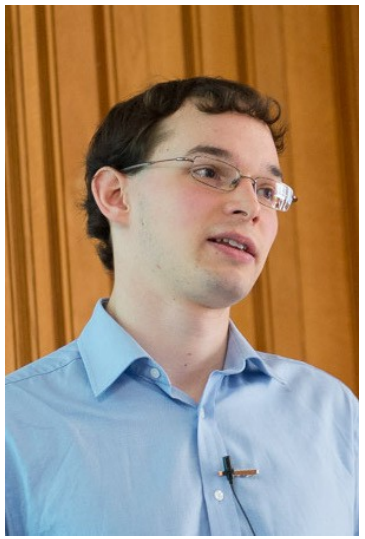
Security metrics for the Android ecosystem



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?

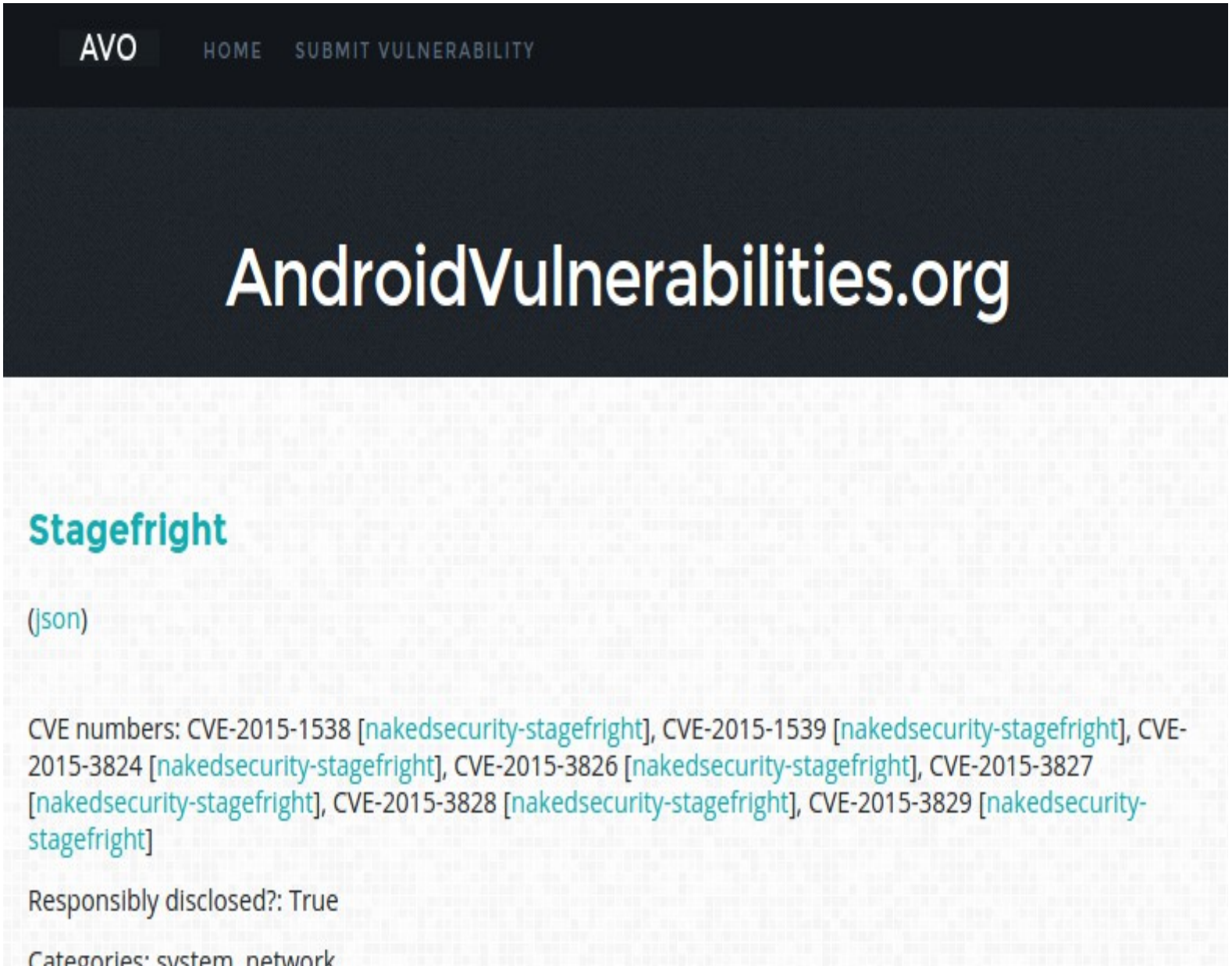
Root/kernel exploits are harmful

- 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

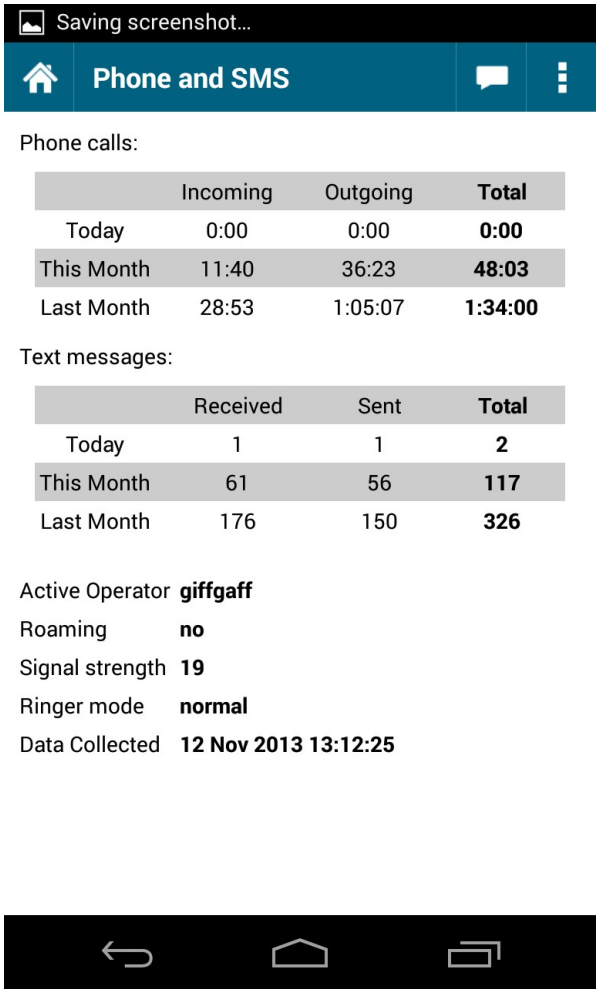
- Android phones, sold on 1-2 year contracts
  - Anecdotal evidence is that updates rarely happen

