

# What, exactly, is different or new about mobile security?

Dan S. Wallach, Rice University



**MOBILE  
SECURITY  
TECHNOLOGIES  
2017**



# tl;dr

## **The “computers inside the computer”**

Every chip has one or more CPUs inside; they have exploitable bugs

## **Usability issues**

Smaller screens mean fewer security indicators

## **The death of app isolation**

Apps have full Internet access, sensitive privileges, and abuse them

## **Threat models: physical attacks**

Or, defending against the San Bernadino iPhone attack

**The computers inside your computer**

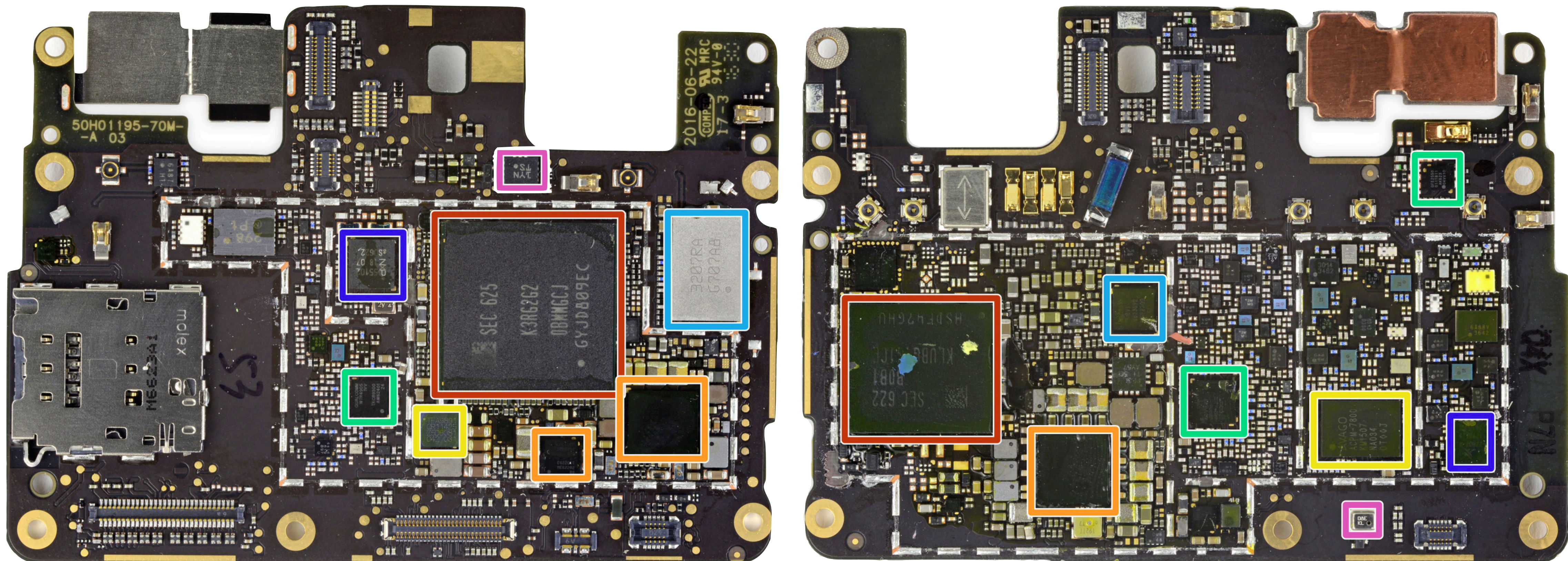


# Have you looked inside a phone lately?

**Each chip has an embedded CPU, typically ARM**

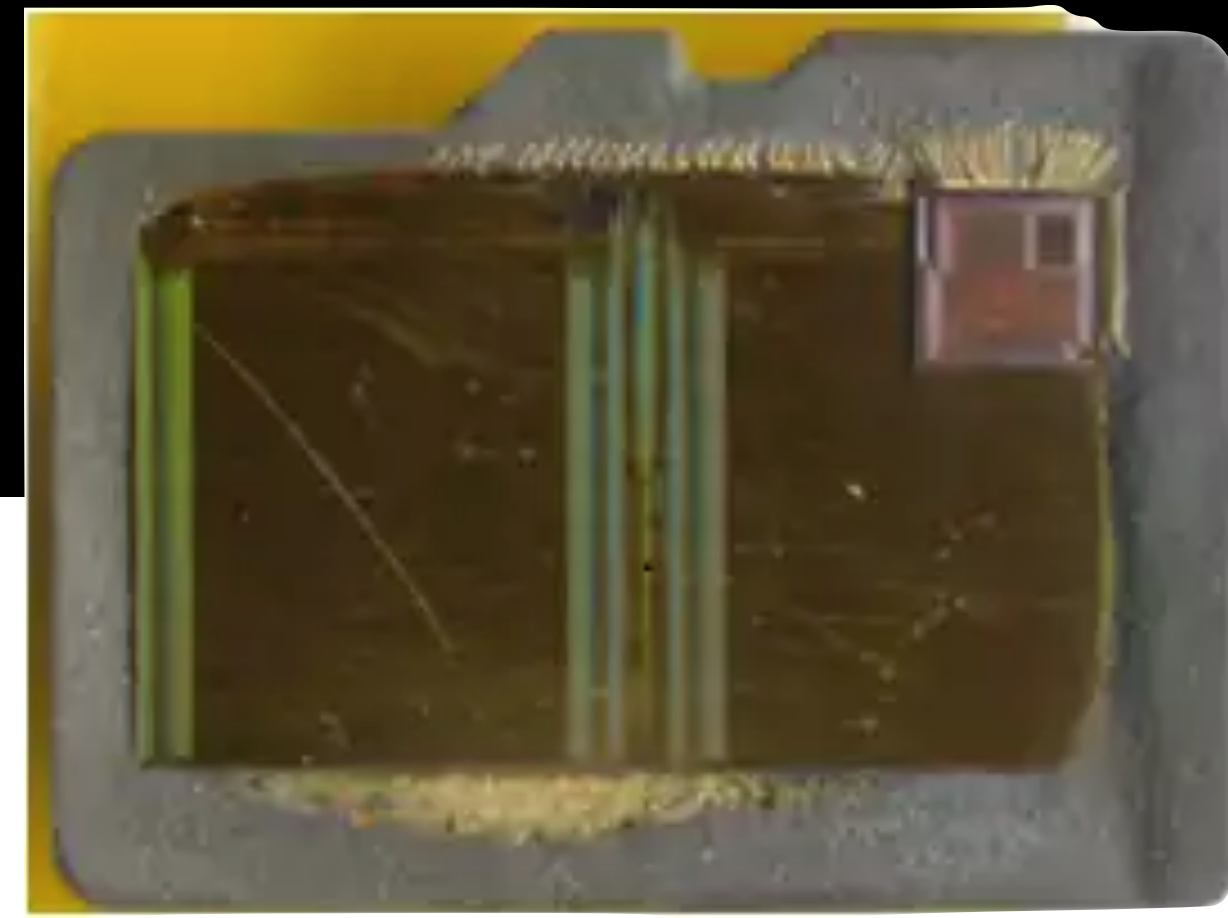
“Firmware” (i.e., software) baked in by vendor, not part of the OS distribution

(Google Pixel photos via iFixit)





# Example: SD card firmware



## **Flash storage is incredibly complicated**

High defect rates, wear leveling / block remapping, etc.

Allows a vanilla filesystem, designed for a hard drive, to “just work”

## **Cheaper to use a general-purpose CPU**

Testing (defect mapping, binning) and runtime (load leveling, remapping) all done in software

Even if 80% of blocks are dead, can still sell as a lower-capacity card



# Quality-control issues?

## Andrew “Bunnie” Huang designed the Chumby

“I realized that all the units failing [in quality control] had Kingston microSD cards from a particular lot code.” (2009)





# Quality-control issues?

## Andrew “Bunnie” Huang designed the Chumby

“I realized that all the units failing [in quality control] had Kingston microSD cards from a particular lot code.” (2009)

“One [Shenzhen] vendor ... interested me; it was literally a mom, pop and one young child sitting in a small stall of the mobile phone market, and **they were busily slapping dozens of non-Kingston marked cards into Kingston retail packaging**. They had no desire to sell to me, but I was persistent; this card interested me in particular because it also had the broken ‘D’ logo but no Kingston marking.”





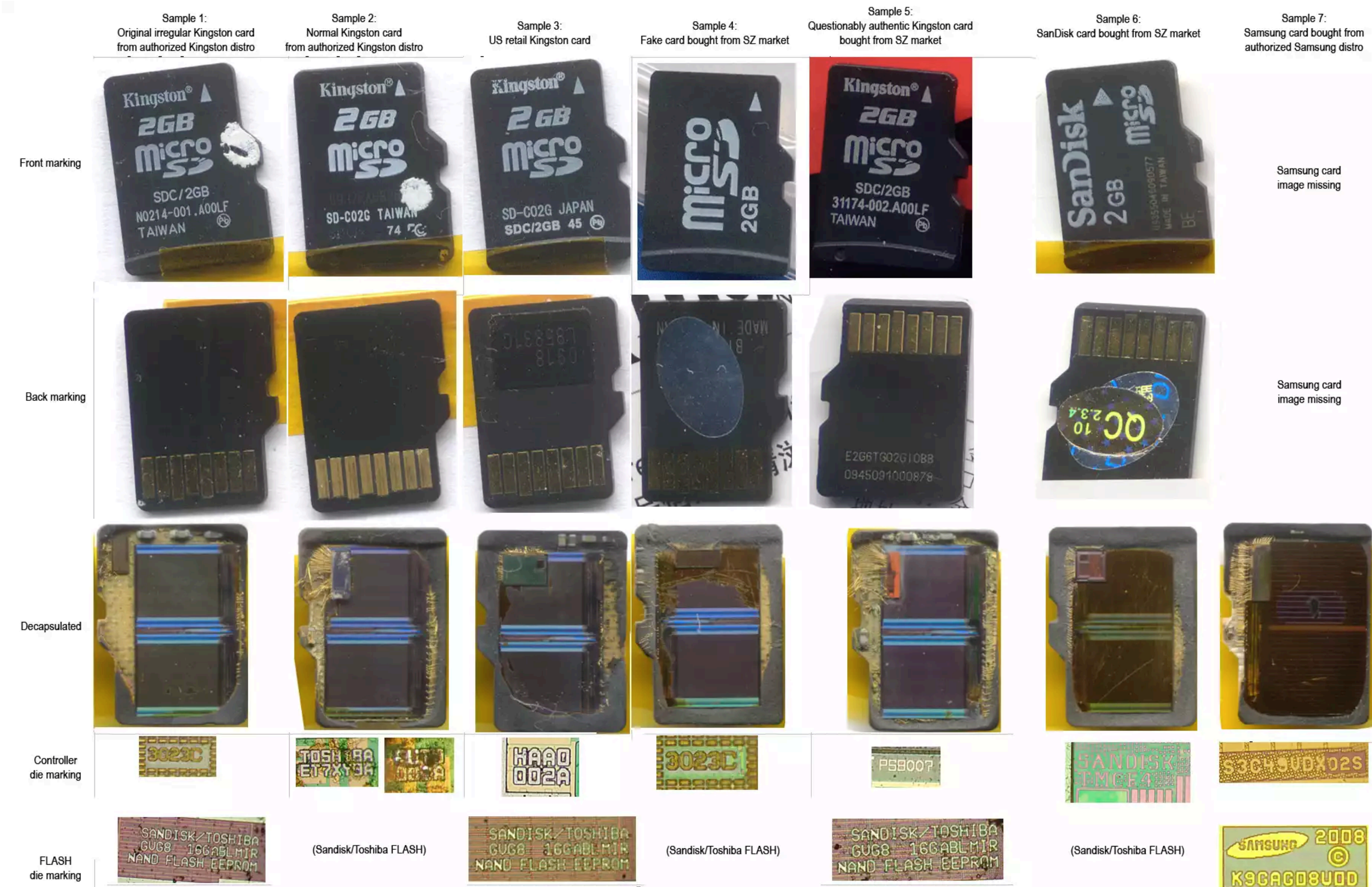
# Counterfeit analysis

## Bunnie bought a bunch of cheap SD cards in Shenzhen

“Normal”: OEM Toshiba

“Sketchy”: alternate  
OEM codes, etc.

Conclusion: Kingston  
resells lower-quality parts  
at tight margins





# Counterfeit analysis

## Bunnie bought a bunch of cheap SD cards in Shenzhen

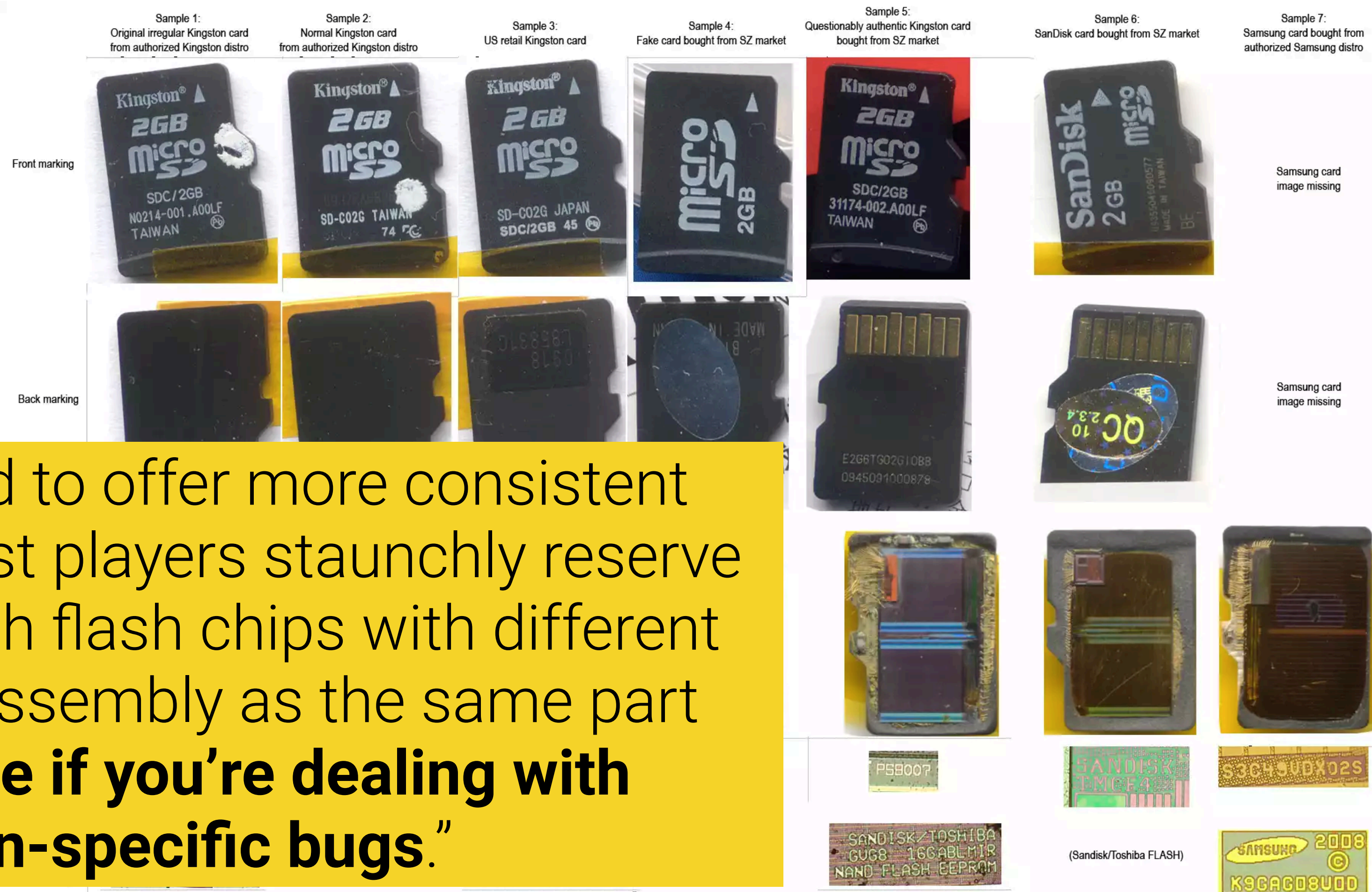
“Normal”: OEM Toshiba

“Sketchy”: alternate OEM codes, etc.

Conclusion: Kingston

resel  
at tig

“Larger vendors will tend to offer more consistent quality, but even the largest players staunchly reserve the right to mix and match flash chips with different controllers, yet sell the assembly as the same part number — **a nightmare if you’re dealing with implementation-specific bugs.**”





# SD firmware hacking

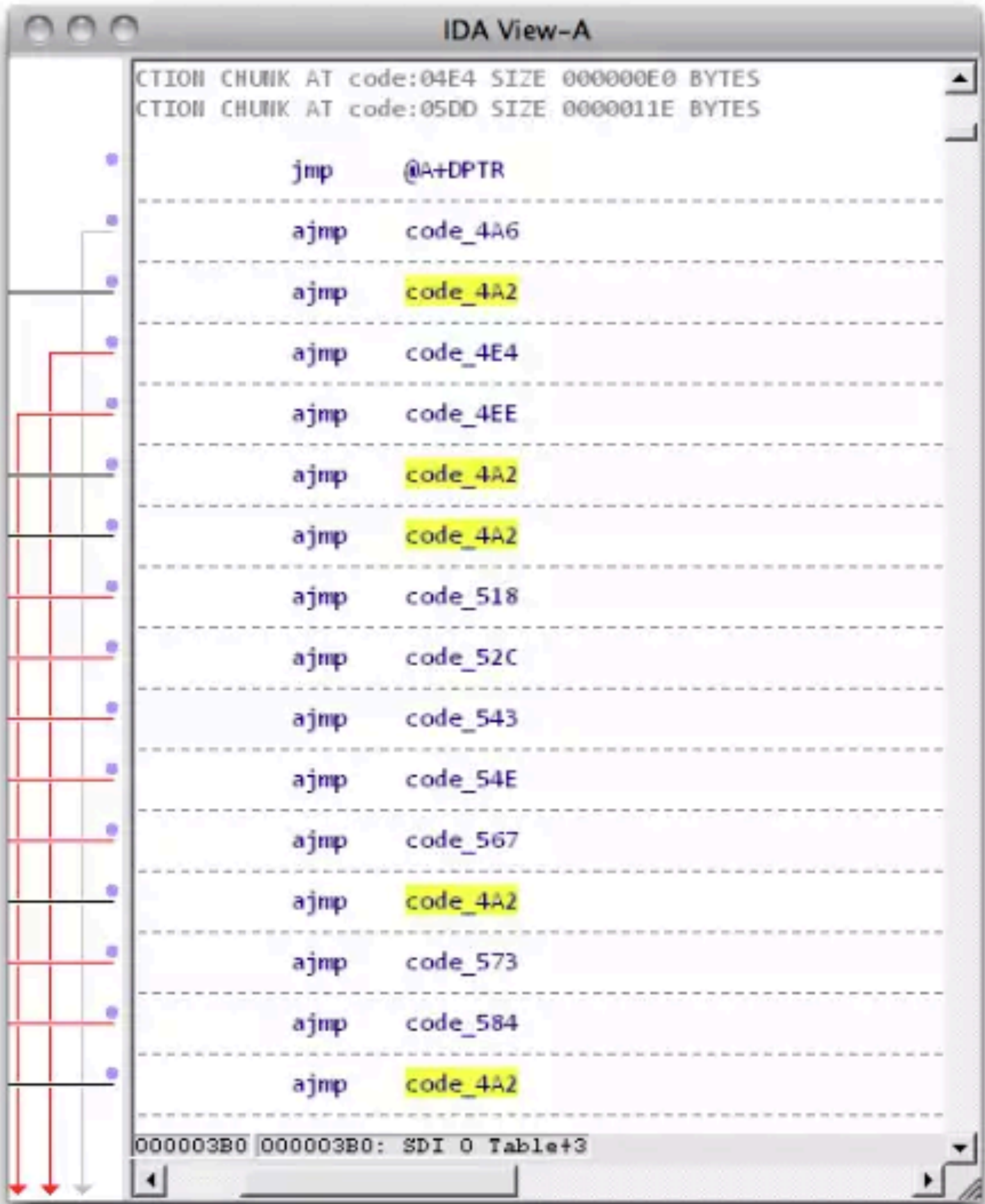


## Bunnie and Sean “Xobs” Cross (2013)

Discovered firmware update command

Able to send 8051 machine code (no code signing, etc.)

👉 MITM attacks from your storage?!



CMD INDEX	type	argument	resp	abbreviation	command description
CMD0	bc	[31:0] stuff bits	-	GO_IDLE_STATE	Resets all cards to idle state
CMD1	reserved				
CMD2	bcr	[31:0] stuff bits	R2	ALL_SEND_CID	Asks any card to send the CID numbers on the CMD line (any card that is connected to the host will respond)
CMD3	bcr	[31:0] stuff bits	R6	SEND_RELATIVE_ADDR	Ask the card to publish a new relative address (RCA)
CMD4	bc	[31:16] DSR [15:0] stuff bits	-	SET_DSR	Programs the DSR of all cards
CMD5	reserved for I/O cards (refer to the "SDIO Card Specification")				
CMD7	ac	[31:16] RCA [15:0] stuff bits	R1b (only from the selected card)	SELECT/DESELECT_CARD	Command toggles a card between the stand-by and transfer states or between the programming and disconnect states. In both cases, the card is selected by its own relative address and gets deselected by any other address; address 0 deselects all. In the case that the RCA equals 0, then the host may do one of the following: <ul style="list-style-type: none"><li>- Use other RCA number to perform card de-selection.</li><li>- Re-send CMD3 to change its RCA number to other than 0 and then use CMD7 with RCA=0 for card de-selection.</li></ul>
CMD8	bcr	[31:12]reserved bits [11:8]supply voltage(VHS) [7:0]check pattern	R7	SEND_IF_COND	Sends SD Memory Card interface condition, which includes host supply voltage information and asks the card whether card supports voltage. Reserved bits shall be set to '0'.
CMD9	ac	[31:16] RCA [15:0] stuff bits	R2	SEND_CSD	Addressed card sends its card-specific data (CSD) on the CMD line.
CMD10	ac	[31:16] RCA [15:0] stuff bits	R2	SEND_CID	Addressed card sends its card identification (CID) on CMD the line.
CMD11	reserved				
CMD12	ac	[31:0] stuff bits	R1b	STOP_TRANSMISSION	Forces the card to stop transmission
CMD13	ac	[31:16] RCA [15:0] stuff bits	R1	SEND_STATUS	Addressed card sends its status register.
CMD14	reserved				



# SD firmware hacking

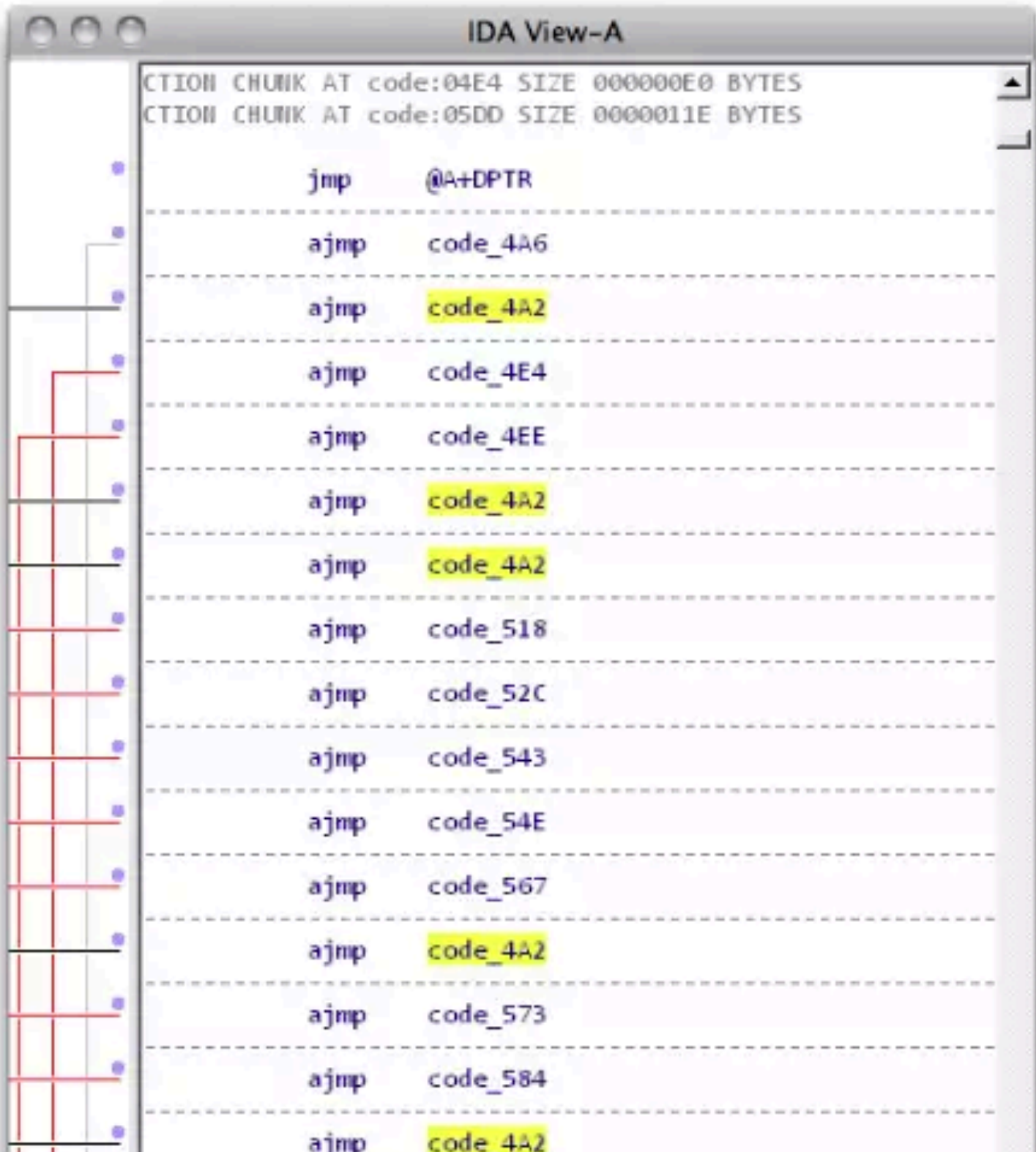


## Bunnie and Sean “Xobs” Cross (2013)

Discovered firmware update command

Able to send 8051 machine code (no code signing, etc.)

👉 MITM attacks from your storage?!



CMD INDEX	type	argument	resp	abbreviation	command description
CMD0	bc	[31:0] stuff bits	-	GO_IDLE_STATE	Resets all cards to idle state
CMD1	reserved				
CMD2	bcr	[31:0] stuff bits	R2	ALL_SEND_CID	Asks any card to send the CID numbers on the CMD line (any card that is connected to the host will respond)
CMD3	bcr	[31:0] stuff bits	R6	SEND_RELATIVE_ADDR	Ask the card to publish a new relative address (RCA)
CMD4	bc	[31:16] DSR [15:0] stuff bits	-	SET_DSR	Programs the DSR of all cards
CMD5	reserved for I/O cards (refer to the "SDIO Card Specification")				
CMD7	ac	[31:16] RCA [15:0] stuff bits	R1b (only from the selected card)	SELECT/DESELECT_CARD	Command toggles a card between the stand-by and transfer states or between the programming and disconnect states. In both cases, the card is selected by its own relative address and gets deselected by any other address; address 0 deselects all. In the case that the RCA equals 0, then the host may do one of the following: <ul style="list-style-type: none"><li>- Use other RCA number to perform card de-selection.</li><li>- Re-send CMD3 to change its RCA number to other than 0 and then use CMD7 with RCA=0 for card de-selection.</li></ul>
CMD8	bcr	[31:12]reserved bits [11:8]supply voltage(VHS) [7:0]check pattern	R7	SEND_IF_COND	Sends SD Memory Card interface condition, which includes host supply voltage information and asks the card whether card supports voltage. Reserved bits shall be set to '0'.
CMD9	ac	[31:16] RCA [15:0] stuff bits	R2	SEND_CSD	Addressed card sends its card-specific data (CSD) on the CMD line.
CMD10	ac	[31:16] RCA [15:0] stuff bits	R2	SEND_CID	Addressed card sends its card identification (CID) on the CMD line.
CMD11	reserved				
CMD12	ac	[31:0] stuff bits	R1b	STOP_TRANSMISSION	Forces the card to stop transmission
CMD13	ac	[31:16] RCA	R1	SEND_STATUS	Addressed card sends its status register.

“It’s as of yet unclear how many other manufacturers leave their firmware updating sequences unsecured.”



