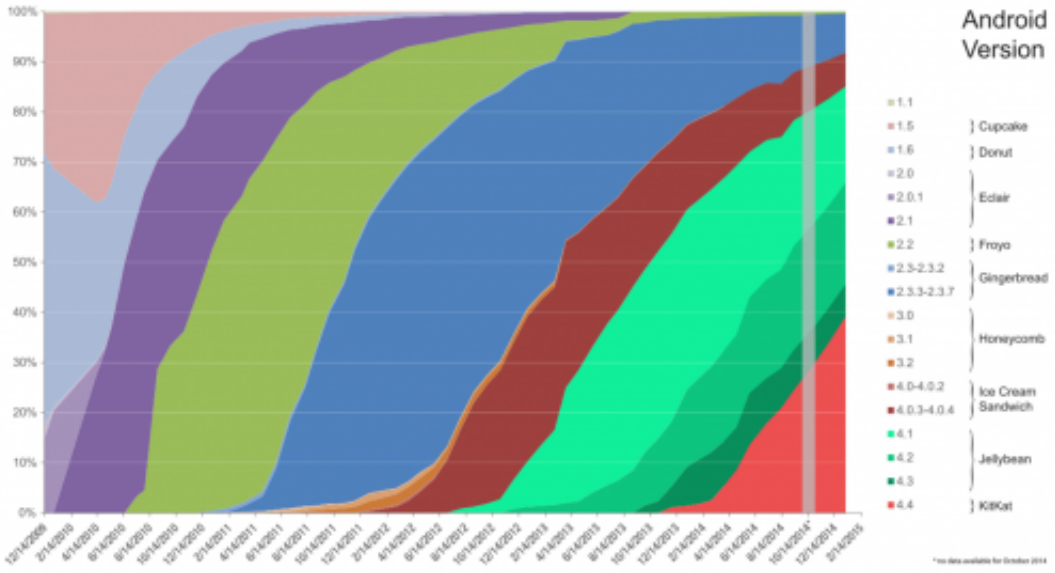
Google deals out 'tough love' as it ends security updates for a billion Android users

January 19 2015, by Aleksej Heinze And Alex Fenton



Android's long tail - many users still run older versions. Credit: Erikrespo/Google data, CC BY-SA

Google's announcement that it will not provide security updates for older versions of its Android mobile operating system means that more than a billion users face growing security risks to their phones or tablets.

While Android phones and tablets have grown exponentially in popularity, from 4% market share in 2009 to 84% in 2014, by abandoning support for versions prior to Android 4.4 "Kit Kat" Google's decision affects more than 60% of Android users running older versions

that will now be vulnerable.

At the heart of this announcement is a piece of software called WebView, a component of the built-in web browser in earlier versions of Android, but which also turns up in many apps. It is WebView that Google is dropping support for, replaced in version 4.4 with a new component taken from Google's browser, Chrome.

The reason for this is largely down to the number of security flaws found in the software, at least in part because it incorporates support for Adobe Flash which has simply proven too difficult to secure – ironically, as it was something Google touted as a plus for Android when Apple dropped Flash support for the iPhone.

There was no official announcement. In response to security researchers Rapid7 who had reported another WebView bug that needed fixing, Google responded:

If the affected version [of WebView] is before 4.4, we generally do not develop the patches ourselves, but welcome patches with the report for consideration. Other than notifying OEMs, we will not be able to take action on any report that is affecting versions before 4.4 that are not accompanied with a patch.

Many hands make light work

So Google is no longer fixing problems in anything but their latest (Android 5.0/Lollipop) or second-latest (Android 4.4/Kit Kat) versions, offloading the responsibility to either those that find the flaw, other interested developers, or phone manufacturers such as Samsung, HTC, or LG.

Android is an open-source operating system developed jointly by Google

and other interested developers around the world who are able to update and maintain the codebase, while Google manages and steers the project. By making Android an open-source project, Google increases the community's ownership of the project, encouraging others to work on it. This approach is contrary to Google's competitors – Apple's iOS and Microsoft's Windows Phone – who develop their operating systems entirely in-house and keep tight control of their code.

So Google's decision makes more sense with that in mind – the code for Apple and Microsoft's operating systems is closed, so those firms wouldn't be able to hand off their responsibility in this way. But Google can at least offer others the chance to tackle the problems.

Keeping you and your data safe

Our mobile phones are used for sensitive activities – from logging in to websites filled with personal data, to online banking or online shopping. It's important to keep any software on any device – phone, tablet, or computer – up-to-date with the latest versions that patch those flaws and vulnerabilities that have been discovered. Encouraging more people to use the latest versions has been a key part of Google's approach, through automatic updates and cloud services.

However, mobile phone manufacturers are keen to sell us their latest phones. Providing ongoing support for older phones is expensive and phone manufacturers, and especially the telecoms companies that sell them to us, are already terrible at updating phones, generally dropping support for older models as soon as they can. Expecting them to provide regular security updates seems far-fetched.

The upshot is that now phones even less than a year old are potentially vulnerable – Android 4.4 may have been "released" in late 2013, but new phones were arriving with 4.3 installed well into 2014. So, what can we

do? Buy a new Android phone, or switch to Apple, Microsoft, or Blackberry?

Apple devices are considered by some to be more secure because of the tightly controlled ecosystem, from the operating system code to the vetting of apps in the App Store. But even iOS is not immune. Part of Android's appeal is the fact that it is open: easy to access and customise, but with a greater risk from rogue apps, viruses, and hacks. It also means that, with the requisite technical skill and patience, Android users can tackle these problems themselves, unlocking, upgrading and customising their own devices as they like – such is the way with open source.

The moral of the story

So, are Google setting more than half their users up for a fall? In practice this may not have a huge impact for most. It may encourage phone manufacturers and the telecoms companies that sell them on to us to be more forthcoming with software updates for their devices, reducing the number of devices running out-of-date software.

Ultimately, the key message is that we need to start thinking of mobile devices as computers, not just phones, with all the caveats about security software, updates and precautions which that entails. This could be the tough love from Google that pushes people in that direction.

Source: The Conversation

billion-android-users.html