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



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



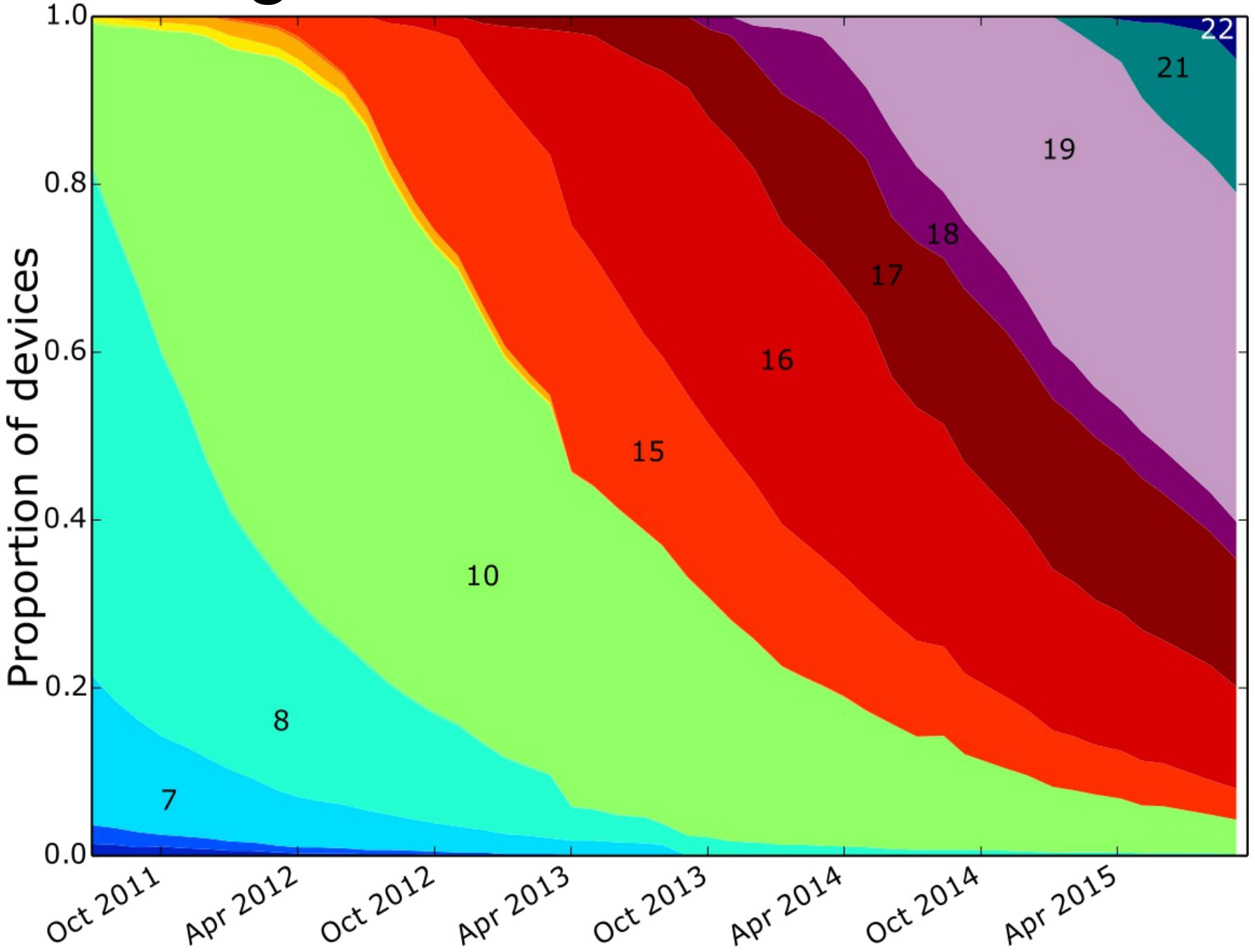
https://deviceanalyzer.cl.cam.ac.uk

Device Analyzer gathers wide variety of data

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

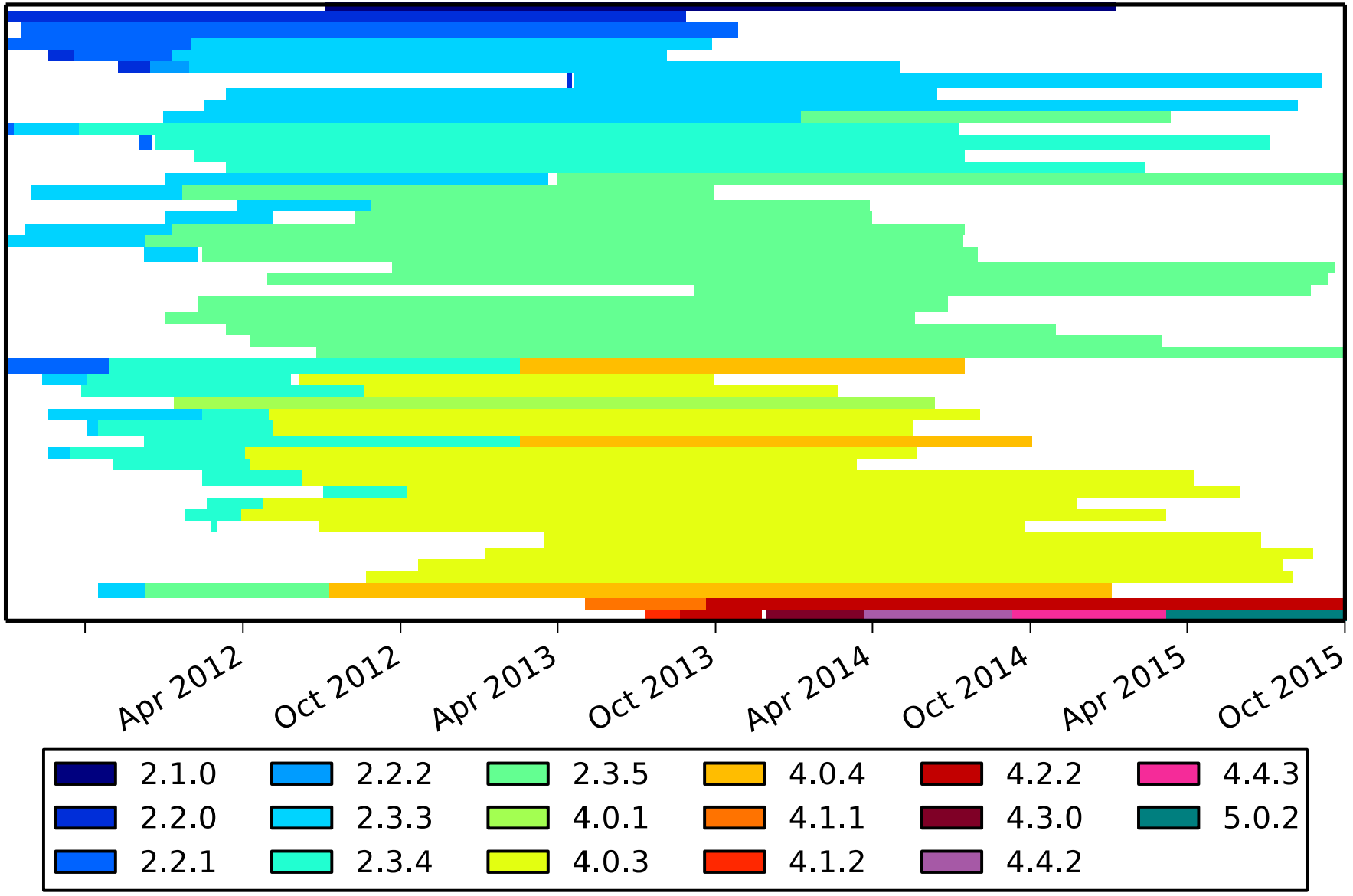
Is the *ecosystem* getting updated?

