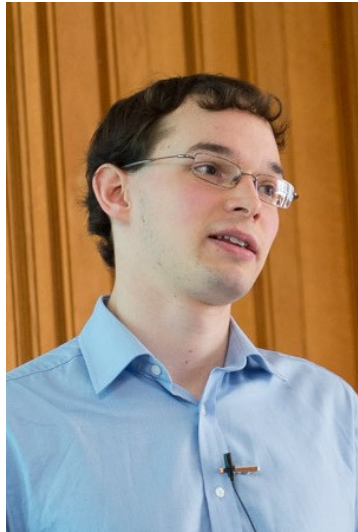


Security metrics for the Android ecosystem



**Daniel
Thomas**



**Alastair
Beresford**



**Andrew
Rice**



**UNIVERSITY OF
CAMBRIDGE**

Daniel gpg: 5017 A1EC 0B29 08E3 CF64 7CCD 5514 35D5 D749 33D9
Alastair gpg: 9217 482D D647 8641 44BA 10D8 83F4 9FBF 1144 D9B3
Andrew gpg: 43BF 45D1 1B36 F45C 3F07 DA49 BDB8 8932 5CAC F039

Smartphones contain many apps written by a spectrum of developers



How “secure” is a smartphone?

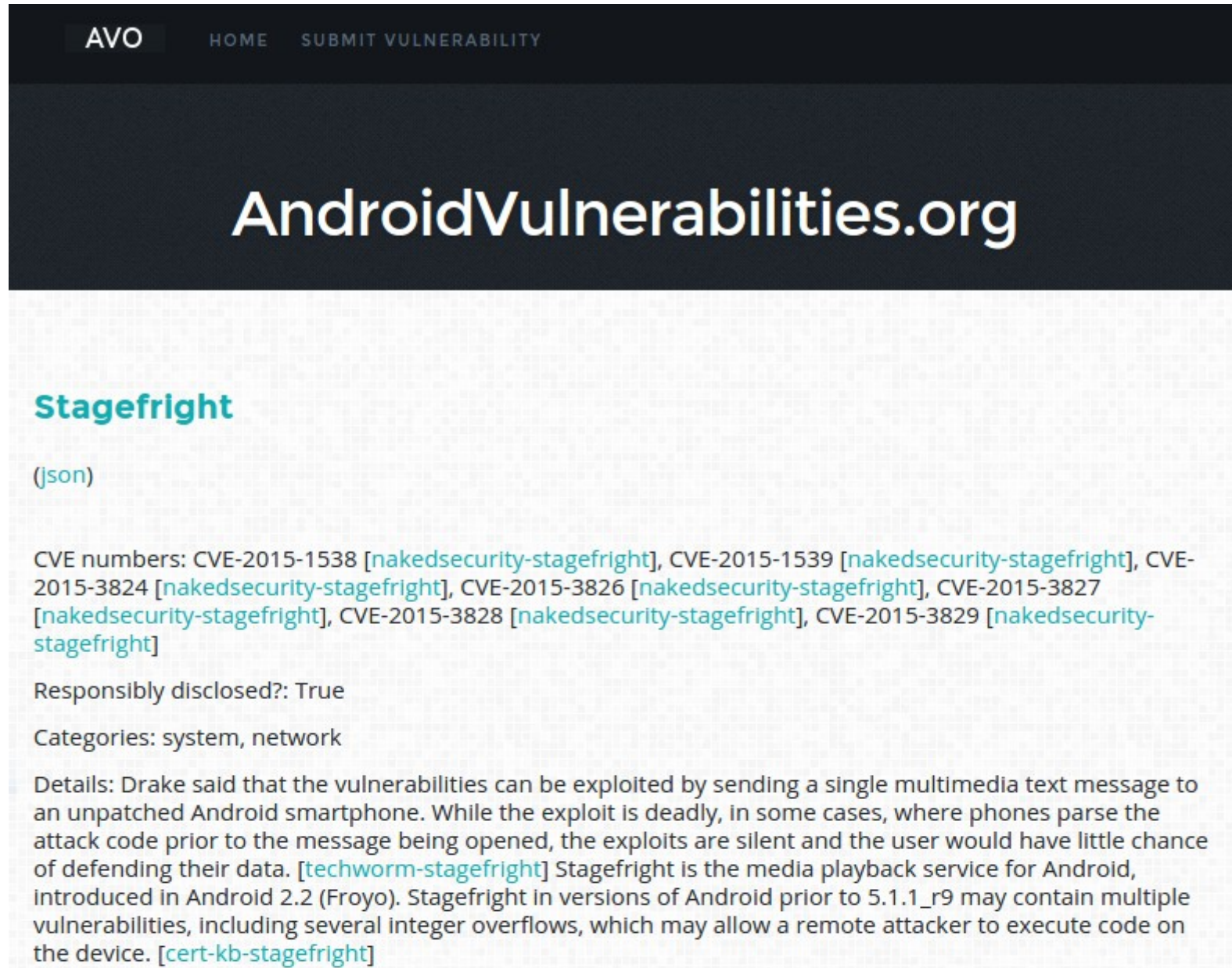
Root/kernel exploits are harmful

- Root exploits break permission model
- Cannot recover to a safe state
- 37% Android malware uses root exploits (2012)
- We're interested in critical vulnerabilities, exploitable by code running on the device

