Computer Networks 65 (2014) 99–110

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Consolidated Identity Management System for secure mobile cloud computing

Issa Khalil [a,*], Abdallah Khreishah [b], Muhammad Azeem [c]

[a] Qatar Computing Research Institute (QCRI), Qatar Foundation, Doha, Qatar
[b] Newark College of Engineering, New Jersey Institute of Technology, University Heights, Newark, NJ 07102, United States
[c] College of Information Technology, United Arab Emirate University, Al Ain, United Arab Emirates

ARTICLE INFO

Article history:
Received 29 August 2013
Received in revised form 26 January 2014
Accepted 19 March 2014
Available online 25 March 2014

Keywords:
Cloud computing security
Privacy
Mobile clients
Identity Management Systems
Security attacks

ABSTRACT

Security issues in cloud computing are shown to be the biggest obstacle that could lower the wide benefits of the cloud systems. This obstacle may be strengthened when cloud services are accessed by mobile devices. Mobile devices could be easily lost or stolen and hence, they are easy to compromise. Additionally, mobile users tend to store access credentials, passwords and other Personal Identifiable Information (PII) in an improperly protected way. We conduct a survey and found that more than 66% of the surveyed users store PIIs in unprotected text files, cookies, or applications. To strengthen the legitimate access process over the clouds and to facilitate authentication and authorization with multiple cloud service providers, third-party Identity Management Systems (IDMs) have been proposed and implemented. In this paper, we discuss the limitations of the state-of-the-art cloud IDMs with respect to mobile clients. Specifically, we show that the current IDMs are vulnerable to three attacks, namely – IDM server compromise, mobile device compromise, and network traffic interception. Most importantly, we propose and validate a new IDM architecture dubbed Consolidated IDM (CIDM) that countermeasures these attacks. We conduct experiments to evaluate the performance and the security guarantees of CIDM and compare them with those of current IDM systems. Our experiments show that CIDM provides its clients with better security guarantees and that it has less energy and communication overhead compared to the current IDM systems.

1. Introduction

In the early age of computers, computational tasks were performed on mainframe computers. Large companies such as IBM, Amdahl and Hitachi owned these mainframe computers. These companies provided computational services to customers where it takes hours, sometimes, even days, in order to get the results. Cloud computing introduces similar concepts by utilizing hardware pooling and virtualization concepts to offer computational services over the Internet and other private/public networks [39,40]. It, thus, represents one of the contemporary key technological advances that enable the delivery of computing resources in a way similar to the delivery of utility-based services. Mobility is also considered another important contemporary key technological step that shifts the trend in client devices from PCs to smartphones, laptops, tablets, etc. [1]. There is a dramatic increase in the number of users with wireless smartphone devices and in the number of public access points used to connect to the cloud [2–4,38]. Mobile devices are becoming more sophisticated and soon will replace PCs to

* Corresponding author. Tel.: +974 77495648.
E-mail addresses: ikhalil@qf.org.qa (I. Khalil), abdallah@njit.edu (A. Khreishah), Muhammad.azeem@uaeu.ac.ae (M. Azeem).

http://dx.doi.org/10.1016/j.comnet.2014.03.015
1389-1286/

perform traditional and cloud computations as they provide the convenience of anywhere, anytime access. According to Digital buzz, the 2013 mobile growth statistics show that 91% of all people on earth have a mobile phone, 50% of mobile phone users, use mobile as their primary Internet source, and 72% of tablet owners purchase online from their tablets each year [5]. This increase is also contributed to the fact that mobile computing has made business easier and less costly by eliminating the need for on-site information systems [6].

However, the convenience offered by mobile devices is accompanied by many security challenges and introduces wide range of vulnerabilities, especially in the area of access control and identity management. Recent figures show that mobile malicious code has advanced greatly [7] and that the number of incidences of malware injections, especially for credential theft, is on rise [8]. Most enterprises are aware of the security challenges and operational vulnerabilities that could be introduced by allowing access to mobile clients. At the same time, corporate security officers realize that preventing users from using their mobile devices is a losing battle against convenience. Unfortunately, mobile software developers (application/system software) do not consider mobility threats during the software development life cycle and this is why, organizations and individuals are on their own to secure their information. Users who are not aware of the security threats introduced by mobile devices are evidently at risk.