Google data: device API levels

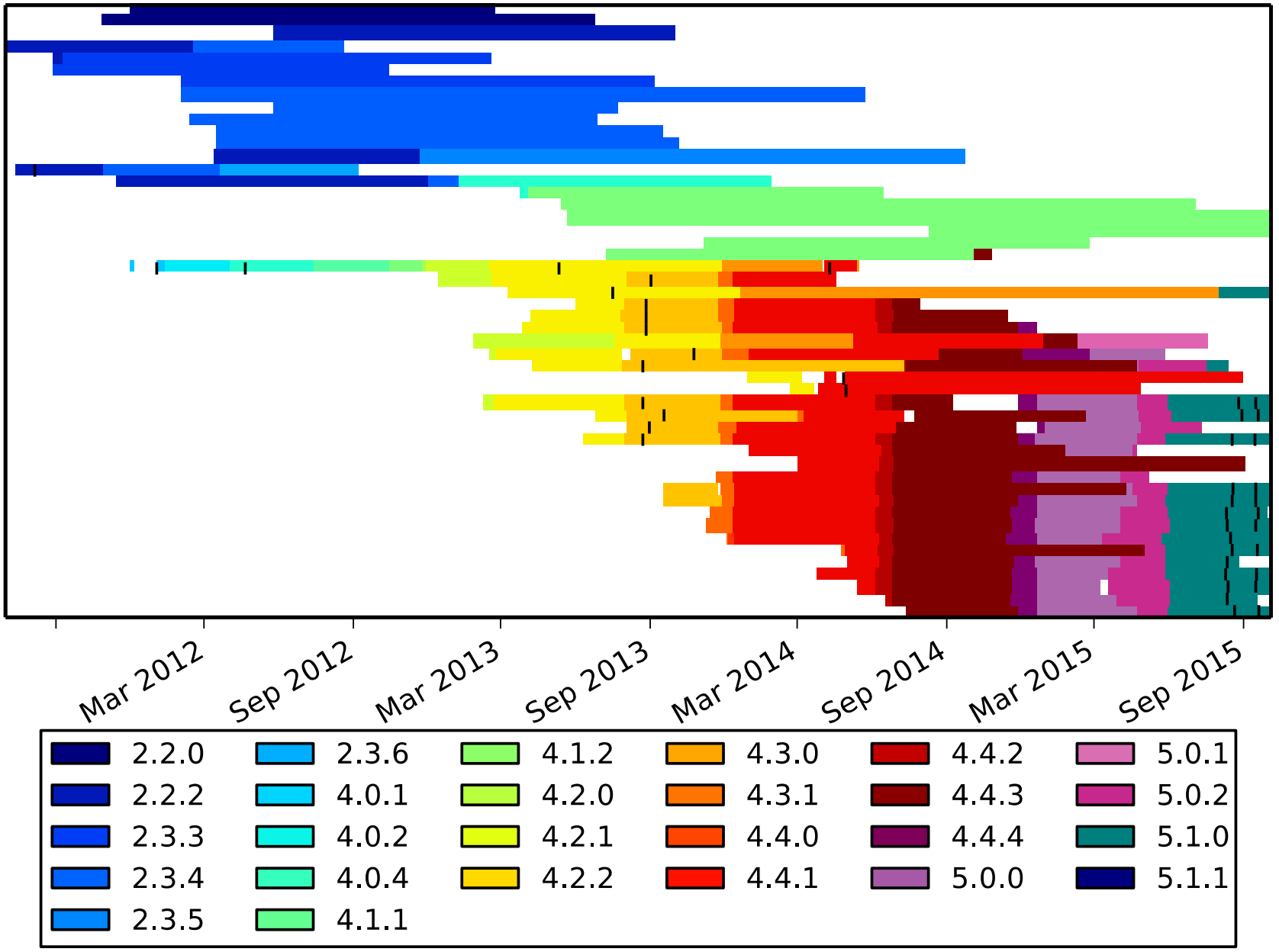


Are *devices* getting updated?