Hypothesis: devices vulnerable because they are not updated

- Android phones, sold on 1-2 year contracts
 - Anecdotal evidence is that updates rarely happen

No central database of Android vulnerabilities: so we're building one



The screenshot shows the website AndroidVulnerabilities.org. The header has a dark blue bar with 'AVO' in white, and 'HOME' and 'SUBMIT VULNERABILITY' in smaller white text. Below the header, the site name 'AndroidVulnerabilities.org' is displayed in large white font. The main content area is white and shows a vulnerability entry for 'Stagefright' in teal. Below the title, '(json)' is written in teal. The CVE numbers are listed in teal: CVE-2015-1538 [nakedsecurity-stagefright], CVE-2015-1539 [nakedsecurity-stagefright], CVE-2015-3824 [nakedsecurity-stagefright], CVE-2015-3826 [nakedsecurity-stagefright], CVE-2015-3827 [nakedsecurity-stagefright], CVE-2015-3828 [nakedsecurity-stagefright], and CVE-2015-3829 [nakedsecurity-stagefright]. The 'Responsibly disclosed?: True' and 'Categories: system, network' are in black. The 'Details' section in black text describes the vulnerability, mentioning Drake, the exploit, and the media playback service Stagefright.

AVO HOME SUBMIT VULNERABILITY

AndroidVulnerabilities.org

Stagefright

(json)

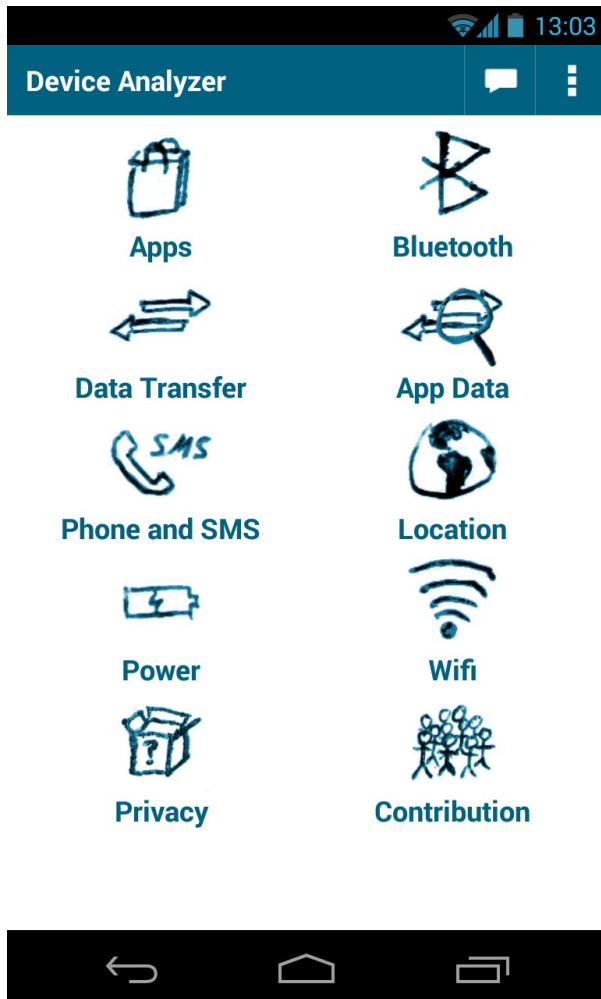
CVE numbers: CVE-2015-1538 [nakedsecurity-stagefright], CVE-2015-1539 [nakedsecurity-stagefright], CVE-2015-3824 [nakedsecurity-stagefright], CVE-2015-3826 [nakedsecurity-stagefright], CVE-2015-3827 [nakedsecurity-stagefright], CVE-2015-3828 [nakedsecurity-stagefright], CVE-2015-3829 [nakedsecurity-stagefright]

Responsibly disclosed?: True

Categories: system, network

Details: Drake said that the vulnerabilities can be exploited by sending a single multimedia text message to an unpatched Android smartphone. While the exploit is deadly, in some cases, where phones parse the attack code prior to the message being opened, the exploits are silent and the user would have little chance of defending their data. [techworm-stagefright] Stagefright is the media playback service for Android, introduced in Android 2.2 (Froyo). Stagefright in versions of Android prior to 5.1.1_r9 may contain multiple vulnerabilities, including several integer overflows, which may allow a remote attacker to execute code on the device. [cert-kb-stagefright]

Device Analyzer gathers statistics on mobile phone usage



- Deployed May '11
- 23,300 contributors
- 2,000 phone years
- 100 billion records
- 10TB of data
- 600 7-day active contributors

Saving screenshot...

