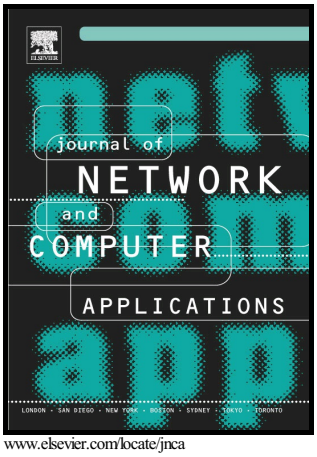
Towards Port-Knocking Authentication Methods for Mobile Cloud Computing

Suleman Khan, Muhammad Shiraz, Laleh Boroumand, Abdullah Gani, Muhammad Khurram Khan



www.elsevier.com/locate/jnca

PII: S1084-8045(17)30281-3
DOI: http://dx.doi.org/10.1016/j.jnca.2017.08.018
Reference: YJNCA1964

To appear in: *Journal of Network and Computer Applications*

Received date: 27 February 2017
Revised date: 1 August 2017
Accepted date: 25 August 2017

Cite this article as: Suleman Khan, Muhammad Shiraz, Laleh Boroumand, Abdullah Gani and Muhammad Khurram Khan, Towards Port-Knocking Authentication Methods for Mobile Cloud Computing, *Journal of Network and Computer Applications,* http://dx.doi.org/10.1016/j.jnca.2017.08.018

Towards Port-Knocking Authentication Methods for Mobile Cloud Computing

Suleman Khan[a*], Muhammad Shiraz[b], Laleh Boroumand[c], Abdullah Gani[c], Muhammad Khurram Khan[d]

[a]School of Information Technology, Monash University Malaysia

[b]Federal Urdu University of Arts, Science & Technology. Author, Islamabad, Pakistan

[c]Center for Mobile Cloud Computing Research (C4MCCR), University of Malaya, Kuala Lumpur, Malaysia

[d]King Saud University, KSA.

[*]**Corresponding author:** (Suleman khan), (suleman.khan@monash.edu)

Abstract

Mobile cloud computing (MCC) is an increasingly popular research topic, partly due to the widespread adoption of mobile devices and cloud services among individual and organizational users. Security and privacy of data-at-rest and data-in-transit are two of several key issues that need to be addressed. Traditional authentication models employ third-party security monitoring mechanisms, which generally require complicated and resource-intensive mechanisms for ensuring security measures. These mechanisms are not adaptive for MCC deployment; thus, it requires lightweight authentication methods. This paper reviews existing port-knocking authentication methods by analyzing the mechanism and classifying the methods into a thematic taxonomy. Current port-knocking authentication methods are compared based on static or dynamic knocked sequences, which tend to solve the Network Address Translation (NAT) knock and Denial of Service (DoS) knock attacks. Finally, we discuss the issues and challenges in implementing port-knocking for MCC.

Index Terms—Mobile Cloud Computing, Port-Knocking, Authentication, Denial-of-Services

1 INTRODUCTION

Recent advances in mobile computing technologies have resulted in significant increases in storage capacity, processing capacity, etc. Similarly, wireless network technologies are becoming much faster with lower latency (e.g. LTE) and are deployed in an increasing array of applications [1]. In recent years, smart mobile devices (SMDs) have replaced a number of handheld devices in all-in-one computing and communication devices. It is reported that an average of 1,600 new applications is uploaded to the app stores daily [2], and an average SMD user downloads 37 applications per year [3]. These applications range from web browsing, communication, personal health tracker, mobile banking, and social network to entertainment [4], [5], [6], [7]. However, despite recent advancements, hardware limitations in terms of storage capacity, processor power, battery life, etc necessitate the need for off-device storage and computation offloading.

Cloud computing offers utility computing [8] with resource flexibility, agility, and scalability [9] for mitigating resource constraints on client devices, including SMDs. MCC employs off-device storage and computational offloading to cloud server nodes for alleviating the resource constraints in SMDs. However, a number of issues are associated with accessing the services and resources of computational clouds on a demand basis, such as a lightweight application execution framework, scalability of services and resources, privacy of data stored in cloud data centers and security of data communication in the mobile cloud computing and similar environments such as Internet-of-Things [10, 104, 105]. Security is challenging in mobile cloud computing because of its mobile nature, wireless access medium, heterogeneity of computing and communication environment, and the variety of client devices (and specifications) [11,12]. Currently, authentication is employed as a primary state of security to guarantee the sole authorized user