HTC updates by OS version



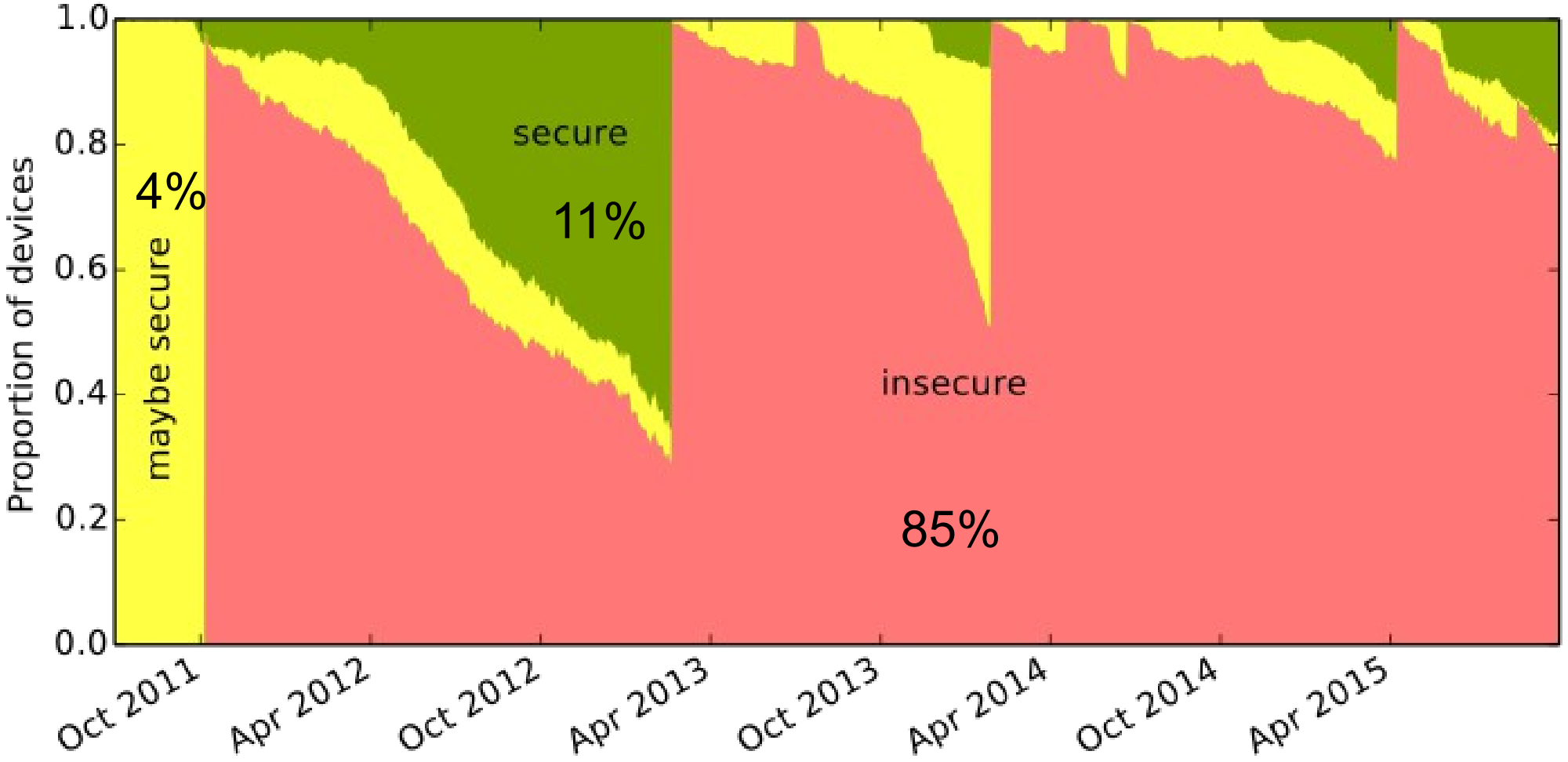
LG updates by OS version



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, 85% are vulnerable



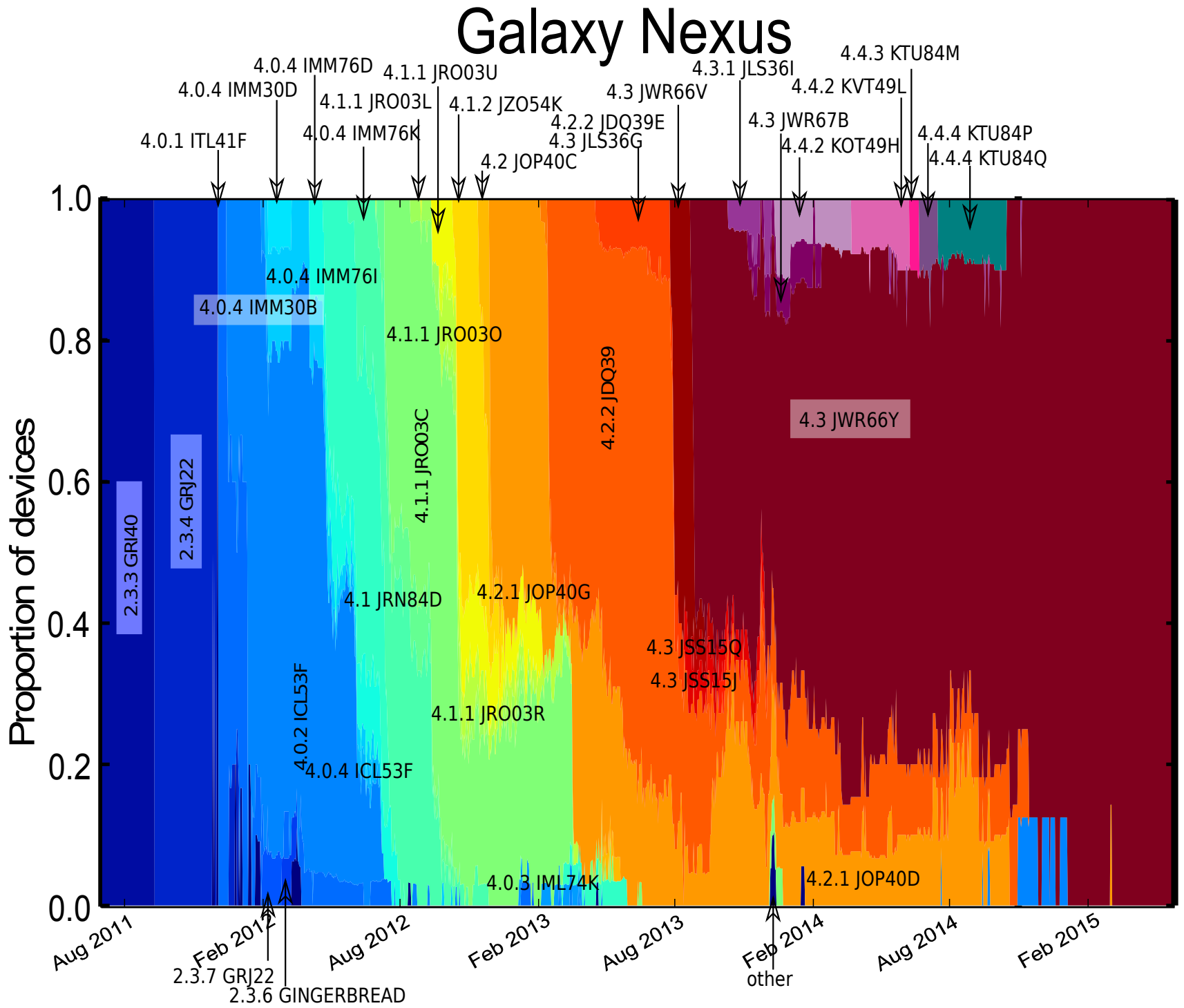
The FUM metric measures the security of Android devices

