Chapter 97
Session Hijacking Over Cloud Environment:
A Literature Survey

Thangavel M.
Thiagarajar College of Engineering, India

Pandiselvi K.
Thiagarajar College of Engineering, India

Sindhuja R.
Thiagarajar College of Engineering, India

ABSTRACT

Cloud computing is a technology that offers an enterprise model to provide resources made available to the client and network access to a shared pool of configurable computing resources and pay-for-peruse basis. Generally, a session is said to be the collective information of an ongoing transaction. This package is typically stored on the server as a temporary file and labeled with an ID, usually consisting of a random number, time and date the session was initiated. That session ID is sent to the client with the first response, and then presented back to the server with each subsequent request. This permits the server to access the stored data appropriate to that session. That, in turn allows each transaction to be logically related to the previous one. Session hijacking is the common problem that is experienced in the cloud environment in which the session id is gained and information is gathered using the session ID compromising its security. This chapter covers session hijacking and the countermeasures to prevent session hijacking.

INTRODUCTION

Cloud Computing is considered as a small or medium-sized data centers with computational power, as this technology equally rely on virtualization for management with large data or information processing requirements and it includes the combination of Software as a Service (SaaS) and utility computing.

DOI: 10.4018/978-1-5225-8176-5.ch097

Due to the innovative hacking techniques the risk in security has increased to a greater extent in the cloud environment. To safeguard security several security management and measures are followed such as Information Technology Infrastructure Library (ITIL) guidelines, ISO/IEC 27001/27002 standards and Open Virtualization Format (OVF) standards that focuses on security principles (Challa 2012). Despite having such measures researchers cannot promise cloud security is the dark side of this picture. Some of the hacking techniques are Heartbleed, ShellShock, Poodle, Rosetta Flash, Hacking PayPal Accounts with 1 Click, Google Two-Factor Authentication Bypass etc. There are two explanations in reality; 1) weaknesses in the security that is currently adopted all over the globe, 2) the innovative hacking techniques that are quickly becoming extraordinarily intelligent, sophisticated and hard to detect.

Clients are the user of the cloud where they store their valuable information and the communication between the clients are taken place. If the client can access the application from any location, then the privacy of the client could be compromised. Authentication techniques are used for securing privacy. While providing authentication the client should be aware of the assaultsin cloud computing. The authentication attacks included in cloud computing are Eavesdropping, Man-in-the-Middle Attacks, Cookie Poisoning, Replay Attack, Session Hijacking, Shoulder Surfing, Cloud Malware Injection, Password Discovery Attacks, Reflection Attack, Customer Fraud Attack, Denial-of service Attack, Insider Attack, Wrapping Attack, Flooding Attack, Browser Attack, Impersonating Attack, SSL Attacks, Guessing Attack, Brute Force Attack, Dictionary Attack, Video Recording Attack, and Stolen Verifier Attack (Misbahuddin 2013).

The authentication attacks that are listed above are explained one after the other. Eavesdropping is the process of listening or monitoring the established communication between two authorized clients by which information are gathered. In Man in the middle attack, hacker impersonates as the authorized client and gains the information that is communicated between authorized users. Cookie poisoning is done where the attacker gains the access permission by modifying the credentials information of the authorized client that is stored in the cookies (Khare 2015). Replay Attack is an attack where the communication between the authorized users is intruded by the attacker, the message from the sender is received then modified by the attacker and it is modified and sent back to the receiver. Shoulder Surfing is to gain the sensitive information by observing the clients entry of data via keyboard by the attacker. Cloud Malware Injection aims to inject a malicious service or virtual machine instance, which appears as the valid service instance running on the cloud platform. Password Discovery is an attack where various techniques are involved to gain the password of the authorized client. Reflection Attack is processed on mutual authentication schemes in which the attacker tricks the victim by revealing the secret to its own challenge. Customer Fraud Attack is where the client deliberately compromises its authentication token. Denial-of-service is harassing in which the hacker sends the request to the target machines by which the legitimate clients request is not responded (Zunnurhain 2012; Dacosta 2012). Among these attacks the most powerful is the Session hijacking attack as the legitimate user is unaware of this attack that compromises his privacy and data security. In this chapter, author will discuss the methodology of session hijacking, its major risks and the countermeasures to prevent it from occurring in the cloud environment.

SESSION HIJACKING

Session hijacking is the process of knowing the session ID (SID) of an active client, so that his account can be impersonated or hijacked. The application tries to identify him based on his cookie value, which