# Same thing for your networking chips

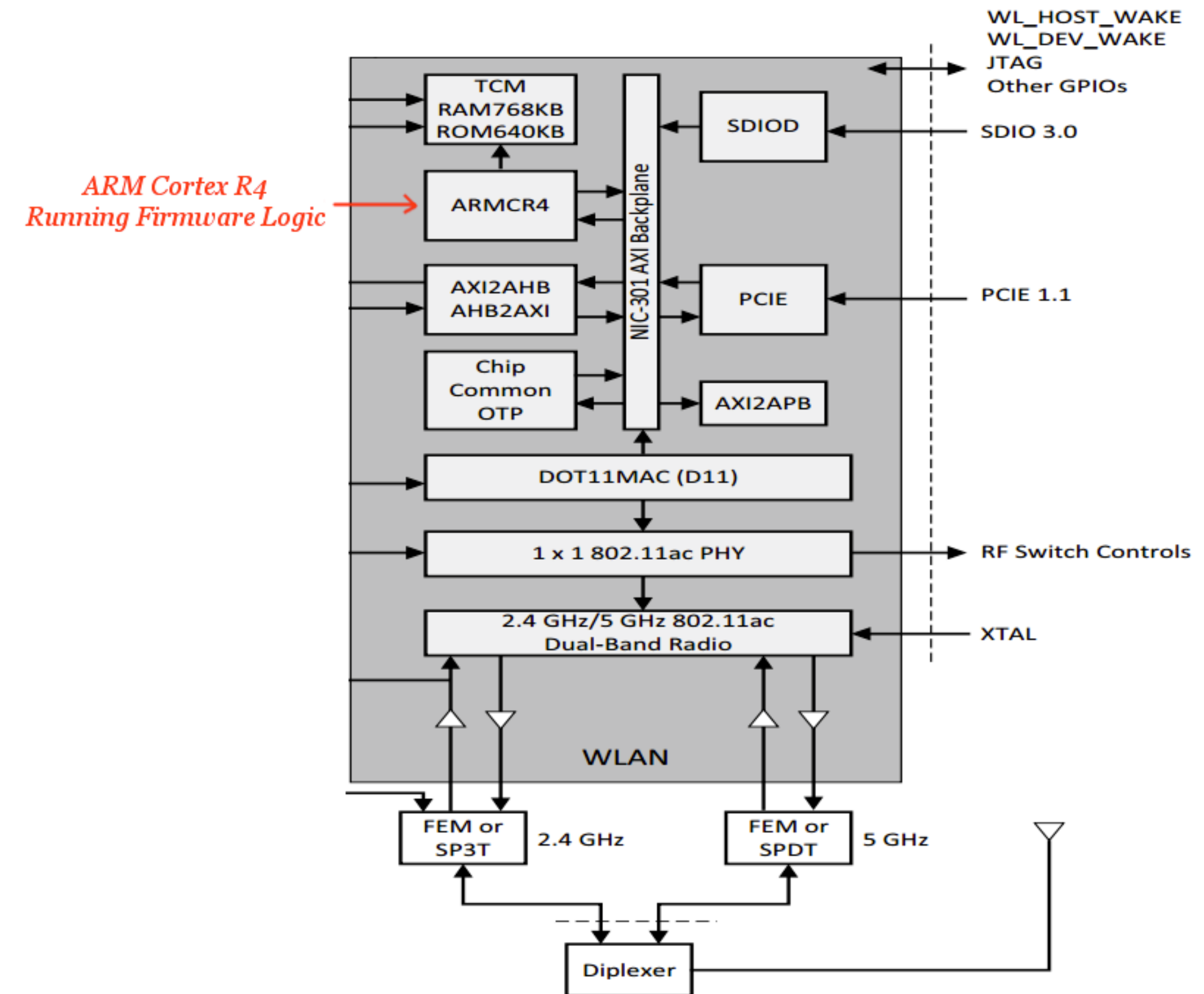
**Modern network chips have embedded CPUs as well**

Support “full stack” WiFi

Don't interrupt the CPU as often

**Exploitable from the outside!**

No use of protection bits: every page is RWX (also no stack cookies, etc.)



(Source: Gal Beniamini, Google Project Zero, [googleprojectzero.blogspot.com/2017/04/over-air-exploiting-broadcoms-wi-fi\\_4.html](https://googleprojectzero.blogspot.com/2017/04/over-air-exploiting-broadcoms-wi-fi_4.html))

# Attacking the main CPU from the NIC

## Option 1: Attack the OS kernel

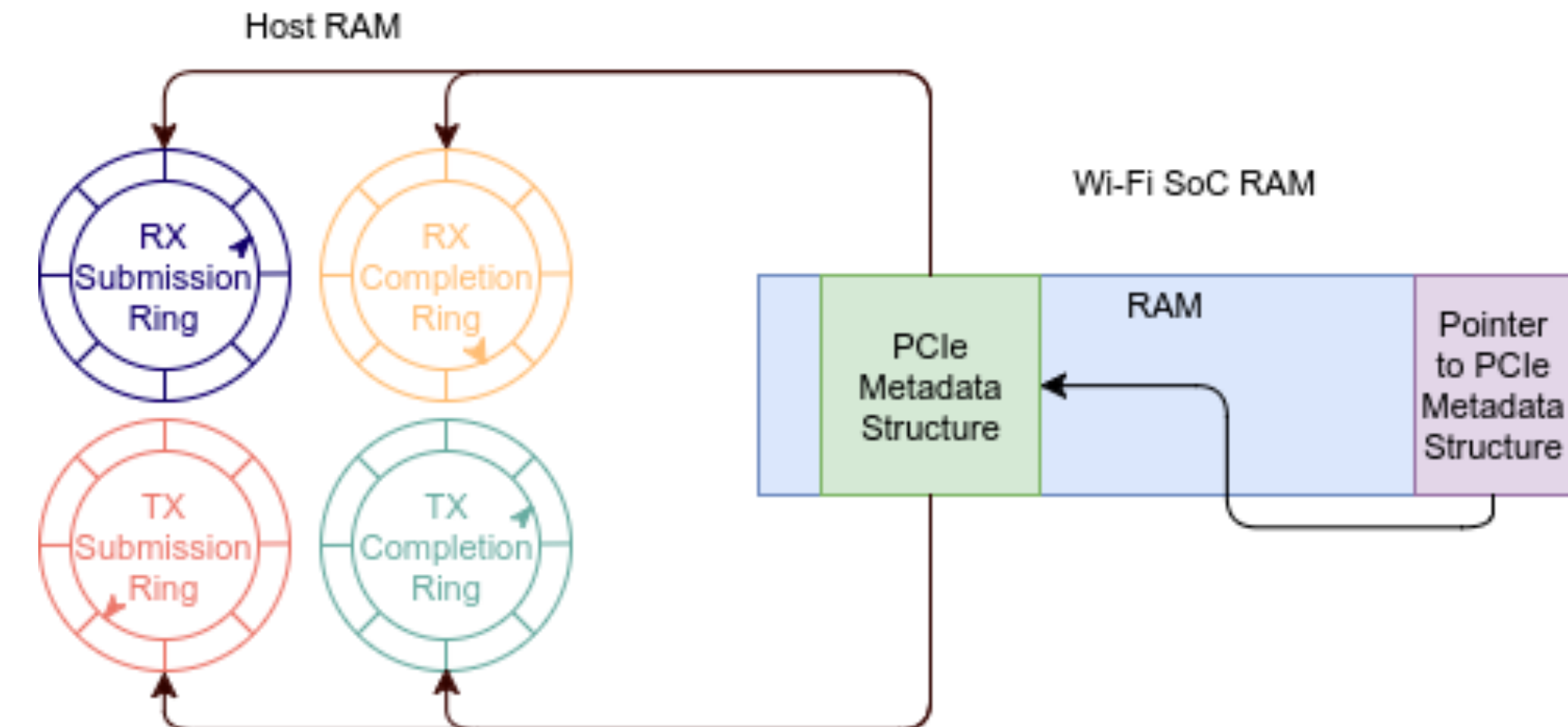
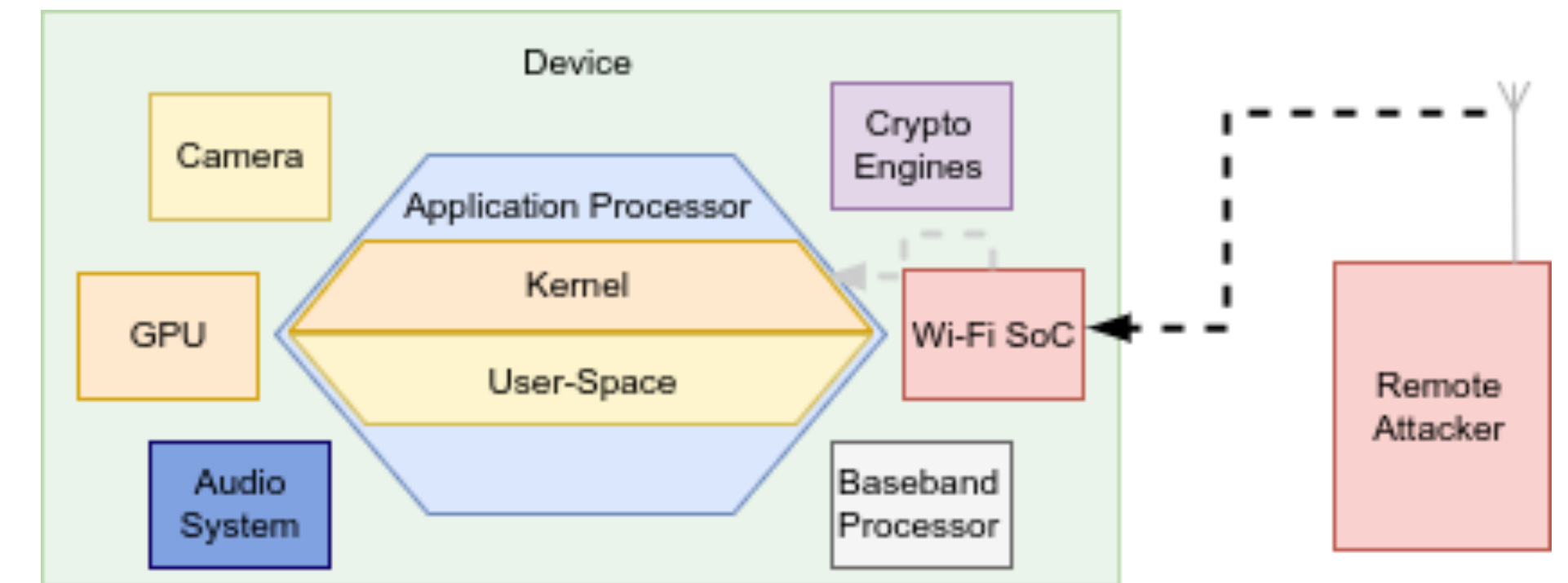
Heap overflow, vulnerable code pointer

## Option 2: Direct memory access

PCIe devices can do DMA

IOMMUs not used to limit visible memory in the kernel

➡ Arbitrary read/write to the OS kernel



(Source: Gal Beniamini, Google Project Zero, [googleprojectzero.blogspot.com/2017/04/over-air-exploiting-broadcoms-wi-fi\\_11.html](https://googleprojectzero.blogspot.com/2017/04/over-air-exploiting-broadcoms-wi-fi_11.html))



# What about ARM TrustZone?

**TrustZone is something of an OS layer below the kernel**

Support for boot locking, DRM, etc.

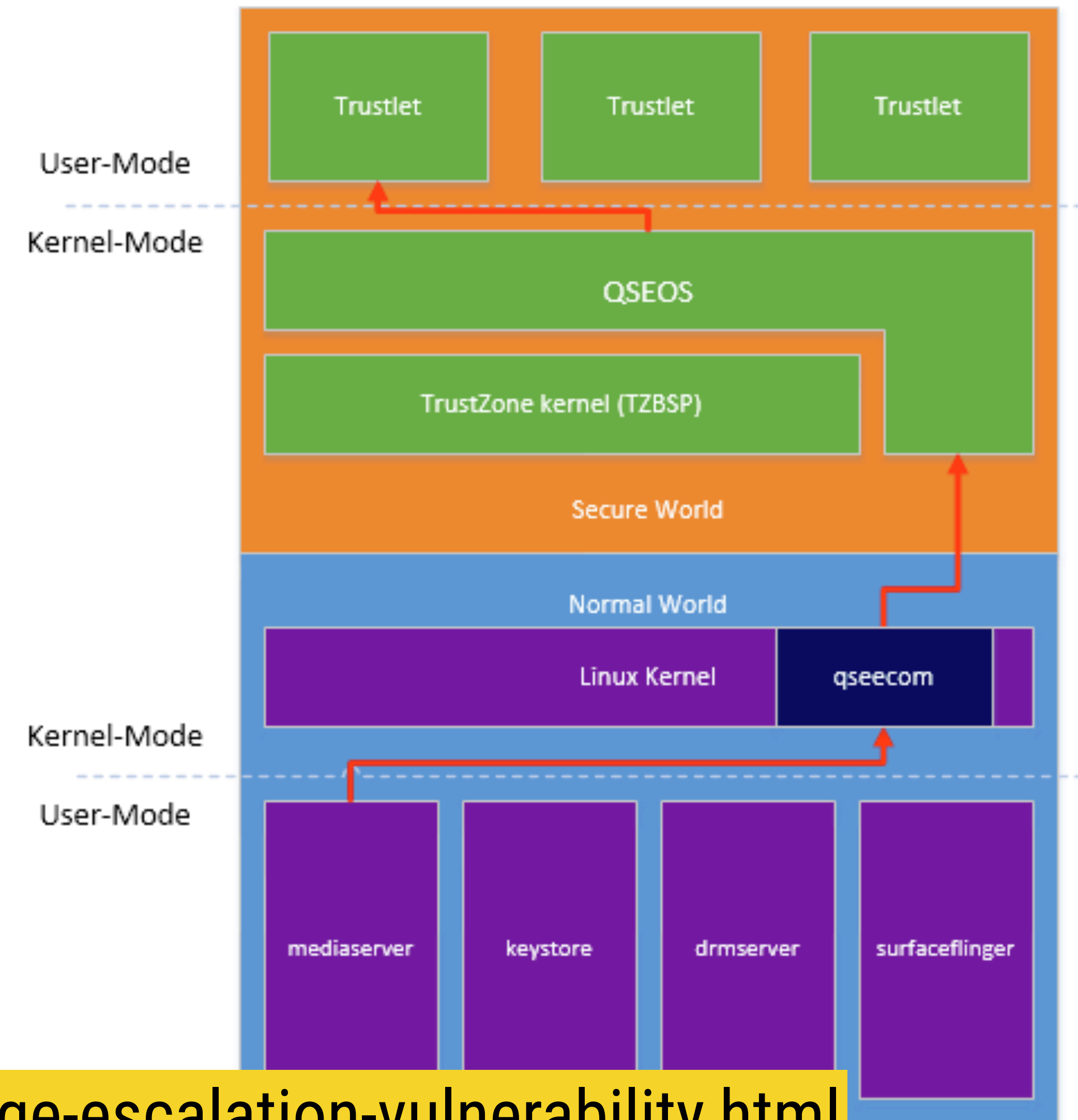
**Of course, it's exploitable**

(Also discovered by Gal Beniamini)

`memcpy( )` buffer overwrite vulnerability

Messy process to build a ROP chain

Shellcode to read/interact with the “secure file system”



[bits-please.blogspot.com/2016/05/qsee-privilege-escalation-vulnerability.html](http://bits-please.blogspot.com/2016/05/qsee-privilege-escalation-vulnerability.html)



# TrustZone security engineering?

## **MobileCore (Samsung)**

No ASLR, no stack cookies

## **QSEE (Qualcomm): slightly better**

9-bit ASLR, no guard page between stack, BSS, heap

## **Trustlets: Proprietary code, bugs can linger**

Many trustlets directly exposed to userland through proxy services

(Source: Gal Beniamini talk, BlueHat Israel 2017, [microsofttrnd.co.il/Press%20Kit/BlueHat%20IL%20Decks/GalBeniamini.pdf](https://microsofttrnd.co.il/Press%20Kit/BlueHat%20IL%20Decks/GalBeniamini.pdf))



# Example: Android Full Disk Encryption

## KeyMaster app manages keys

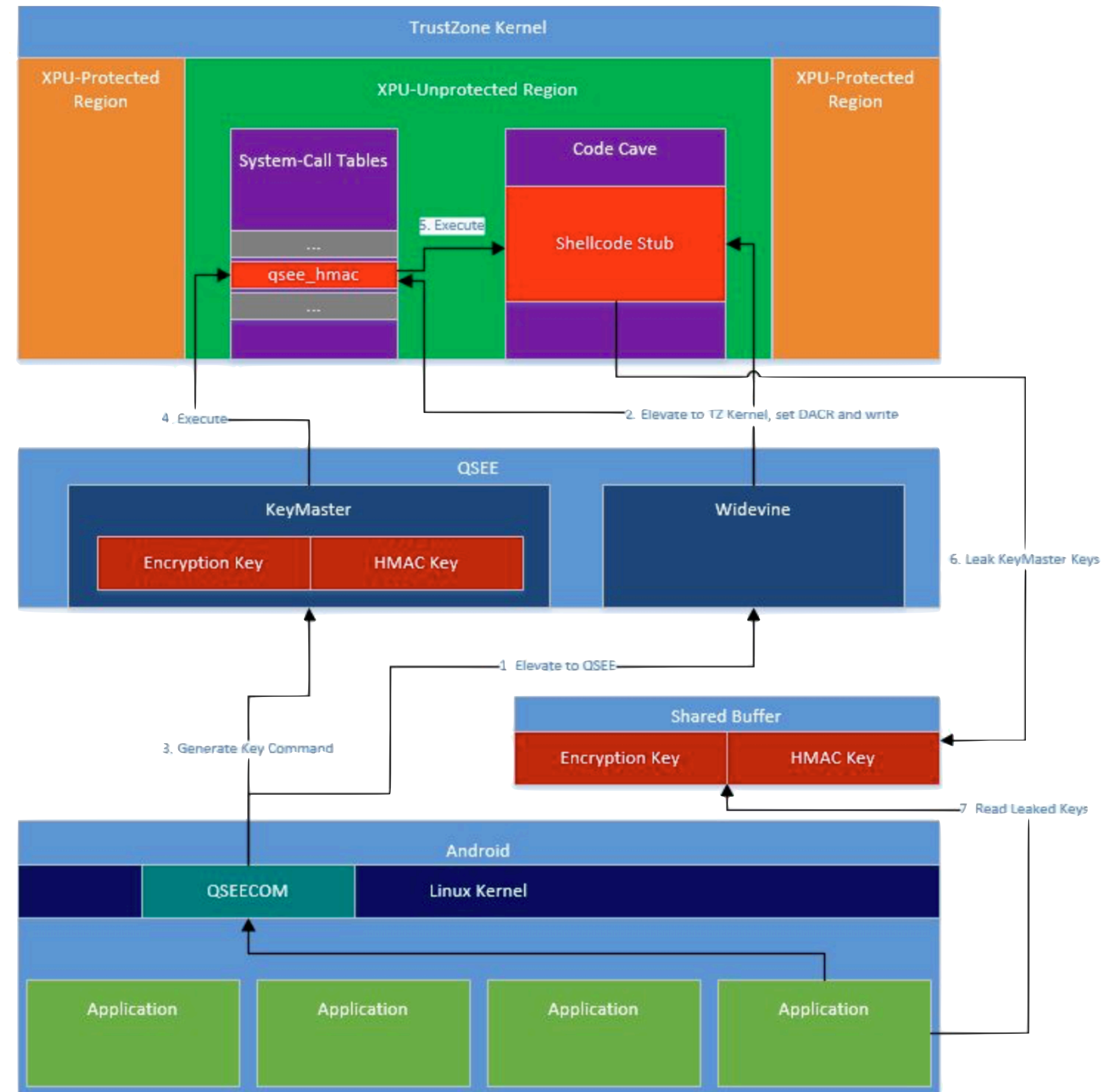
Vulnerabilities in other trustlets

- ➡ Privilege escalation
- ➡ Lack of separation across trustlets
- ➡ Master keys can leak

## Qualcomm, others support hardware-fused keys

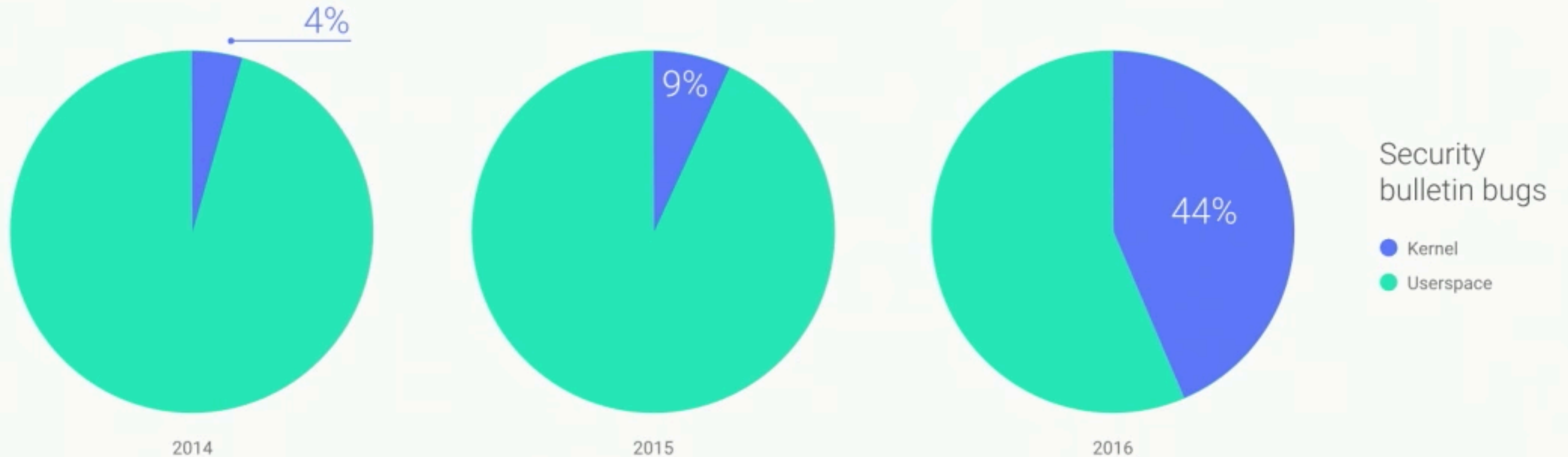
Not currently used by KeyMaster

Maybe in Android “O”?





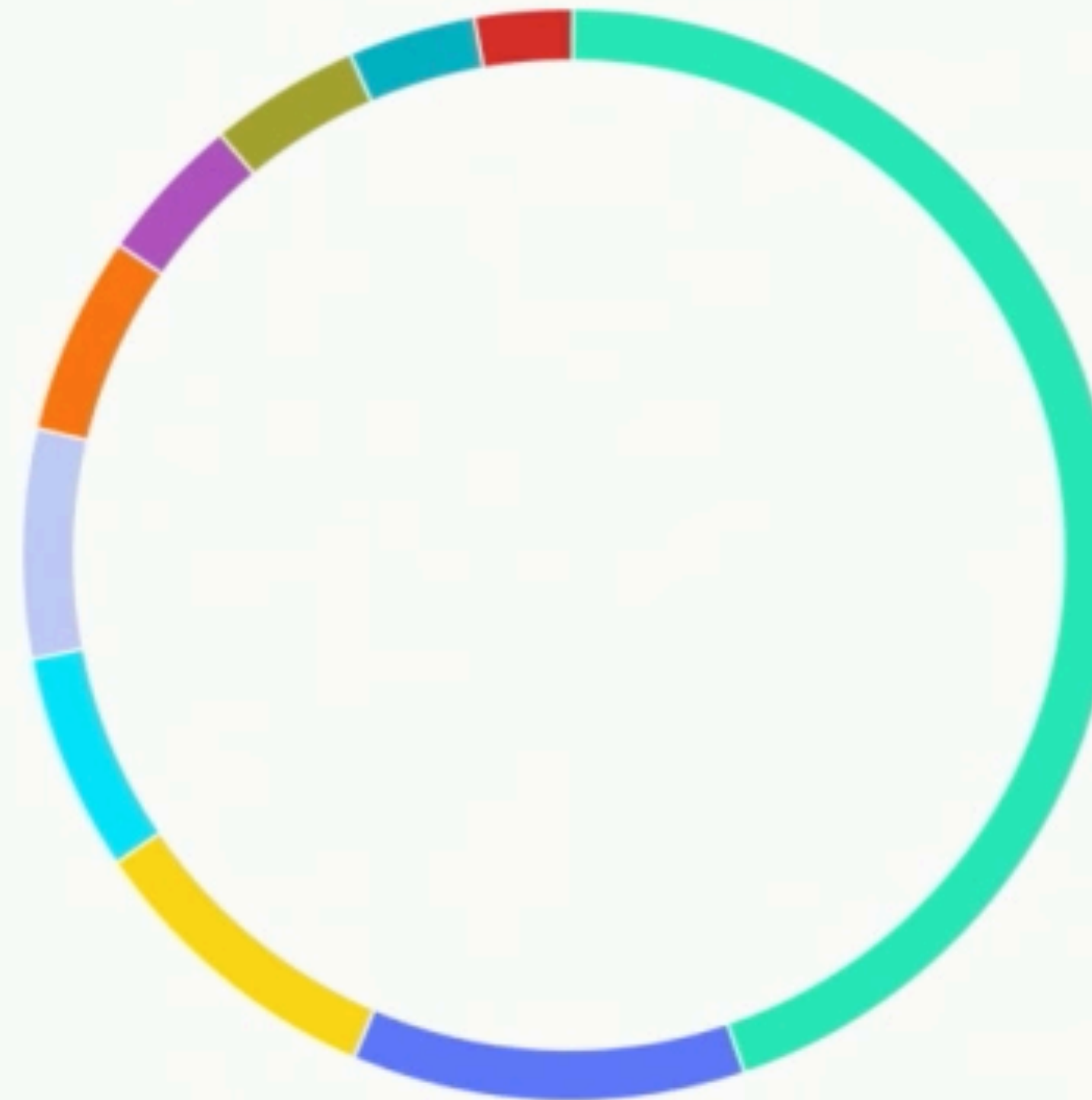
# Kernel bugs increasingly targeted



(Source: “What’s New in Android Security”, Google I/O 2017.  
[https://www.youtube.com/watch?v=C9\\_ytg6MUP0](https://www.youtube.com/watch?v=C9_ytg6MUP0))

# What kinds of bugs?

- Missing/incorrect bounds check
- Null pointer dereference
- Information leak
- Missing permission check
- Use after free
- Race condition
- Memory corruption (other)
- Other
- Integer overflow
- Uninitialized data



44.8%

**Missing/incorrect bounds check**  
Addressed by hardened usercopy,  
backported to Android kernel 3.18+


Kernel security bulletin bugs 2014 - 2016

#iO17

(Source: “What’s New in Android Security”, Google I/O 2017.  
[https://www.youtube.com/watch?v=C9\\_ytg6MUP0](https://www.youtube.com/watch?v=C9_ytg6MUP0))



# If we used a safe programming language

- 
- Missing/incorrect bounds check
  - Null pointer dereference
  - Information leak
  - Missing permission check
  - Use after free
  - Race condition
  - Memory corruption (other)
  - Other
  - Integer overflow
  - Uninitialized data

Plenty of PL and systems research that addresses these remaining concerns!

# Summary so far

**All the computers inside the computer are vulnerable.**

All the same attack types (buffer overflow, heap grooming, ROP, etc.)

Less competitive pressure  $\Rightarrow$  less use of standard defenses

**OS kernels tend to trust their devices to act reasonably.**

An “evil component” has a large attack surface

IOMMUs can help limit this

Unclear whether vendor isolation layer (Android “O” Treble) will help



# Challenges so far

**All the usual vulnerabilities that come from C programming.**

Can we please get rid of C? Is Rust a good alternative?

At least most Android apps and many system services are in Java.

**Vulnerability discovery, patch delivery.**

If Beniamini can do it, so can others. Are similar vulns being exploited?

**Supply chain integrity.**

Are you even getting the chips you expect?



# **The death of app isolation**



# Default security policies

**Every web page has an *origin* (DNS name, protocol, etc.)**

Separation enforced by browser's *same origin policy*

Network connections limited (unless the receiving server allows it)

Limited visibility of native OS resources

**Android apps have private storage, but unlimited networking**

Scan your internal network? Why not?

Easy to abuse privileges

# Example: exfiltration of contacts list

## The Wrong Way: Path Uploads iOS Users' Address Books Without Permission



CHRIS VELAZCO ✓

Tuesday, February 7th, 2012

Comments



What started as a bit of aimless tinkering for developer [Arun Thampi](#) ultimately unearthed something very surprising about personal life-sharing service Path. As a fan of the app, Thampi took it upon himself to look at the API calls that the app made to Path's service and found that his "entire address book (including full names, emails and phone numbers) was being sent as a plist to Path."

Puzzled, Thampi created an entirely new Path and tried again, only to be faced with the same results. Feel free to try it for yourself if you're curious, as Thampi has written up the test procedures on his blog.

According to a comment left by Path co-founder and CEO Dave Morin, uploading the user's address book is meant simply to connect users with each other. As [VentureBeat](#) points out, this isn't exactly a secret — the practice is pointed out in the company's [Wikipedia entry](#). Still, it's not exactly the easiest information to come across unless you're actively looking for it, especially when no mention of it is made during the initial sign-up process.



# Example: exfiltration of contacts list

## The Wrong Way: Path Uploads iOS Users' Address Books Without Permission

When asked why Path didn't give users the choice to opt-in right from the start, [Path CEO] Morin responded with the following:

***This is currently the industry best practice and the App Store guidelines do not specifically discuss contact information. However, as mentioned, we believe users need further transparency on how this works, so we've been proactively addressing this.***

[techcrunch.com/2012/02/07/path-uploads-your-iphones-address-book-to-their-servers-without-a-peep/](http://techcrunch.com/2012/02/07/path-uploads-your-iphones-address-book-to-their-servers-without-a-peep/)

Comments

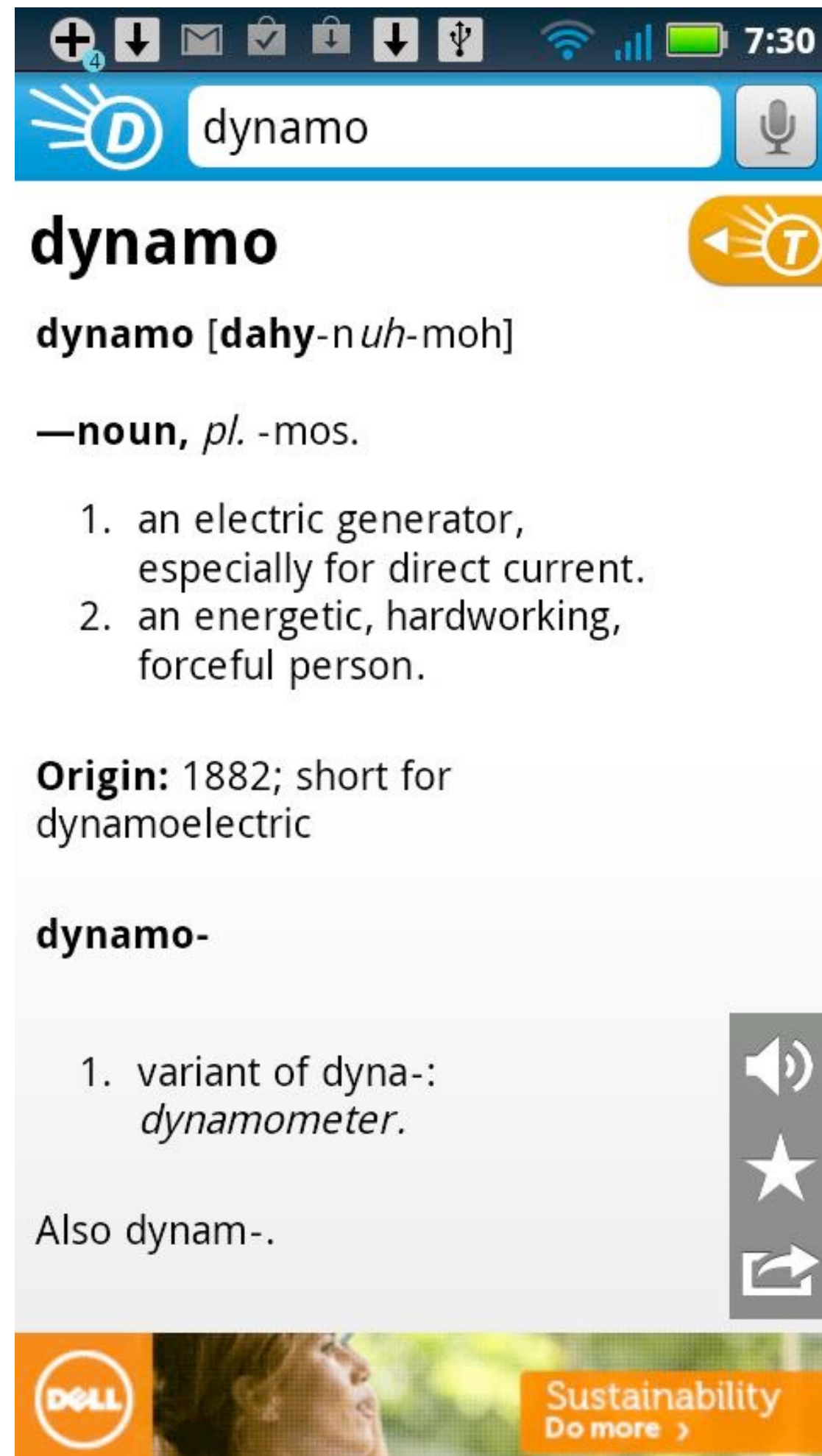
at started as a bit of aimless tinkering for developer **Arun Thampi** ultimately unearthed something very surprising about personal life-sharing service Path. As a fan of the app, Thampi took it upon himself to look at the API that the app made to Path's service and found that his "entire address book (including names, emails and phone numbers) was being sent as a plist to Path."

