Root exploit detection and features optimization: Mobile device and blockchain based medical data management

Ahmad Firdaus[a]; Nor Badrul Anuar[b]; Mohd Faizal Ab Razak[ab]; Ibrahim Abaker Targio Hashem[c]; Syafiq Bachok[ab]; Arun Kumar Sangaiah[d]

[a] Faculty of Computer Systems and Software EngineeringUniversiti Malaysia PahangKuantanMalaysia

[b] Department of Computer System and Technology, Faculty of Computer Science and Information TechnologyUniversity of MalayaKuala LumpurMalaysia

[c] School of Computing & ITTaylor's UniversitySubang JayaMalaysia

[d] School of Computing Science and EngineeringVellore Institute of TechnologyVelloreIndia

ABSTRACT

The increasing demand for Android mobile devices and blockchain has motivated malware creators to develop mobile malware to compromise the blockchain. Although the blockchain is secure, attackers have managed to gain access into the blockchain as legal users, thereby comprising important and crucial information. Examples of mobile malware include root exploit, botnets, and Trojans and root exploit is one of the most dangerous malware. It compromises the operating system kernel in order to gain root privileges which are then used by attackers to bypass the security mechanisms, to gain complete control of the operating system, to install other possible types of malware to the devices, and finally, to steal victims' private keys linked to the blockchain. For the purpose of maximizing the security of the blockchain-based medical data management (BMDM), it is crucial to investigate the novel features and approaches contained in root exploit malware. This study proposes to use the bio-inspired method of practical swarm optimization (PSO) which automatically select the exclusive features that contain the novel android debug bridge (ADB). This study also adopts boosting (adaboost, realadaboost, logitboost, and multiboost) to enhance the machine learning prediction that detects unknown root exploit, and scrutinized three categories of features including (1) system command, (2) directory path and (3) code-based. The evaluation gathered from this study suggests a marked accuracy value of 93% with Logitboost in the simulation. Logitboost also helped to predicted all the root exploit samples in our developed system, the root exploit detection system (RODS).

KEYWORDS:

Blockchain; Root exploit; Static analysis; Android; Machine learning