Arab J Sci Eng
DOI 10.1007/s13369-016-2400-3

REVIEW ARTICLE - COMPUTER ENGINEERING AND COMPUTER SCIENCE

Cloud-Based Intrusion Detection and Response System: Open Research Issues, and Solutions

Zakira Inayat[1,2] · Abdullah Gani[1] · Nor Badrul Anuar[1] · Shahid Anwar[3] · Muhammad Khurram Khan[4]

Received: 1 August 2016 / Accepted: 13 December 2016

Abstract Mobile cloud computing (MCC) allows smart mobile devices (SMD) to access the cloud resources in order to offload data from smartphones and to acquire computational services for application processing. A distinctive factor in accessing cloud resources is the communication link. However, the communication links between SMD and cloud resources are weak, which allows intruders to perform malicious activities by exploiting their vulnerabilities. This makes security a key challenge in the MCC environment. Several intrusion detection and response systems (IDRSs) are adapted to address the exploitation of vulnerabilities that affect smartphones, communication links between cloud resources and smartphones, as well as cloud resources. In this article, we discuss the cloud-based IDRS in the context of SMD and cloud resources in the MCC infrastructure. The stringent security requirements are provided as open issues along with possible solutions. The article aims at providing motivations for researchers, academicians, security administrators, and cloud service providers to discover mechanisms, frameworks, standards, and protocols to address the challenges faced by cloud-based IDRS for SMD.

✉ Zakira Inayat
Zakirainayat@uetpeshawar.edu.pk

✉ Abdullah Gani
abdullah@um.edu.my

[1] Center for Mobile Cloud Computing Research (C4MCCR), Faculty of Computer Science and Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia

[2] Department of Computer Science, University of Engineering and Technology Peshawar, Peshawar 2500, Pakistan

[3] Faculty of Computer Systems and Software Engineering, Universiti Malaysia Pahang, 26300 Gambang, Malaysia

[4] Center of Excellence in Information Assurance (CoEIA), King Saud University, Riyadh, Saudi Arabia

Published online: 10 January 2017

Keywords Intrusion · Security · Intrusion response system · Cloud-based IDRS · Mobile cloud computing

1 Introduction

Mobile cloud computing (MCC) has gained popularity in the last few years among smartphone users with its rapid adaptability. In fact, according to a recent study by ABI research [1], the number of businesses accessing cloud-based services through smart mobile devices (SMD) is expected to exceed 240 million by 2017, which is predicted to push MCC revenues to $5.2 billion. Similarly, a recent report from Juniper research forecasts that more than 3.6 billion MCC subscribers are expected to use cloud services by 2018, rising from an estimated 2.4 billion in 2013 [2]. The core concept behind MCC is to improve the performance of SMD by merging three Internet-related technologies, namely mobile Internet, mobile computing, and cloud computing [3]. Although mobile computing facilitates the users to use a tool continuously regardless of their moment, SMD faces its inherent problem such as limited energy, resource deficiency, and low connectivity. Therefore, the concept of adopting MCC is to allow resource-constrained devices to use data storage and data processing of powerful and centralized computational cloud to address the inherent problem of mobile computing [4]. The technology enables smart devices (e.g., tablet PC and smartphone) to flexibly utilize cloud resources on-demand to take advantage of services, such as social networks, email, and search engines. The cloud resources on-demand concept has attracted smartphone users to utilize various CC services, namely "infrastructure, platform, and software" as-a-service ("IaaS, PaaS, and SaaS") at low cost [5]. These service models provide reliable, scalable, and reconfigurable aggregation