Amazed, Thampi created an entirely new Path app and tried again, only to be faced with the same results. Feel free to try it for yourself if you're curious, as Thampi has written up the test procedures on his blog.

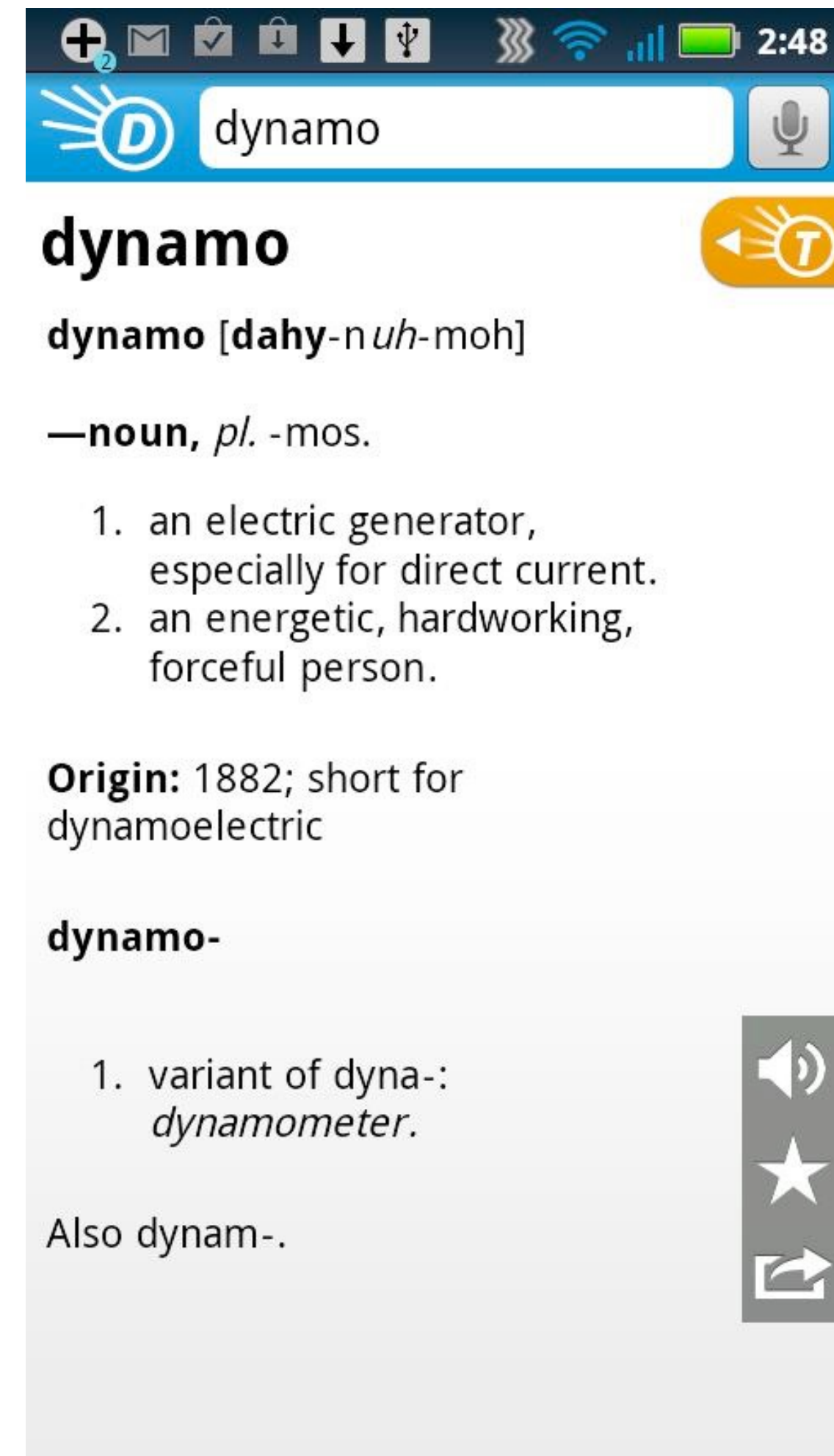
According to a comment left by Path co-founder and CEO Dave Morin, uploading the user's address book is meant simply to connect users with each other. As **VentureBeat** points out, this isn't exactly a secret — the practice is pointed out in the company's **Wikipedia entry**. Still, it's not exactly the easiest information to come across unless you're actively looking for it, especially when no mention of it is made during the initial sign-up process.



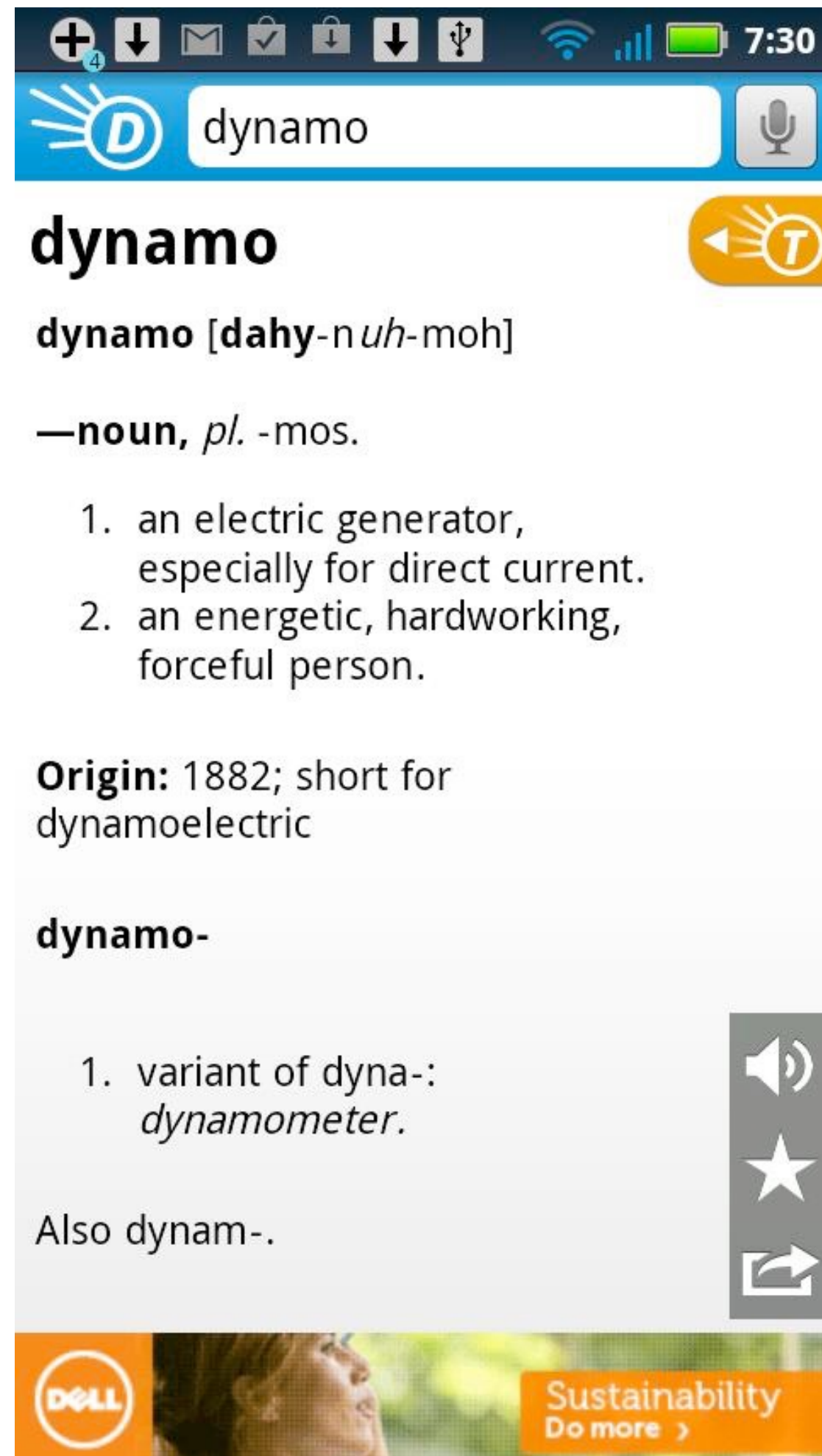




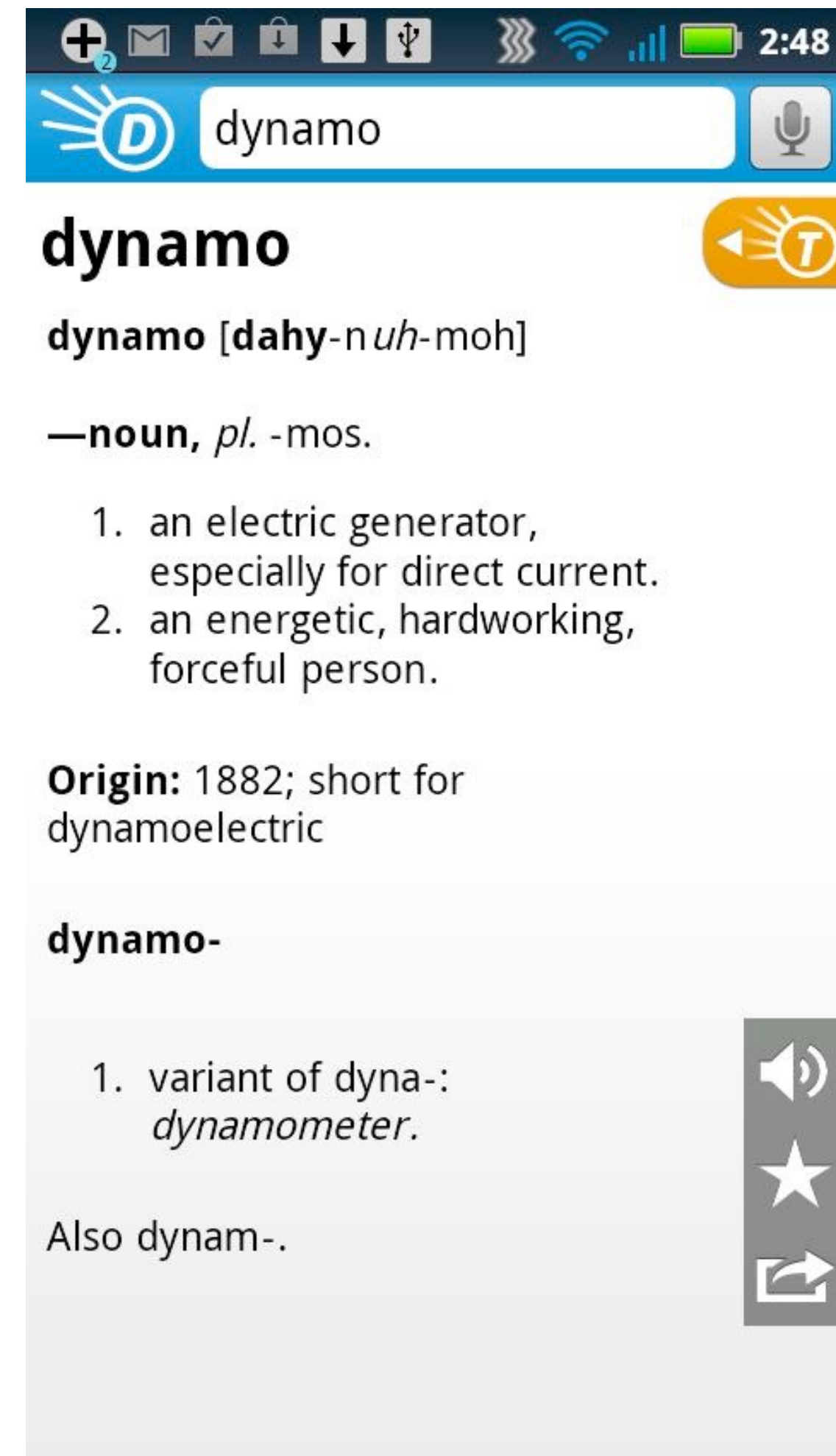
Cost : **Free**



Cost : **\$2.99**



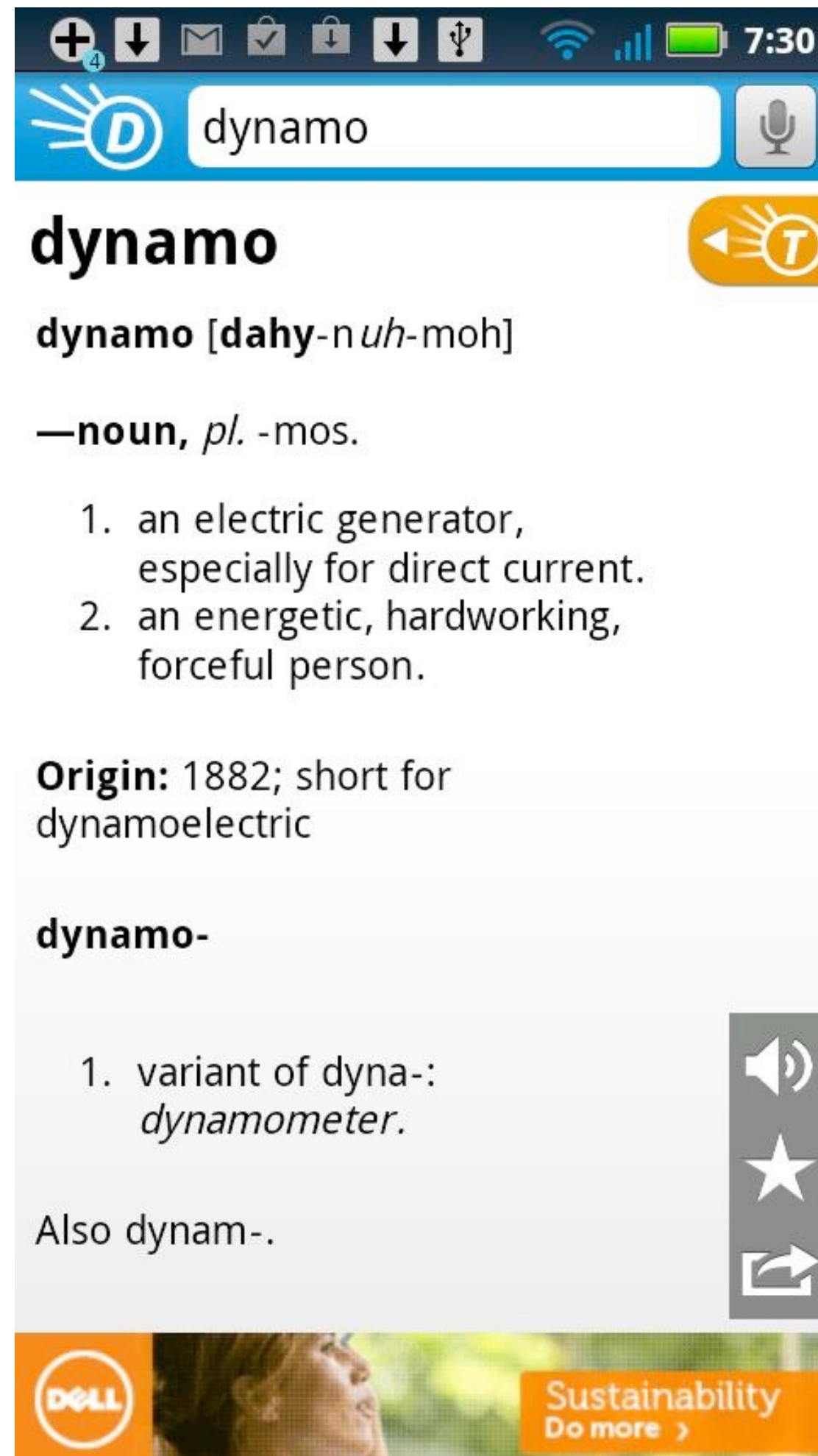
**Cost : Free**



**Cost : \$2.99**

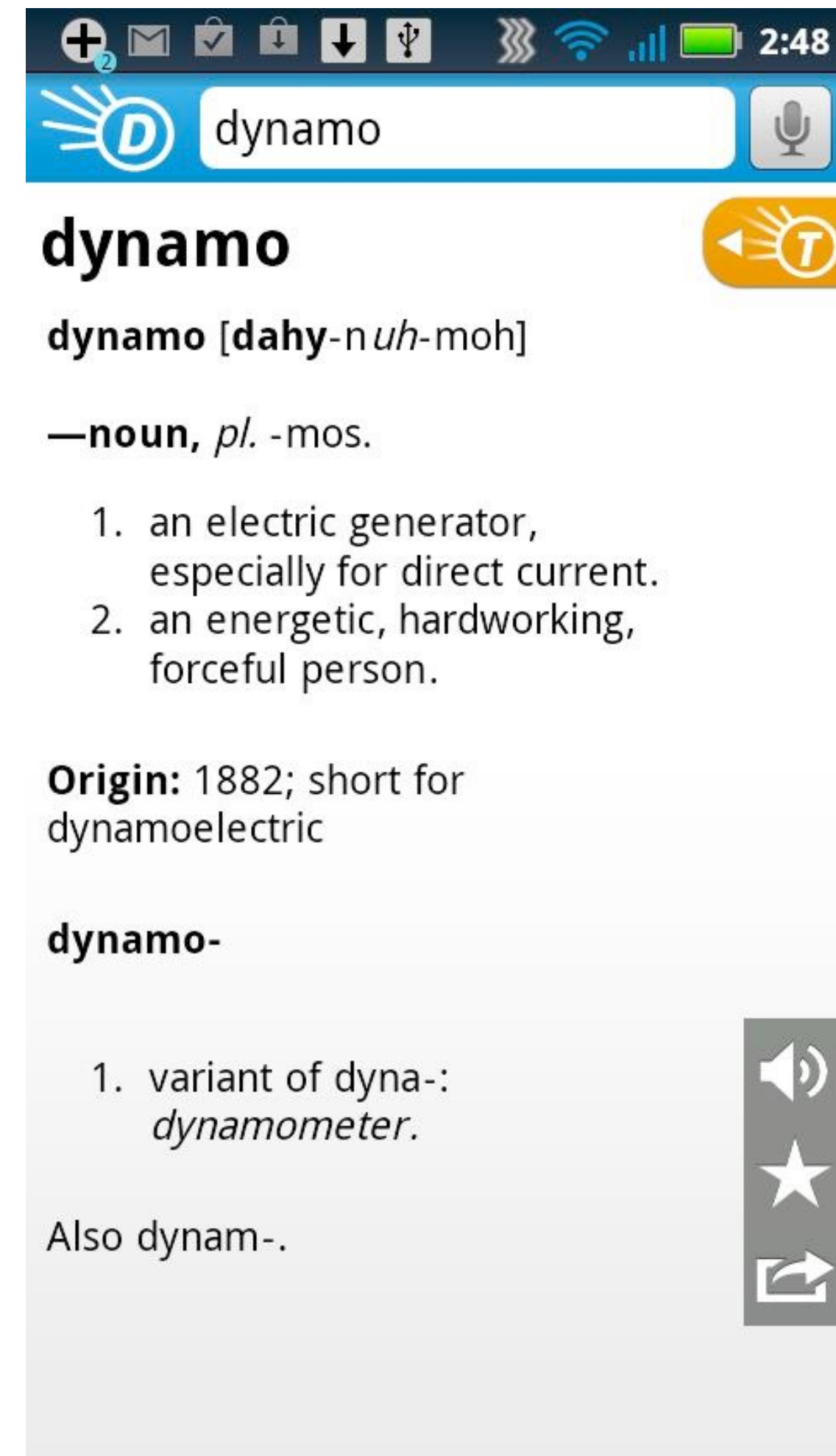
**Downloads:  
100,000 – 500,000**





Cost : **Free**

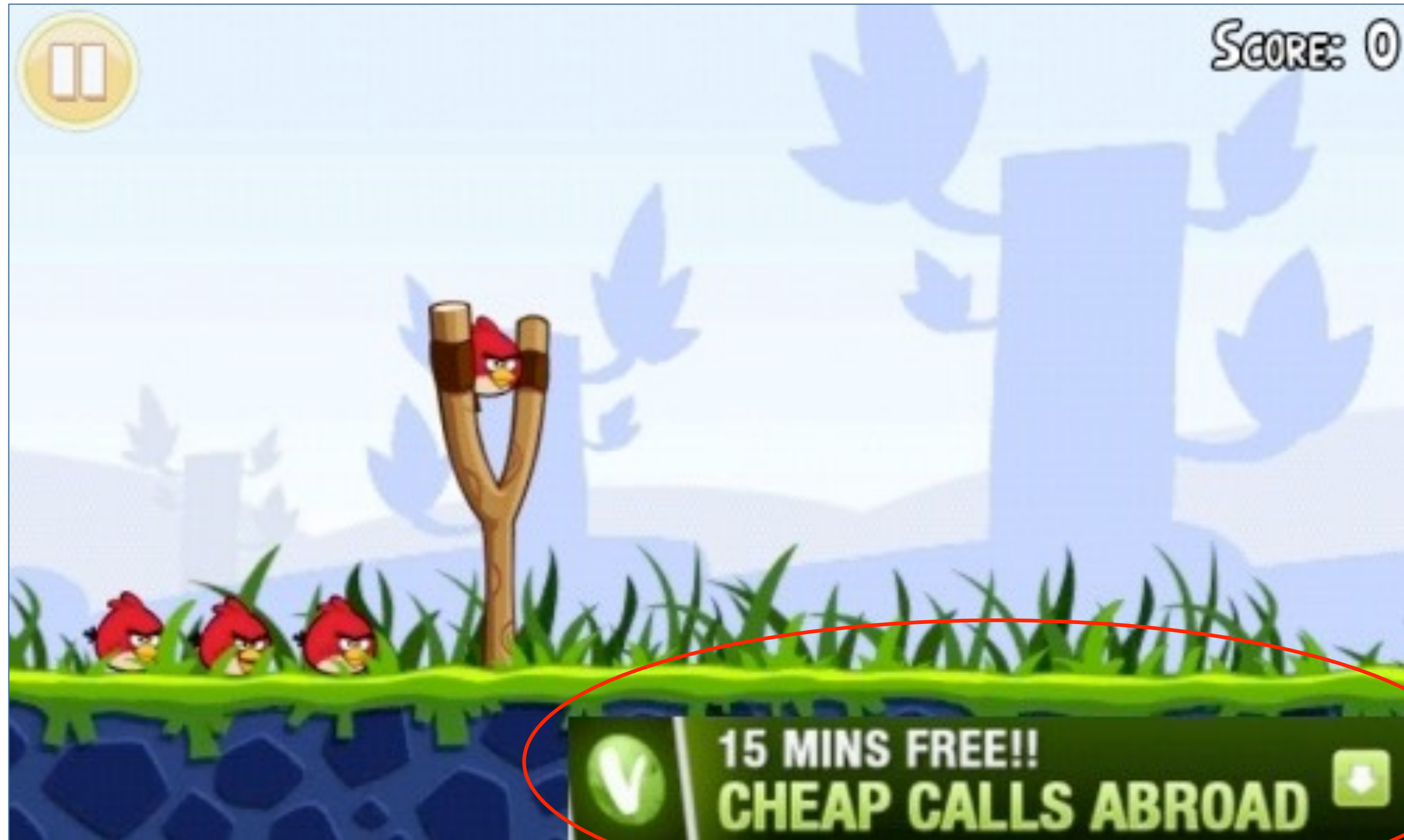
Downloads:  
10,000,000 – 50,000,000



Cost : **\$2.99**

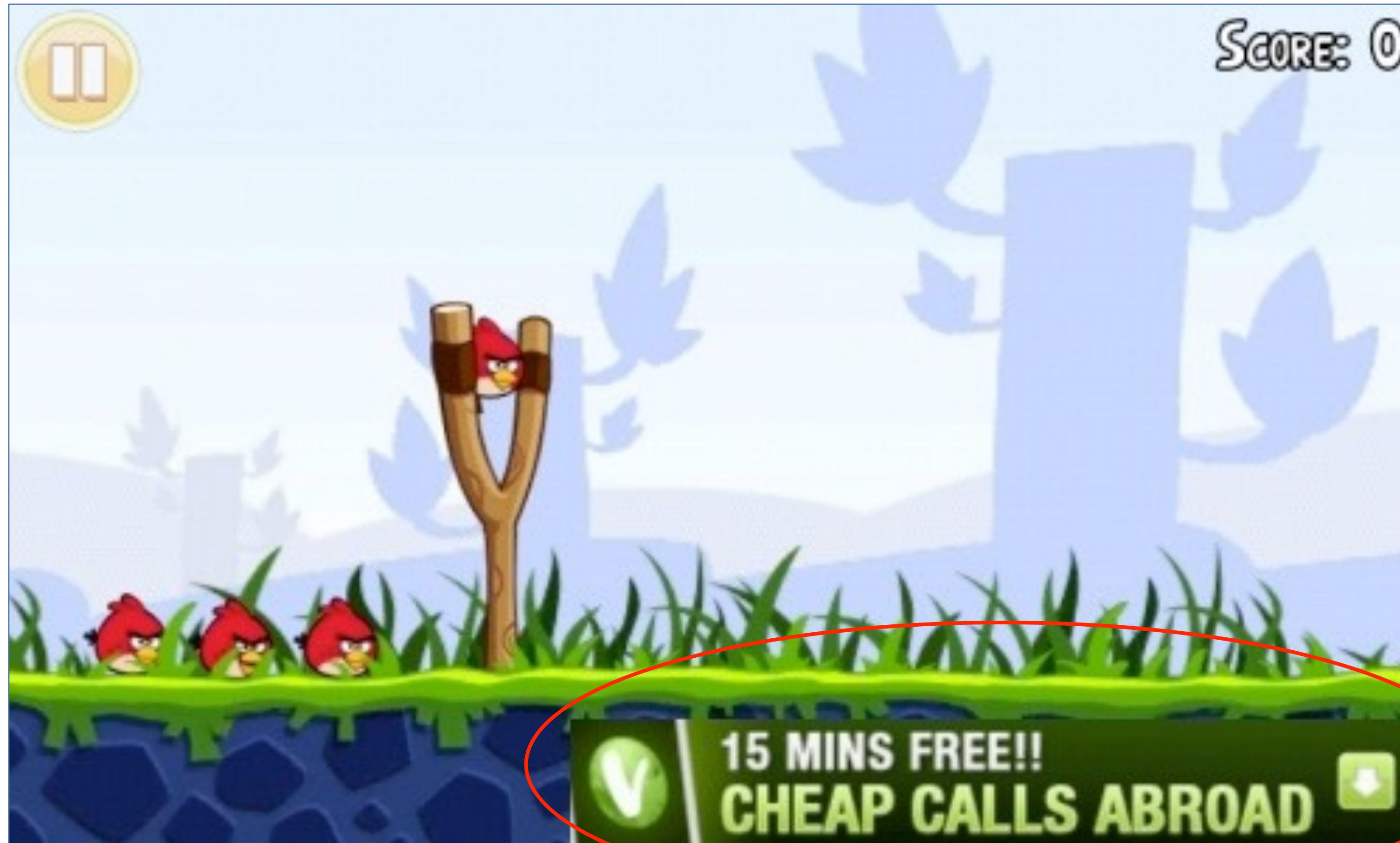
Downloads:  
100,000 – 500,000

# Ads are widely used





# Ads are widely used



(and advertising uses 75% of the power budget - Pathak et al., Eurosys 2012)



# Dubious Android apps may not be malware--just ads

Verizon-affiliated ICSA Labs steps into the controversy over Android apps that Symantec identified as malware.



by [Elinor Mills](#) | February 1, 2012 1:21 PM PST



Android Market

Apps ▾

Music ▾

Books ▾

Movies ▾

My Library ▾

[Home](#) > [Apps](#) > [Brain & Puzzle](#)

## Deal or BE Millionaire

Ogre Games



★★★★★ (14,463)

INSTALL

[More from developer](#)

OVERVIEW

USER REVIEWS

WHAT'S NEW

PERMISSIONS

### Description

Deal & Be Millionaire

WE ARE NOT MALWARE!!