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

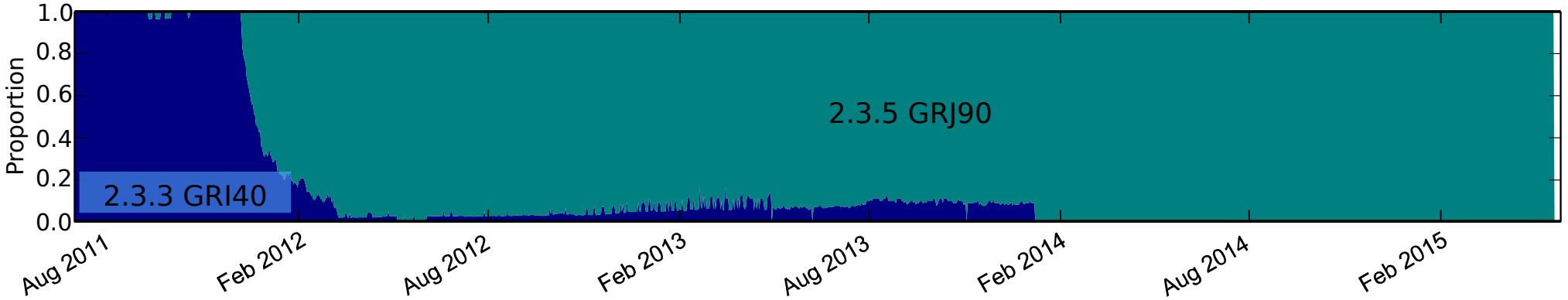
free from vulnerabilities

updated to the latest version

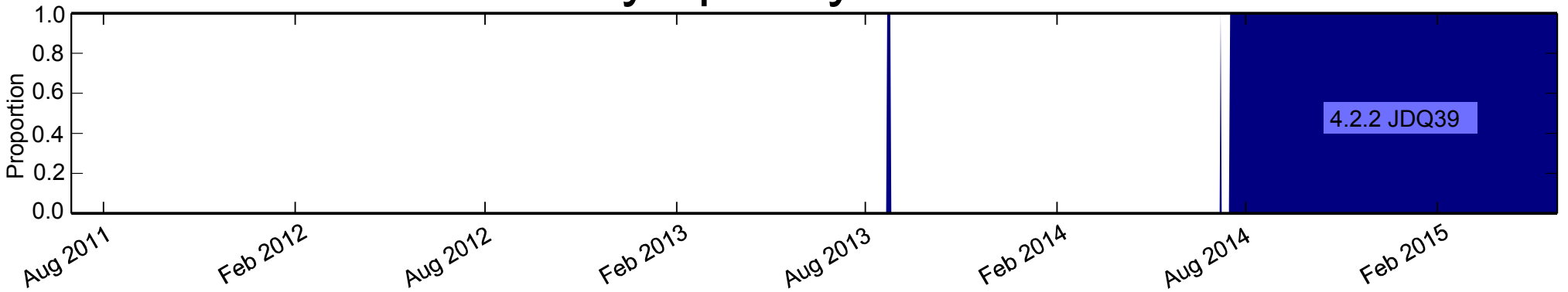
mean unfixed vulnerabilities

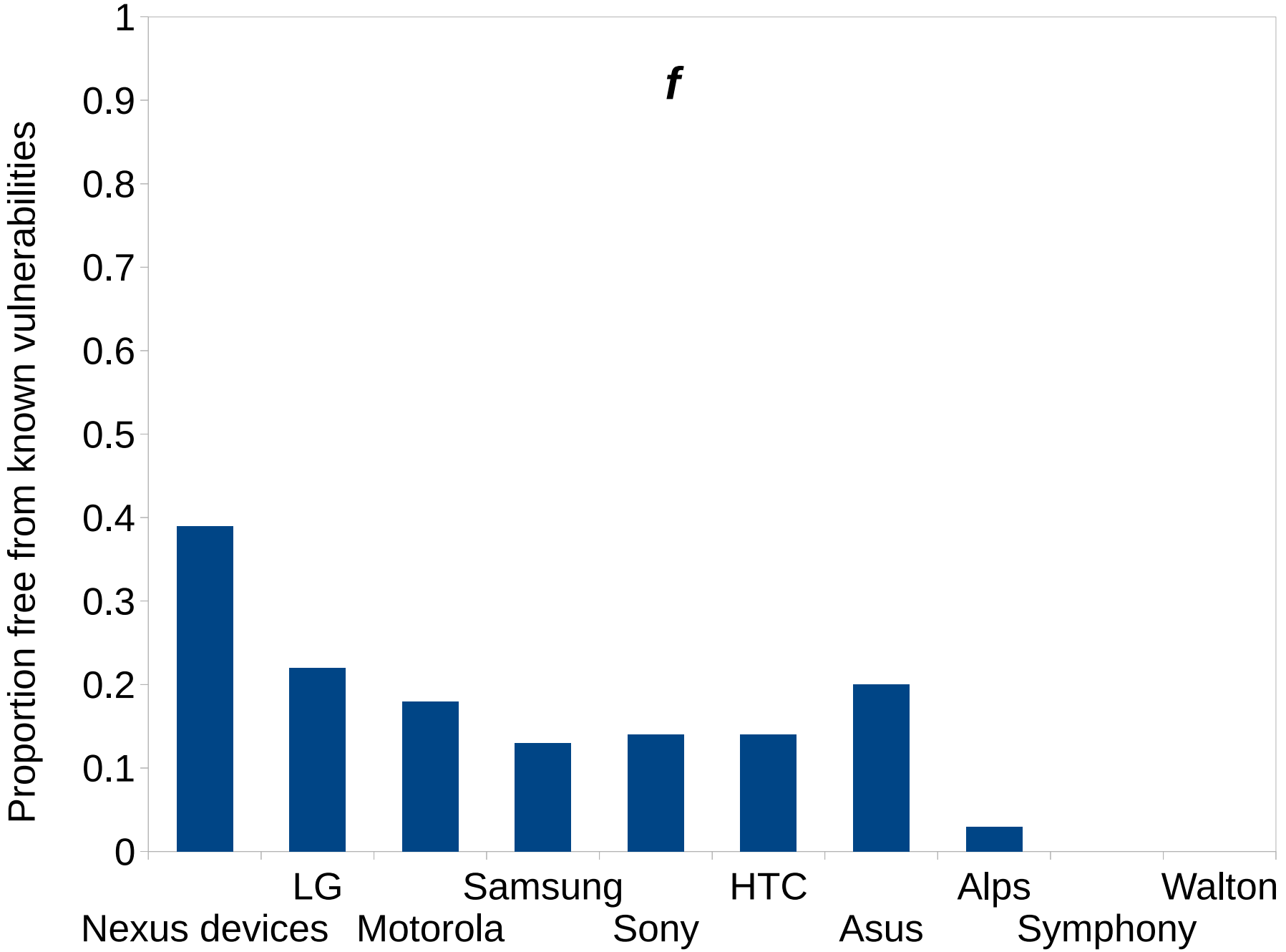

Galaxy Nexus
4.0.1 ITL41F
4.0.4 IMM30D
4.0.4 IMM76D
4.0.4 IMM76K
4.1.1 JRO03L
4.1.1 JRO03U
4.1.2 JZO54K
4.2 JOP40C
4.2.2 JDQ39E
4.3 JLS36G
4.3 JWR66V
4.3.1 JLS36I
4.3 JWR67B
4.4.2 KOT49H
4.4.2 KVT49L
4.4.3 KTU84M
4.4.4 KTU84P
4.4.4 KTU84Q
4.0.4 IMM76I
4.0.4 IMM30B
4.1.1 JRO03O
4.1.1 JRO03C
4.2.2 JDQ39
4.3 JWR66Y
2.3.3 GRI40
2.3.4 GRJ22
4.1 JRN84D
4.2.1 JOP40G
4.3 JSS15Q
4.3 JSS15J
4.0.2 ICL53F
4.1.1 JRO03R
4.0.4 ICL53F
4.0.3 IML74K
4.2.1 JOP40D
Proportion of devices
1.0
0.8
0.6
0.4
0.2
0.0
Aug 2011
Feb 2012
Aug 2012
Feb 2013
Aug 2013
Feb 2014
Aug 2014
Feb 2015
2.3.7 GRJ22
2.3.6 GINGERBREAD
other

