New malware detection for Android at the source code level

23 July 2021, by David Bradley

Credit: Unsplash/CC0 Public Domain

There are numerous malware detection and antivirus apps for mobile devices running the Android operating system. However, a team in China introduces a new approach that can detect malicious activity at the source code level. They provide details in the International Journal of Information and Computer Security.

Junaid Akram, Majid Mumtaz, Gul Jabeen, and Ping Luo of The Key State Laboratory of Information Security at Tsinghua University, explain how their approach is not only scalable but offers self-optimisation of the signature set as it detects malicious apps by reading their source code. The team has developed a prototype of their software, DroidMD. They have tested it against almost 30000 applications of which 3,670 are already identified as malware. It is reliable because it analyzes only the code and has a high detection accuracy of 95.5%. The team points out that one of the unique characteristics of their software is that it can detect malware that is a clone or "near-miss" of known viruses and malware. Conventional antivirus and malware detection often fails to detect such malware where the software signature may well be only marginally different from the original virus.

Given that there are millions of users downloading thousands of apps every day, it is imperative that an effective and reliable approach to controlling malware be found to slow the assimilation of devices into bot nets and other malicious networks and reduce the risk of user data and privacy being compromised by malware.

"In our future work, we will make DroidMD more resilient for minimizing the obfuscation and improving its run time. Meanwhile, we will extend it for other programming languages to detect malware or malicious code fragments from source code to overcome security threats," the team writes.

More information: Junaid Akram et al, DroidMD: an efficient and scalable Android malware detection approach at source code level, *International Journal of Information and Computer Security* (2021). DOI: 10.1504/IJICS.2021.116310

Provided by Inderscience