Symantec, the company that wrongly labelled this app as malware the other day, contacted us and are in the process of un-doing the mistake they did and whitelisting the product.



# Measuring permission usage

**Separate library code from application code**

**Simple static analysis of library code**

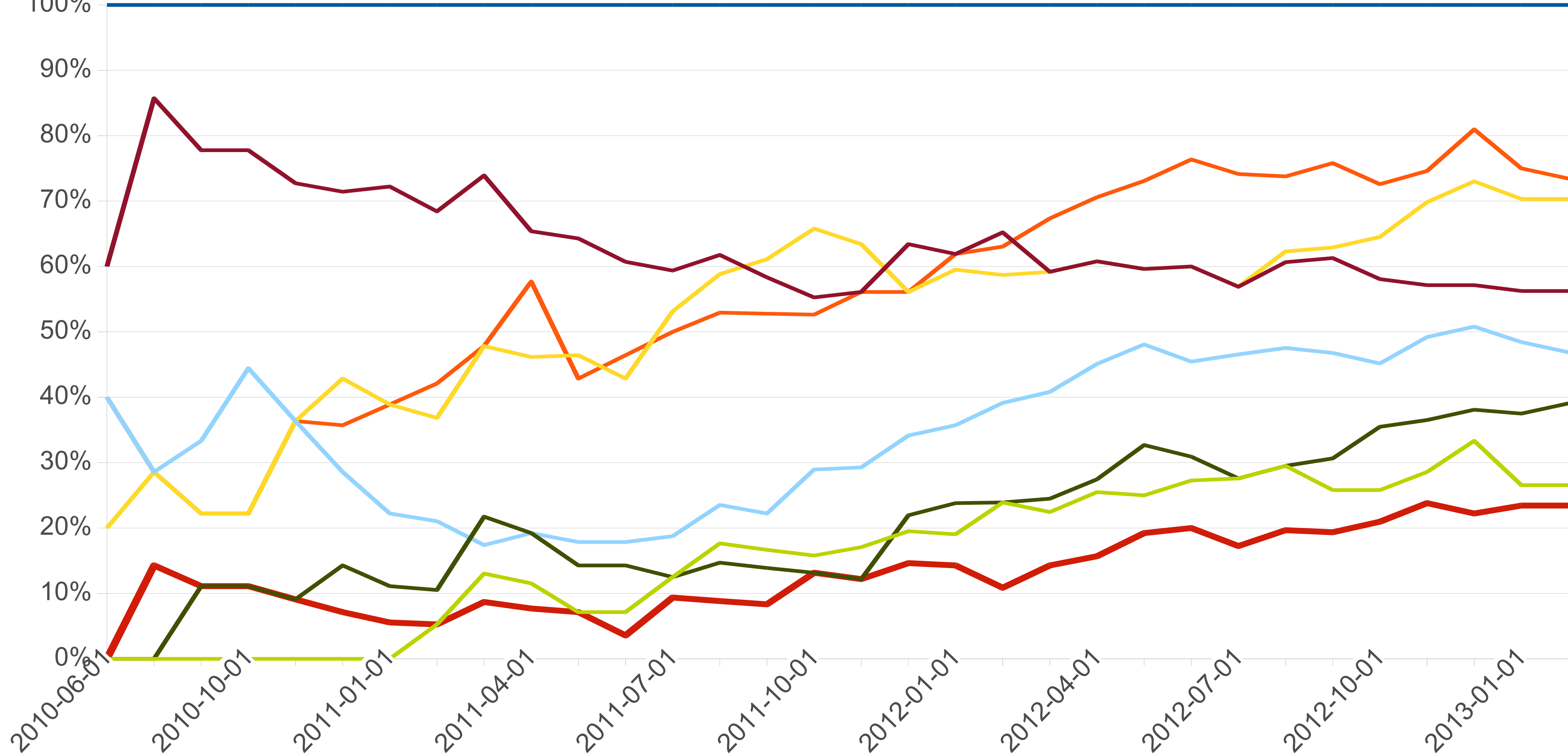
Stowaway (Felt et al., 2011)

**Map API calls to Android permissions**

Scout (Au et al., 2012)

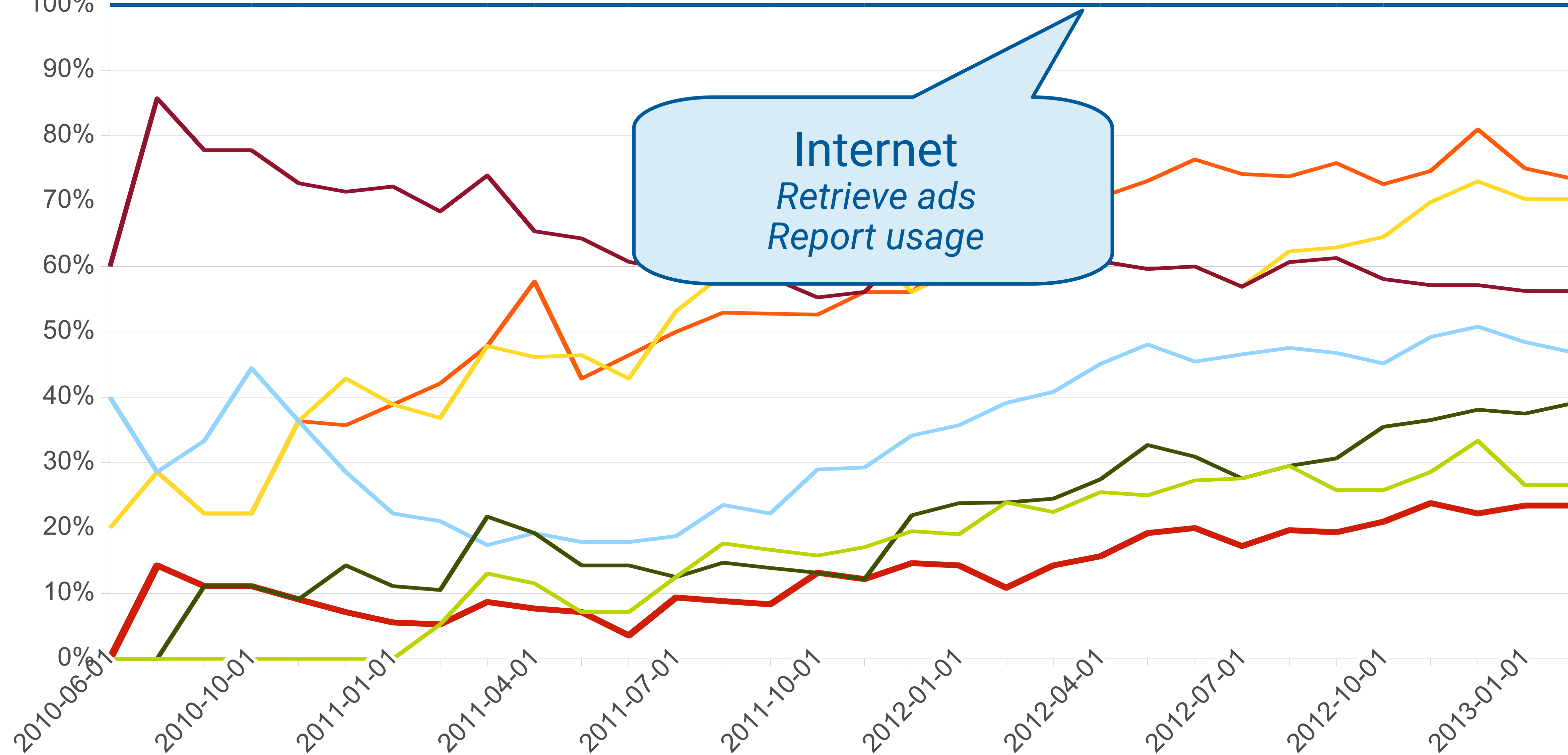
Theodore Book, Adam Pridgen, and Dan S. Wallach, **Longitudinal analysis of Android ad library permissions**. Mobile Security Technologies (MOST) 2013.

Theodore Book and Dan S. Wallach, **A case of collusion: A study of the interface between ad libraries and their apps**. 3rd ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM), November 2013.

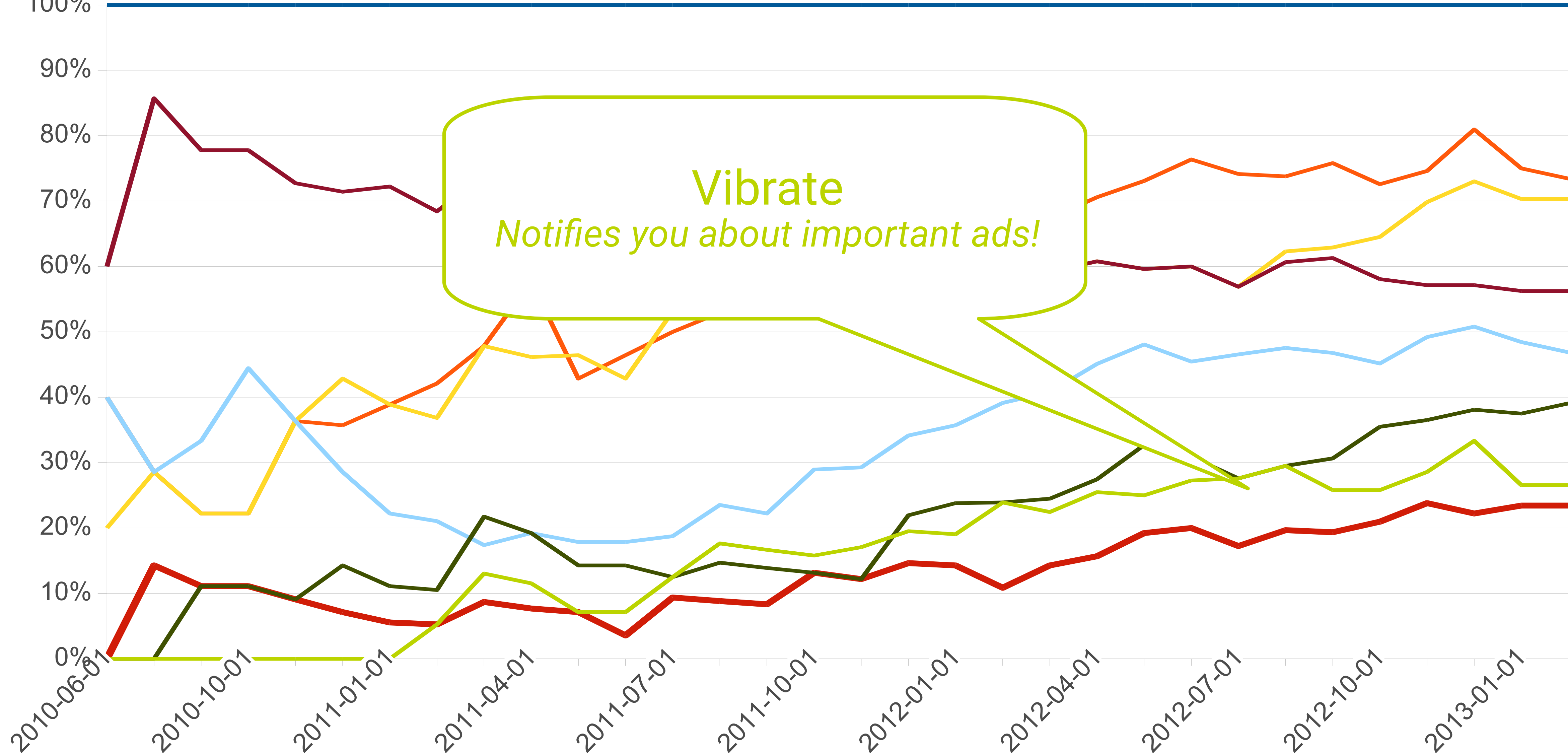


INTERNET      ACCESS\_NETWORK\_STATE      READ\_PHONE\_STATE      Dangerous      ACCESS\_FINE\_LOCATION  
WAKE\_LOCK      ACCESS\_WIFI\_STATE      VIBRATE



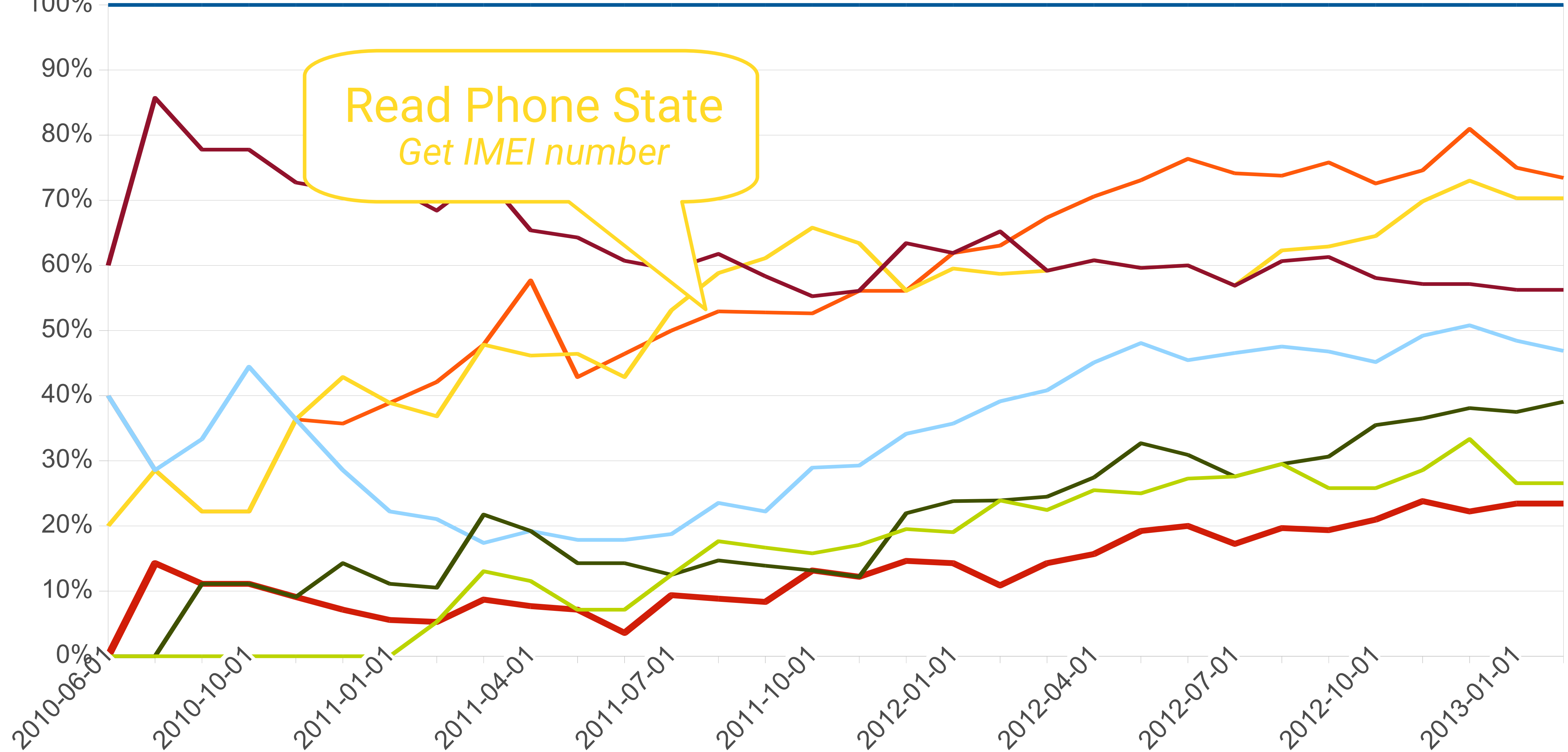


INTERNET      ACCESS\_NETWORK\_STATE      READ\_PHONE\_STATE      Dangerous      ACCESS\_FINE\_LOCATION  
WAKE\_LOCK      ACCESS\_WIFI\_STATE      VIBRATE

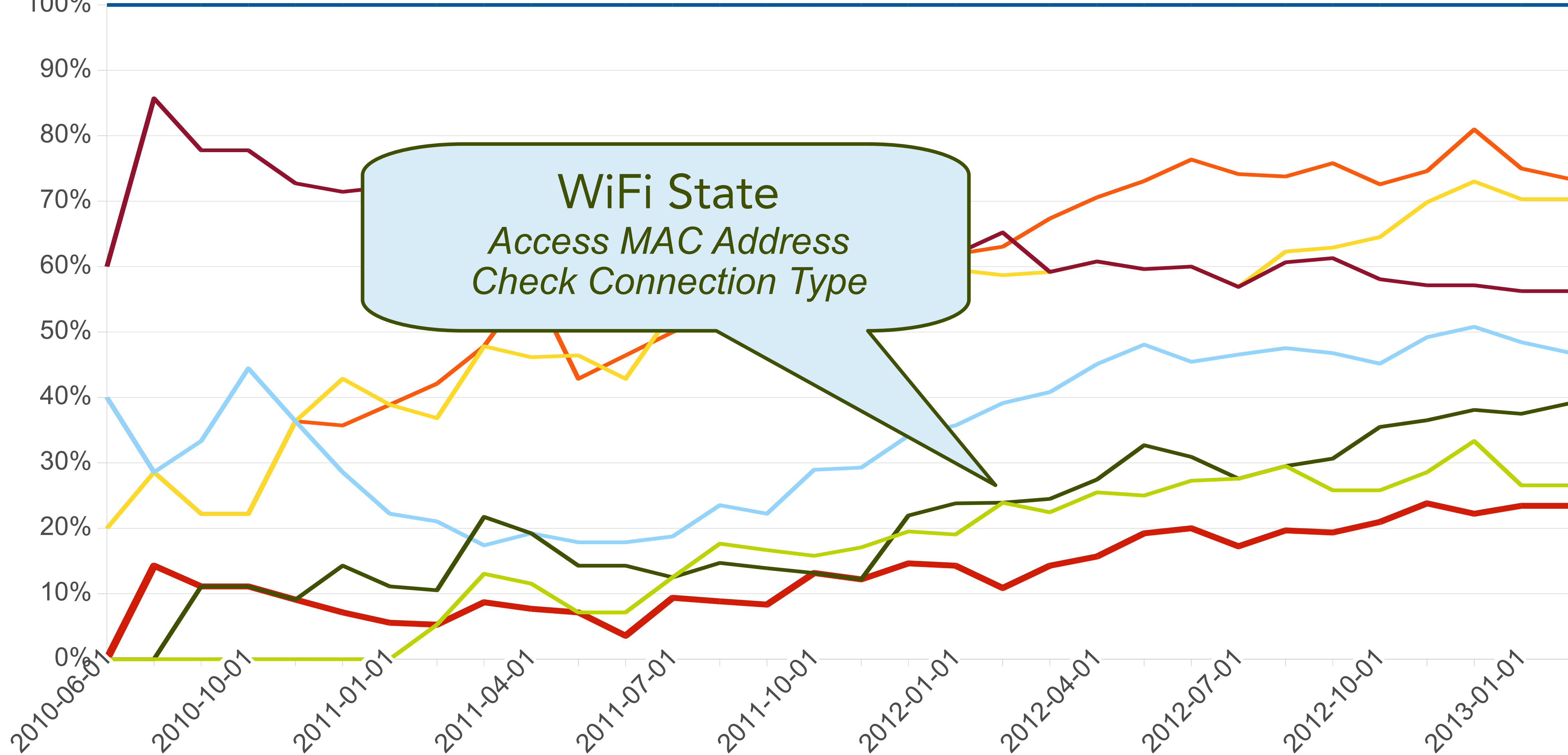


INTERNET ACCESS\_NETWORK\_STATE READ\_PHONE\_STATE Dangerous ACCESS\_FINE\_LOCATION  
WAKE\_LOCK ACCESS\_WIFI\_STATE VIBRATE





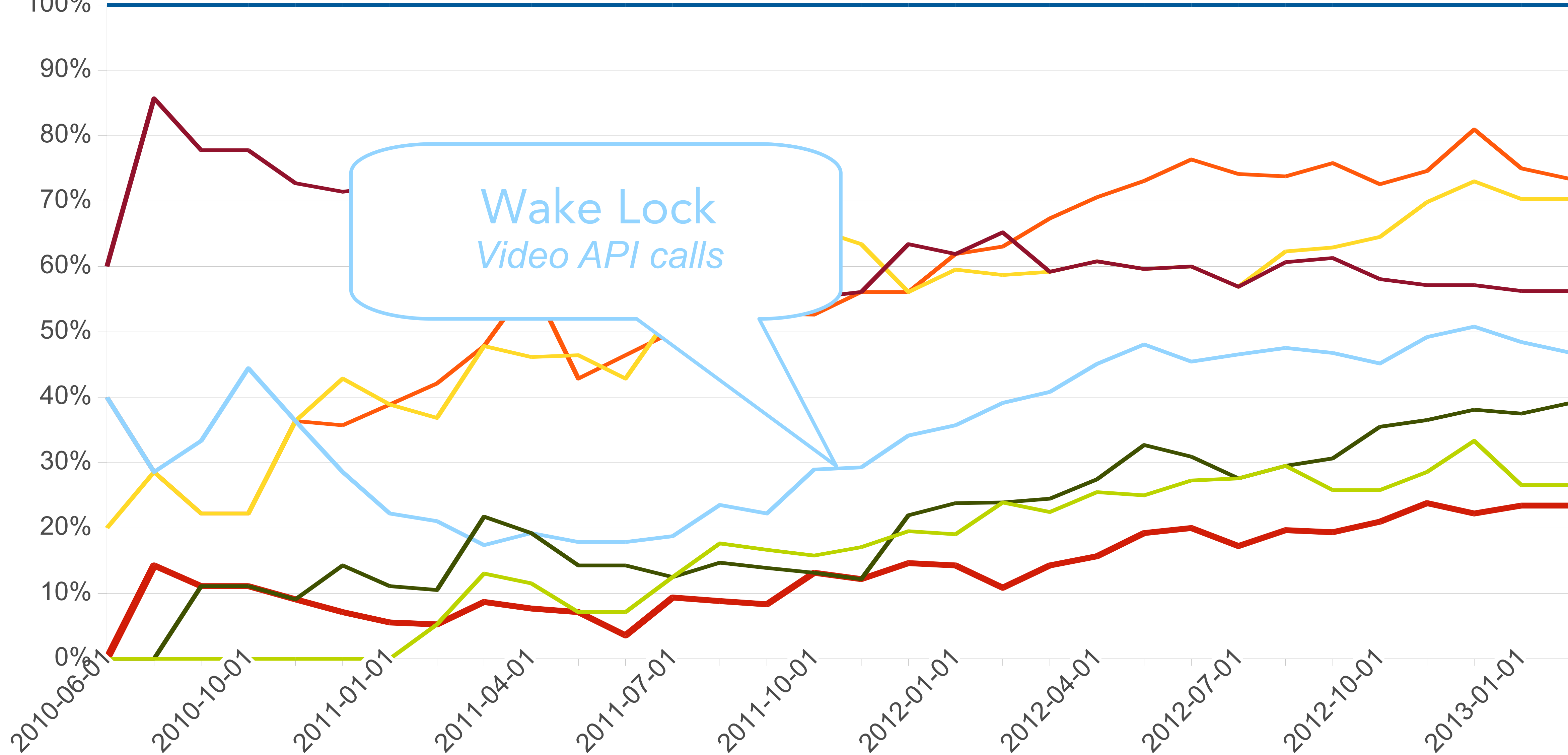
INTERNET   ACCESS\_NETWORK\_STATE   READ\_PHONE\_STATE   DANGEROUS   ACCESS\_FINE\_LOCATION  
WAKE\_LOCK   ACCESS\_WIFI\_STATE   VIBRATE



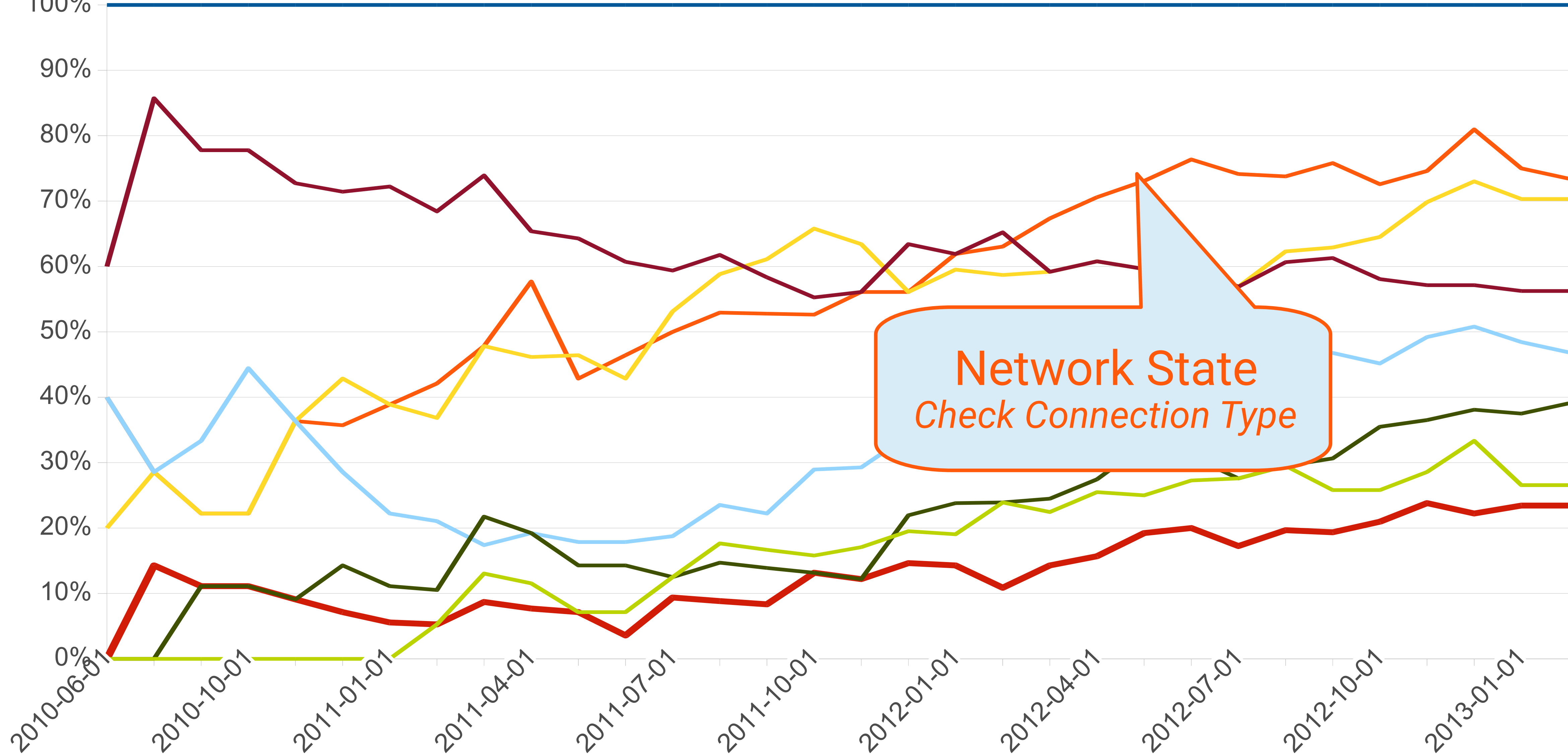
WiFi State  
Access MAC Address  
Check Connection Type

- INTERNET
- WAKE\_LOCK
- ACCESS\_NETWORK\_STATE
- ACCESS\_WIFI\_STATE
- READ\_PHONE\_STATE
- VIBRATE
- Dangerous
- ACCESS\_FINE\_LOCATION





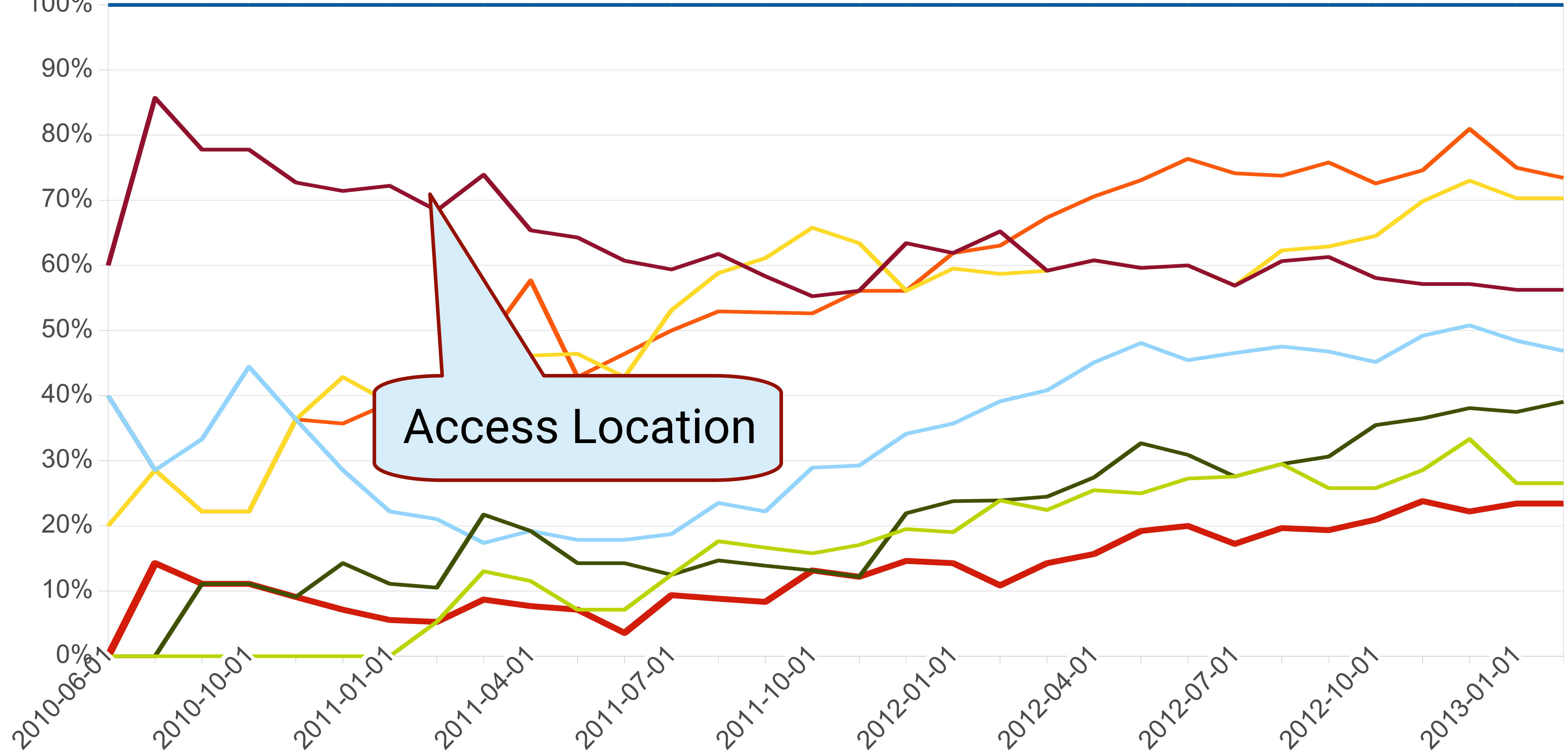
INTERNET      ACCESS\_NETWORK\_STATE      READ\_PHONE\_STATE      Dangerous      ACCESS\_FINE\_LOCATION  
WAKE\_LOCK      ACCESS\_WIFI\_STATE      VIBRATE