Phone and SMS

Phone calls:

	Incoming	Outgoing	Total
Today	0:00	0:00	0:00
This Month	11:40	36:23	48:03
Last Month	28:53	1:05:07	1:34:00

Text messages:

	Received	Sent	Total
Today	1	1	2
This Month	61	56	117
Last Month	176	150	326

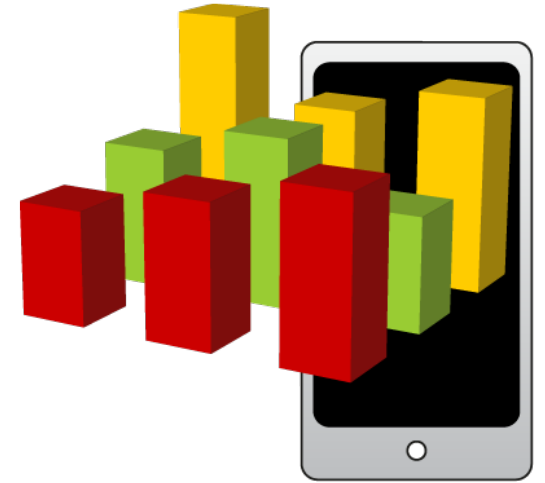
Active Operator **giffgaff**
Roaming **no**
Signal strength **19**
Ringer mode **normal**
Data Collected **12 Nov 2013 13:12:25**

<https://deviceanalyzer.cl.cam.ac.uk>



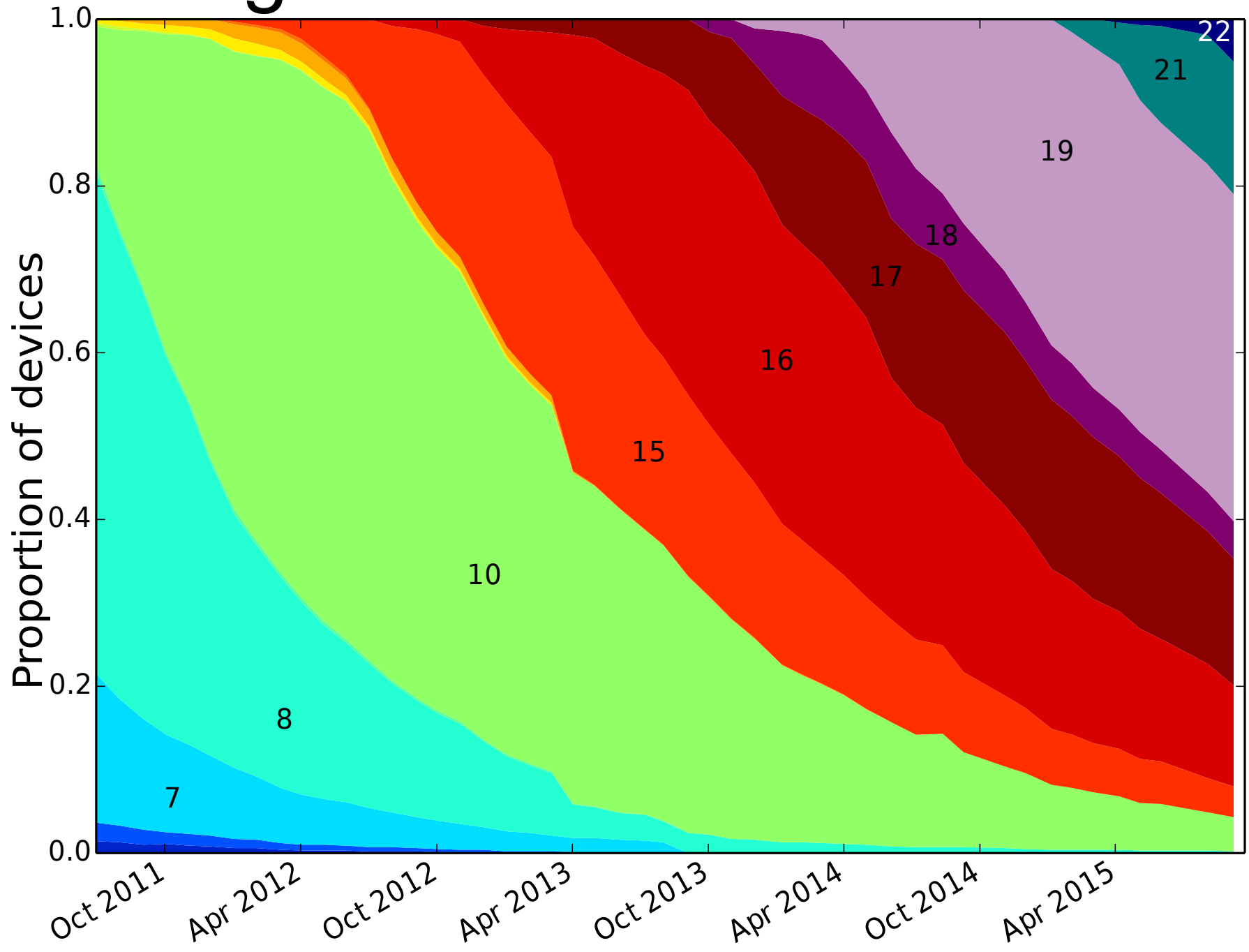
Device Analyzer gathers wide variety of data

- Including: system stats
 - OS version and build number
 - Manufacturer and device model



