THE 4TH CYBERSECURITY EDUCATION & RESEARCH CONFERENCE

Measuring Android security

René Mayrhofer[1], Michael Roland[1], (many others),
Daniel R. Thomas[5]

1. Johannes Kepler University – Institute of Networks and Security,
2. University of Cambridge – Computer Science & Technology,
3. Fraunhofer AISEC, 4. Google
5. University of Strathclyde – Computer & Information Sciences,
6. Technische Universität Darmstadt, Secure Mobile Networking

Cyber Education & Research Conference (CERC) 2022-10-25–26

Smartphones contain many apps written by a spectrum of developers

How “secure” is a smartphone?

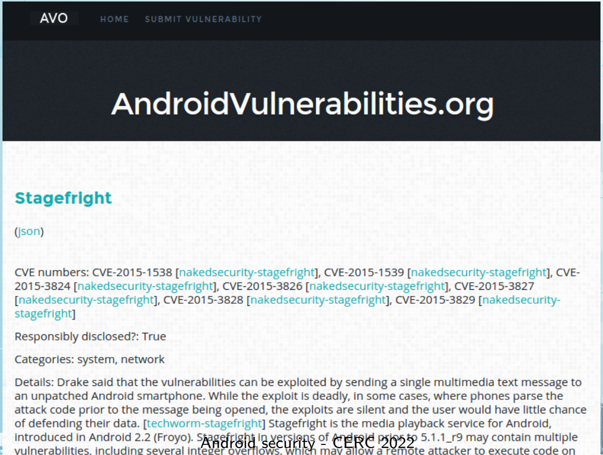
Need to incentivise device security

- Personal and enterprise customers cannot check security
- Companies cannot market their security
- Security is expensive
- Market for lemons

Hypothesis: devices vulnerable because they are not updated

- Anecdotal evidence was that updates rarely happened
- Android phones, sold on 1-2 year contracts

No central database of Android vulnerabilities: so we built one



AndroidVulnerabilities.org

Stagefright

(json)

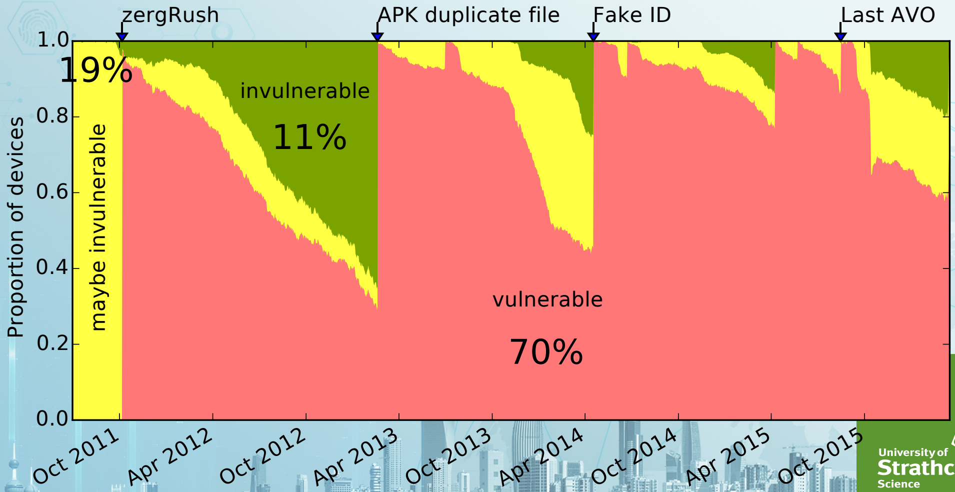
CVE numbers: CVE-2015-1538 [nakedsecurity-stagefright], CVE-2015-1539 [nakedsecurity-stagefright], CVE-2015-3824 [nakedsecurity-stagefright], CVE-2015-3826 [nakedsecurity-stagefright], CVE-2015-3827 [nakedsecurity-stagefright], CVE-2015-3828 [nakedsecurity-stagefright], CVE-2015-3829 [nakedsecurity-stagefright]

