How secure is Android?: Anant Shrivastava

Anant Shrivastava, creator of Android Tamer, a Linux environment specially designed for Android Testing, speaks to Krishna Bahirwani and shares his thoughts about how safe Android is after the WebView vulnerability

SHARE

WRITTEN BY

Krishna Bahirwani

SOURCE

DNA

Updated: Jan 19, 2015, 06:50 AM IST

How does Android security differ from iOS security?Android was conceptualised with open development model and hence Initial focus was more on keeping it open rather then keeping it secure. Google has in past few years done an amazing job at tightening the security of an out of the box Android system. Where as when iOS is considered we have to understand that they spend considerable time in scrutinising the software that are made available via App Store although that doesn't guarantees protection against security issues. at this point android 5.0 is still not exploited where as iOS 8.1 series was exploited within 10-15 days of launch as they didn't fixed a already known security issue properly.

Tell me about Android Tamer and your previous work with Android! started working on android around 2010 when india was catching up on android and the whole smartphone race. I started out with running custom rom's modifying them as per my need and that's when i started looking at various security aspects of android. I did research on various custom roms available online and various security issues associated with them. The research was presented as a whitepaper during c0c0n 2011 security conference in Kerala.

This lead to creation of Android Tamer which is a Linux based customised operating system pre packaged and optimised for android related work. If someone is starting in android field and they need a basic setup they can quickly download android tamer from https://androidtamer.com and get started by booting it in Virtualbox or VMWare software. We have curated and configured best android specific tools for android professions. So you could be an android programmer or a android security researcher or malware analyst or forensic investigator you will find tools for your specific use case preconfigured in it.

What is your opinion of CyanogenMod from a security perspective?
Cyanogenmod is a aftermarket firmware which basically takes AOSP (the open source version of android) and customise it to add new features. Cyanogenmod does offer some advance features like privacy guard which are very useful if you do not want to expose your personal information to all your applications.Overall Cyanogenmod could be a good fit from security perspective however the effort required to get it up and running on a device varies with each devices and manufacturer.

How easy is it to backdoor Android?In past 2-3 years security has grown leaps and bounds in android core. As of now core system is not the one being backdoored actively, it is generally the custom OEM components which are used to get backdoors running on the machines. Here off course one exception is physical access. if you give your unlocked phone to an unknown person it is just a matter of connecting a usb cable to your phone and changing some settings to get it backdoored. However thing to be kept in mind this kind of backdoor is always possible with any computing system. Physical access is considered Gameover for all.

What can be done to truly harden the Android operating system to prevent exploitation?This is where we need to start with a renewed mindset. With Android its not just the phone manufacturer who needs to keep hardening in mind its every user itself. That's how android was conceptualised and is one of the core reason for it being so open, and so customisable. It is assumed that user will make informed decision about installing a software. So if you see that a alarm clock wants to access your contacts or have access to camera it is time to relook if you want to use it. Or worse if your ringtone editor wants access to send SMS you need to be cautious. Google is streamling how permissions are displayed but User is the ultimate authority and hence its upto the user to make final call.

Besides application stealing data another general incident is that the phone is lost. With newer versions of android it is possible to encrypt the phone. It is recommended to encrypt the phone if you have sensitive information on your phone (sensitive information could be your love letters, personal pics, to official documents or conversations). It is also recommended to keep a screen lock which is not simple password like 1234 or 4321. Many applications trick users by forcing them to change specific security settings such as allowing unknown source applications installation. Do not change system settings just because an application is asking you to do it.

How secure is stock Android?When you talk about AOSP or Nexus lineup there has been very few rooting or exploitation around them in past couple of years. Google team on a general level does an excellent job at increasing the security level of a system. The security issue generally arise in the OEM customisation layer. So people should be cautious about picking any android phone. If there are many customisations done in the phone this mean there are more chances of finding security issues in them.

What resources would you recommend for people who are interested in this subject but will not be able to attend your training ?This time I have joined hands with another good android security researcher Aditya Gupta to deliver the most advanced course material for Android Security. I would definitely recommend people to attend it. However if you are not able to make it. The newer version of android tamer would be available at https://androidtamer.com so you can download that and to start with understanding how security works in android you can look at source.android.com. we also manage a twitter feed on android security news as @androidtamer twitter id. so Following this id will ensure you get your daily dose of android security.

What is your opinion on the recent WebView vulnerability disclosure and no support from Google ?Google has basically stopped supporting the Android versions prior to version 4.4 and that's the reason for discontinuing the patches. However, another consideration is that Google doesn't properly list when a specific version of the Android OS will no longer be supported. Hence, there is something left to be desired from Google's end as well. This however, doesn't stop manufecturers from developing their own patches and protecting their own customers from the issues, but this would require manufacturers to spend some effort on their part.

Initially, Webview was part of the Android operating system, in which case if webview needs to be updated then there needs to be a whole OS update.

Although the Android ecosystem is not in direct control of Google, yet Google works on core Android which they provide as AOSP (Android Open Source Project) and as an operating system in the Nexus line of devices. For other devices vendors add their own layers as well as Google services in a package and then provide that to the consumers. Hence in this scenario, when say Google receives a vulnerability report about webview and let's assume they fix the issue then this will be the flow - they will issue a notice to all vendors that a fix is available and depending on how vendors want to support their devices they will issue an over-the-air (OTA) update which may or may not be performed by many vendors. This is where Google has changed the whole ball game from version 5.0 by decoupling webview from the core OS and is putting this as part of Play Store. This way Google has more control over ecosystem and can issue patches for devices irrespective of thevendors.

So if we look at this issue from a consumer's point of view, it is of the utmost importance that they buy Android devices from vendors which support Android updates as well as ensure that latest version of Android is installed in the phone by default. At this point, this would mean 4.4 or above. If you have an older device and there is no update for your device, then the only possible solution would be to buy a new device. It's harsh but that's what is needed to ensure the safety of the end user.

Google no longer has your back About a billion users all over the world own an Android device running Android 4.3 or earlier and now Google has put all of them at risk by ending support for older versions of Android WebView - the default Android web browser and the component used to render we pages. WebView was replaced by a Chromium-based version in Android KitKat 4.4.Tod Beardsley, who discovered the vulnerability informed Google about the same and the incident handlers at security@android.com responded with this -"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."

Learn more at NullconNullcon 2015 will be conducting hands-on training by Anant Shrivastava and Aditya Gupta for two days for those who are interested in Android's security flaws and how they are exploited.The training will take place on the 4th and 5th of February 2015 at the conference venue, The Bogmallo Beach Resort, Goa. The training will cover the internals of the Android platform and it's weaknesses, how Android applications are analyzed and reverse engineered and lastly how vulnerabilities are found and exploited.Nullcon 2015 will also feature training by other security researchers including Justin Searle, Mario Heiderich, Abhishek Datta, Joerg Simon, Prajal Kulkarni, Himanshu Kumar Das, Omair, Amol Naik, Anil Aphale, Akash Mahajan and Riyaz Walikar. They will cover a range of information security related topics ranging from web hacking to attack monitoring.You can find out more at - *http://nullcon.net/website/goa-15/training.php*

Kerala | Goa | Twitter | Google | India | Android | security | Nexus | Development | software | iOS | safety | smartphone | hacking | applications | Information Security | manufacturers | App Store | Open Source | iOS 8

http://dnai.in/cswt