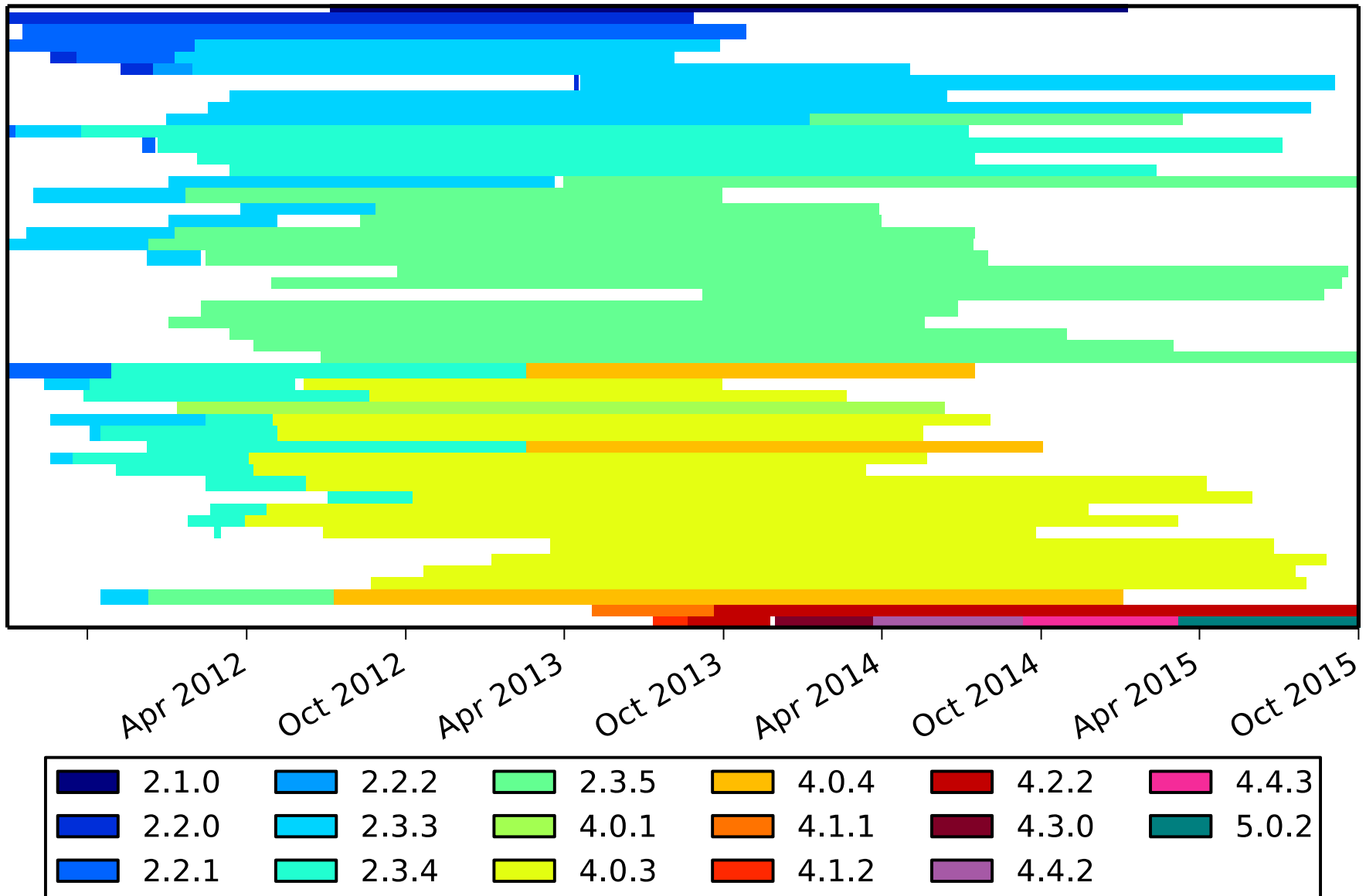
Is the *ecosystem* getting updated?