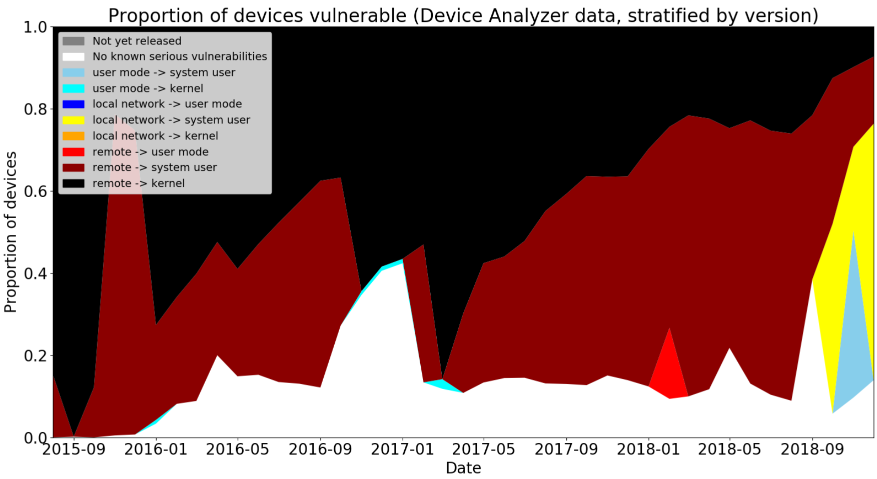
Responsibly disclosed?: True

Categories: system, network

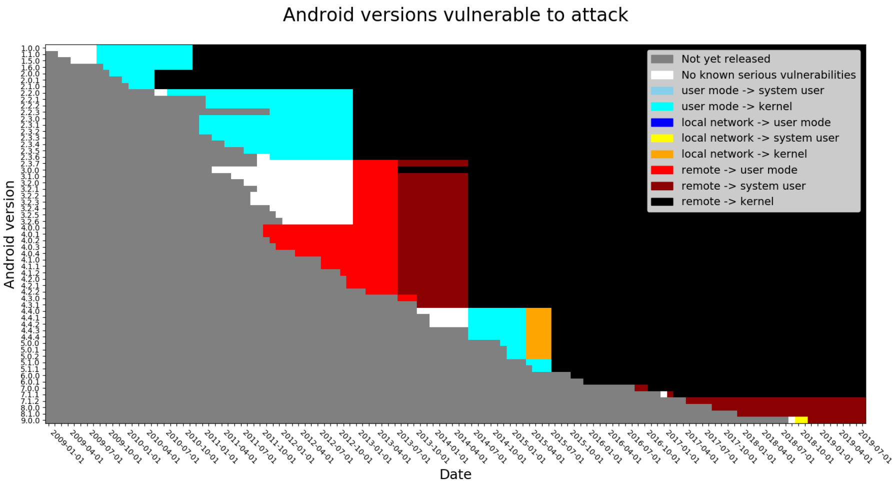
Details: Drake said that the vulnerabilities can be exploited by sending a single multimedia text message to an unpatched Android smartphone. While the exploit is deadly, in some cases, where phones parse the attack code prior to the message being opened, the exploits are silent and the user would have 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

Vulnerability varies over time





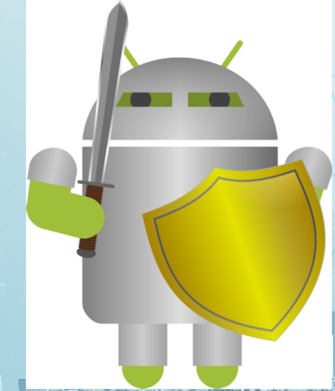
Work by Daniel Carter, Daniel R. Thomas, Alastair R. Beresford



Work by Daniel Carter, Daniel R. Thomas, Alastair R. Beresford

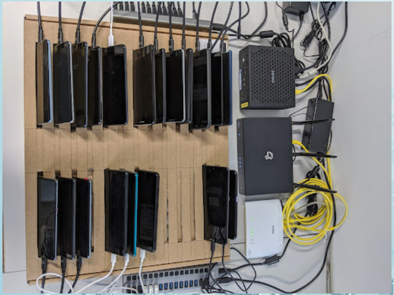
Reveal security state of Android

Want to give meaningful data to users and organisations to make an informed decision concerning the security of a particular device



Measure all the things

- Device farms at 3 different institutions
- App for crowd sourcing data (in progress)
- Data from testing labs (biometric tests etc.)



Collect lots of attributes

- Average patch frequency [days]
- Guaranteed patch availability [years]
- Latest security patch level [date]
- Device encryption type [”file” or ”block”]
- Preloaded apps with system privileges [count]
- Software mitigations: kernel / userspace CFI/SCS, integer overflow sanitization enabled, etc.
- Biometric sensors false accept/reject rates spoof/impostor accept rates, etc.
- `https://www.android-device-security.org/attributes/`

Best means of communication?

- Some sort of score?[1,2]
- Something journalists can include in reviews
- Minimum standard for manufacturers? (Label on the box)
  - ETSI TS 103 645
  - Internet of Secure Things Alliance

[1] Billy Lau, Jiexin Zhang, Alastair R Bereford, Daniel Thomas, and René Mayrhofer. 2020. Uraniborg's device preloaded app risks scoring metrics. *Institute of Networks and Security: Linz, Austria* .

[2] Daniel R. Thomas, Alastair R. Beresford, and Andrew Rice. 2015. Security metrics for the Android ecosystem. In *ACM CCS workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*. ACM, Denver, Colorado, USA, (Oct. 2015), 87–98.

Interested? Get in touch!

- Communicating measured security
- Better ways of measuring security

d.thomas@strath.ac.uk

https://personal.cis.strath.ac.uk/d.thomas/

References I

[1] Billy Lau, Jiexin Zhang, Alastair R Bereford, Daniel Thomas, and René Mayrhofer. 2020. Uraniborg's device preloaded app risks scoring metrics. *Institute of Networks and Security: Linz, Austria*.

[2] Daniel R. Thomas, Alastair R. Beresford, and Andrew Rice. 2015. Security metrics for the Android ecosystem. In *ACM CCS workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*. ACM, Denver, Colorado, USA, (Oct. 2015), 87–98.