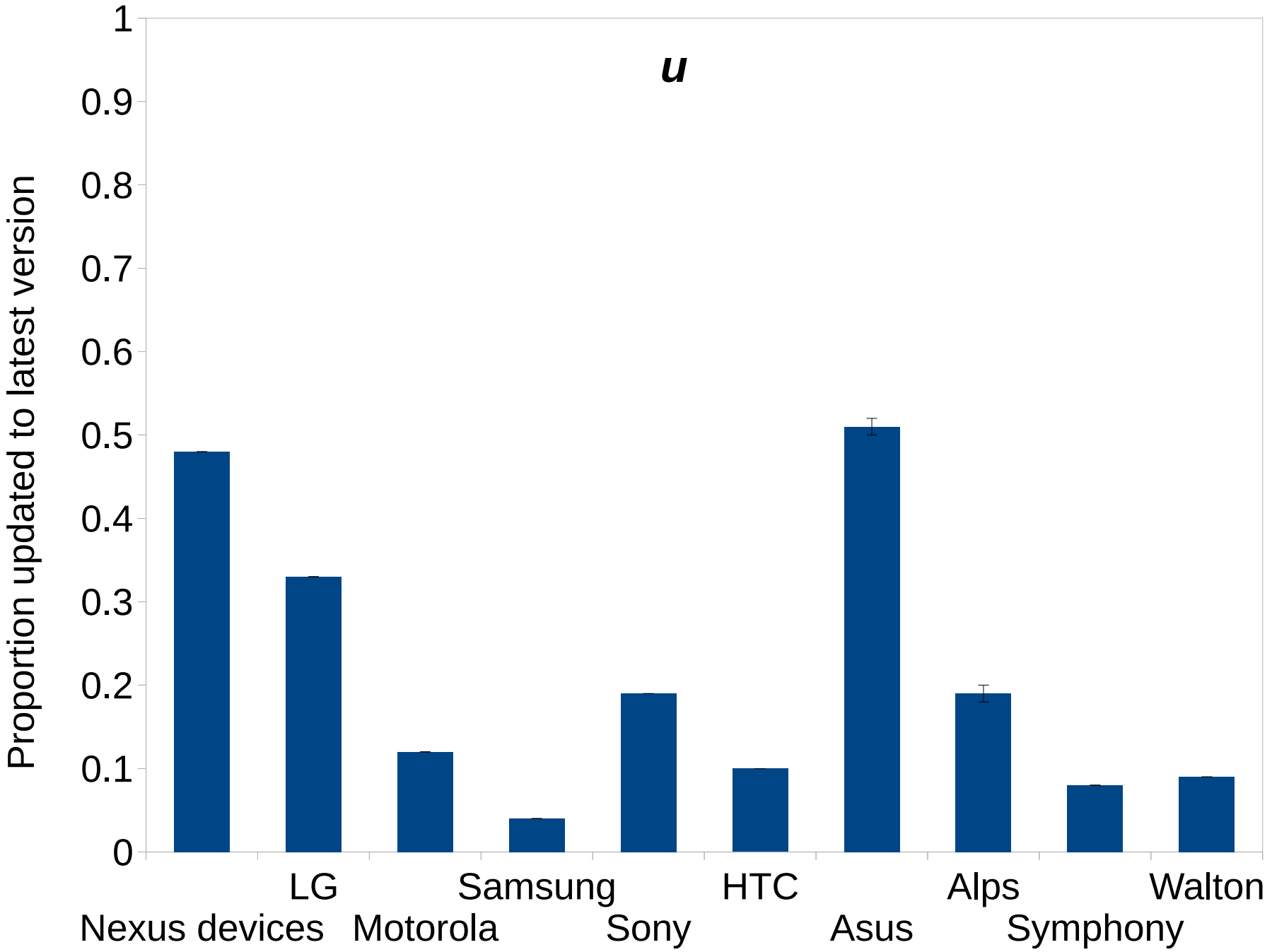
HTC Desire HD A9191

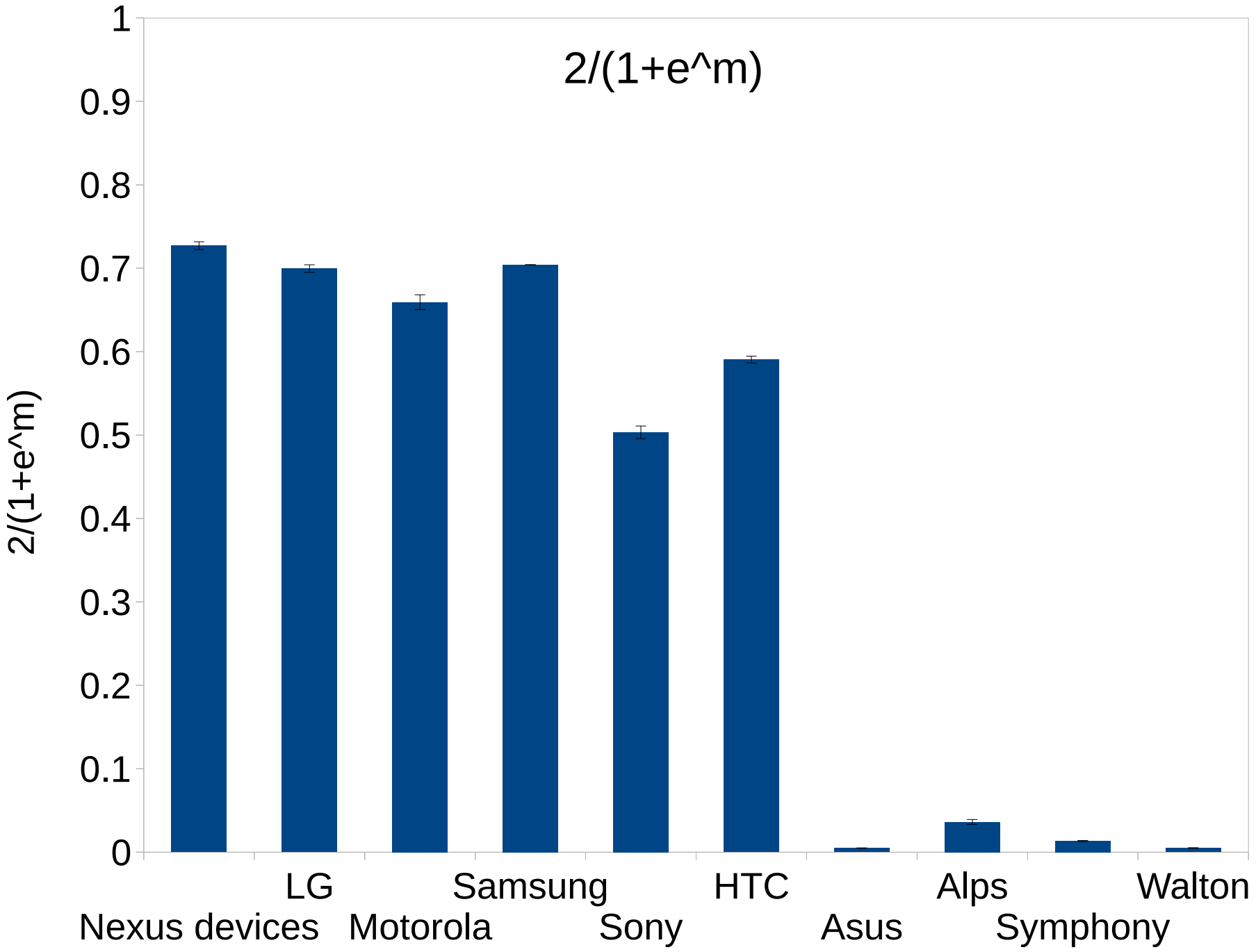


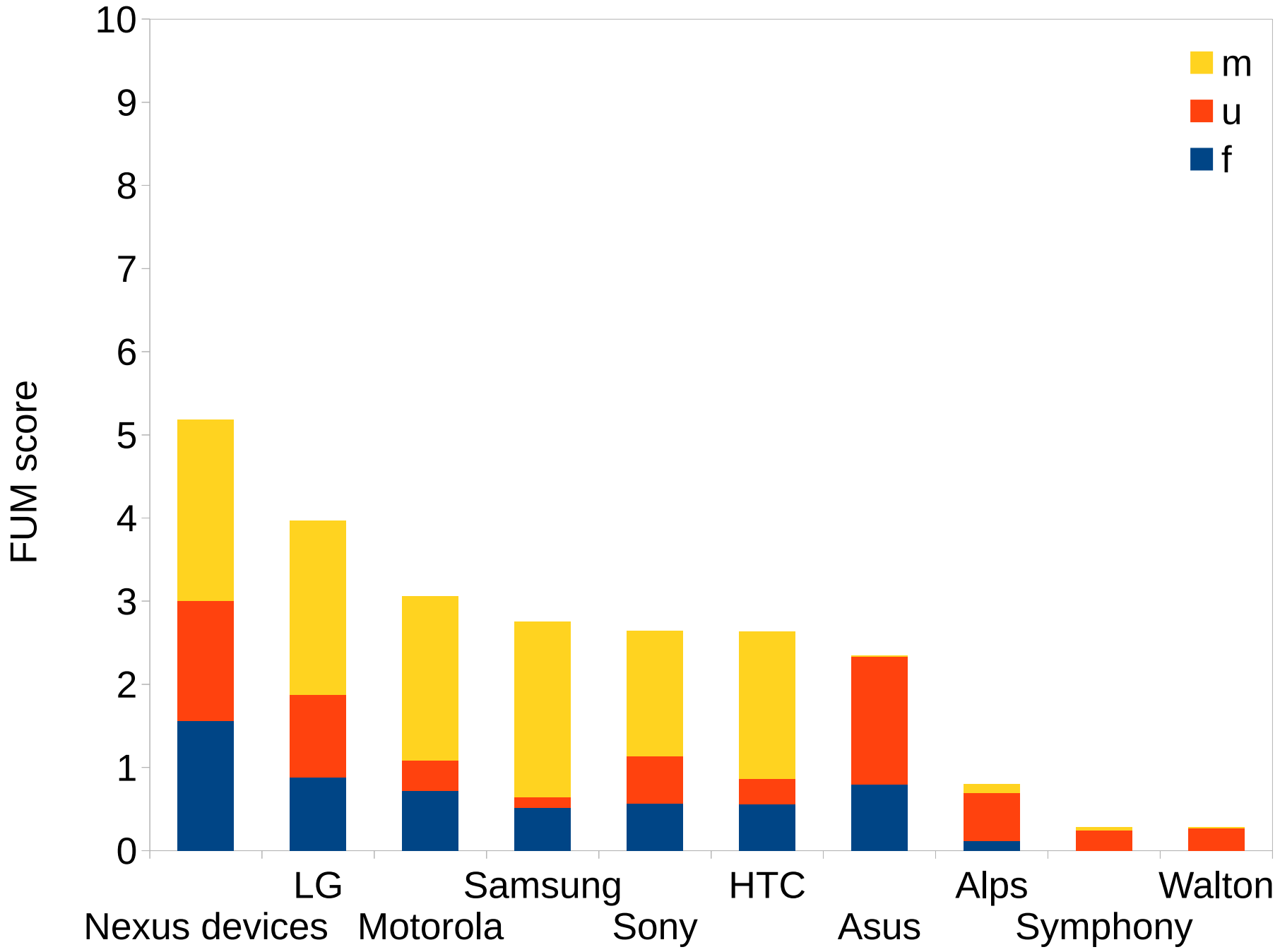
Symphony W68




f
Proportion free from known vulnerabilities
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
Nexus devices
LG
Motorola
Samsung
Sony
HTC
Asus
Alps
Symphony
Walton


u