Google data: device API levels

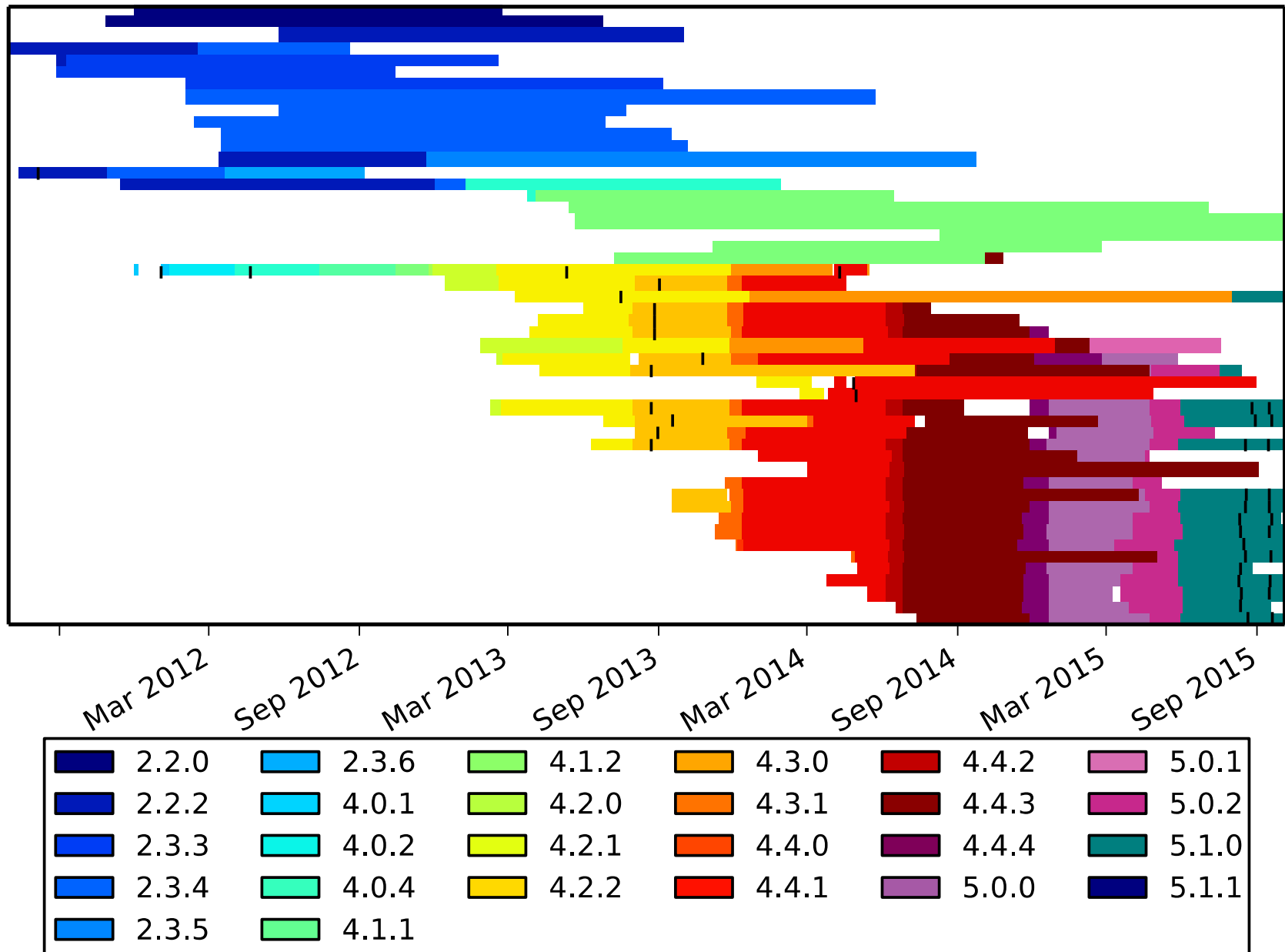


Are *devices* getting updated?

