DAIDS: An Architecture for Modular Mobile IDS

Title	DAIDS: An Architecture for Modular Mobile IDS
Publication Type	Conference Paper
Year of Publication	2014
Authors	Salman, A., Elhajj, I.H., Chehab, A., Kayssi, A.
Conference Name	Advanced Information Networking and Applications Workshops (WAINA), 2014 28th International Conference on
Date Published	May
Keywords	Android (operating system), Android platform, Androids, anomaly detection, behavior analysis, behavior profiling, DAIDS, Databases, detection algorithms, Detectors, dynamic analysis, Humanoid robots, Intrusion detection, intrusion detection system, malicious behavior, Malware, mobile computing, mobile devices, mobile radio, modular mobile IDS, Monitoring, North America, profile applications, security of data, telecom operator, third party mobile applications

Abstract

The popularity of mobile devices and the enormous number of third party mobile applications in the market have naturally lead to several vulnerabilities being identified and abused. This is coupled with the immaturity of intrusion detection system (IDS) technology targeting mobile devices. In this paper we propose a modular host-based IDS framework for mobile devices that uses behavior analysis to profile applications on the Android platform. Anomaly detection can then be used to categorize malicious behavior and alert users. The proposed system accommodates different detection algorithms, and is being tested at a major telecom operator in North America. This paper highlights the architecture, findings, and lessons learned.

DOI	10.1109/WAINA.2014.54
Citation Key	6844659

Android (operating system) Android platform Androids Anomaly Detection behavior analysis behavior profiling DAIDS Databases detection algorithms Detectors dynamic analysis Humanoid robots Intrusion Detection intrusion detection system malicious behavior malware mobile computing mobile devices mobile radio modular mobile IDS Monitoring North America profile applications security of data telecom operator third party mobile applications