

Home > News > Software

Android or CyanogenMod, which is more secure?

By Krishna Bahirwani April 20, 2016 Software

Battle of open source



CyanogenMod or Cyanogen OS, the commercial version of CyanogenMod have been a preferred choice of security-conscious mobile users thanks to features such as Privacy Guard, PIN Scramble, and Protected Apps. Android has since been improving its security and the latest versions of the operating system bring with it features like regular patches, app permissions, and encryption. In an exclusive interview, Krishna Bahirwani speaks to Anant Shrivastava, developer, Android Tamer, a Linux-based operating system for Android security professionals to discuss the security of both operating systems.

What are the security strengths of stock Android over CyanogenMod?

To begin with stock android is a vague term, the correct word to be used is AOSP or Nexus build. Any other devices besides the Nexus series that are sold by Google themselves have vendor specific customization.

CyanogenMod, on the other hand, is a community driven ROM which strives to provide better software support for a large range of hardware. The core team behind CyanogenMod also runs Cyanogen INC which is responsible for Cyanogen OS. You will not find any device officially using CyanogenMod however Cyanogen OS is used by YU as well as One Plus One and a couple of other companies.

With these distinctions aside, let's look at various area's where stock Android or Nexus build has the advantage over CyanogenMod. As soon as google pushes out security fixes, Nexus devices are the first ones to receive it via OTA and if you don't want to wait for OTA you can grab the files directly from the google website also.

Google has now started to push security fixes on a monthly basis and only Nexus devices and Android One devices are guaranteed to be getting the update in the same month. Other devices are at the mercy of the vendors. CyanogenMod, on the other hand, can only provide a security fix once it's compiled in its codebase and OTA is created for your specific devices.

CyanogenOS has been lacking a lot when it comes to providing monthly security updates. Android 6.0 or Marshmallow has been out for a very long time now and Cyanogen OS or CyanogenMod don't have a stable version of OS.

What aspects of CyanogenMod are more secure than Android?

Being a community-driven approach, the first priority is a feature rich and optimized OS. As a by-product, they also had a good security fix cycle earlier. However, with monthly OTA updates by google that include security fixes, Cyanogen is slowly losing pace. However, features like privacy guard were first available on CyanogenMod and are still present in the OS. Privacy guard allows you to separate the application and selectively allow access to contacts and SMS. If we leave this aside, CyanogenMod doesn't have much of an advantage over AOSP or Nexus builds. However, if we add firmware like CopperHeadOS and or the kind that is present in the Blackphone, you see a massive amount of security-specific features being added.

What are the areas in which they both can improve?

There is a lot of improvement that is possible and that is quite evident by the development efforts on projects like Blackphone, and Copperhead OS. While Copperhead OS wants to bring in enhanced protection against attacks for the device, the Blackphone project is trying to build anonymity and confidentiality into communication.

If you ask me what I would want to see in Android in the next 1 or 2 years, it would be a basic core that takes inspiration from these security-centric projects and has features like privacy and protections added to it.

Is it okay to buy mobile phones with older versions of Android or CyanogenMod?

I would strongly recommend against buying such devices. These devices are in the market because we as consumers don't question manufacturers. If we start doing that we will have a better system. The advantage we have with the newest version of Android is that the latest developments are happening in this version whereas older versions are just maintained and in a lot of cases, not even maintained at all. The major disadvantage that the users have is the fact that there is no incentive for manufacturers to keep updating their OS and hence we see a lot of devices which might never see an update in their whole life.

This was the exact issue that CyanogenMod was trying to solve and somehow, somewhere, that aim is now lost. This is most likely because the community is not able to cope with the constant update cycle. The fact is that CyanogenMod has also been stuck at android 5.1 for a long time now.

Which one of the two comes out a winner in terms of security?

I would personally side with AOSP. AOSP has really been trying to ramp up the game by adding lots and lots of security features.