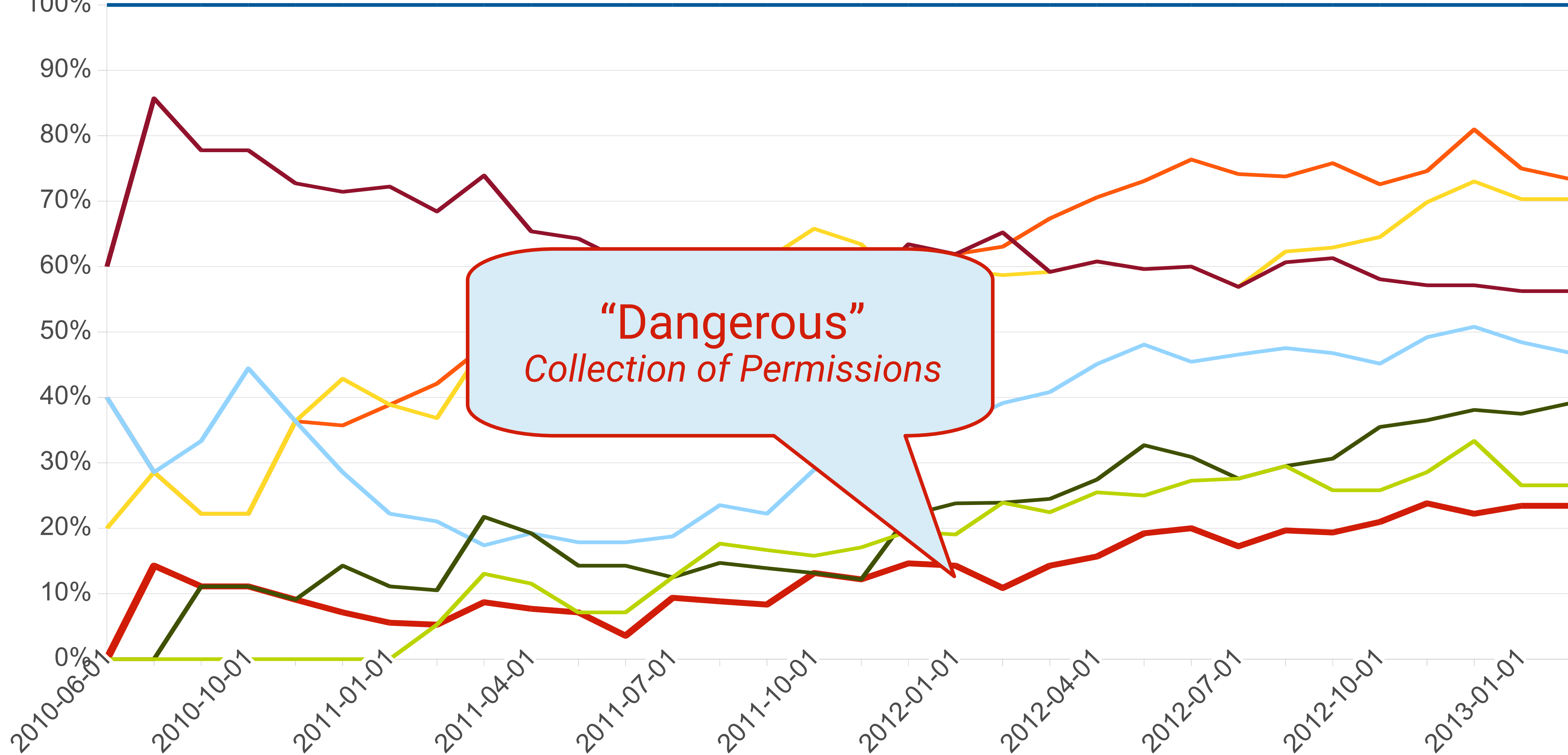
Network State  
Check Connection Type

INTERNET ACCESS\_NETWORK\_STATE READ\_PHONE\_STATE Dangerous ACCESS\_FINE\_LOCATION  
WAKE\_LOCK ACCESS\_WIFI\_STATE VIBRATE





INTERNET   ACCESS\_NETWORK\_STATE   READ\_PHONE\_STATE   Dangerous   ACCESS\_FINE\_LOCATION  
WAKE\_LOCK   ACCESS\_WIFI\_STATE   VIBRATE

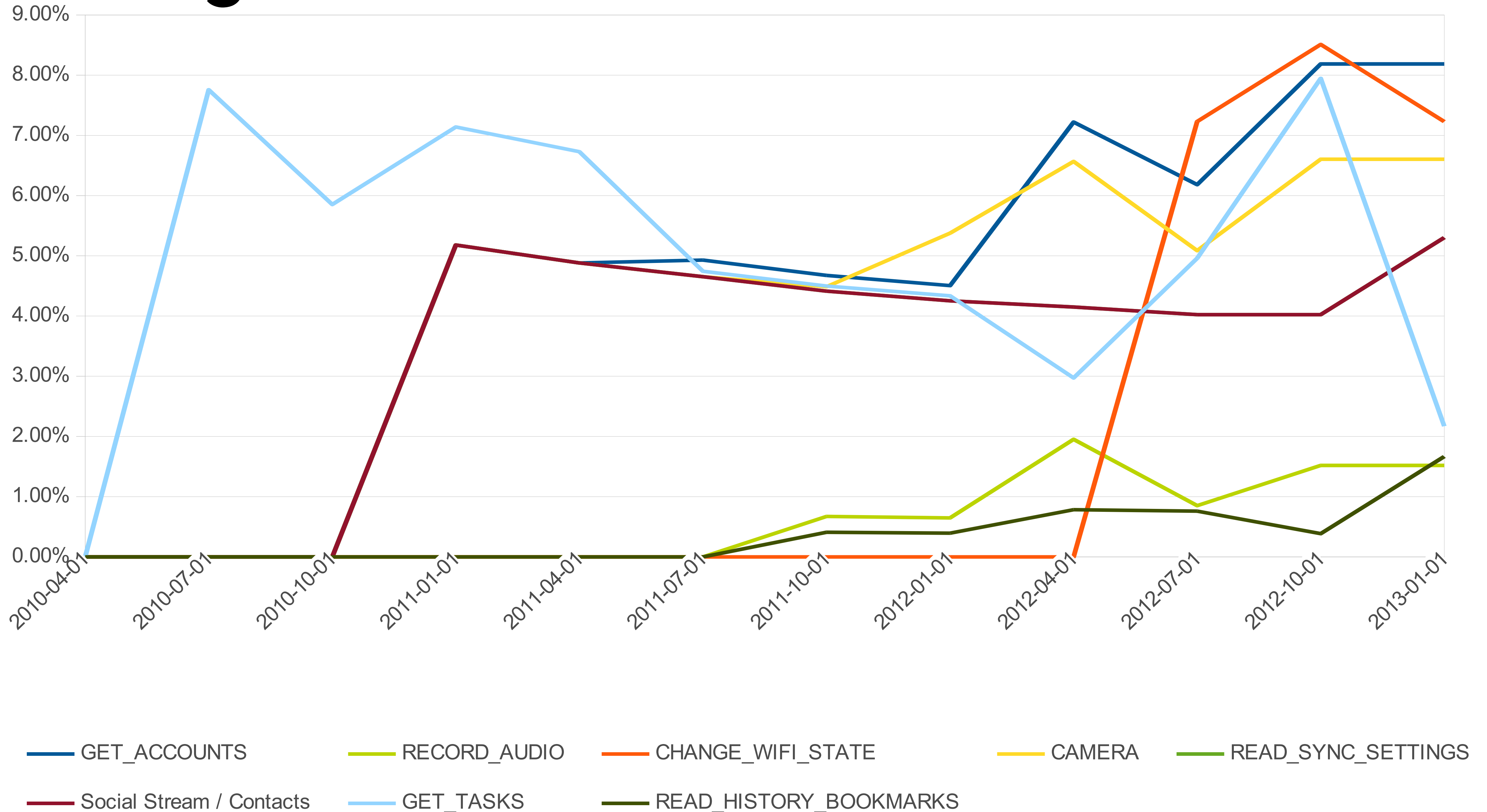


**"Dangerous"**  
*Collection of Permissions*

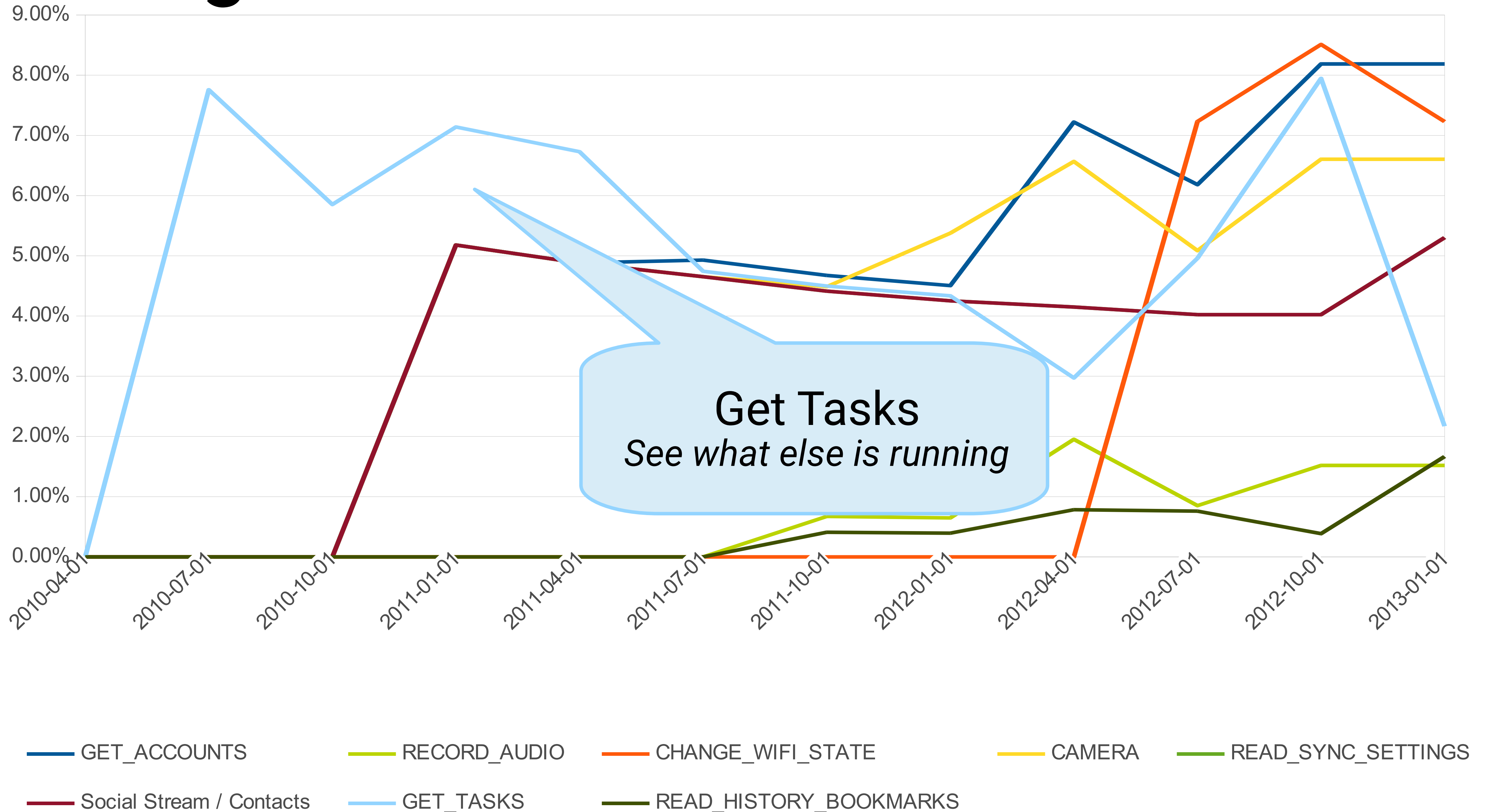
INTERNET   ACCESS\_NETWORK\_STATE   READ\_PHONE\_STATE   Dangerous   ACCESS\_FINE\_LOCATION  
WAKE\_LOCK   ACCESS\_WIFI\_STATE   VIBRATE



