Detecting the malicious broadcast receivers

December 6 2021, by David Bradley

Credit: Pixabay/CC0 Public Domain

How might we enhance the detection of malware on the Android operating system commonly used to run mobile phones and tablets? Research published in the *International Journal of Information Privacy, Security and Integrity* looks to the concept of broadcaster receivers as one possible answer to that question.

Halil Bisgin of the University of Michigan-Flint, in Flint, Rachael

Havens of AVL Test Systems Inc., in Plymouth, Michigan, Vincent Nwobodo of the Financial Industry Regulatory Authority, in Rockville, Maryland, U.S., and Fadi Mohsen of the University of Groningen in The Netherlands, explain that the Android operating system has a large share of the mobile market and as such is a target for malware creators and other third parties who would manipulate the system for personal gain.

There are numerous malware detection methods employed on the Android system that monitor permission requests to the AndroidManifest.xml file. However, one aspect of the workings of malicious apps that has not been considered in detail is the exploitation of the Android broadcast receivers (ABR). ABRs are used heavily by malware and might well correlate with permissions granted to such unwanted apps. Monitoring access to ABRs could improve the accuracy of malware detection without needing to use disproportionate amounts of computer resources in the device as may well be the case with other malware detection approaches.

Each year there are billions of instances of mobile apps installed on devices around the globe. They represent a vast market and business opportunity for legitimate companies but also for the criminal world. The amount of malware increases year by year and as with every aspect of security involves security companies always playing catch-up with the creators of malware.

The team explains that malware detection based on the behavior of software on a device is very effective but uses a lot of the device's resources. In contrast, signature-based solutions are light on resource usage but do not necessarily detect all malware. The team's focus has been on the component that lets apps register to listen to system events such as when a text message is received, calls are made, etc. This component, the team says, is vital in detecting malicious behavior in an app. The team explains that correlation values suggest that malware

shows slightly stronger ties between the actions it registers to listen to and the permissions it requests and this characteristic can be exploited to reveal the presence of malware.

More information: Halil Bisgin et al, Enhancing malware detection in Android application by incorporating broadcast receivers, *International Journal of Information Privacy, Security and Integrity* (2021). DOI: 10.1504/IJIPSI.2021.119168