University of Cambridge: Android comfort zones are few

October 15 2015, by Nancy Owano

By now everyone gets it. Android as a mobile operating system has been a malice magnet, and the scenario by now is familiar: Android teams rush out their patches to manufacturers but a lot of white noise from some of the manufacturers deters neat endings.

A new study offers a sobering look at Android. Research revealed that 87% of Android devices are vulnerable to attacks through malicious apps and messages. The blame appears to close in on those

manufacturers who do not deliver timely or regular security updates. "We showed that the bottleneck for the delivery of updates in the Android ecosystem rests with the manufacturers, who fail to provide updates to fix critical vulnerabilities," said the researchers in their study.

This report is well documented, basing its stats on over 21,700 devices, with the information gathered thanks to Device Analyzer. This is an app that researchers at the Computer Laboratory of the University of Cambridge created. The app has been available for free on the Play Store since May 2011, said *iProgrammer*.

Their findings: "We find that on average 87.7% of Android devices are exposed to at least one of 11 known critical vulnerabilities and, across the ecosystem as a whole, assign a FUM security score of 2.87 out of 10."

Harry Fairhead of *iProgrammer* explained the research process: "After participants opted into the survey, researchers collected daily Android version and build number information and compared this against a list of critical vulnerabilities dating back to 2010."

Each device got a "secure" or "insecure" label, he continued, based on whether its OS version was or was not patched against these vulnerabilities or placed in a special "maybe secure" category if it could have obtained an update with a backported fix.

The team authored the paper "Security Metrics for the Android Ecosystem."

What's the point of yet another Android-has-vulnerabilities story? A means for security sleuths to gain publicity? Not at all. In this instance, the research stands as a contribution toward stronger incentives for more manufacturers and operators to deliver needed updates.

The research paper stated that "The security of Android depends on the timely delivery of updates to fix critical vulnerabilities. Unfortunately few devices receive prompt updates, with an overall average of 1.26 updates per year, leaving devices unpatched for long periods."

The researchers said, "there is information asymmetry between the manufacturer, who knows whether the device is currently secure and will receive updates, and the consumer, who does not. Consequently there is little incentive for manufacturers to provide updates."

According to their "Security Metrics for the Android Ecosystem," in their data, Nexus devices did considerably better than average with a score of 5.17; and LG was the best manufacturer with a score of 3.97.

The research is ongoing and the team have set up a website, AndroidVulnerabilities.org, to report its progress. The group developed a score to compare the security provided by different device manufacturers. The score gives each Android manufacturer a score out of 10 based on the security they provided customers over the last four years.

Alastair Beresford, a co-author of the paper, shared this comment in *Light Blue Touchpaper*, a weblog written by researchers at the University of Cambridge Computer Laboratory.

"Google has done a good job at mitigating many of the risks, and we recommend users only install apps from Google's Play Store since it performs additional safety checks on apps. Unfortunately Google can only do so much, and recent Android security problems have shown that this is not enough to protect users. Devices require updates from manufacturers, and the majority of devices aren't getting them."

Moving on, if most of the blame rests with OEMs, Ron Amadeo,

Reviews Editor at *Ars Technica*, delivered his take on Android and security. "With 87 percent of devices flagged as insecure on any given day, the study really shows how far the Android ecosystem has to go to protect its users. Google and some OEMs have committed to a monthly security update program, but that is usually for devices that are less than two years old (Google recently bumped Nexus devices to three years) and only for flagship devices. The vast majority of Android sales are not flagship devices."

Amadeo spelled out what he thinks needs to happen. "Until Google re-architects Android to support centralized, device-agnostic updates, we just don't see a solution to Android's security problems."