HTC updates by OS version



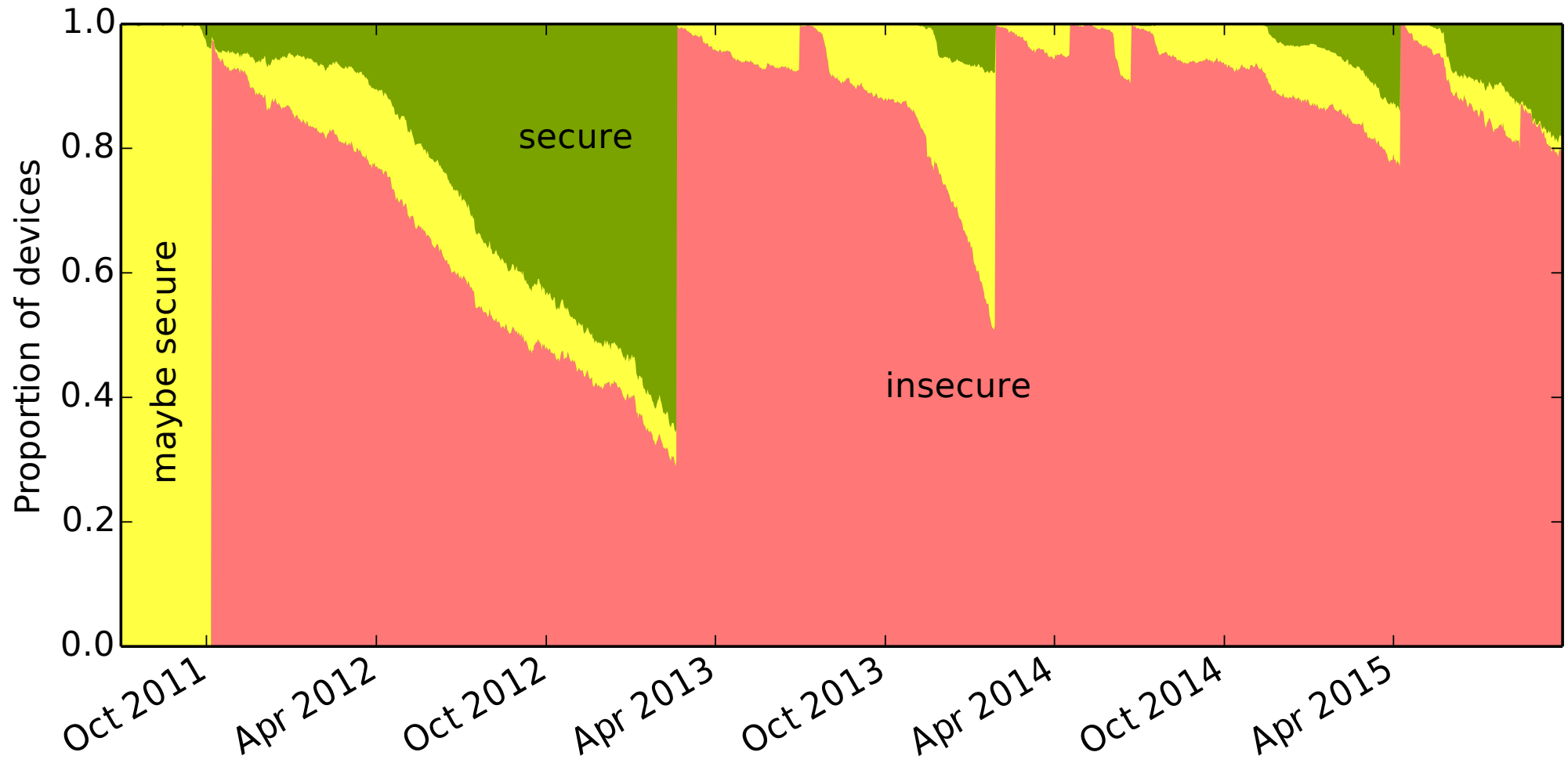
LG updates by OS version



Connecting the two data sets: assume OS version → vulnerability

- We have an OS version from Device Analyzer
- We have vulnerability data with OS versions
- Match on OS and Build Number
 - Phone in set of {insecure, maybe secure, secure}

On average, 87% are vulnerable



The FUM metric measures the security of Android devices

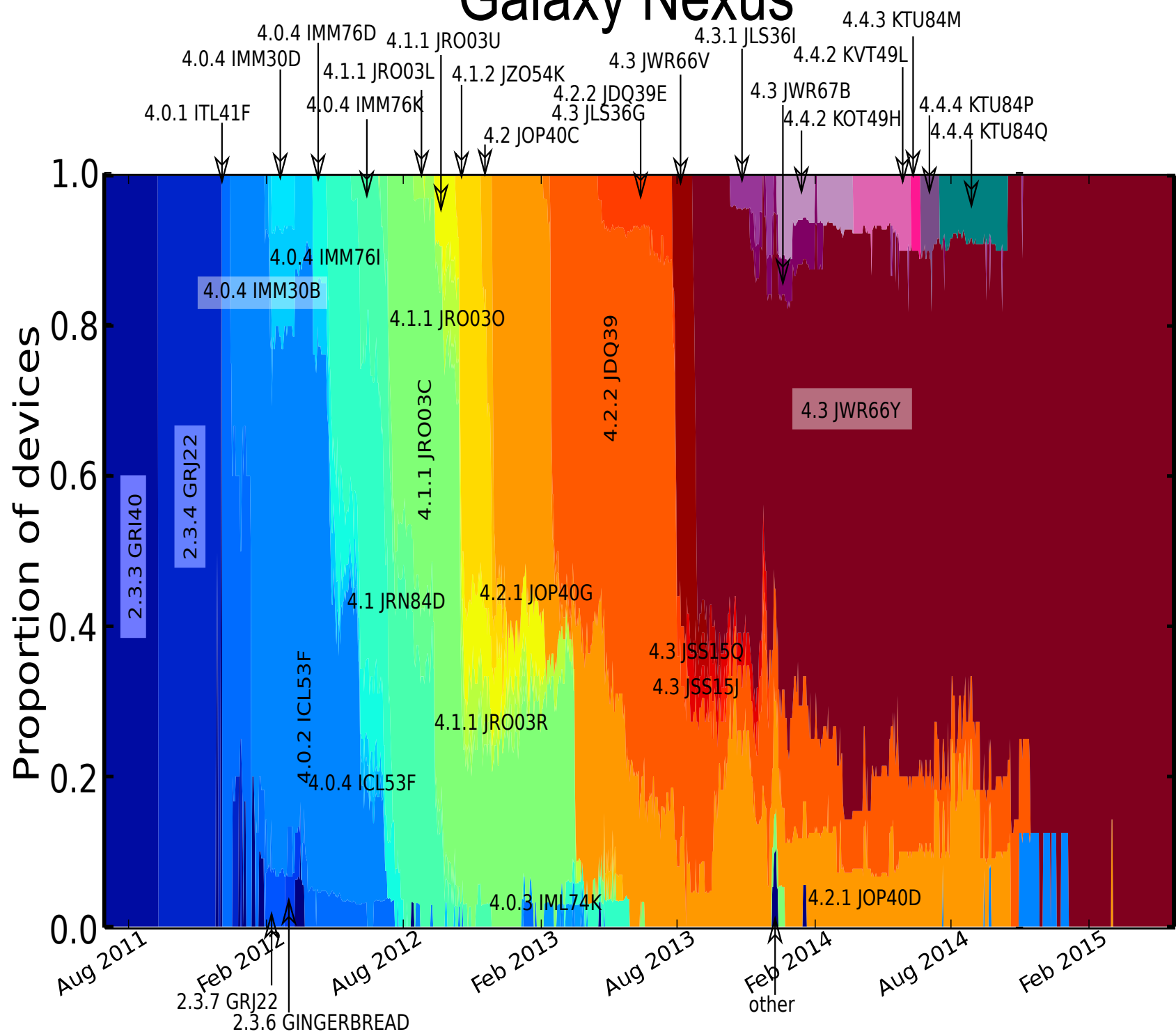
$$FUM\ score = 4 \cdot f + 3 \cdot u + 3 \cdot \frac{2}{1 + e^m}$$

