Taking Control of Permissions on your Android Phone

by Aaron Grothe
NEbraskaCERT

Disclaimer

Some of the things we are talking about tonight can take your nice shiny device and turn it into a nice shiny paperweight.

We claim no responsibility if trying any of these things lead to anything up to and including your device achieving sentience and trying to wipe out the human race

Permissions Land Grab

Ordered from most to least evil???

Jay Z's Magna Carta app
Romney/Obama Campaign Apps
Can Knockdown/Others
Serious Sam: Kamikaze
Mozilla Firefox

Jay Z's Magna Carta App

Offered to Samsung Galaxy users - access to album 3 days in advance

EPIC has failed a suit with the Federal Trade Comission over the amount of permissions requested - https://epic.org/ftc/EPICsamsungcomplaintFINAL.pdf

What did it ask for?

Jay Z's App Request List - Page 1

- To modify or delete contents of USB storage
- To prevent phone from sleeping and view all running apps
- To access your precise (GPS) and approximate (network-based) location
- For full network access
- Read phone status and identity

Jay Z's App Request List - Page 2

- To run at Startup
- Control vibration
- Find accounts on your phone
- List all phone numbers contacted
- To modify or delete your USB contents - technically this is included twice, but come on

But I need the app to get the album

After you run the app the music becomes part of your regular music library

Little is said about how long the data will be held, will it be resold, etc

That is Just One App

Romney VP and Obama for America Apps

Both apps got the following base set of info

- Device ID
- Carrier
- Phone Number
- GPS location
- Cell Location
- Package Info on other installed apps

Romney App

Ability to record audio on your phone <Danger Will Robinsion!!!, Danger>

Encouraged you to sign up for a MyMitt account or login with your Facebook info

If you used Facebook you gave the app permission to do posts on your behalf, also the ability to get your friends list

Obama for America App

- Access users's phone contact list (names and numbers)
- Contents of the SD card
- App logs user location info
- Canvasing tool to help you meet other Obama supporters - gave registered voters first name, last initial, age and home address

Can Knockdown/Others

Currently have about 4 apps on my Google Nexus 7 I'm not going to update because of additional application requests. The app was working fine before why do they need these additional permissions

Serious Sam Kamikaze

App released on the Amazon App Store

Had several very dubious permissions including

- Ability to take screenshots of other running apps. WTF???
- SMS Access and more

Fixed in a release shortly after the reviews started coming in

Mozilla Firefox

Mozilla's Firefox is starting to add the capability to do Real Time Chat (RTC) to their browsers. This means they are requesting additional privs in terms of turning cameras and microphones on and so on.

What if I just want a browser and don't want my browser to have these new privs?

We will talk about 4 Cases tonight

- Device with pre-android 4.3 / not unlocked
- Device with Android 4.3 / not unlocked
- Device with CM 7 (Android 2.3.x) / unlocked/root
- Device with CM 10.1 (Android 4.2) / unlocked/root

Root/Unlock/Jailbreak

What is the difference between Rooting/Unlocking and Jailbreaking

- Jailbreaking/Rooting gives you full access to the current o/s on the device. You can bypass the permissions on the device.
- Unlocking is when you've unlocked the bootloader and can install any o/s on the system

How to display Android Screen on PC

I’m using Android Screen Mirror (ASM) for this
Other tools include AndroidScreenCast, MirroCast and so on

- Works well, resize options, rotation etc
- Slow 4-5 FPS - please let me know to slow down if I’m going too fast
- Also please remind me to rotate screen if I forget

Basic Steps any Device

Figuring out what permissions are being used on your device

- Permission Dog - quick demo of it
- Play Store - review permissions when updating
- If there are new permissions being requested ask developer why
- Put these in the Market reviews as well

Pre Android 4.3 Stock Devices

- Your options for controlling an application are pretty limited without rooting your device
- Your best advice is to be aware of what you are installing and review your options
- This is where I’m stuck at with my current phone

Android 4.3 Stock Device

- Android 4.3 has added the ability to control the access that an app can have
- Infrastructure is in place need a 3rd party app to control these
- Lets take a look at Permissions Manager - demo
- Note: once you start doing this you might “anger” your apps

Android CM 7 Device - Unlocked

- Cyanogenmod 7 provides you the ability to restrict permissions on a per app basis. Quite a bit like Android 4.3
- Lets take a quick look at what it looks like
- Lets run Angry Birds a bit and see how it likes a restricted app environment
- Disappeared from later CM versions. Android 4.3's version will be present in CM 10.2

Android CM 10.1 - With OpenPDroid - the Golden Path

Lets see what we can do to get some control over the information we send back to the App's owners

