Accepted Manuscript

A secure and cost-efficient offloading policy for mobile cloud computing against timing attacks

Tianhui Meng, Katinka Wolter, Huaming Wu, Qiushi Wang

PII: S1574-1192(16)30430-8
DOI: https://doi.org/10.1016/j.pmcj.2018.01.007
Reference: PMCJ 919

To appear in: Pervasive and Mobile Computing

Received date: 11 December 2016
Revised date: 22 September 2017
Accepted date: 30 January 2018

Please cite this article as: T. Meng, K. Wolter, H. Wu, Q. Wang, A secure and cost-efficient offloading policy for mobile cloud computing against timing attacks, Pervasive and Mobile Computing (2018), https://doi.org/10.1016/j.pmcj.2018.01.007

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.
A Secure and Cost-efficient Offloading Policy for Mobile Cloud Computing against Timing Attacks

Tianhui Meng¹, Katinka Wolter¹, Huaming Wu² and Qiushi Wang¹

¹ Department of Mathematics and Computer Science, Freie Universität Berlin, Takustr.9, 14195 Berlin, Germany
² Center for Applied Mathematics, Tianjin University, 300072 Tianjin, China

Abstract

In Mobile Cloud Computing (MCC), offloading is a popular technique proposed to augment the capabilities of mobile systems by mitigating complex computation to resourceful cloud servers. While this may be beneficial from the performance and energy perspective, it certainly exhibits new challenges in terms of security due to increased data transmission over networks with potentially unknown threats. Among possible security issues are timing attacks which are not prevented by traditional cryptographic security. Timing attacks belong to side channel attacks in which the attacker attempts to compromise a system by analyzing the time it takes to respond to various queries. Offloading is particularly vulnerable to timing attacks because it often needs many times sending/receiving. This paper considers the specific threat of timing attacks against MCC systems. We present and evaluate a secure and cost-efficient offloading scheme which is the combination of regular rekeying and random padding. In order to proceed to a quantitative treatment, a hybrid Continuous-time Markov chain (CTMC) and queueing model is put forward, and the tradeoff analysis of the security and performance attributes is carried out. We propose security metrics which system architects need to make informed tradeoff decisions involving system security. The numerical results based on experimental data show that the security performance tradeoff is improved through the proposed scheme. Further, we found that the variance of random delays is the primary influencing factor to the mitigation effectiveness of random padding and that the extra number of measurements an attacker has to make grows linearly with the standard deviation of the random delays.

Keywords: Mobile cloud computing, security, computation offloading, side-channel attack.

1. Introduction

Mobile devices have become mandatory items in today’s world. They are no longer used only for voice communication and short message service (SMS); instead, they are used for watching videos, gaming, recording health data and social networking. While the last decades witness great advances in hardware technology, new applications have also become much more demanding. Hence, mobile devices still face the restrictions in resources, such as battery life and network bandwidth. On the other hand, cloud servers are readily to be used by the mobile systems.

Mobile cloud offloading is a promising solution to augment the mobile systems’ capabilities by migrating computation via WiFi or 3G/LTE to more resourceful servers (i.e., Windows Azure and Amazon EC2 web services)[1]. This is different from the traditional client-server architecture, where a thin client always migrates computation to a server [2]. In mobile cloud offloading, applications are divided into those parts that can be offloaded and those that must be executed on the mobile device, such as the user interface [3].

Offloading is an important technique in mobile cloud computing (MCC) [4]. Due to the relatively low battery capacity of mobile devices as well as fragile mobile networks, a significant amount of research has been performed
دریافت فوری متن کامل مقاله

امکان دانلود نسخه تمام متن مقالات انگلیسی
امکان دانلود نسخه ترجمه شده مقالات
پذیرش سفارش ترجمه تخصصی
امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
امکان دانلود رایگان ۲ صفحه اول هر مقاله
امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
دانلود فوری مقاله پس از پرداخت آنلاین
پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات