Cloud Security Concerns and Solutions

Nguyen Ngoc Khiem and Nguyen Van Cuong

March 12, 2022

Cloud Security Concerns and Solutions

Nguyễn Ngọc Khiêm and Nguyễn Văn Cường

CyberSecurity Department
University of Science and Technology of Hanoi
khiemnn.ba9028@st.usth.edu.vn
cuongnv.ba9011@st.usth.edu.vn

Abstract. Many systems only require a simple user-generated password to gain access, while others are more robust. Think about the needs of your application, what data breach laws might apply to you, and try to mitigate your risk through good security practices. SNMP, encryption, firewall, antivirus, and strong passwords are required to effectively monitor and protect any cloud platform from attacks. Human security neglect is arguably the biggest contributor to cloud and network encroachment. According to the Online Trust Alliance, 90% of data breaches could have been prevented if companies had better internal controls. The Online Trust Alliance otalliance.org provides more information on data breach protection. Insufficient password selection, stolen laptops, sharing the same password on different websites, and turning computers on and unlocking them to facilitate access for physical use are some of the top threats.

Keywords: Layers of Security, Password, Authentication, Operating System, Encryption, Problems.

1 Introduction

Managing cloud security access may be a difficult issue. Hundreds of people accessing systems from all over the world and using a variety of devices might need a lot of thinking and preparation.

Having several layers of possible security concerns makes hackers of all sorts easy targets; the weakest link will break and cause problems; if you have a weak link, the chain will break (see Fig.1)

Fig. 1. Weak link will break chain.

Having many levels of possible security concerns makes you a primary target for all kinds of illegal activities.

We are increasingly living in a dispersed world with numerous gadgets vying for quick and safe access to information. Virtual servers are hosted by multinational corporations all over the world. Employees and users are in one area of the globe, but the systems they utilize are in another. We now have "moving targets" to safeguard as servers are relocated from one data center to another based on the time of day or an increase in demand from a different region of the world.

2 Levels of Security need to concern

The device layer is the initial and most susceptible layer. We begin with the user and work our way through each point where security must be considered. The primary user interface device is usually the user layer. To access the cloud system, most people utilize a personal computer, tablet, or mobile phone. Internet Explorer, Chrome, Firefox, Opera, and Safari are the most common online browsers on most devices. Each phone vendor may have their own browser, which may or may not meet with your organization's security standards. A browser that functions great on one phone model may pose security concerns on another.

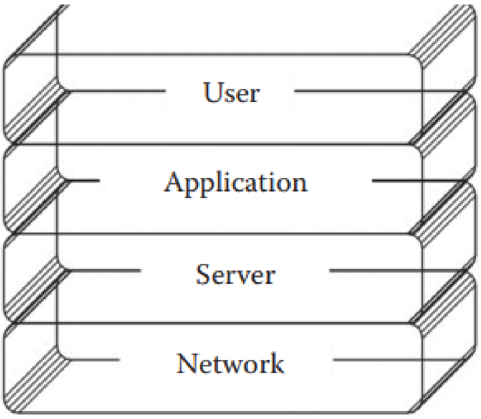

Fig. 2. Layers of Security

2.1 User’s devices layer

The user interface (UI) includes everything a user may interact with when browsing an application or website, including the menu bar and toolbar, as well as windows, buttons, and other controls.

Failure to secure the UI enables hackers simple access and allows them to penetrate web browsers to alter web pages, transaction content, or insert new transactions entirely surreptitiously. This form of content manipulation is known as a man-in-the-browser attack and can cause devastating consequences for users and companies alike, resulting in financial loss and reputational damage.

Hackers with unlimited access to the UI can also modify communication between two parties, intercepting all pertinent messages and inserting their own for personal advantage. This type of eavesdropping is known as a man-in-the-middle assault, and it may be used to broker fraudulent agreements or steal important private information, causing economic loss and a damaged reputation.

To these attacks, organizations must ensure their UI is protected.

A "front end" user interface is required to access the cloud. The web browser serves as the front end for many cloud systems. When you connect to a browser-based application, you are in the cloud, using the resources of a server in a data center somewhere in the globe.

It is critical to have a front end that functions as a firewall against infiltration. The front-end check is essential for protecting the network and cloud servers before anyone has access.

2.2 Software layer

Software programmers have a wide range of programming languages to select from when creating cloud-based software. Most people choose lower-complexity programming languages because of their ability to interact with computer hardware and their high-speed processing; C program language is one of these languages.

Securing the application layer is a difficult mission. The programmer must avoid stack overflows, keep an eye out for code injection, and consider all of the various things a user or application on the user's machine may do.