f free from vulnerabilities

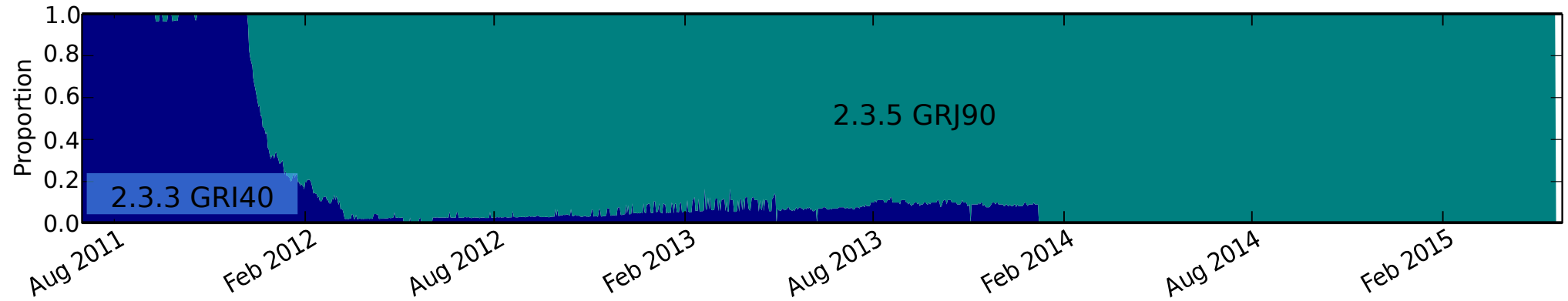
u updated to the latest version

m mean unfixed vulnerabilities

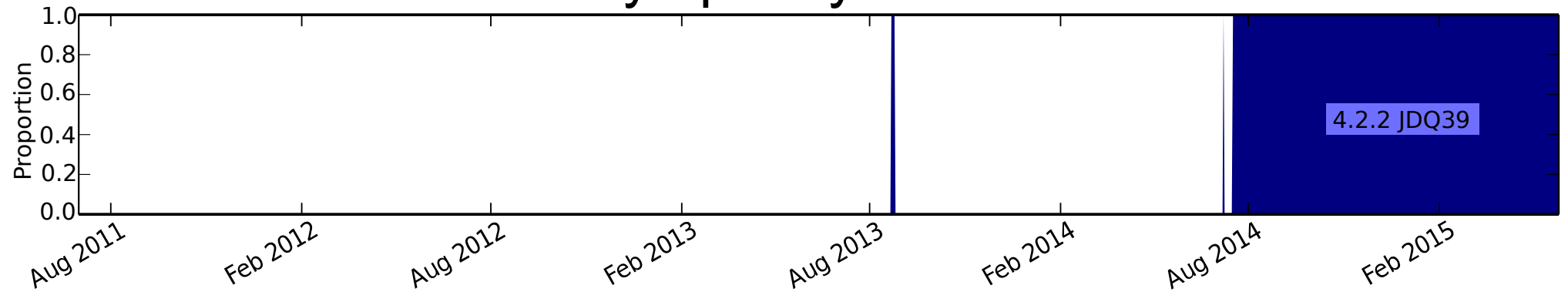
Galaxy Nexus



HTC Desire HD A9191



Symphony W68

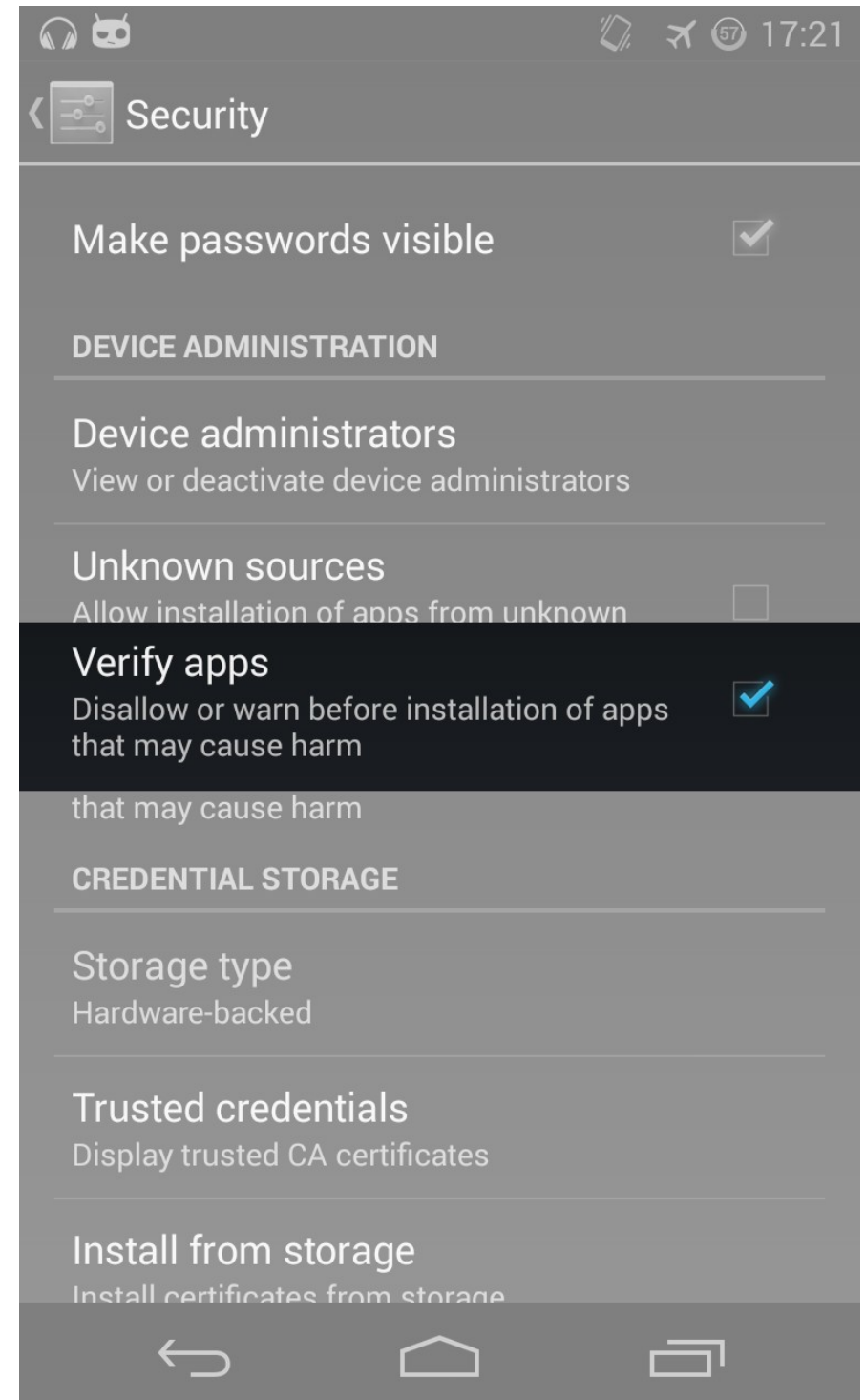


Name	f	u	m	score (out of 10)
nexus	0.39 ± 0.00	0.48 ± 0.00	0.56 ± 0.01	5.17 ± 0.02
LG	0.22 ± 0.00	0.33 ± 0.00	0.62 ± 0.01	3.97 ± 0.02
Motorola	0.18 ± 0.00	0.12 ± 0.00	0.71 ± 0.02	3.07 ± 0.02
Samsung	0.13 ± 0.00	0.04 ± 0.00	0.61 ± 0.00	2.75 ± 0.00
Sony	0.14 ± 0.00	0.19 ± 0.00	1.09 ± 0.02	2.63 ± 0.02
HTC	0.14 ± 0.00	0.10 ± 0.00	0.87 ± 0.01	2.63 ± 0.02
asus	0.20 ± 0.00	0.51 ± 0.01	6.01 ± 0.07	2.35 ± 0.02
other	0.06 ± 0.00	0.05 ± 0.00	1.04 ± 0.01	1.97 ± 0.02
alps	0.03 ± 0.00	0.19 ± 0.01	3.99 ± 0.08	0.80 ± 0.02
Symphony	0.00 ± 0.00	0.08 ± 0.00	5.00 ± 0.05	0.30 ± 0.01
walton	0.00 ± 0.00	0.09 ± 0.00	6.00 ± 0.08	0.27 ± 0.01

Why is fixing vulnerabilities hard: software ecosystem is complex

- Division of labour
 - Open source software
 - Core OS production
 - Driver writer
 - Device manufacturer
 - Retailer
 - Customer
- Apple and Google have different models
 - Hypothesis: Apple's model is more secure

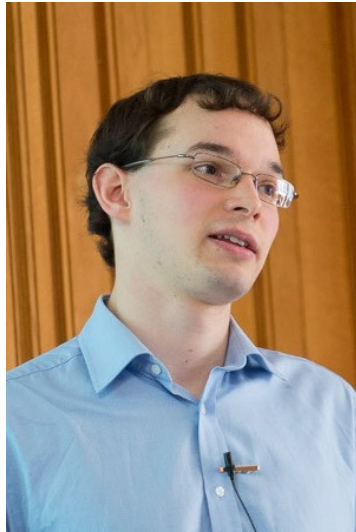
Google to the
rescue: *Play Store*
and *Verify apps*
provide security



Conclusions

- 87% of Android devices are vulnerable
