World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:11, No:05, 2017

Malware Detection in Mobile Devices by Analyzing Sequences of System Calls

Authors : Jorge Maestre Vidal, Ana Lucila Sandoval Orozco, Luis Javier García Villalba

Abstract : With the increase in popularity of mobile devices, new and varied forms of malware have emerged. Consequently, the organizations for cyberdefense have echoed the need to deploy more effective defensive schemes adapted to the challenges posed by these recent monitoring environments. In order to contribute to their development, this paper presents a malware detection strategy for mobile devices based on sequence alignment algorithms. Unlike the previous proposals, only the system calls performed during the startup of applications are studied. In this way, it is possible to efficiently study in depth, the sequences of system calls executed by the applications just downloaded from app stores, and initialize them in a secure and isolated environment. As demonstrated in the performed experimentation, most of the analyzed malicious activities were successfully identified in their boot processes.

Keywords : android, information security, intrusion detection systems, malware, mobile devices
Conference Title : ICIT 2017 : International Conference on Information Technology
Conference Location : Paris, France
Conference Dates : May 18-19, 2017