Marcantonio Soda

CSE-343

Professor Chuah

3 April 2022

The main issue defined in the paper is that the potential security threats caused by the exploitation of Android's custom permissions have been overlooked by the security community. The team developed software to thoroughly test the possible vulnerabilities of Android custom permissions and found that there are multiple security flaws in said permission system that could be taken advantage of by malicious parties.

The strengths of the paper far outweigh the weaknesses. The researchers showed that, given the billions of Android users in the world, the importance of the identified security issues cannot be overlooked. The team has done an effective job at proving that security vulnerabilities do exist surrounding custom permissions in Android. They give the reader enough background information on Android permission mechanisms so they may understand the proposed problems and solutions to the fullest extent. They thoroughly document the software, CuPerFuzzer, that they created to bring these issues to light. They go into enough technical detail on the inner-workings of their software to completely prove that it is a very useful tool in detecting flaws in the Android permission system. CuPerFuzzer was designed to act as a "black box". It is able to be operated with no knowledge of the internal implementation of Android permissions. The information that they give is quite technical, but abstract enough for the average user to digest. They enumerate four specific problems in the custom permission mechanism in an effort to thoroughly break them down later in the paper. They even go so far as to pose seemingly airtight solutions to the problems that they identified in a very effective manner.

Despite how well-done the research and the paper was, there are a few small shortcomings. The team does a great job proving that vulnerabilities in the Android custom permission system do exist, but they do not explain how these vulnerabilities could impact the

average user. A main intent of the paper seems to be to develop a sense of urgency in the reader. A better way to make the average person care about the proposed issues is to make him/her understand exactly how they could be affected. What should he/she do to avoid being exploited by one of the mentioned security flaws? What should he/she look for while they are choosing which apps to download? Another flaw in the research involves the CuPerFuzzer system. The paper points out that it randomly generates attack patterns. This yields the possibility that a less-likely lethal attack pattern(s) could not be generated by the system at all, and therefore not be exposed to the security community.

This work is extremely relevant today. The paper states that the Android operating system is constantly being developed and with each new update, Android permission mechanisms become more and more convoluted and therefore harder to understand, debug, and maintain. There are billions of Android users with billions of Android devices, all able to be exploited by some overlooked bug in some part of the firmware. Research like this is invaluable to the Android security community and therefore the Android users of the world. If issues such as the ones documented by the researchers of this paper were not brought to light, the security of billions of users is threatened.