# “Dangerous” Permissions

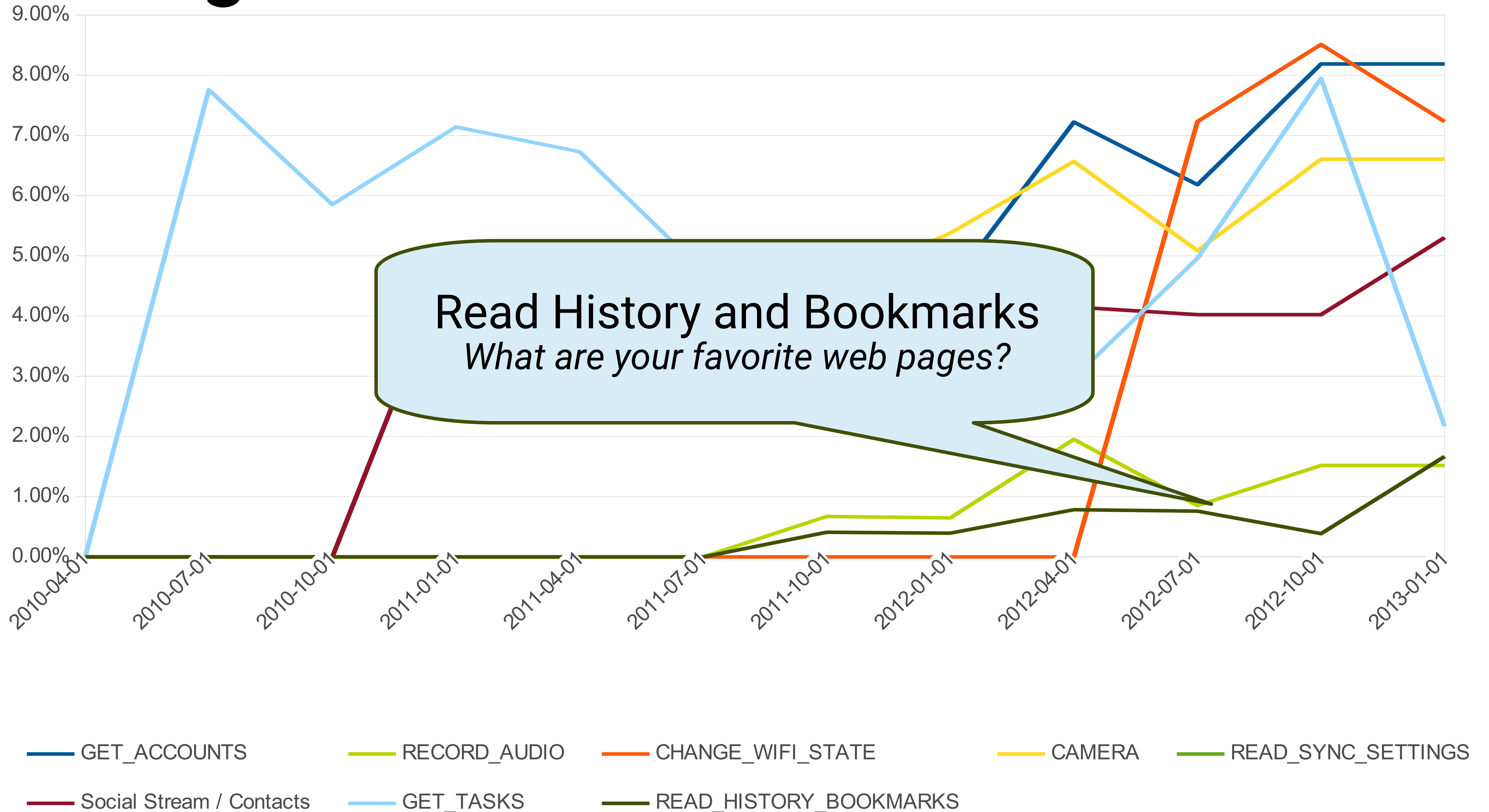


# “Dangerous” Permissions

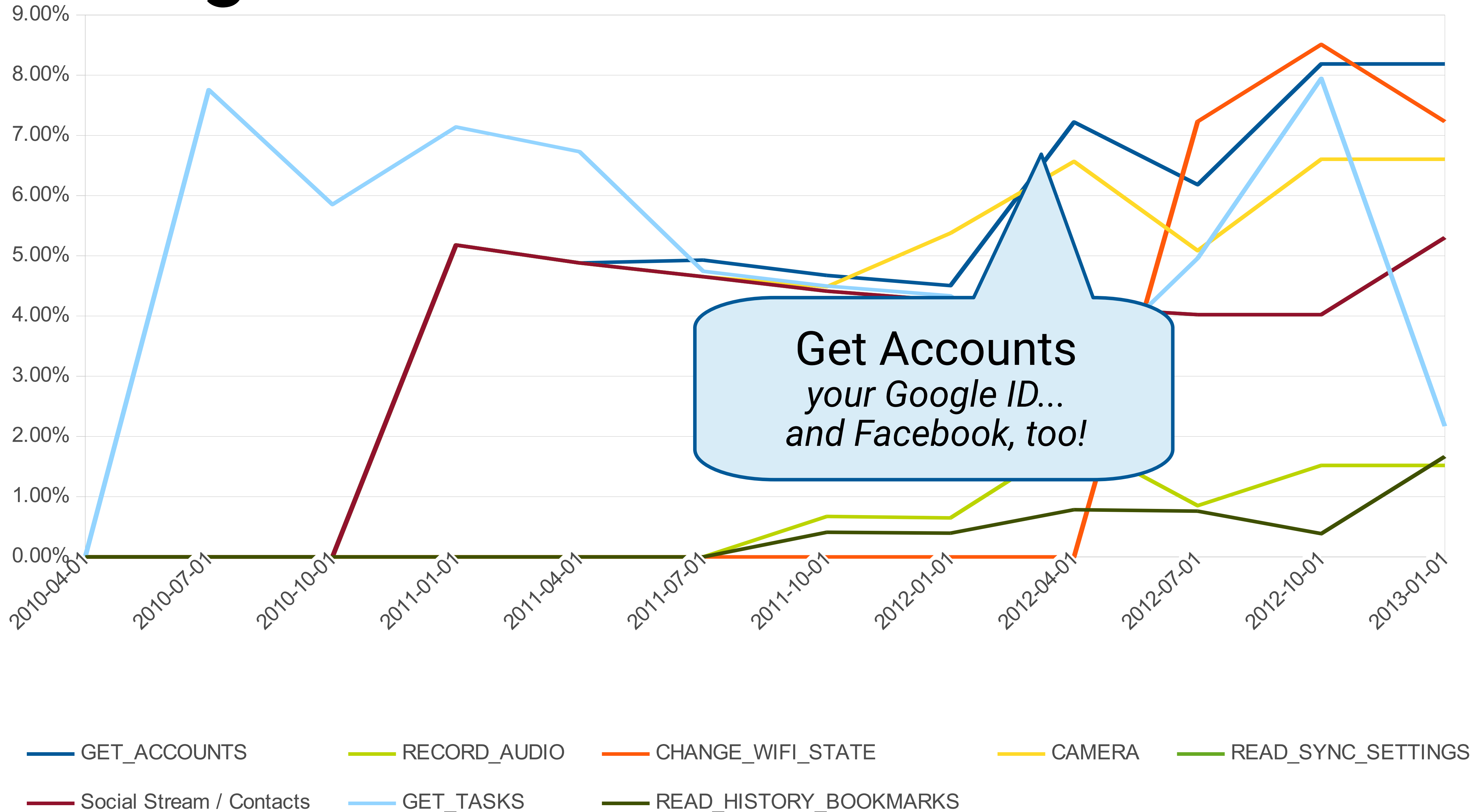




# “Dangerous” Permissions

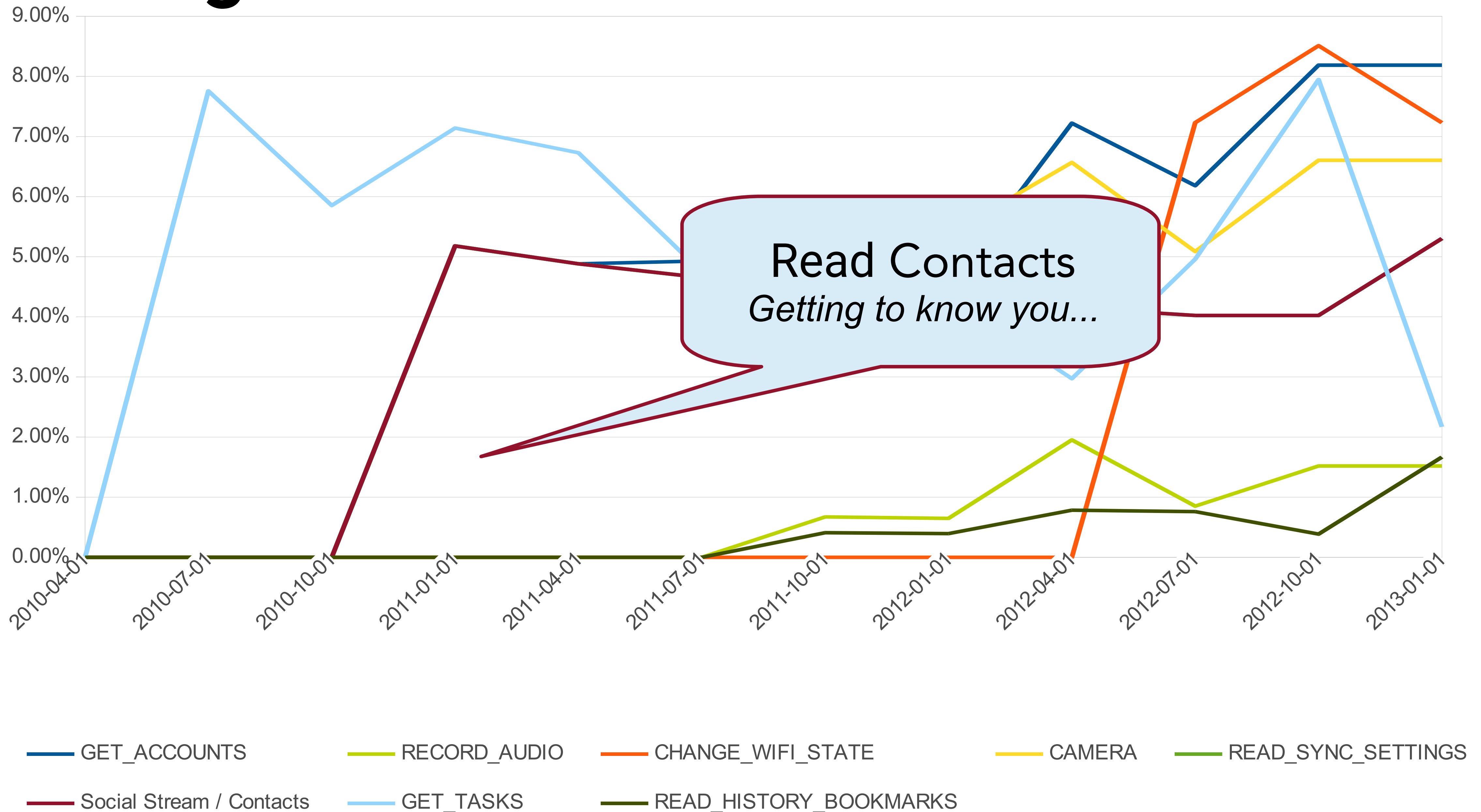


# “Dangerous” Permissions

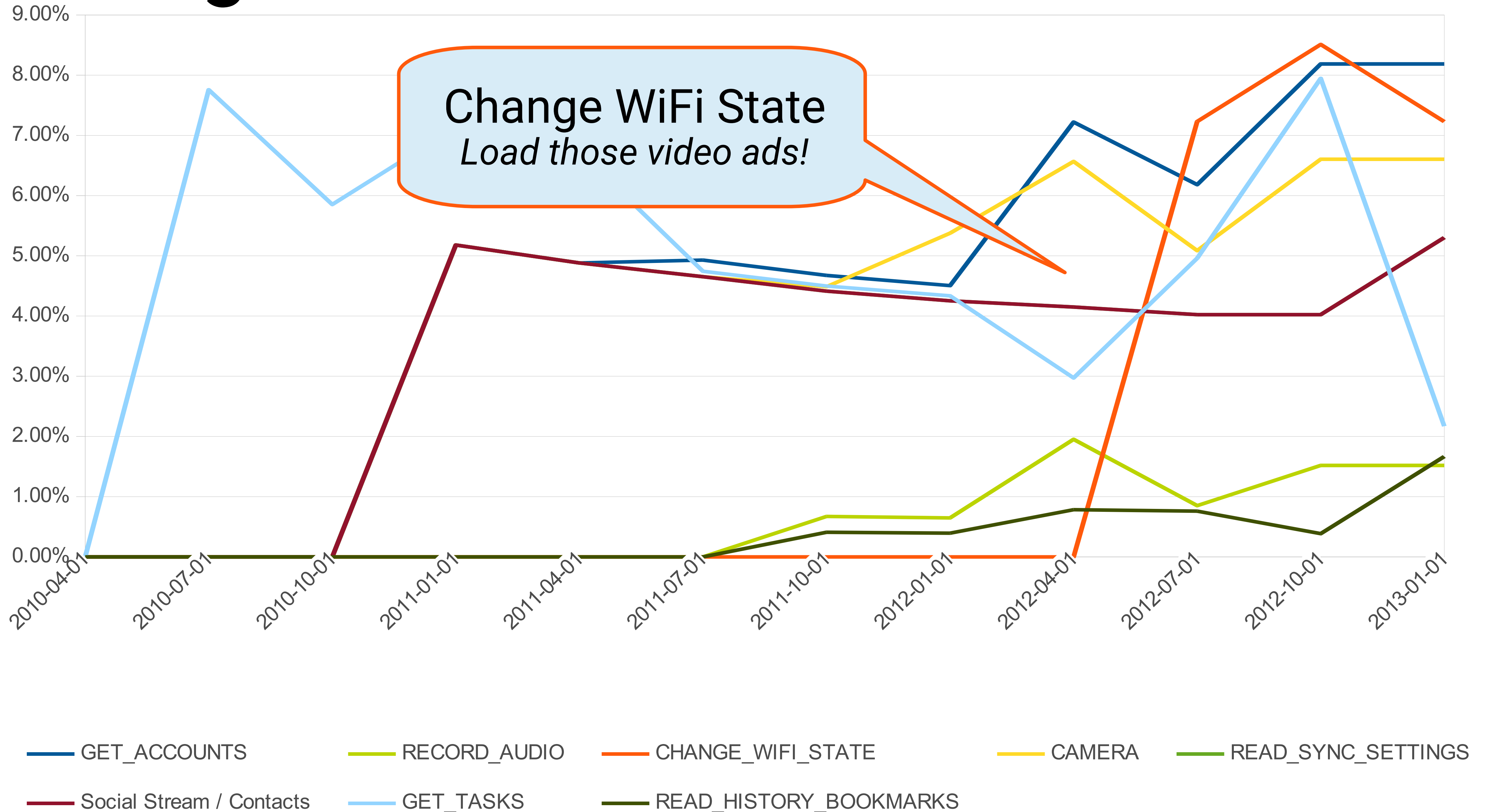




# “Dangerous” Permissions

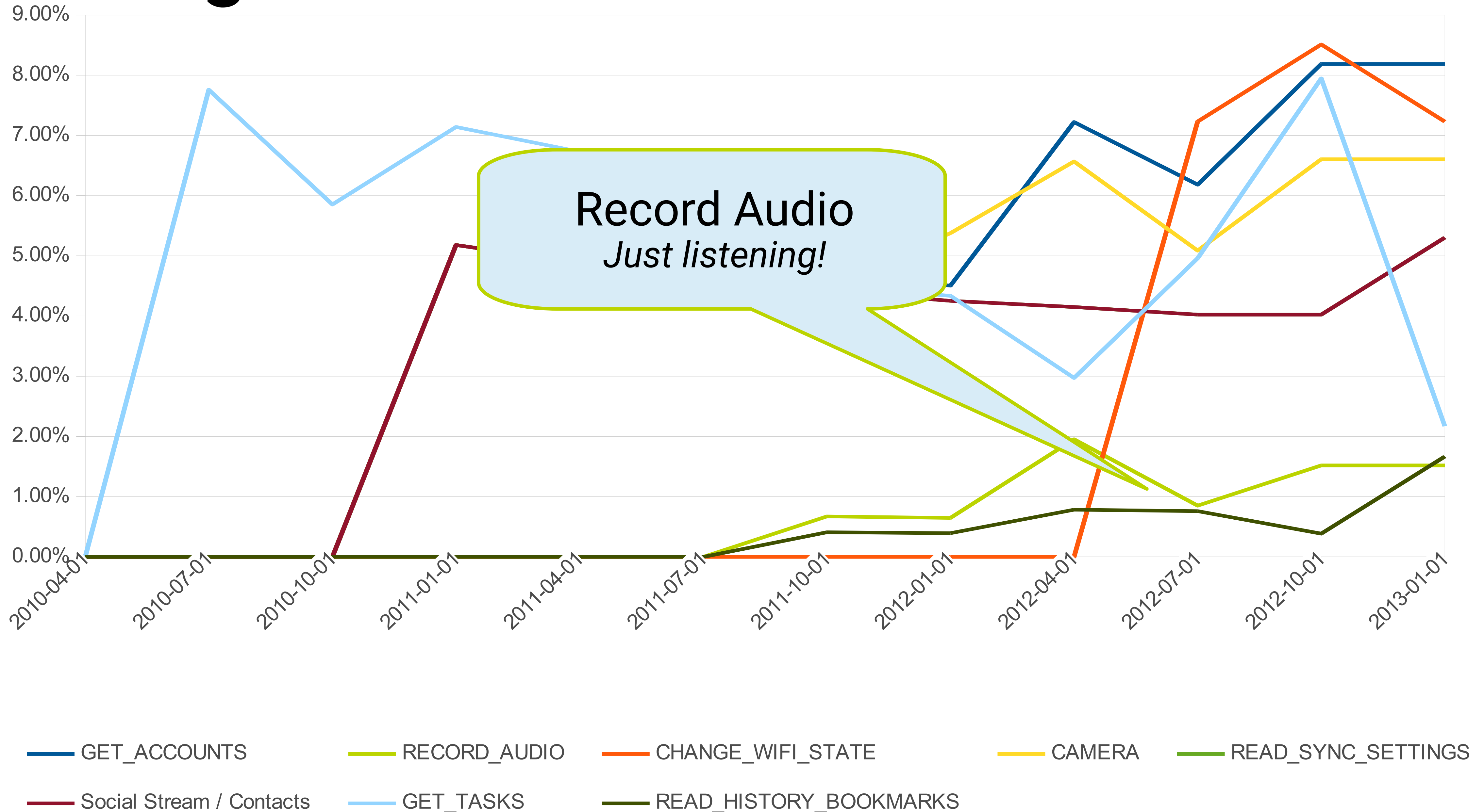


# “Dangerous” Permissions

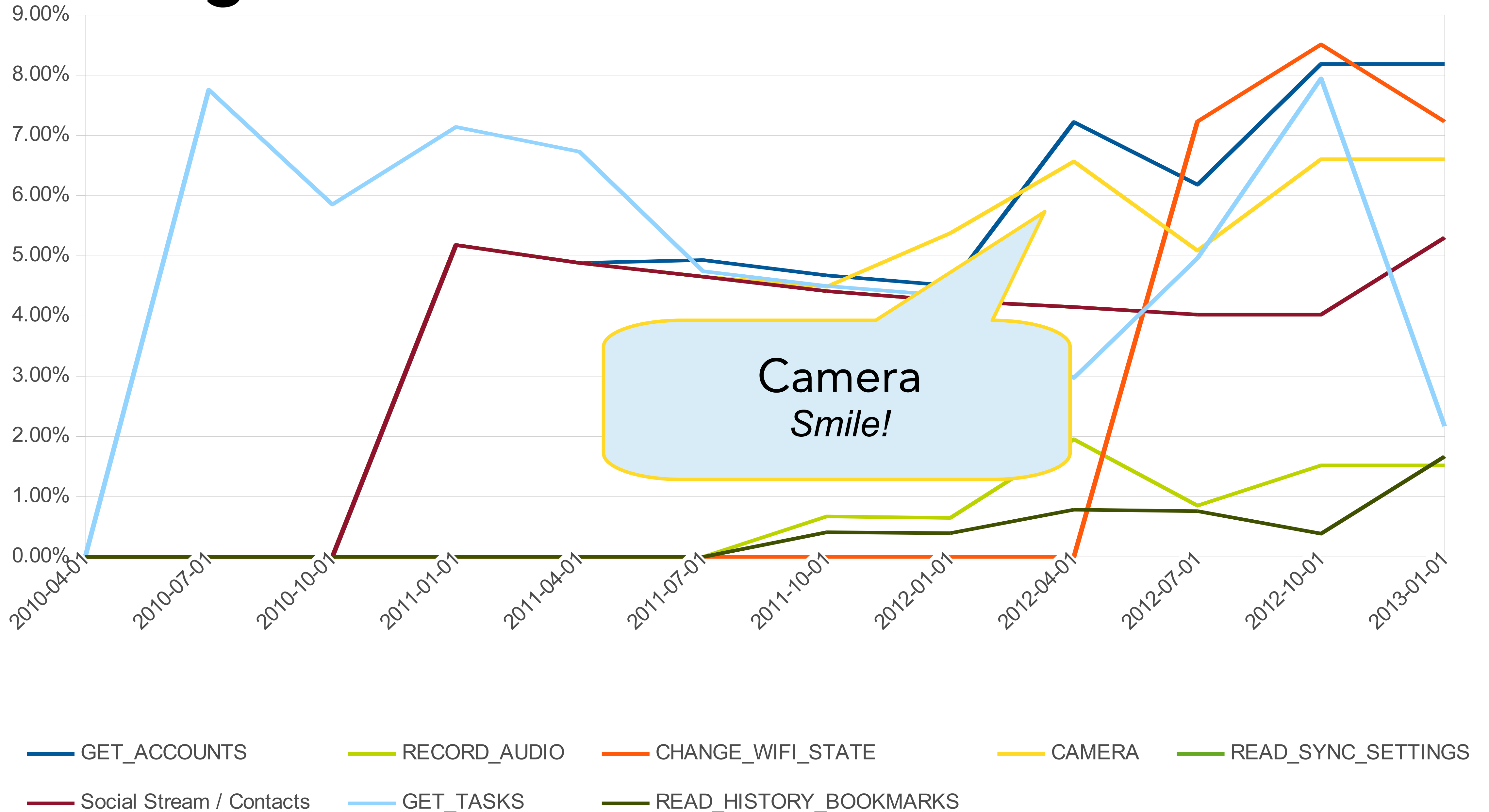




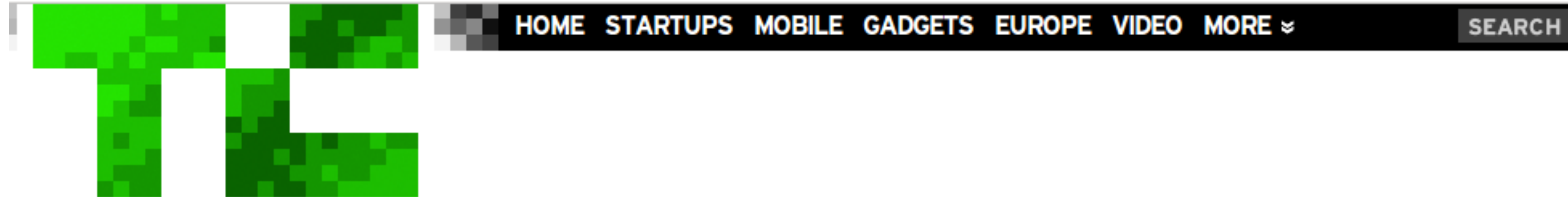
# “Dangerous” Permissions



# “Dangerous” Permissions



# The Great App Purge of 2013



HOT TOPICS [YAHOO](#) [APPLE](#) [FACEBOOK](#) [TWITTER](#) [GOOGLE](#) [MICROSOFT](#)

[CrunchGov](#) [CrunchU](#) [Guides](#) [Events](#)

[Comment](#) 27 [Like](#) 346 [Tweet](#) 791 [Share](#) 162 [+1](#) 168

## Nearly 60K Low-Quality Apps Booted From Google Play Store In February, Points To Increased Spam-Fighting

 **SARAH PEREZ** 

Monday, April 8th, 2013

27 Comments

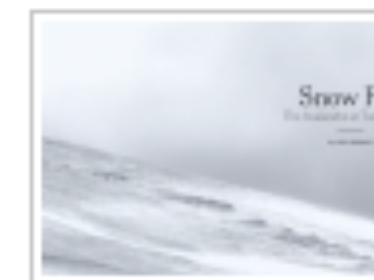


Google has stepped up its efforts to remove spammy or otherwise non-compliant applications from its mobile application marketplace, Google Play, in recent weeks. App deletions hit a record high in February, with 60,000 apps removed during the course of the month – the largest round of app deletions to date. The news of this massive app removal comes just ahead of the **rumored** launch of a revamped version of Google Play (version



HAVE A TIP, PITCH OR  
GUEST COLUMN? TELL US.

### TRENDING STORIES



**Snow Fail**



**Here's Your New  
Xbox One**



**He Should Have Ju  
Spelled It JIF Then**



# Google's actions vs. ad library

Ad Library	Percent of Apps Removed
EverBadge	60.5%
Hunt Mobile	45.5%
AirPush	40.7%
SendDroid	31.2%
Waps	29.7%
TapIt	28.4%
Average	11.6%

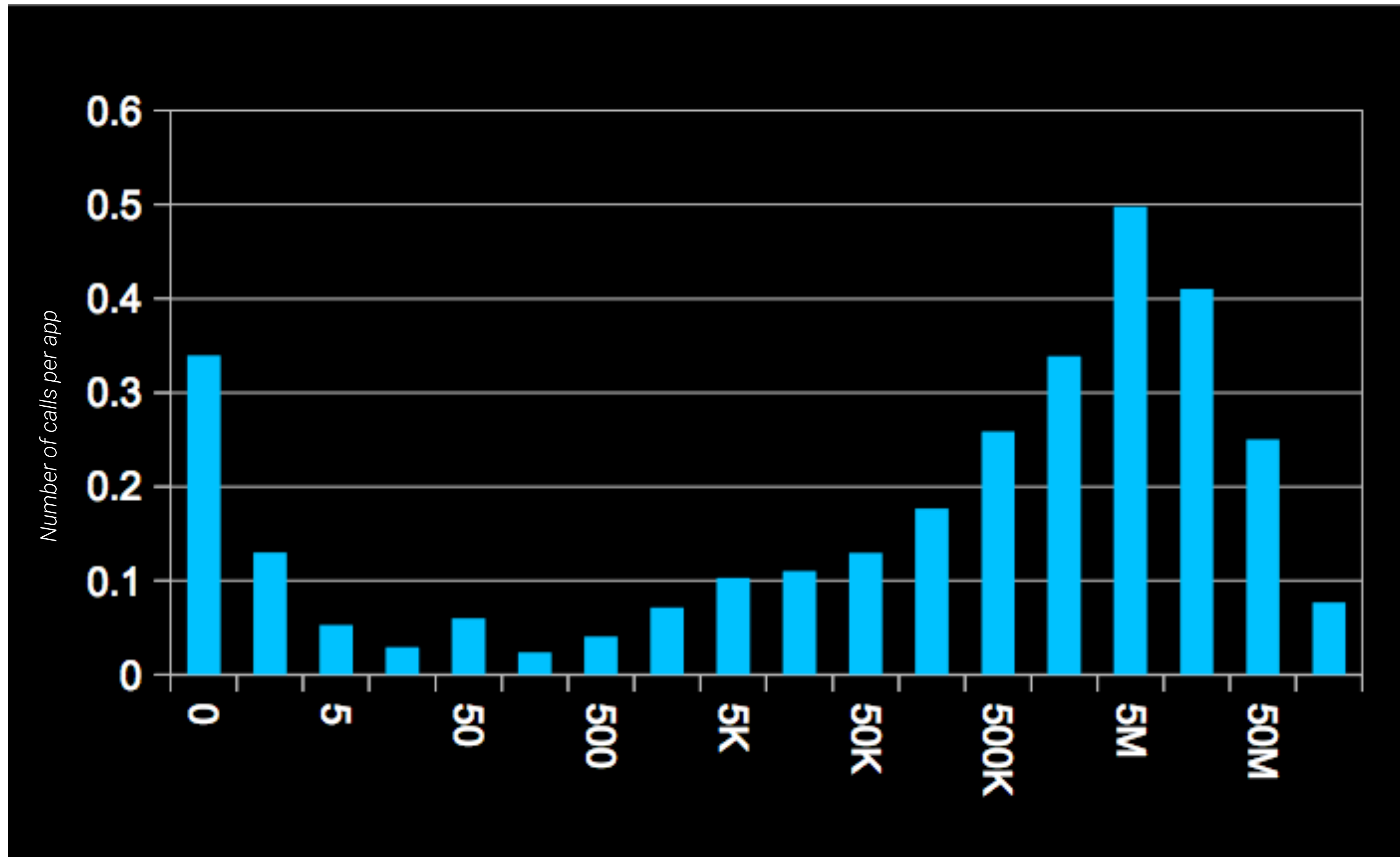
# Ad libraries have sensitive APIs

Classification	API Call
Keywords	void setKeywords(String)
Keywords	void setSearchString(String)
Gender	void setGender(GenderType)
Location	void setCurrentLocation(Location)
Age	void setAge(int)
Multiple Factors	void setRequestParams(Map)
Postal Code	void setPostalCode(String)
Enable Location	void setLocationInquiryAllowed(boolean )
Income	void setIncome(int)
Interests	void setInterests(String)
Area Code	void setAreaCode(String)
Education	void setEducation(EducationType)
Ethnicity	void setEthnicity(EthnicityType)

**Table 1: Privacy-related API calls found in the InMobi API**

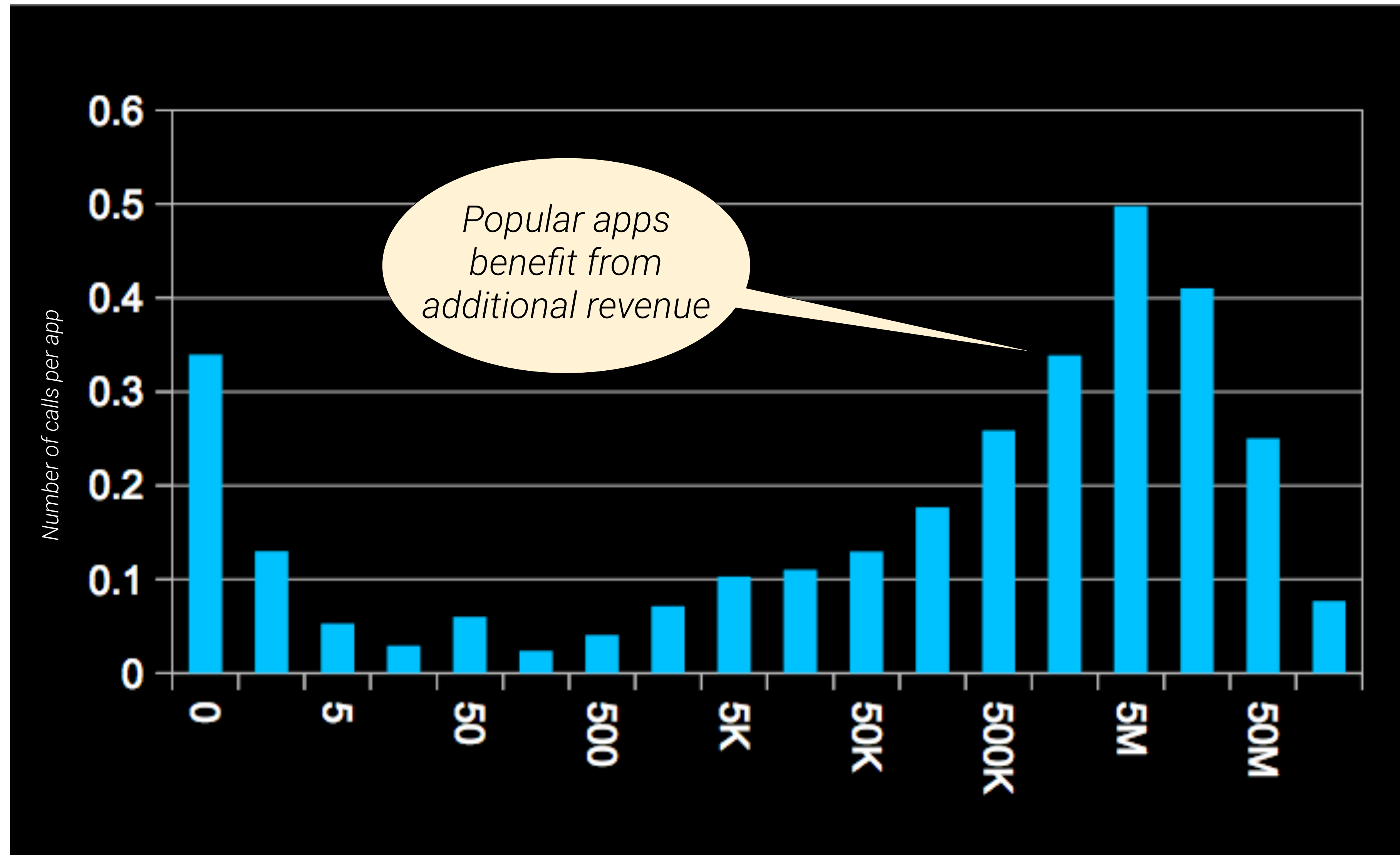
**Goal: enumerate use of these APIs in top libraries from large corpus of Android apps**

# Calls vs. Install Count

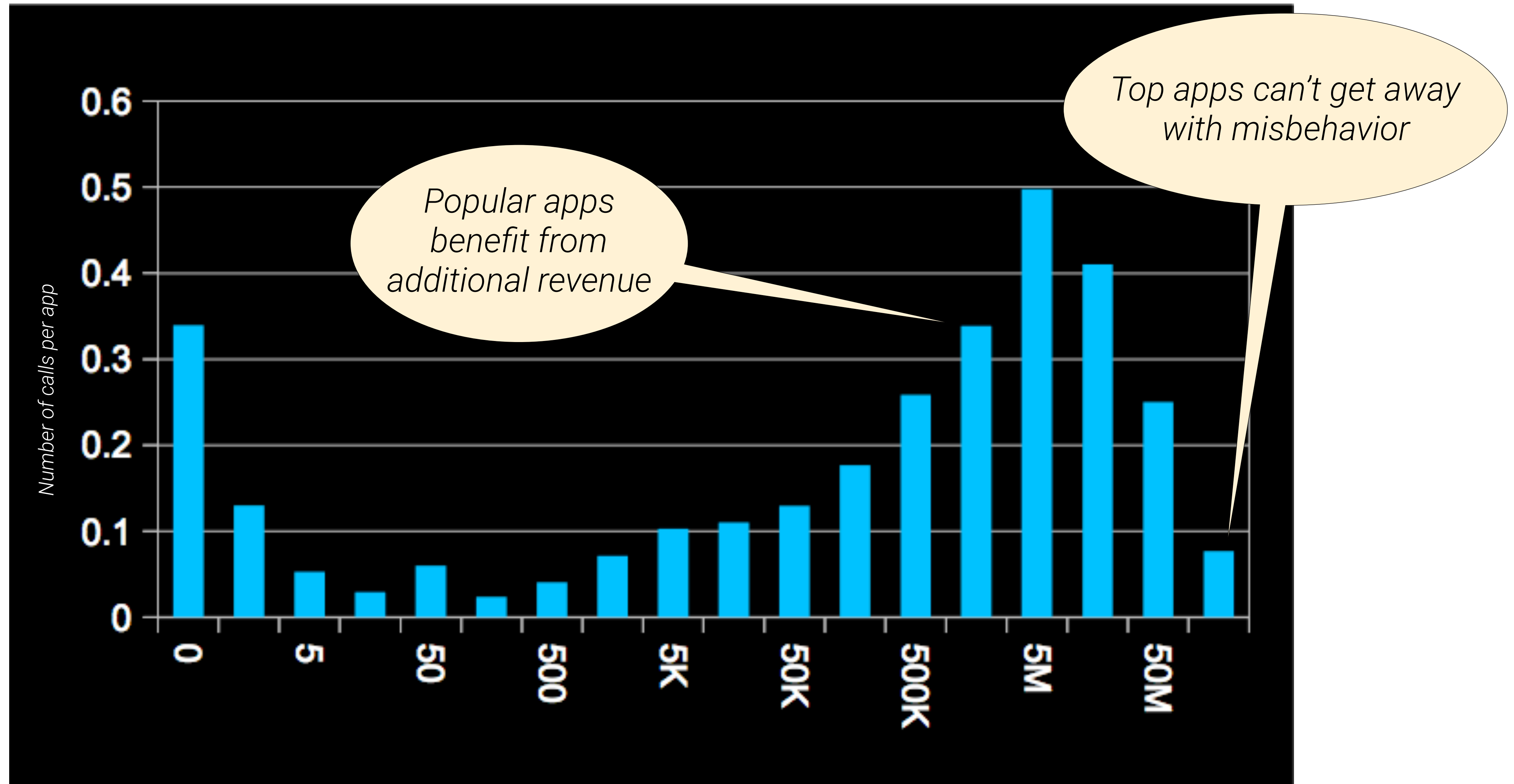




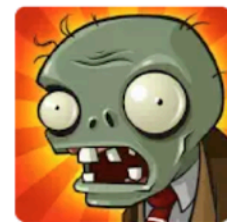
# Calls vs. Install Count



# Calls vs. Install Count



# Fine, I'll just deny them permissions



## Plants vs. Zombies FREE

ELECTRONIC ARTS 

 Everyone 10+

INSTALL

Contains ads • In-app purchases



Downloads



3,173,527 



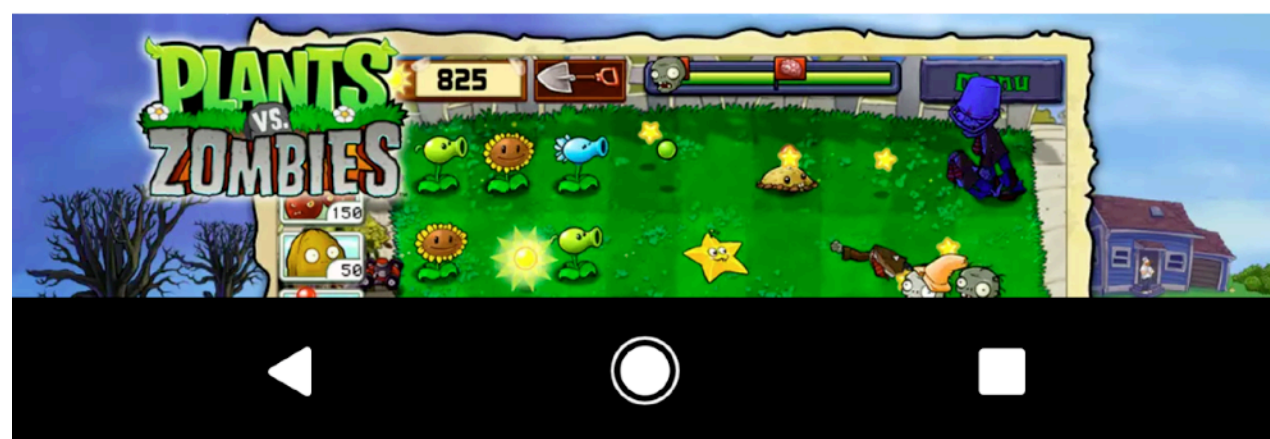
Strategy



Similar

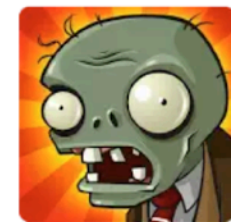
Stem a zombie attack on your yard with the help  
of powerful plants!

[READ MORE](#)





# Fine, I'll just deny them permissions



**Plants vs. Zombies FREE**

ELECTRONIC ARTS 

 Everyone 10+

INSTALL

Contains ads • In-app purchases

100  
MILLION

Downloads

4.4  
★★★★★

3,173,527 



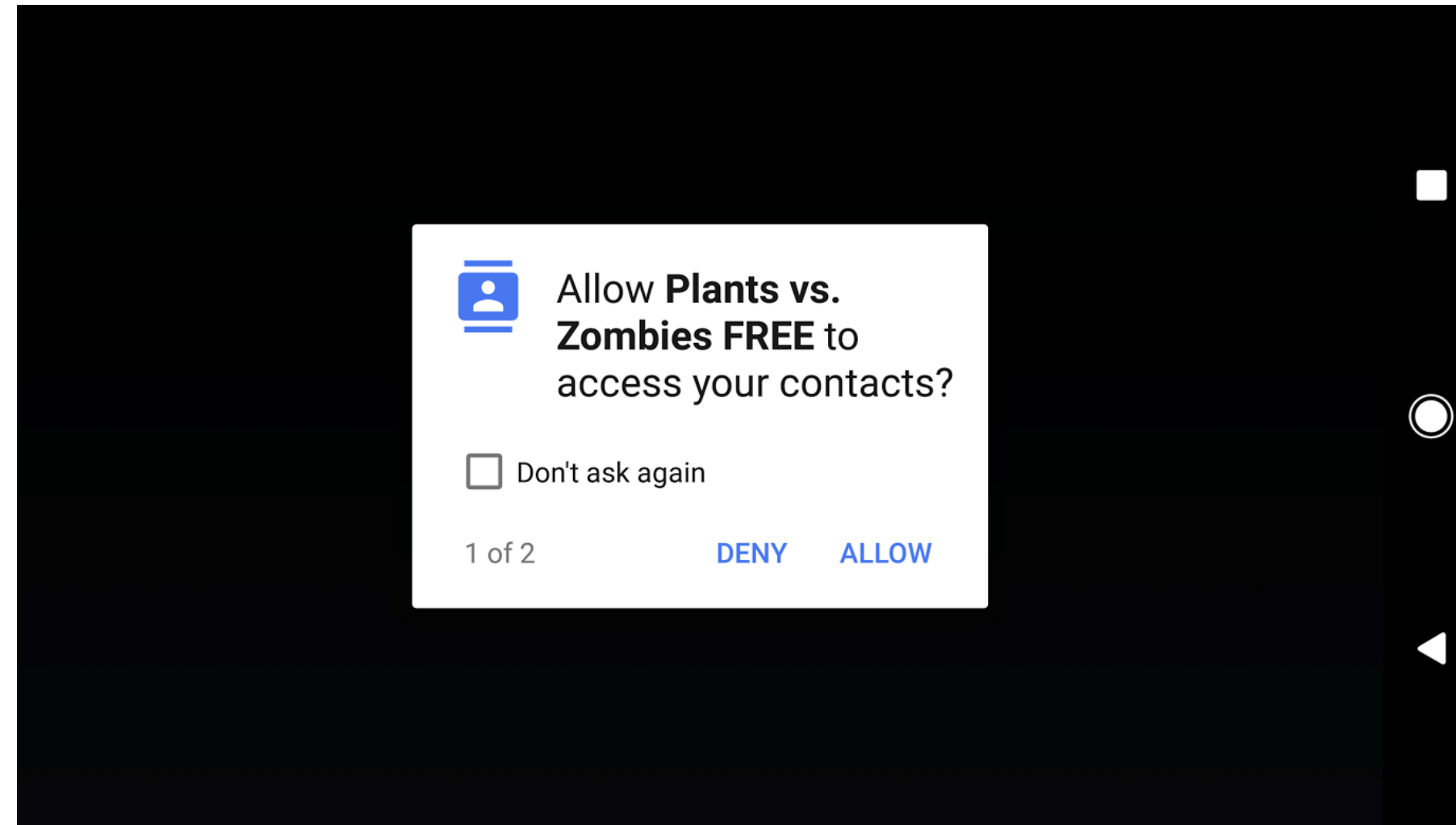
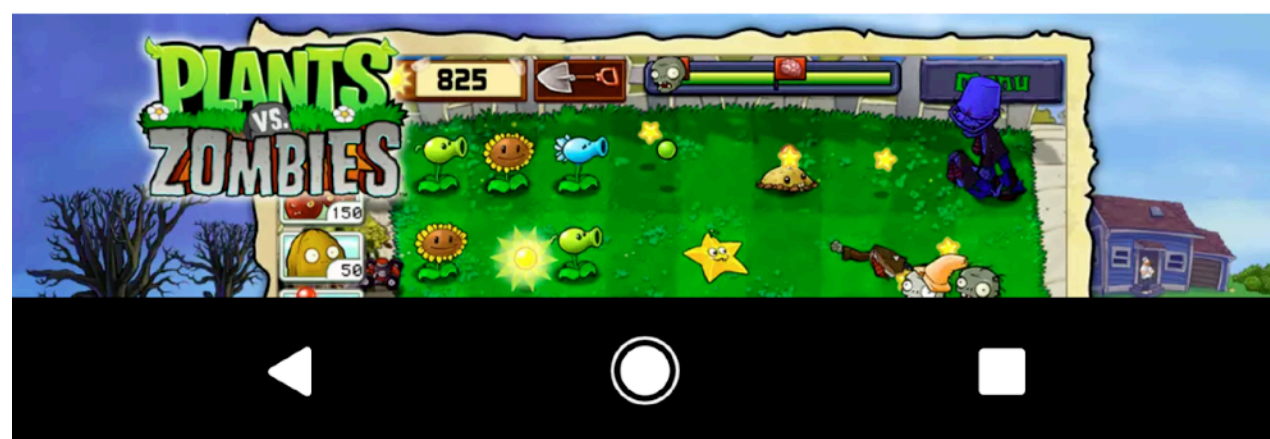
Strategy



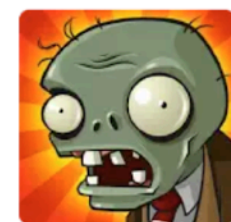
Similar

Stem a zombie attack on your yard with the help  
of powerful plants!