- Ecosystem complex; lack of transparency
- FUM metric is a robust measure of security
 - A step towards an economic incentive

Security metrics for the Android ecosystem



**Daniel
Thomas**



**Alastair
Beresford**



**Andrew
Rice**



UNIVERSITY OF
CAMBRIDGE

Firstname.Surname@cl.cam.ac.uk
<http://androidvulnerabilities.org>

Daniel gpg: 5017 A1EC 0B29 08E3 CF64 7CCD 5514 35D5 D749 33D9
Alastair gpg: 9217 482D D647 8641 44BA 10D8 83F4 9FBF 1144 D9B3
Andrew gpg: 43BF 45D1 1B36 F45C 3F07 DA49 BDB8 8932 5CAC F039

Example: Android APK duplicate file

- OS does not check for duplicate files in APK
- Not a traditional kernel vulnerability
- Affected all manufacturers and versions > 1.5
- Timeline:
 - February 2013: discovered
 - February 2013: fixed
 - July 2013: Public announcement
- Is the responsible disclosure period sufficient to protect users?

Device Analyzer is a good example of Privacy by Design principles

- Transparency, consent, notice and disclosure
- Purpose
- Security
- Access to data and withdrawal
- Proactive privacy design
- Privacy by default

Device Analyzer is representative

- Compared with Google Play API data: Device Analyzer is slightly better
- Compared with User-Agent headers from Rwanda: Device Analyzer is better
- Compared with MDM data from a FTSE 100 company: Device Analyzer is slightly worse

Nexus and non-Nexus devices

