Bridget OConnor

Software 401

Assignment 1: Article Summary

This article talks about how a study has found that an alarming amount of android apps have secret commands, access keys, and master passwords. The researchers identified 12,706 apps that had some of the backdoor's listed above, and they "analyzed the top 100,000 Play Store apps (based by their number of installations), the top 20,000 apps hosted on third-party app stores, and more than 30,000 apps that came pre-installed on Samsung handsets"(Cimpanu). The reason why the general public should be alarmed that that so many apps have backdoor is that these backdoors could allow hackers to gain unauthorized access to many accounts of users, and this could also allow hackers to run commands on the phone with elevated privileges due to hidden secret command present in the apps input fields. They give actual concrete examples of this in the article even including a video of a master password being used to enter debug mode. They also put the number of downloads to show how many people are using these apps that contain backdoors. For example, there was a popular remote control app with around 10 million downloaded that could unlock access to a phone remotely with a master password even if the user lost their phone or if they had locked their own phone. A powerful and scary concept. Though some of the debugging modes that the researchers found were harmless, there were also many like the remote control app that posed a danger to users. Additionally, some of the apps that help these backdoor functions came preinstalled on phones so it is not even as if the user could be considered at fault for downloading the app in the first place. The researchers let app devs know about the backdoors in their app but not all responded, additionally researchers also uncovered hidden bad word filters in apps some of which were politically motivated.

This article definitely was eye-opening and has a very strong connection to software engineering and development because the problem lies in the way that the developers developed the app. Often it seems that devs include master passwords or backdoor functionality so that they might be better able to debug their own app. This is great before your app is released and might also even be harmless in some cases to leave a debug mode in the app when it is released (like google chrome inspect). However, it seems in many cases these master passwords and backdoors resulted in potential danger for the users. The failure of the smaller system, app developers, would be the fact that they left these kinds of things in their app. But the failure of the greater system would be that the android app store did not stop these apps from being in their store. As someone who has a Samsung phone and often uses the play store, I had a certain expectation that apps on the play store would be safe to download as they have to meet certain requirements to be on the play store. The failure of the system of the play store is that they allow for apps that have these vulnerabilities to be easily accessible to users and not warn the users about the possibilities of the repercussions these master passwords and back doors can have when they choose to download the apps. This is either because the app store does not know that the apps have thee features or that they do not care that their users might download apps with these features.

It is similarly disturbing that certain apps have secret "bad word" filters and politically motivated blacklists. As users, we would want the app store to tell us that the app contains these things when we choose to download it, or we would want apps that have these things, like certain secret political motivations, to not be in the play-store in the first place. A disaster that could happen would be what if an app has a politically motivated blacklist and gets hacked and third parties get and sell that blacklist. Then the users could potentially be harassed or arrested or something worse depending on what type of blacklist this is, who gets ahold of the data, and how much of that users' data they get a hold of. Also, the master passwords for the remote control app could go disastrous in a variety of ways. For example, if a political figure loses control of their phone that could go horribly wrong. I'm from Hawai'i and there was mass panic after someone hit the missile warning button on accident but our state representative forgot his Twitter password so he was not able to state that it was false for a good period of time so many people assumed it was real and minor panic and chaos in the real world ensued due to this virtual error. If someone had control of his phone and state that it really was real there is no telling how people would react or what kind of chaos would ensue.

There are a few ways to prevent these types of disasters, on the smaller level it would require that when devs choose to deploy their apps that they make sure that they do not release versions of that app that contain backdoors or master passwords for debugging. Additionally, that devs individually practice having basic ethics and not storing politically motivated blacklists, or employing secret “bad-word” filters and consider that these sorts of things could be harmful to users and ethically wrong and so they should not include them in their apps in the first place. The second way to fix this would be for the system of the app store to change. They would want to make the process of vetting apps for the play-store more rigorous they could employ people or software that could work to detect these backdoors and master passwords similarly to how these researchers did it with their tool InputScope, and not let apps that have these features be released on to the app store. In this way, users would never even download the apps in the first place. The third way would have to also be vetting apps that come pre-downloaded on phones and have the companies, like Samsung, who release apps with these backdoors preloaded on their phones face legal and public backlash for having these. In this way the companies that preload apps on their phone would be forced to also behave ethically to avoid lawsuits and public backlash even though their apps don't have to go through the app store to be on the phone. These are the 3 main solutions I can think of for this problem.

Cimpanu, Catalin. “12k+ Android Apps Contain Master Passwords, Secret Access Keys, Secret Commands.” *ZDNet*, https://www.zdnet.com/article/12k-android-apps-contain-master-passwords-secret-access-keys-secret-commands/. Accessed 28 Sept. 2020.