[READ MORE](#)



# Fine, I'll just deny them permissions



Plants vs. Zombies FREE

ELECTRONIC ARTS

Everyone 10+

INSTALL

Contains ads • In-app purchases

100  
MILLION

Downloads

4.4  
★★★★★

3,173,527



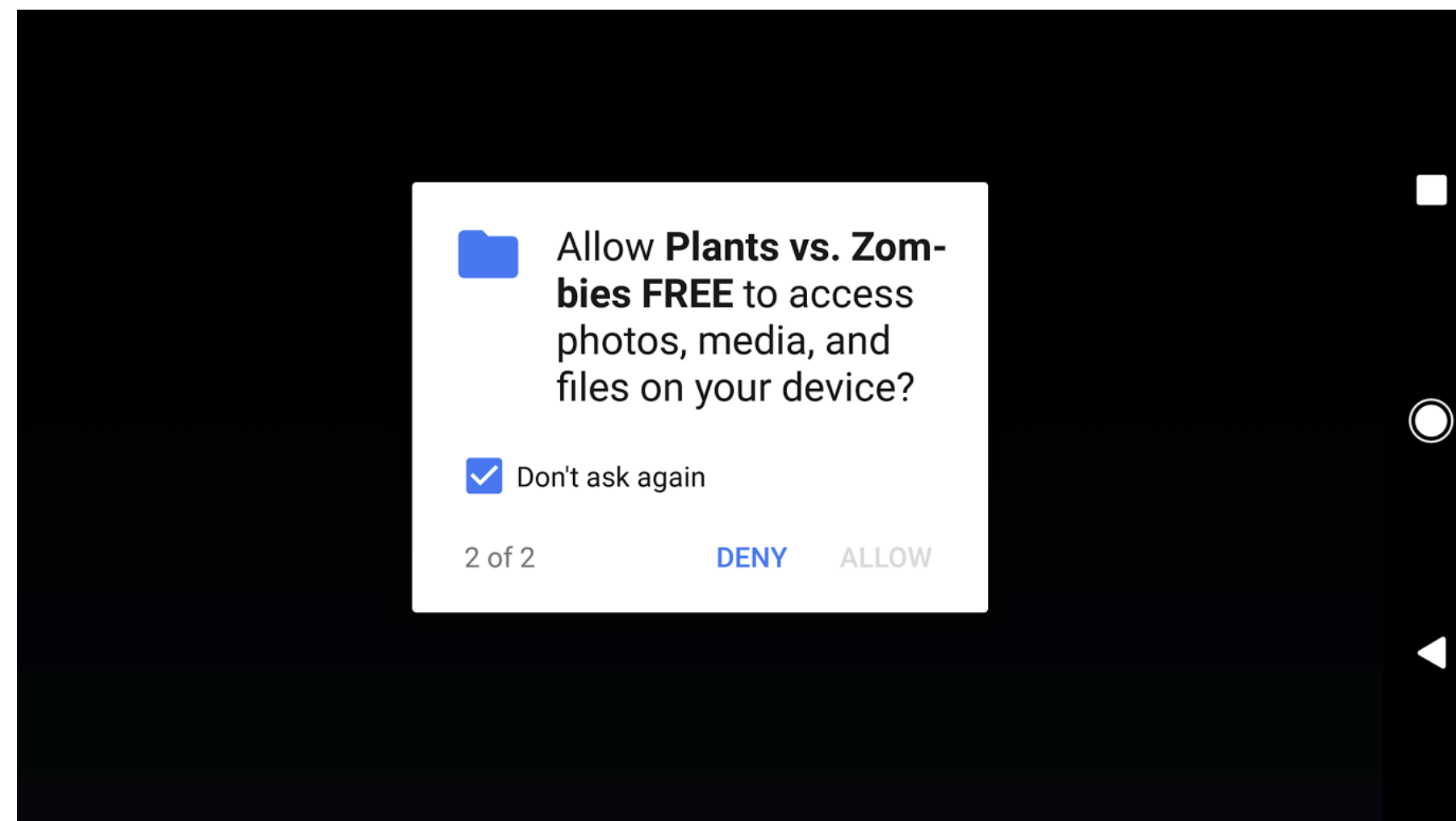
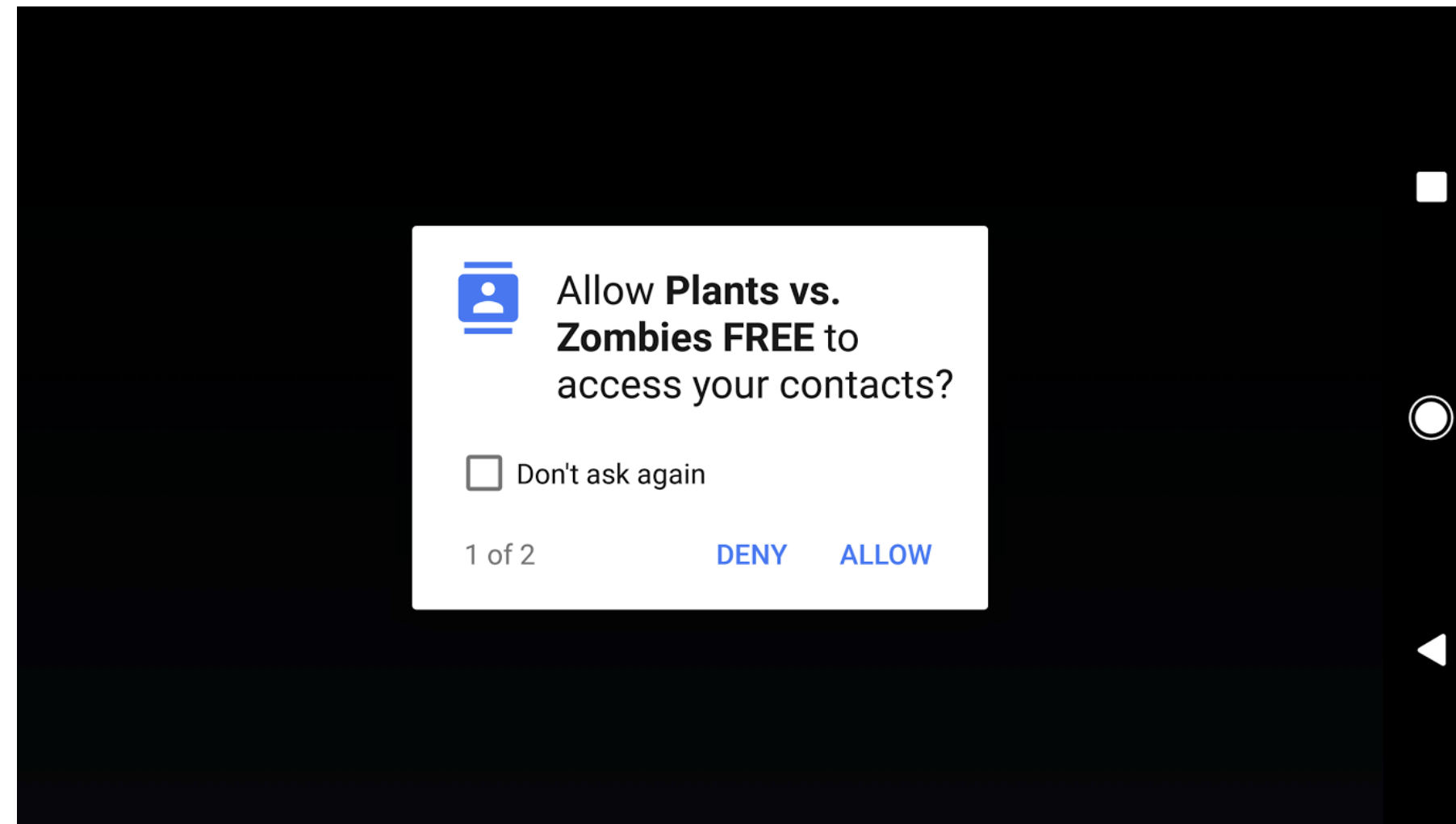
Strategy



Similar

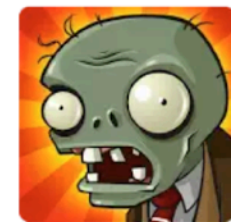
Stem a zombie attack on your yard with the help of powerful plants!

READ MORE





# Fine, I'll just deny them permissions



Plants vs. Zombies FREE

ELECTRONIC ARTS

Everyone 10+

INSTALL

Contains ads • In-app purchases

100  
MILLION

Downloads

4.4  
★★★★★

3,173,527



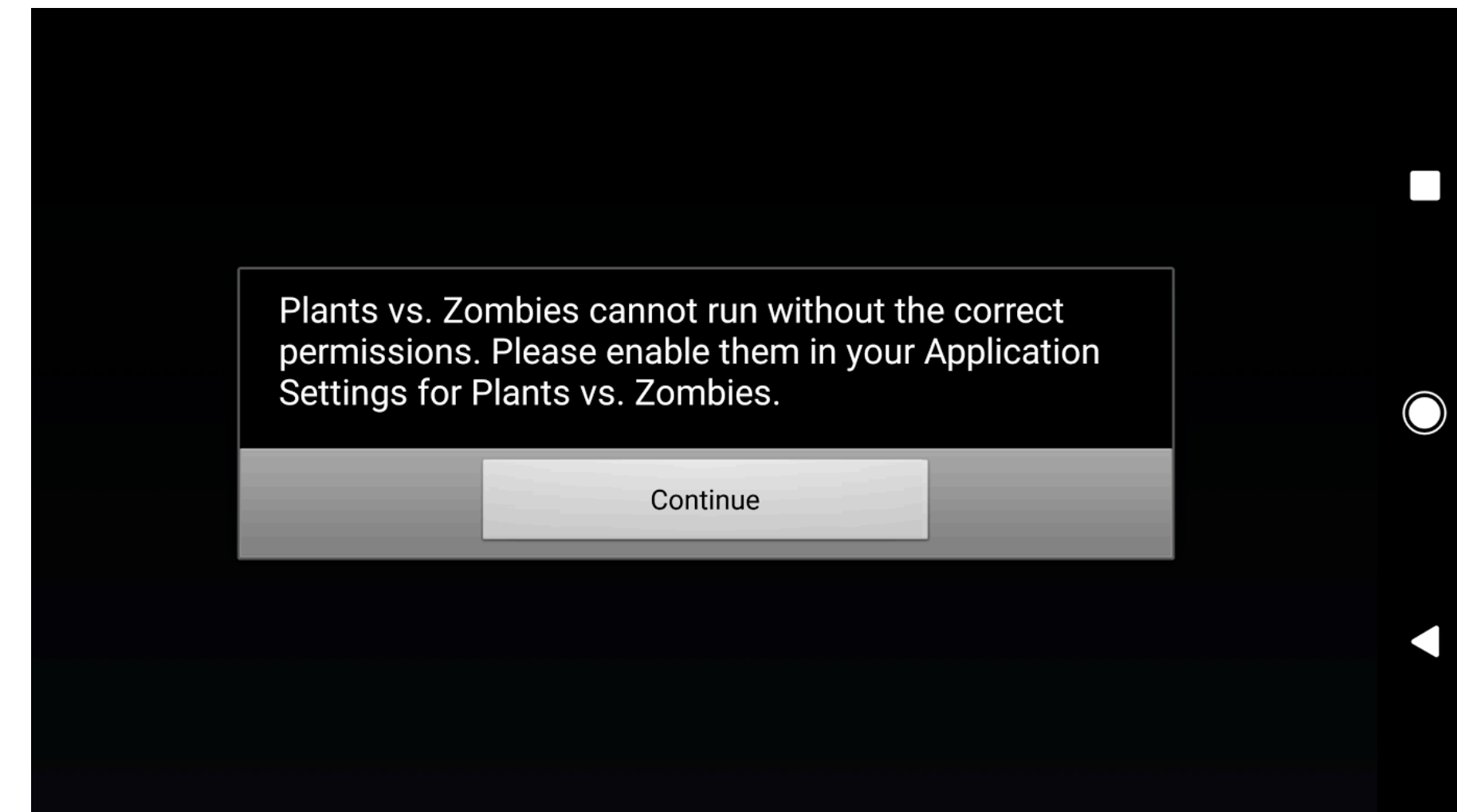
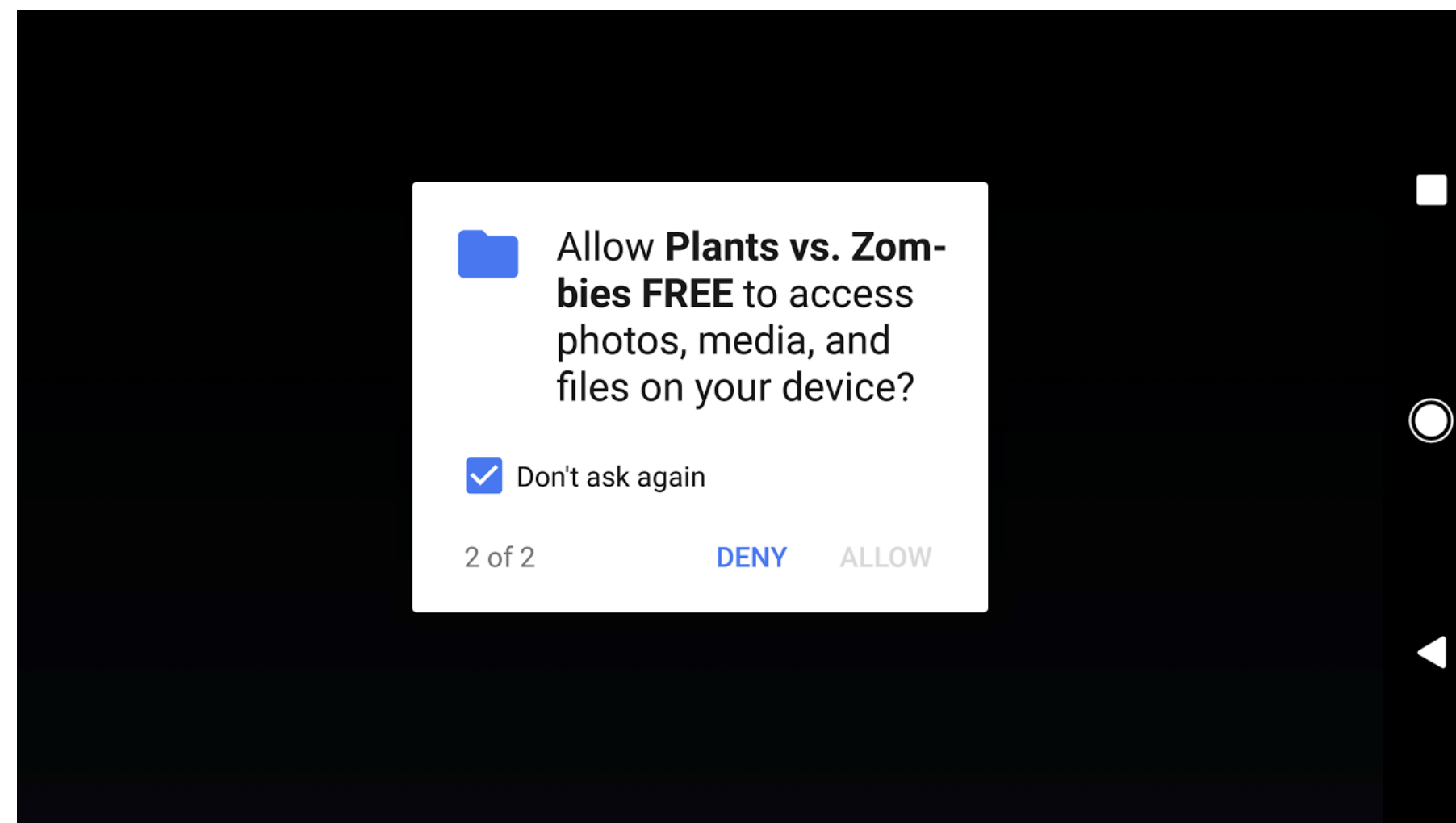
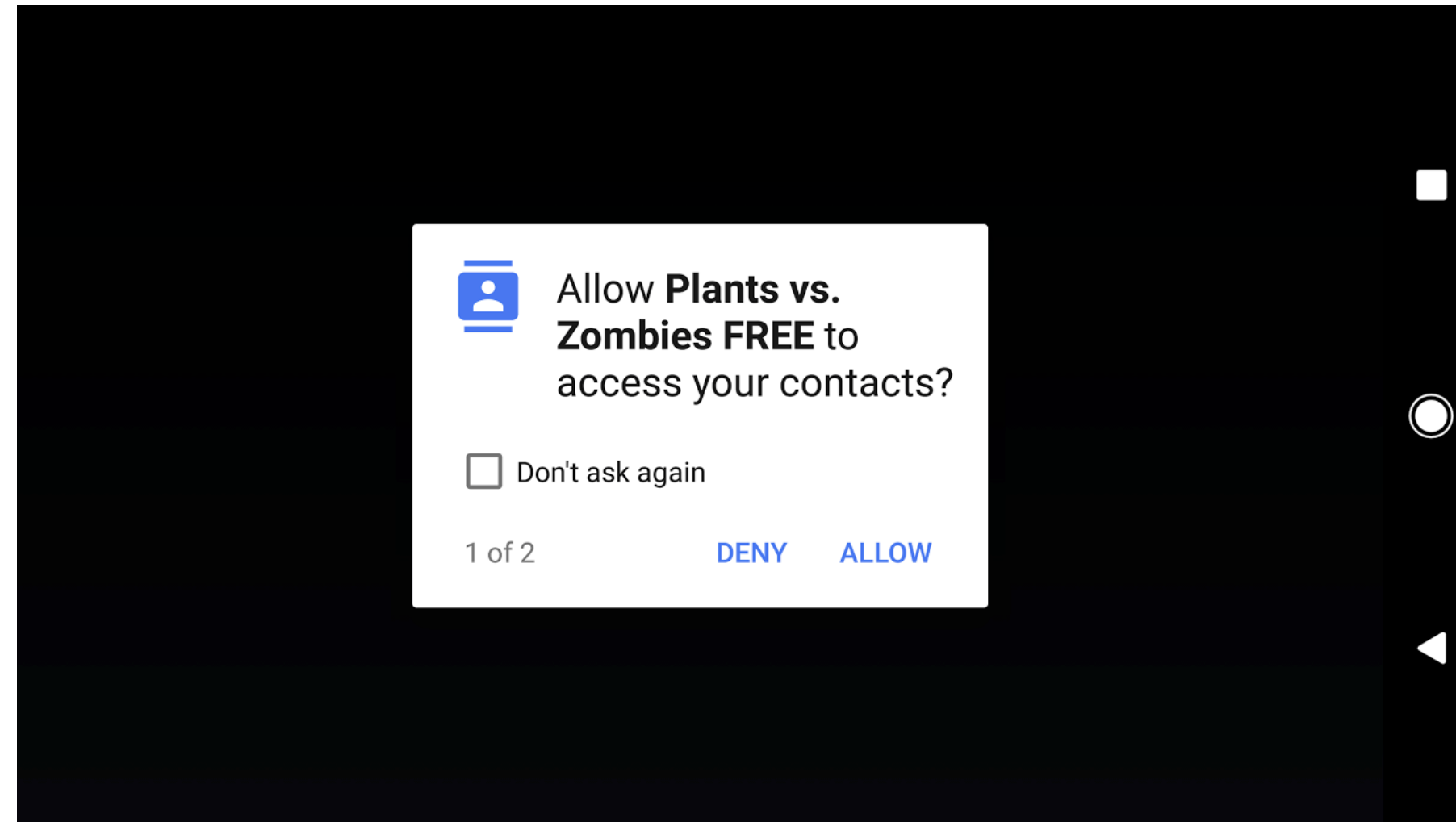
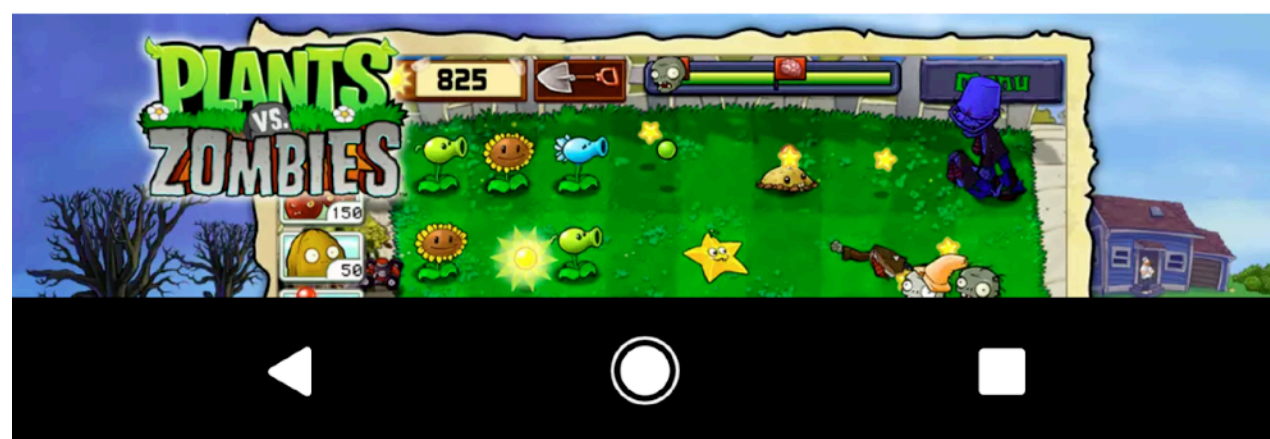
Strategy



Similar

Stem a zombie attack on your yard with the help of powerful plants!

READ MORE

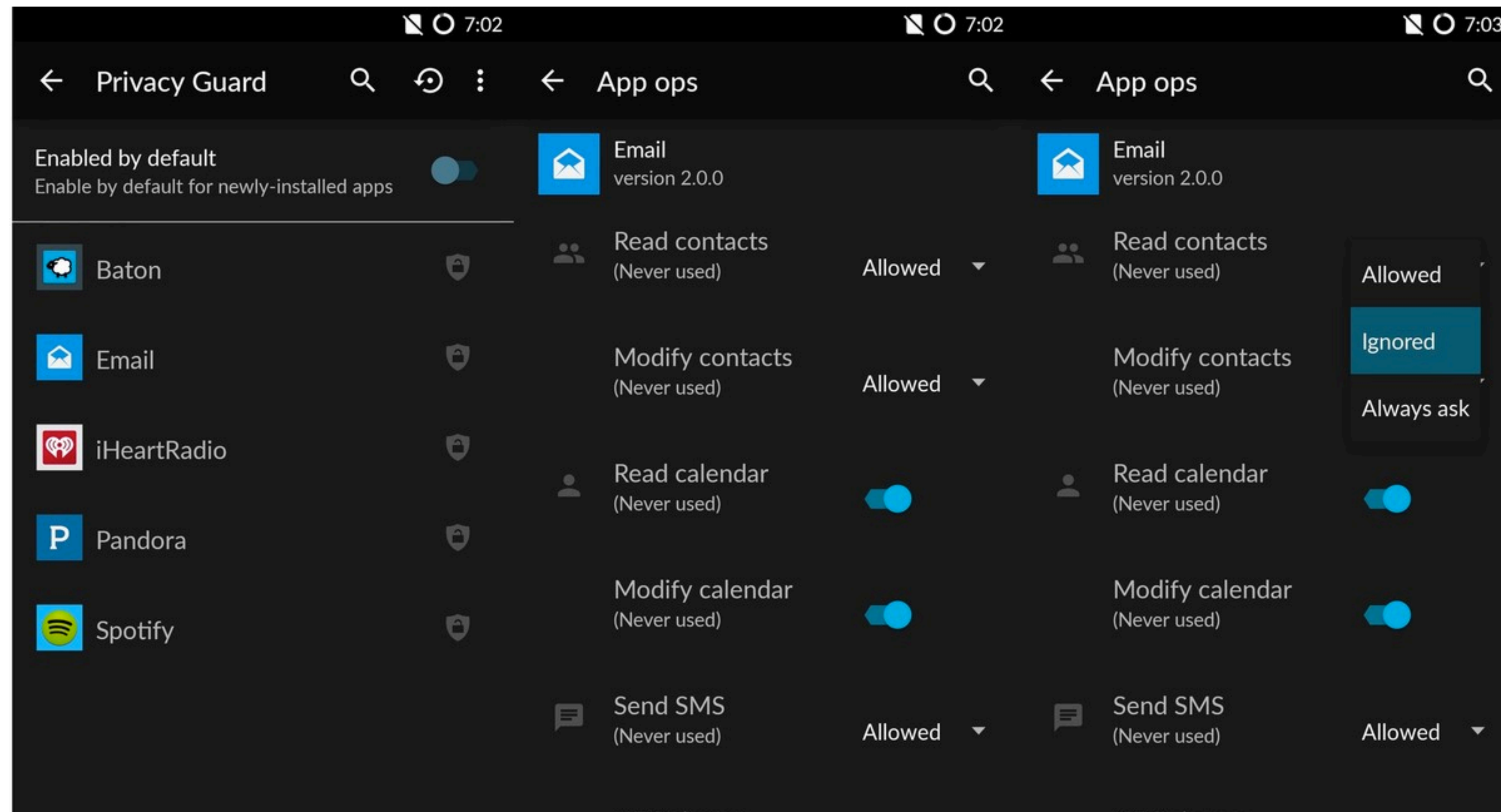




# The OS should provide privacy features

## Cyanogen / LineageOS have a “PrivacyGuard” feature

Example: Provides a contacts list with zero entries



# To root or not to root...

**Rooted phones can install ad blockers (e.g., AdAway)**

More control, better security

**Rooted phones can violate DRM**

Also, malicious apps can abuse superuser privs

Game cheats as well

**Android “O” attestation features effectively block rooting**

The screenshot shows the Android Police website. At the top, there's a navigation bar with a menu icon, the Android Police logo, and a red badge indicating '12 NEW ARTICLES'. Below the navigation bar, the main content area features a post titled '[Update: Netflix confirms] Netflix is vanishing from the Play Store for some rooted users' by Corbin Davenport, posted 8 hours ago. The post includes social media share counts (G+: 66, Facebook: 262, Twitter: 70) and a total share count of 398. The post content shows the Netflix app page with a warning: 'Your device isn't compatible with this version.' Below the warning, there are four green circular icons: '100 MILLION', '4.4', a ticket icon, and a book icon. The post is updated with two updates: 'UPDATE 1: 2017/05/13 9:36AM PDT' and 'UPDATE 2: 2017/05/13 3:24PM PDT'. The right sidebar contains a list of links: 'FOLLOW ANDROID POLICE', 'LATEST DEALS', 'LATEST POLL', 'RECENT REVIEWS', 'LATEST ROUNDUPS', 'RECENT APPS AND GAMES', and 'BLAST FROM THE PAST'.

[Update: Netflix confirms] Netflix is vanishing from the Play Store for some rooted users

Corbin Davenport  
8 hours ago

134  
G+ 66 f 262 t 70  
Total Shares 398

APPLICATIONS NEWS

**Netflix**  
Netflix, Inc.   
Teen

In-app purchases

! Your device isn't compatible with this version.

100 MILLION 4.4 ★★★★★

UPDATE 1: 2017/05/13 9:36AM PDT  
Unlocked devices without custom ROMs or root also seem to be affected. There's a chance that this could

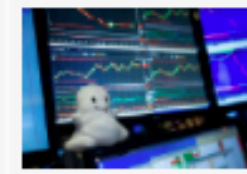
UPDATE 2: 2017/05/13 3:24PM PDT  
Netflix has confirmed it is blocking unlocked/rooted devices from installing Netflix. See this post for more

You don't see many high-profile apps blocking root users these days, with perhaps the most recent offender [being Pokemon GO](#). Now it looks like Netflix might be next. According to several reports on Reddit and other sites), the Netflix app is showing up as incompatible with some rooted devices.

FOLLOW ANDROID POLICE  
LATEST DEALS  
LATEST POLL  
RECENT REVIEWS  
LATEST ROUNDUPS  
RECENT APPS AND GAMES  
BLAST FROM THE PAST



## CMO TODAY



What Marketers  
Should Note From  
Snap's First Earnings  
Call



Digital Media World  
Tries to Decode  
Facebook's Latest  
Algorithm Tweak



Fox Names Joe  
Marchese President  
of Ad Revenue



Hulu Names AMC's  
Joel Stillerman as  
Chief Content Officer



Sinclair-  
Combo C  
Future A  
TV Giant



[BUSINESS](#) | [MEDIA & MARKETING](#) | [CMO](#)

# Google Plans Ad-Blocking Feature in Popular Chrome Browser

Filter could strip out ads that provide bad experiences for users



PHOTO: AGENCE FRANCE-PRESSE/GETTY IMAGES

By **Jack Marshall**

Updated April 19, 2017 7:18 p.m. ET

 86 COMMENTS

Alphabet Inc.'s Google is planning to introduce an ad-blocking feature in the mobile and desktop versions of its popular Chrome web browser, according to people familiar with the company's plans.

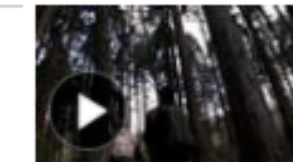
The ad-blocking feature, which could be switched on by default within Chrome, would filter out certain online ad types deemed to provide bad experiences for users as they move around the web.

## Recommended Videos

1. **Comey Firing  
Fallout: 3 Things to  
Know**



2. **'Forest Bathers'  
Seek Therapeutic  
Effects of Trees**



3. **Bargains Off the  
Beaten Track**



4. **Lesson From  
France: Has  
Populism Peaked?**




5. **Senate Leaders  
Respond to Comey  
Firing**



## Most Popular Articles

1. **Comey's Firing  
Came as  
Investigators  
Stepped Up Russia  
Probe** 




2. **Snapchat Parent  
Posts Disappointing  
User Growth; Stock  
Plunges** 



3. **Opinion: Comey's  
Deserved Dismissal** 



4. **Opinion: The James  
Comey Show** 



What about  
Android-native  
ad libraries?