The software engineers must be aware of any abuse of their permitted access and take steps to prevent unauthorized data access. Applications must be built to test for both legitimate and invalid requests. The programmer must constantly keep in mind the goal of preventing authorized users from executing illegal transactions.

The most efficiency ways to secure software layer is that make sure programmer test again and again their software under any attack situation to ensure that the application is safe.

2.3 Server Operating Systems

The majority of the Internet is powered by Linux and all of its variants, as well as the Microsoft Windows server and all of its variants. The host operating system (OS) is frequently forced by the application development platform chosen by the project manager, programmer, and administrator. When choosing on application development, numerous essential characteristics of server operating systems should be addressed. The cost of the software and hosting services might be a concern.

The most popular methods for protecting operating systems include the use of antivirus software and other endpoint protection measures, frequent OS patch updates, a firewall for monitoring network traffic, and the enforcement of safe access through least privileges and user restrictions.

In other hand, administrator also need to secure OS by physically way. One of the top ways to keep the operating system secured is to limit physical access to the server to a small number of people. Most hosting centers have video of each person entering and leaving. Some weigh a person going in and going out and weigh any equipment they bring with them. On exit, they check to make sure the weight is in line with what they left behind.

Fig. 3. Fingerprint Authentication Technology

Some server rooms use hand geometry while others use fingerprint technology. Otherwise, some use retinal eyes scanner and facial recognition.

Fig. 4. Facial recognition Technology

2.4 Hosting Networking

Securing Hosting services room is very important. You really do not want you server room get access by unauthorized person. A person with physical access may remove power and network cords, insert malicious drives, wiped server data, or take control the entire physical server. Many hosting businesses have secured server rack doors with high technology security layer, in order to access server room, only allowed person can get in. Most data center facilities are also monitored 24/7 powerful technology camera.

In addition to the server hardware, the network hardware should be protected also. Non-authorized workers should not have access to main switches, routers of secured systems. The most popular method of securing network hardware is setup that important network hardware in a secured area with protection methods such as security guard, camera and locked doors.

Another solution is managing the connections and only allowing request from authorized devices. Also, install good spyware and antivirus software or up to date the OS is great way to protecting network from within.

3 Improvement Security in All Layers

Improvement Security in All Layers is also very good way to secure your cloud. A server to back up all the data from your cloud to avoid server provider goes bankrupt and lost data.

4 Encryption and Managing Password

When a user connects to the cloud using a single machine, the keys for end-to-end encryption might be stored by a program on that system. With users having access to the cloud via numerous devices such as smartphones and tablet computers, it might be difficult to securely transfer these credentials between devices.

Two-Factor Authentication is a best way to secure user login information. Two-Factor Authentication (2FA) works by adding an additional layer of security to your online accounts. It requires an additional login credential – beyond just the username and password – to gain account access, and getting that second credential requires access to something that belongs to you (1). Google Authentication Google Authenticator is the application based on two-factor Authentication (2FA) that helps for identifying user identity and the confirmation on what a user claim to be and whether he actually is. Google Authenticator is used for two-step verification based on Time-based One Time Password (TOTP) and HMAC-based One Time Password (HOTP) for authenticating users. TOTP is an algorithm that computes a one-time password from a shared secret key and the current time. HTOP is an algorithm which uses HMAC algorithm to generate one-time password (2).

In other way, user can use a USB Token. A USB token is a physical device that is used to establish personal identity without use of a password to access a network. A USB token is used to prove the user’s identity electronically, thus enhancing digital security. It provides secure and strong authentication for network access (3).

5 Managing Server

Google, Microsoft, and Amazon have transitioned from discrete scattered server centers to large, expansive data centers. These data centers hold hundreds of servers, all of which are dedicated to cloud computing and the provision of Internet services to customers. The popularity of cloud-hosted data centers has enabled corporations and ordinary consumers to save both time and money.

Through an Internet connection, distributed cloud servers offer remote access to data from anywhere in the globe.

When selecting a hosting provider, it is critical to evaluate if you will be sharing resources with another website, obtaining a virtual machine on a computer, or obtaining a full server for your apps. When it comes to security, owning your own gear is definitely the best option.

References

1. How Does Two-Factor Authentication (2FA) Work? - Merchant Fraud Journal (https://www.merchantfraudjournal.com/two-factor-authentication-work/)
2. Google Authenticator and how it works? | by Tilak Lodha | Medium (https:// medium.com/@tilaklodha/google-authenticator-and-how-it-works-2933a4ece8c2)
3. What is a USB Token? - Definition from Techopedia (https://www.techopedia.com/definition/23943/usb-token)
4. Cloud Computing Security Foundations and Challenges – John R. Vacca