy	2	1	2	17.25
Pandora	3	1	6	3.63
Shazam	3	1	8	2.61
Shazam-$$	1	1	1	0.84
YouTube	0	1	0	11.10
Amazon	3	0	0	–
Facebook	2	0	0	–
Dolphin	0	1	17	5.10
Dolphin-$$	0	1	4	2.99
Angry Birds	1	1	6	2.26
Angry Birds-$$	2	1	0	1.04
Craigslist	6	0	3	–
CNN	1	0	0	–
InstHeartRate	1	1	1	2.41
InstHeartRate-$$	1	1	0	1.21

Limitations & Conclusions

- Requires both Android device and PC, lightweight version only on mobile
- No layer collects/ analyses power consumption data, crucial for mobile

- **ProfileDroid** is an Android app monitor and profiling tool
- Characterizes app via a multi-layer approach
- Proposed an ensemble of metric to compare apps
- Used to better understand apps with limited resource commitment to foster improvements in many areas, end-user and development

Thanks for your attention

Questions?