# Summary so far

**Advertising-supported free apps want to make money**

More user information = more money

**OS permission requests only partially protect users**

Some apps really do need to read your contacts or learn your location

Some apps *refuse to run if you deny them permissions*

**Very little that third-party researchers can do here**

**Usability: trusted path**

# Old-school idea: trusted path

## Unforgeable labels

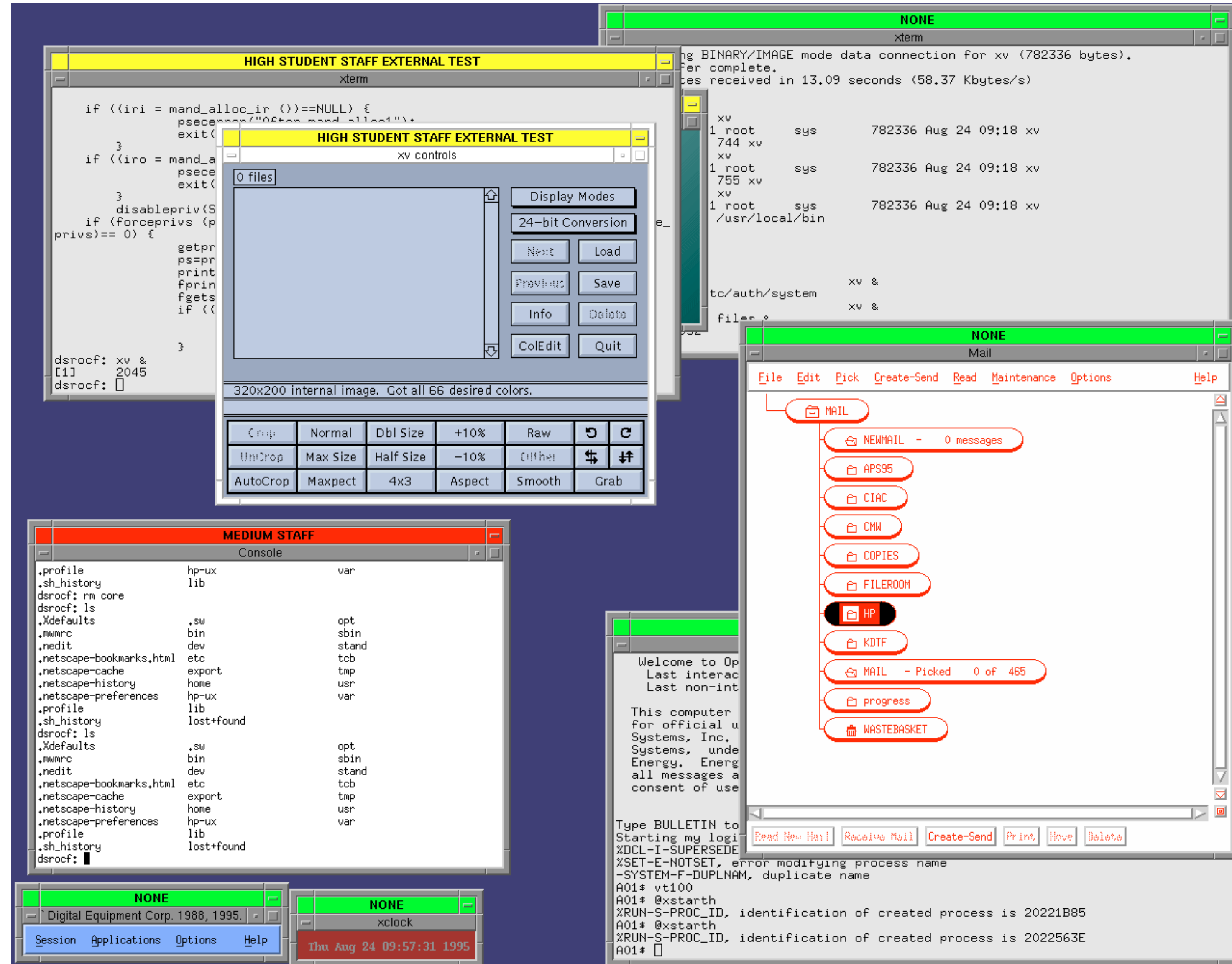
Prevent apps from spoofing one another

## Trusted user input paths

Uninterruptible path for user to speak to the system

(Example: Ctrl-Alt-Del in older Windows NT for login.)

Screenshot: Compartmented Mode Workstation (early 1990's)







# GDC4S SME PED





# Trusted path features

Launch Keys  
Windows Start,  
Web Browser

Call / Send Key  
Place and answer  
phone calls

QWERTY Keyboard  
Full keyboard & phone  
with backlighting

Unclassified Key  
Unclassified PDA

Incoming calls, messages,  
appointments  
• Unlocked (PIN entered)

Power / End Key  
Turn device on/off, exit  
previous menu and end  
calls

Classified Key  
Selects Classified PDA  
Security Menu

Trusted Display  
Security menus



# Trusted path features

Launch Keys  
Windows Start,  
Web Browser

Call / Send Key  
Place and answer  
phone calls

QWERTY Keyboard  
Full keyboard & phone  
with backlighting

Unclassified Key  
Unclassified PDA

Incoming calls, messages,  
appointments  
• Unlocked (PIN entered)

Power / End Key  
Turn device on/off, exit  
previous menu and end  
calls

Classified Key  
Selects Classified PDA  
Security Menu

Separate display, managed by  
crypto module



# Trusted path features

Launch Keys  
Windows Start,  
Web Browser

e / Send Key  
Place and answer  
phone calls

TY Keyboard  
keyboard & phone  
with backlighting

Unclassified Key  
Unclassified PDA

Incoming calls, messages,  
appointments  
• Unlocked (PIN entered)

Power / End Key  
Turn device on/off, exit  
menu and end  
calls

Classified Key  
Selects Classified PDA  
Security Menu

Dedicated mode selectors

Separate display, managed by  
crypto module

# OAuth phishing

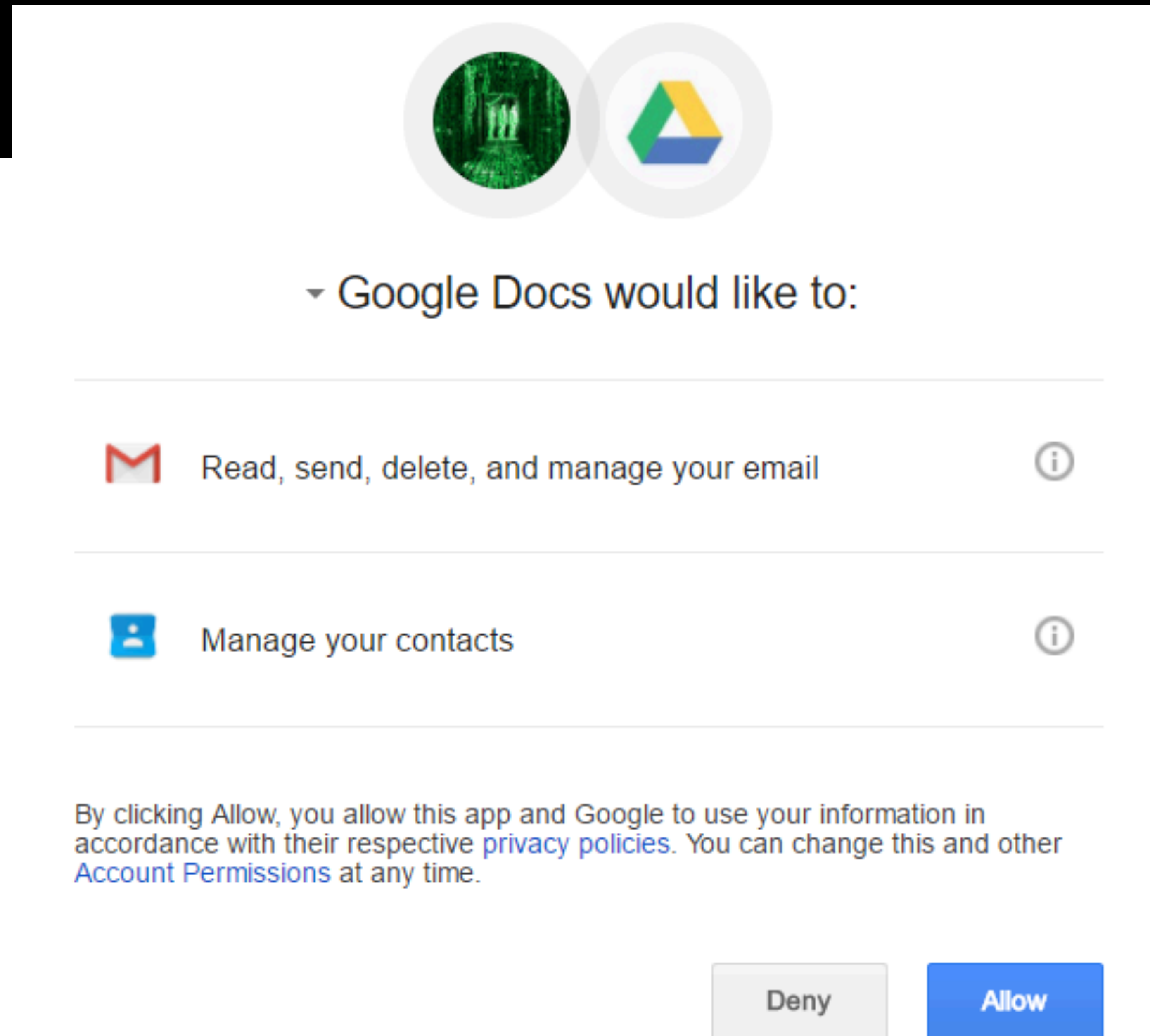
**We want to hide security indicators**

Users probably wouldn't notice, even if prominent

**Google's solution?**

Better anti-spam features

"Google" in name now special





# OAuth phishing

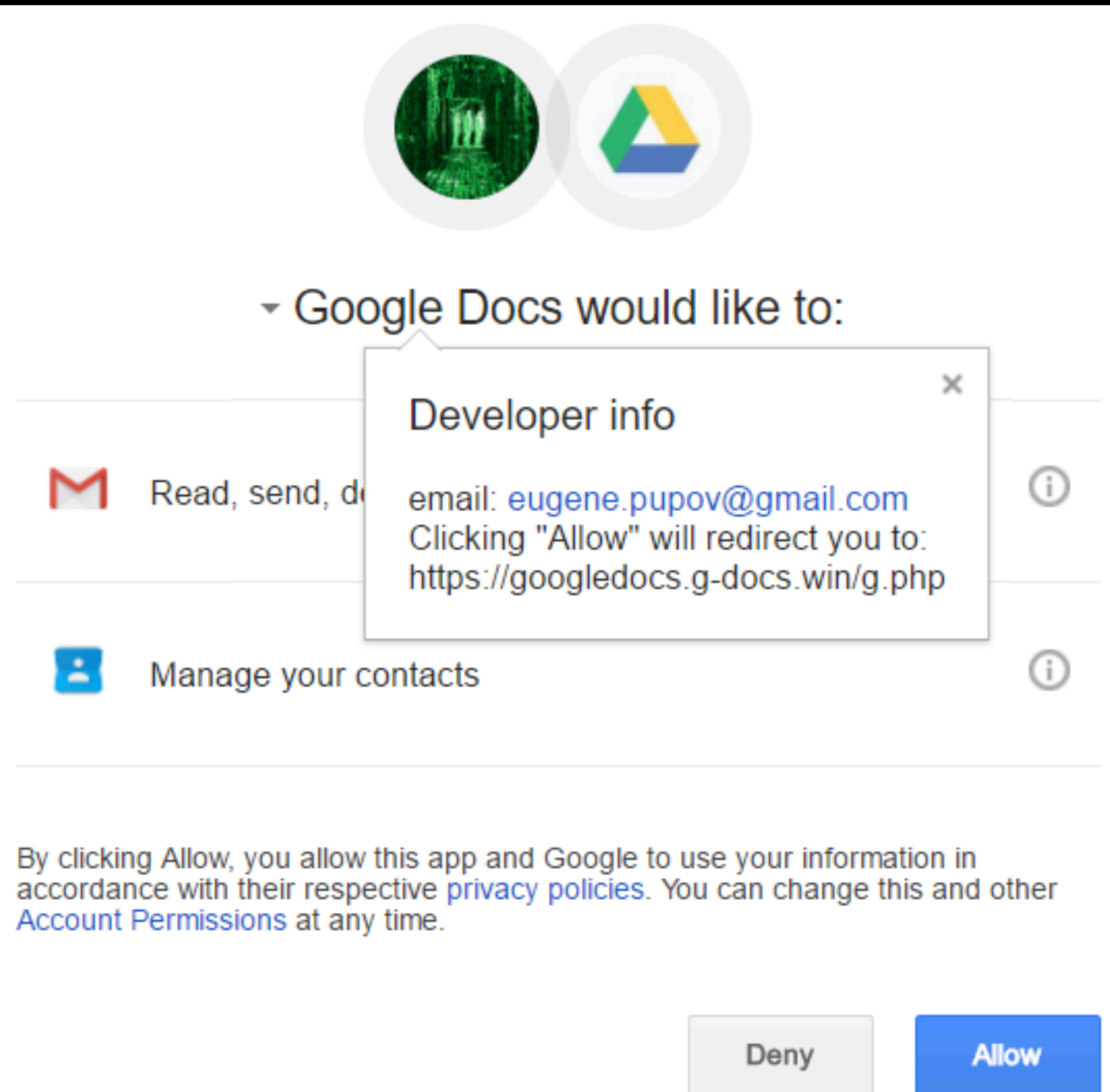
**We want to hide security indicators**

Users probably wouldn't notice, even if prominent

**Google's solution?**

Better anti-spam features

"Google" in name now special





# Phishing on mobile

**Web browsers try to get out of the way**

Less chance for chrome context to help you

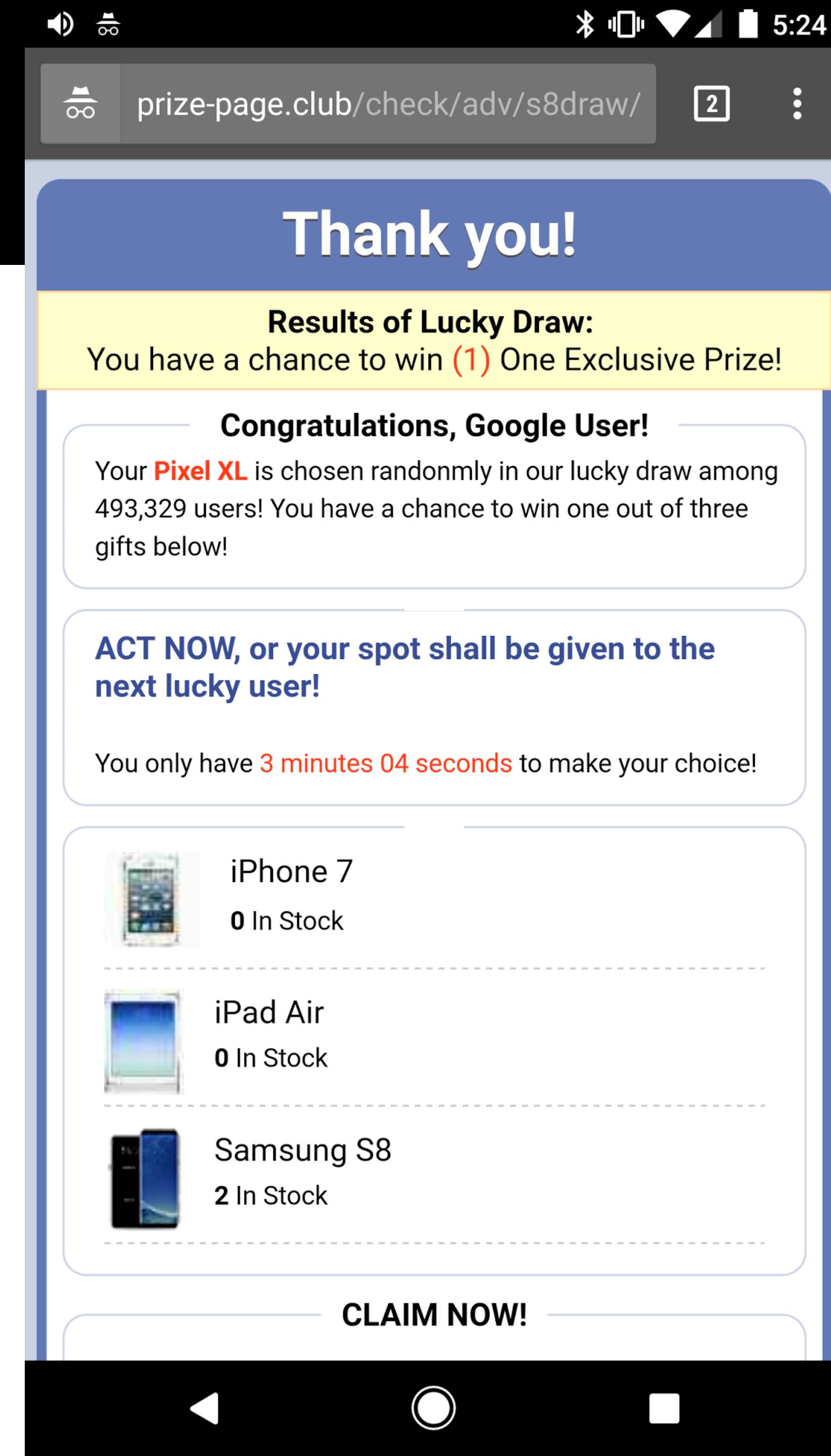
**Apps are, by nature, full-screen**

Home button is still a “trusted path” feature

(Not that this is obvious to users.)

**Central control from app stores can help**

Misbehaving apps will be globally uninstalled!





# Maybe two-factor auth will help?

## Security

48

### After years of warnings, mobile network hackers exploit SS7 flaws to drain bank accounts

O2 confirms online thefts using stolen 2FA SMS codes

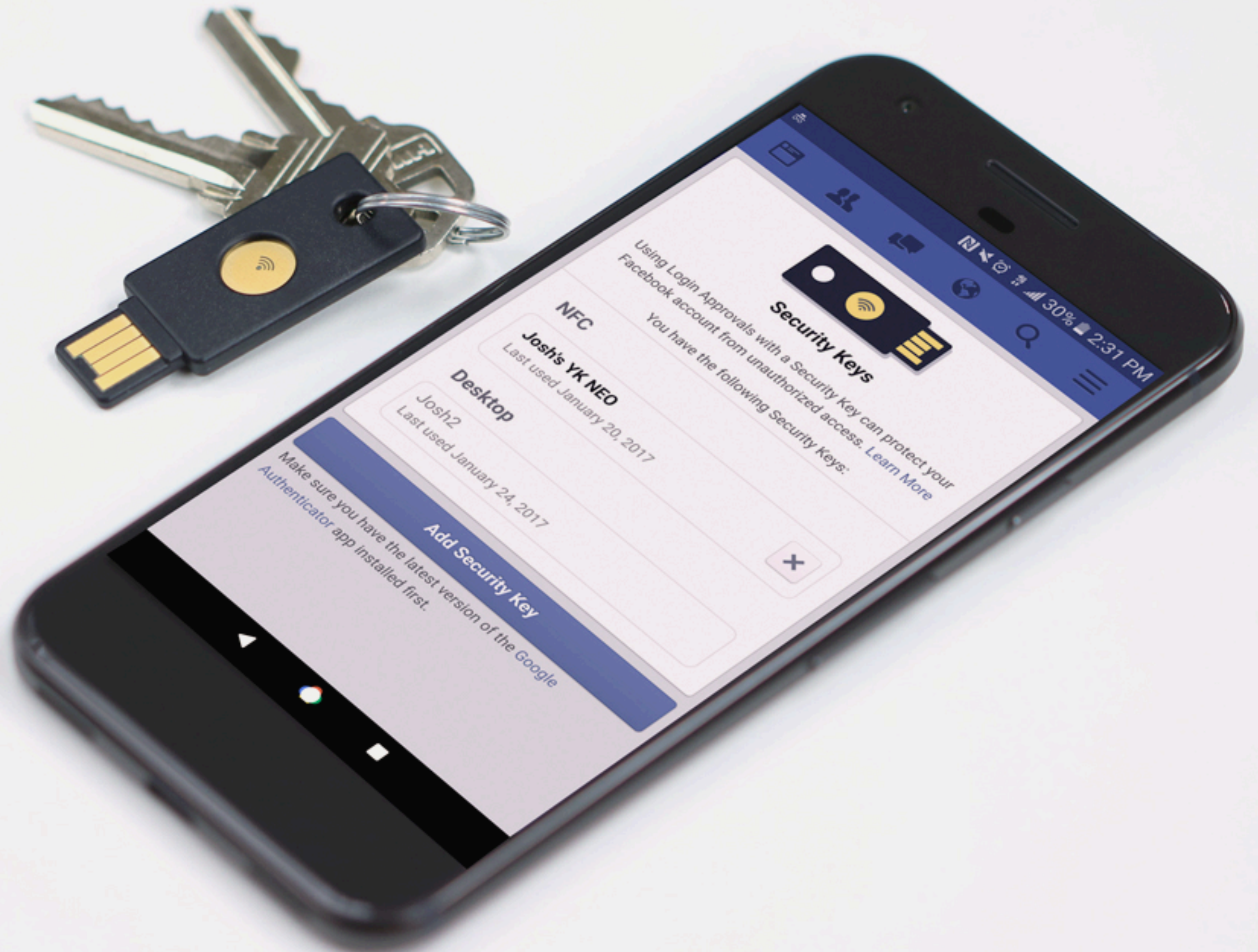


3 May 2017 at 20:02, [Iain Thomson](#)

Experts have been warning for years about security blunders in the Signaling System 7 protocol – the magic glue used by cellphone networks to communicate with each other.

These shortcomings can be potentially abused to, for example, redirect people's calls and text messages to miscreants' devices. Now we've seen the first case of crooks exploiting the design flaws to line their pockets with victims' cash.

O2-Telefonica in Germany [has confirmed](#) to Süddeutsche Zeitung that some of its customers have had their bank accounts drained using a two-stage attack that exploits





# And pairing is a huge problem

## Long, complicated instructions

*Nest Protect*: scan QR code

*Nest Thermostat*: dial in your WiFi password

*Rachio / Electric Imp*: screen flashing to a light sensor

**Needs to be easier!**

### Scan the QR code

The Nest app will turn on your phone or tablet's camera. Use it to scan the QR code on the back of your Nest Protect.

The Nest app will automatically recognize it.

My phone's camera won't scan the QR code, what should I do? >





# Threat models

“I’m still clinging to my BlackBerry,” Mr. Obama said Wednesday [7 Jan ’09]. “They’re going to pry it out of my hands.”

*The New York Times*





# In person vs. remote attacks

**Do we need to defend devices against “local” threats?**

Storage encryption?

Fingerprint vs. PIN?

- Privacy from shoulder surfing
- Privacy from gov’t search

Radio emissions?

## Senator reveals that the FBI paid \$900,000 to hack into the San Bernardino killer's iPhone



Eric Tucker, Associated Press

🕒 May 8, 2017, 9:26 AM 🔥 7,825

Sen. Dianne Feinstein, the top Democrat on the Senate committee that oversees the FBI, said publicly last week that the government paid \$900,000 to break into the locked iPhone of a gunman in the San Bernardino, California, shootings.

The FBI considers the figure to be classified information. It also has protected the identity of the vendor it paid to do the work. Both pieces of information are the subject of a federal lawsuit by The Associated Press and other news organizations that have sued to force the FBI to reveal them.



Dianne Feinstein AP

# Whose job is it to protect you?

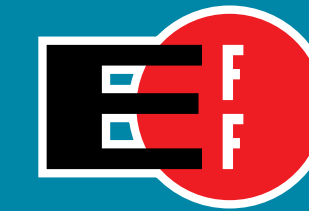
**The hardware vendor? The OS vendor?  
The chipset vendor?**

What about your cloud services?

**Can the government compel a vendor to  
add a backdoor?**

**Who provides ongoing security updates?**

Example: Mirai webcam botnet



**ELECTRONIC FRONTIER FOUNDATION**

Protecting Rights and Defending Freedom on the Electronic Frontier

454 SHOTWELL STREET, SAN FRANCISCO, CA, USA 415.436.9333 WWW.EFF.ORG

## AT&T's Role in Dragnet Surveillance of Millions of Its Customers

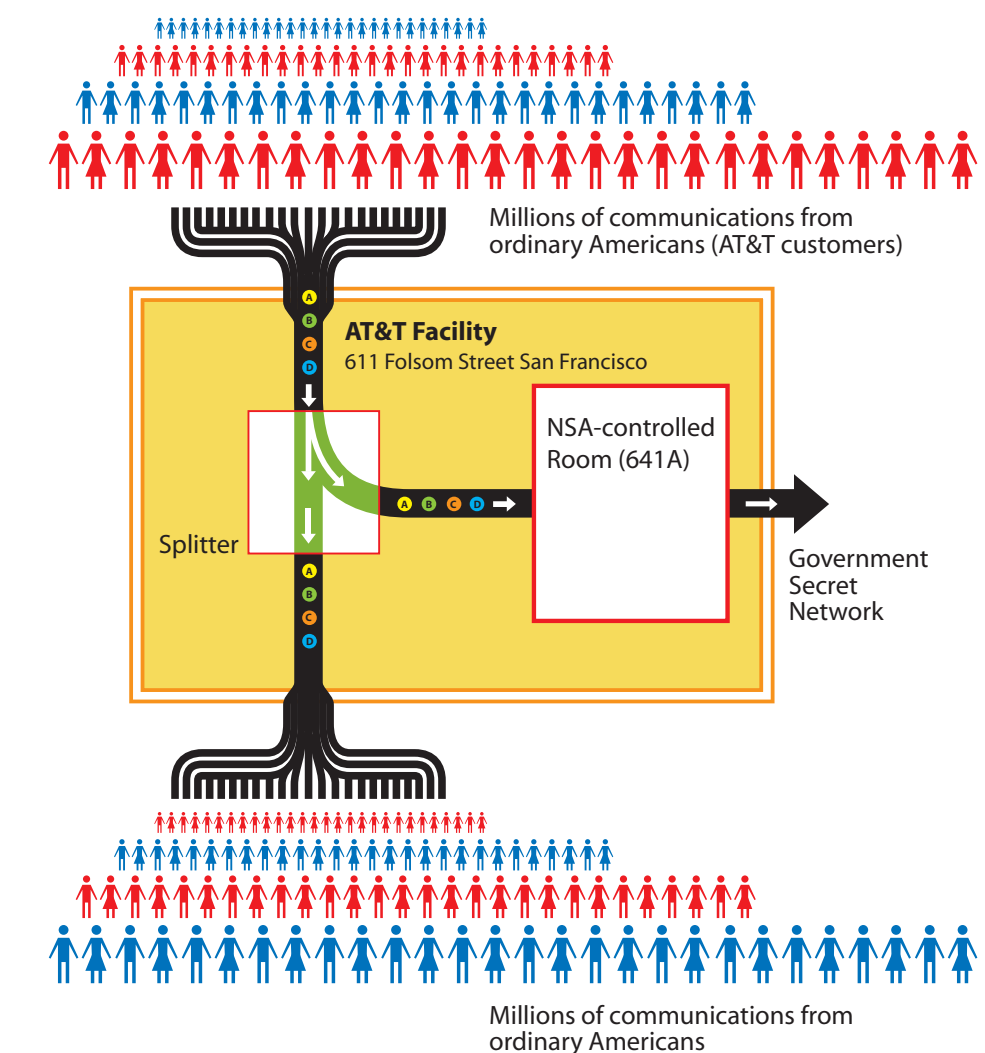
INTERNET SPYING IN SAN FRANCISCO<sup>1</sup>

AT&T's internet traffic in San Francisco runs through fiber-optic cables at an AT&T facility located at 611 Folsom Street in San Francisco. Using a device called a "splitter" a complete copy of the internet traffic that AT&T receives – email, web browsing requests, and other electronic communications sent to or from the customers of AT&T's WorldNet Internet service from people who use another internet service provider – is diverted onto a separate fiber-optic cable which is connected to a room, known as the SG-3 room, which is controlled by the NSA. The other copy of the traffic continues onto the internet to its destination.

The SG-3 room was created under the supervision of the NSA, and contains powerful computer equipment connecting to separate networks. This equipment is designed to analyze communications at high speed, and can be programmed to review and select out the contents and traffic patterns of communications according to user-defined rules. Only personnel with NSA clearances – people assisting or acting on behalf of the NSA – have access to this room.

AT&T's deployment of NSA-controlled surveillance capability apparently involves considerably more locations than would be required to catch only international traffic. The evidence of the San Francisco room is consistent with an overall national AT&T deployment to from 15 to 20 similar sites, possibly more. This implies that a substantial fraction, probably well over half, of AT&T's purely domestic traffic was diverted to the NSA. At the same time, the equipment in the room is well suited to the capture and analysis of large volumes of data for purposes of surveillance.

Intercepting Communications at  
AT&T Folsom Street Facility





## TECHNOLOGY

# Internet Giants Erect Barriers to Spy Agencies

By DAVID E. SANGER and NICOLE PERLROTH    JUNE 6, 2014

MOUNTAIN VIEW, Calif. — Just down the road from Google’s main campus here, engineers for the company are accelerating what has become the newest arms race in modern technology: They are making it far more difficult — and far more expensive — for the National Security Agency and the intelligence arms of other governments around the world to pierce their systems.

As fast as it can, Google is sealing up cracks in its systems that Edward J. Snowden revealed the N.S.A. had brilliantly exploited. It is encrypting more data as it moves among its servers and helping customers encode their own emails. Facebook, Microsoft and Yahoo are taking similar steps.

After years of cooperating with the government, the immediate goal now is to thwart Washington — as well as Beijing and Moscow. The strategy is also intended to preserve business overseas in places like Brazil and Germany that have threatened to entrust data only to local providers.

Google, for example, is laying its own fiber optic cable under the world’s oceans, a project that began as an effort to cut costs and extend its influence, but now has an added purpose: to assure that the company will have more control over the movement of its customer data.



TECHNOLOGY

# Internet Giants Erect Barriers to Spy Agencies

By DAVID E. SANGER and NICOLE PERLROTH JUNE 6, 2014

MOUNTAIN VIEW, Calif. — Just down the road from Google’s main campus here, engineers for the company are accelerating what has become the newest arms race in modern technology: They are making it far more difficult — and far more expensive — for the National Security Agency to intercept their communications.



Eric Grosse, Google’s security chief, suggested in an interview that the N.S.A.’s own behavior invited the new arms race.

**“I am willing to help on the purely defensive side of things,”** he said, referring to Washington’s efforts to enlist Silicon Valley in cybersecurity efforts. **“But signals intercept is totally off the table,”** he said, referring to national intelligence gathering.

**“No hard feelings, but my job is to make their job hard,”** he added.



# Open challenges

# Ease of use

## **Internet of Things are hard to install**

Pre-installed trust (at purchase time)?

## **Power user features vs. security lockdown**

Apple: one app store

Google: you can install a 3rd-party store



# The computers inside the computer

***Disaggregated computing:*** Our definition of a computer is changing

Embedded computers need to be exposed, managed

## **Nasty challenges**

What should it mean to “boot” a computer?

What does it mean to not trust one of your own devices?

How to protect vendor “intellectual property”?

# Code correctness

**Buffer overflows have been known since the 1980's, maybe earlier.**

We have tools that try to make C safe (e.g., Coverity)

Inherently safe systems tend to require GC memory (e.g., Java)

**Maybe it's time to go with something else?**

Even tiny embedded CPUs are insanely fast and have lots of RAM\*

*\* If you're old enough to remember the bad old days.*







**We've got a lot of work to do**