Device running CM 10.1 with OpenPDroid

OpenPDroid is a kernel patch that allows you fine grained control over apps

Lets take a bit of a look at Angry Birds and what we can do there

- Take a look at PDroid manager
- Set permissions for Angry Birds
- Give it a run

How does OpenPDroid Work

There are two branches of this software PDroid and OpenPDroid. OpenPDroid has worked out better for me on later CM versions

You create a custom .zip file that you install on your phone using either ClockworkMod Recovery or TWRP

You then install PDroidManager to let you set permissions

How to install OpenPDroid

- Download autopatcher, CM 10.x to your PC
- Run autopatcher to create .zip file for your phone's Rom
- Copy CM, OpenPDroid.zip and Gapps to phone
- Root/Unlock Phone
- Install ClockworkMod Recovery or Twrp
- Boot into ClockworkMod Recovery
- Install CM/OpenPDroid.zip Gapps
- Install PDroid Manager from Google Stor

Some Changes last 6 Months

Android 4.3

- Ability to control permissions on a per app basis
- SELinux is incorporated into Android 4.3

Replicant
Qemu/KVM running on Arm-64 bit chips
Vmware POC on ARM

Replicant???

Replicant is a project to create a totally Open Source version of Android for devices

If you try to build your own version of CM you will have to get various binary blobs to do things like run displays, 3g/4g, phone access and so on. This is a project to have a totally open phone
New Nexus 7 can't be run without Binary Blobs - developer of AOSP left because of it

Changes next 6-12 Months

- GUI control for SELinux on your phone
- LXC for Android is coming
- Virtual Machines on your phone
- Smack/AppArmor for Android
- Firefox OS/Tinzen/Sailfish/Ubuntu, etc

Changes next 6-12 Months

- More support for unlocking phones
- Replicant will continue to evolve
- Linux/Android kernels continue to sync
- Incognito mode/Privacy Mode in CM
- CM phone locator/remote wipe
- CM without root

I have an Ipad/Iphone what can I do?

Out of the box you can restrict what apps have access to your contacts list

If you jailbreak your phone there is an app called Protect My Privacy (PMP) is available in the Cydia store. Which can do a lot of the same things that PDroid manager can

Is there an Enterprise Solution?

Some of the BYOD solutions can whitelist apps that are allowed to be installed. Problem is there are a lot of apps that people want.

If a company had enough resources and wanted to only have an approved set of phones something could be done with CM, etc.

Some Tips

- Do not start to play with your phone after 10pm if you have to work the next day. The phone gods will kick your butt
- If you have a demo do not screw with your phone. One more update is the way of the devil
- XDA Forums are an amazing resource. Every 5 minutes spent there will save you an hour later
- AutoPatch is your friend

Some Tips

- Titanium Backup is your friend
- Craigslist is a great way to get a device to experiment with. HTC Droid Eris on Craigslist today for $40.00 in pretty good shape
- Get a supported phone
- HTC is offering a very nice program through their HTCdev site to unlock your phone
- DON’T PANIC - you probably didn’t screw it up permanently

Summary

There is a saying “If you’re not paying for it you’re the product being sold. - many people claim ownership of this saying

“Even if you are paying for it you’re probably being sold” - Grothe’s Corollary

Questions?

The slides will be on the NEbraskaCERT site sometime later tonight

Links

- auto_patcher - http://forum.xda-developers.com/showthread.php?t=1719408
- ClockworkMod ROM Manager - http://www.clockworkmod.com/
- Cyanogenmod - http://www.cyanogenmod.org/
  HTCdev - http://www.htcdev.com

Links

- Motorola's Boot Loader Unlock page - https://motorola-global-portal.custhelp.com/app/standalone/bootloader/unlock-your-device-a
- OpenPDroid - http://forum.xda-developers.com/showthread.php?t=2098156
- PDroid - http://forum.xda-developers.com/showthread.php?t=1923576

Links

- PDroid Manager - http://forum.xda-developers.com/showthread.php?p=34190204
- Permissions Dog - https://play.google.com/store/apps/details?id=com.PermissioDog&hl=en -
- Protect My Privacy - http://www.protectmyprivacy.org/

Links

- Serious Sam App Review on Amazon - http://www.amazon.com/Devolver-Digital-Serious-Sam-Kamikaze/dp/B005SJTLUS/ref=sr_1_1?s=mobile-apps&ie=UTF8&qid=1377063542&sr=1-1&keywords=serious+sam
- XDA Forums - http://forum.xda-developers.com - the place to go for more information and troubleshooting on issues with permissions.