Proportion updated to latest version
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
Nexus devices
LG
Motorola
Samsung
Sony
HTC
Asus
Alps
Symphony
Walton

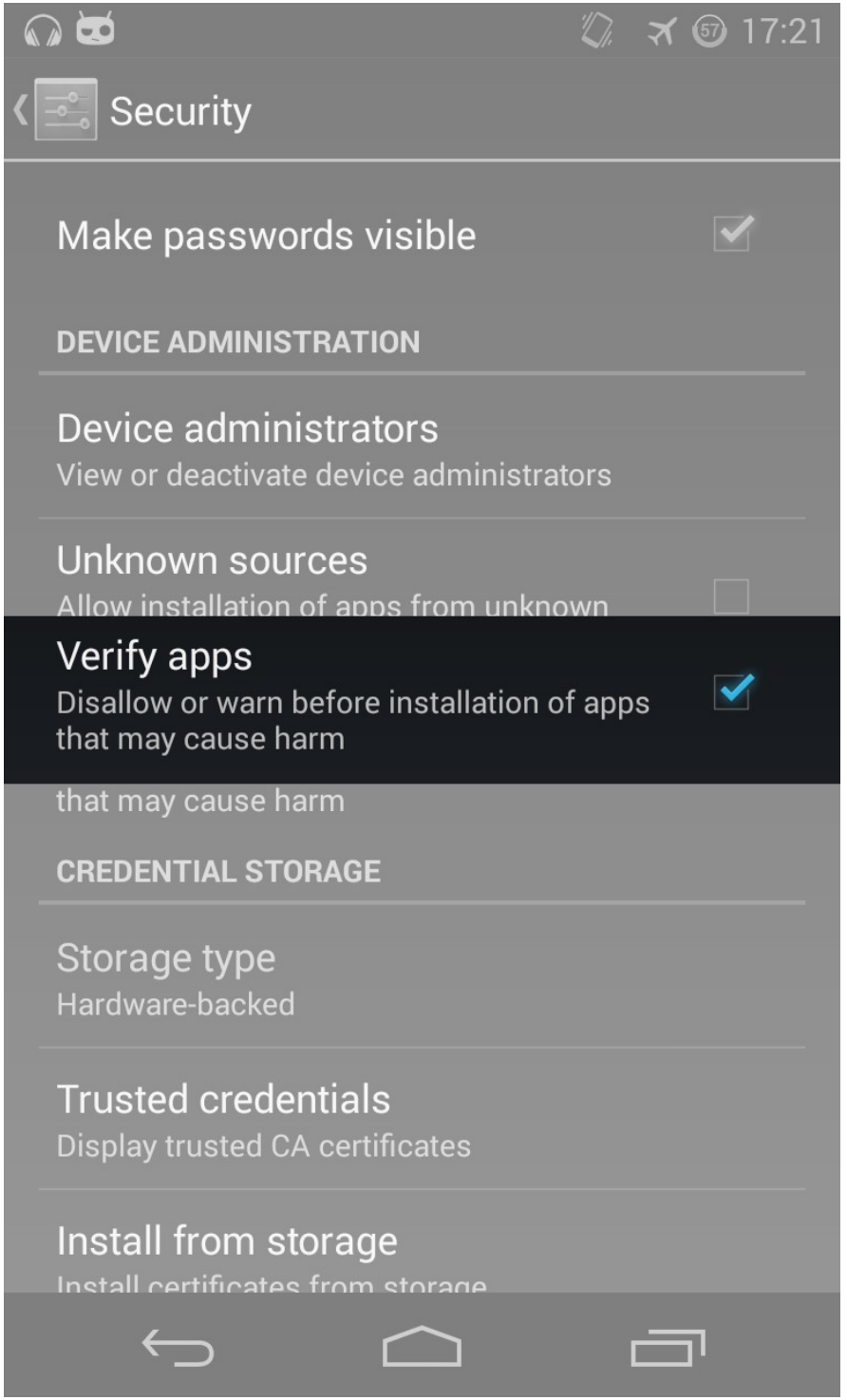

2/(1+e^m)
2/(1+e^m)
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
LG
Samsung
HTC
Alps
Walton
Nexus devices
Motorola
Sony
Asus
Symphony


FUM score
10
9
8
7
6
5
4
3
2
1
0
m
u
f
Nexus devices
LG
Motorola
Samsung
Sony
HTC
Asus
Alps
Symphony
Walton

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

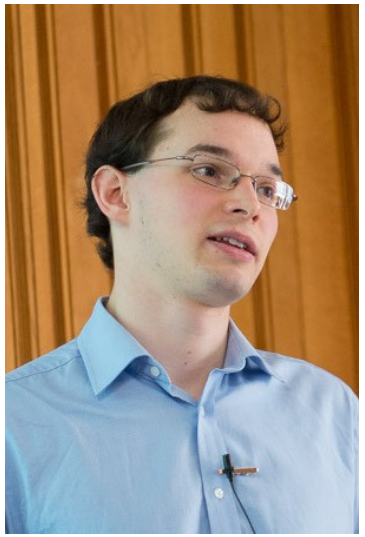
Google to the rescue: *Play Store* and *Verify apps* provide security



Conclusions

- 85% 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