Unauthorized access is one of the major security challenges introduced by mobility, which signifies a serious threat to clouds. Mobile devices increase the probability of unauthorized access due to many different facts. First, mobile devices use wireless communication which is easier to intercept and analyze compared to the wired counterpart. Second, it is relatively easy to lose or steal a mobile device, and hence it is easy to capture and compromise. Third, many mobile users tend to store access credentials, passwords, Personal Identifiable Information (PII), and other valuable digital assets in an improperly protected way and hence, easy to collect. We conduct a survey (Section 4.2) and found that more than 66% of the surveyed users store PIIs either in text files, cookies, or applications in an easily accessible format. Fourth, as mobile devices roam from one network to another, they may connect to improperly protected networks and access remote untrusted sites that could disseminate malware. Combining all these facts with the proliferation of mobile devices make them attractive targets to obtain unauthorized access. Therefore, it is an urgent priority to develop and implement reliable, secure and efficient access management systems that cope with the mobility challenges.

Many techniques have been developed to control the unauthorized access to cloud services and data. One of the most widely used security techniques in that direction is the control of user access through proper access management systems. However, proper access management systems rely on proper Identity Management Systems (IDMs) for identity generation, authentication, and authorization. IDMs are mainly designed to maintain the integrity of cyber identities throughout their life cycle to make them and their related data (e.g., authentication and authorization results) available to different services in a secure, reliable and privacy-protected manner. IDMs are also responsible for identity management tasks such as allowing an identity's subject to establish links between her various identities. These links can further be used for different services, across geographical, temporal and organizational borders. This IDM feature has been called an identity federation [9]. The federation refers to the group of organizations that are responsible for establishing trust among them to cooperate safely in business. The particular type of user's authentication such as "Single Sign-On" is an example of federated identity systems [10]. However, Single Sign-On service introduces vulnerabilities that can lead to serious attacks if user's identity has been compromised. With one time successful sign-in, the illegitimate user will not be verified again, resulting in higher level of information leakage.

Fig. 1 represents a generic architecture of current IDMs. The architecture consists of three players – the client, the cloud service provider (CSP), and the IDM provider. The steps involved in acquiring access to a CSP are: (1) The user login to the IDM provider with her pre-assigned username and password, (2) the user requests to access cloud application/data from the CSP, (3) the CSP asks for a token, (4) the user requests a token from the IDM provider, (5) the IDM provider generates a token and sends it to both the user and the CSP, (6) the user forwards the token received from the IDM to the CSP, (7) the CSP compares the tokens received from the user and the IDM provider, and (8) on successful comparison, the cloud allows the user to access the requested data or application.

Researchers and practitioners have implemented many flavors of IDMs. However, the security and privacy issues introduced when traditional IDMs are used to serve mobile clients have not been sufficiently addressed. Our analysis and experiments show that the current IDMs do not provide adequate security guarantees for mobile cloud computing. In this paper, we initially discuss the security vulnerabilities and the privacy issues of the current traditional IDMs, especially in mobile client environments. Then, we propose and evaluate a new IDM architecture dubbed *Consolidated IDM* (*CIDM*) that addresses the coupled challenges of mobility and identity management in mobile cloud computing. In this work, we assume an attack model in which the attacker's goal is to gain unauthorized access on behalf of a legitimate user. Therefore, we do not consider DoS or DDoS attacks in which the attacker tries to prevent a legitimate user from being able to prove its identity.

Up to our knowledge, we are the first to study and address the security and privacy threats introduced when using traditional IDMs to serve mobile cloud clients. Our contributions can be summarized as follows:

- Introduce and investigate the impact of three threats against current IDMs, namely – IDM server compromise, mobile device compromise, and network traffic interception. We explain each threat and show how current IDMs are vulnerable to that threat.
- Conduct extensive experiments and surveys to motivate the need for developing and implementing reliable, secure and efficient access management systems that cope with the mobility challenges.