Cloud computer architecture, S&V (Security & Vulnerability)

Bhupesh Thakur, Ramandeep Singh, Sonika Mittal

Lovely Professional University
Jalandhar, Punjab, India

Lovely Professional University
Jalandhar, Punjab, India

Lovely Professional University
Jalandhar, Punjab, India

ABSTRACT

Cloud computing is getting popular and IT giants such as Google, Amazon, Microsoft, IBM have started their cloud computing infrastructure. However, current cloud implementations are often isolated from other cloud implementations. This paper gives an overview survey of current cloud computing architectures and S&V (security & vulnerabilities), discusses issues that current cloud computing implementations have and proposes a Service-Oriented Cloud Computing Architecture (SOCCA) so that clouds can interoperate with each other. Furthermore, the SOCCA also proposes high level designs to better support multi-tenancy feature of cloud computing**.**

Keywords: *Cloud computing, architecture, Security and vulnerability.*

1. Introduction

In recent years cloud computing has become a growing interest for organizations looking to reduce their IT costs by offloading infrastructure and software costs onto 3rd party organizations who offer software-as-a-service (Saas) (e.g. Google Apps [3]), platform-as-a-service (PaaS) (e.g. Google App Engine[2]), and infrastructure-as-a-service (IaaS) (e.g. Amazon EC2 [1]). However, due to the relative infancy of cloud based computing services, there exists uncertainty about the level of information security offered by these services. IaaS cloud services are largely reliant on virtualization technology, which is seen as providing all the security and process isolation a customer might want. While virtualization offers some potential security, there are drawbacks and complexities of which cloud providers and customers should be aware. This paper will summarize and critique a selection of recent literature in the area of cloud security, with a specific focus on virtualization security.

One of the bigger issues is the security part and one of the most important parts for a company that is thinking of moving services to the cloud. They need to know that their data is safe, both at the provider's site and during transmissions between the host and server. Furthermore, the authentication procedure must be very secure; the best encryption algorithms in the world will not protect the data if someone has figured out your password.

Since cloud computing is a quite new subject, most of the cloud providers have not yet tighten up their security and still use insecure or complicated login methods. The authentication part of cloud computing must be easy and flexible for the millions of user that it has, but at the same time be very secure to protect the data that it stored in the cloud. At the same time the encryption method used during transmissions must also be very secure and, since the cloud's vast amount of users, a fast algorithm that doesn't require much computer power and processing.

2. Cloud architecture

As previously defined cloud computing is referred to as the cash on delivery use the service and pay for the usage. Cloud computing is divided into following three client-server services:-

1. Software as a service (Saas): Application services delivered to the client.
2. Platform as a service (PaaS): Platform as a service is referred to as the pay as you go services. It's also service on demand.
3. Infrastructure as a service (Iaas): it's also same as the PaaS and Saas for pay as you use which includes storage, network and resources.

Cloud can be differentiated as follows into three different categories:

1. Public cloud: includes the cloud service which comes under the services where users are made to share the services bases on their usage and to some extend services are free.
2. Private cloud: it is refers to as the space provided over the network where special services and a private storage is provided as per the user requirements. No sharing is done in this type of cloud; it's like your own personal home no rent facility.

3. Hybrid cloud: it is refers to as the cloud service which includes involvement of moth public and private cloud services. Its usage depends on the demand or the requirement..

3. Risk factor in cloud

Following are the risk factors in cloud

1. Resource exhaustion
2. Customer isolation failure
3. Interception of data in transmission
4. Data leakage on upload/download , intra cloud
5. Distributed denial of service (DDOS)
6. Loss or comprise of encryption key
7. Network failure
8. Networking management
9. Modification of network traffic
10. Social engineering attack
11. Loss or compromise of security logs
12. Backups lost or stolen

4. Authentication problem

The most common login form used today, not only for cloud services, is to use static passwords. Many can agree that static password have a lot of security problems. Static passwords are often very easy to crack, since users prefer non-complex passwords. The users also rarely change their passwords or use the same password to access multiple services. Therefore, different cloud providers have lately started with *one time password* with *two-factor authentication.* The problem with their solutions is that it cost money, for the user or the provider, it can be complicated to use, or that the user have to carry a separate authentication device with him at all time.

One of the main concerns regarding cloud services is the security part, and is one large factor to why companies and customer hesitate to migrate their services into the cloud. At the same time, the security must be easy for the customers to understand and appeal to all kinds of people with different technical knowledge. And lastly, the security solutions should be very cheap or free of charge to implement, both for providers and customers, to attract more people to the cloud. So, in conclusion, for cloud services to grow even more, it needs a simple and cheap security solution.

4.1 Authentication

In general authentication is the act of creating or validating something (or someone) as authentic and claims made about the topic are true. This might engage proving the identity of a person, guarantee that a product is what it's wrapping and tagging claims to be, tracing the origins of a relic, or assuring that a computer program is a trusted one.

In computer networks and Internet or any web based services; authentication is usually done using the login password. Knowledge of the password is adopted to ensure that the user is authentic. Each user registers first or get registered by someone else and using an assigned or self-stated password. On each subsequent use, the user must know and use the previously declared password. The weakness of this system is that passwords can often be stolen, unintentionally revealed or forgotten.

There are a couple of possible authentication attacks:-

- *Eavesdropper attacks*: - Attacker gains information from an authentication exchange and restoring data, such as authentication key values may be used to authenticate.
- *Man-in-the-middle attacks:* - Where an attacker inserts himself in between the client and the verifier in an authentication process. The attacker attempts to authenticate by pretending as the client to the verifier and the verifier to the client.
- *Replay attacks:* - Where the attacker traces the data of a successful authentication and replays this information to get an untruly authentication to the verifier.
- *Verifier impersonation attacks:* - Where the attacker pretends to be the verifier to the customer to obtain authentication keys or data that may be used to authenticate fallaciously to the verifier.
- *Session hijacking attacks*: - Where the attacker hijacks a session following successful authentication by stealing session key or session cookie.
- *Verifier impersonation attacks, Customer fraud attacks , Key logger attacks etc.*

Following are the authentication or encryption standards being used by the cloud providers:-

1. *AES(advanced encryption standard)*
2. *RC4*
3. *Two-factor authentication with OTP*
4. One time passwords
5. Time-based OTPs
6. Counter-synchronized OTPs

Of the above defined authentication standards two-factor authentication has been the most reliable method used so far. In two factor authentication a user has to supply two terms in order to authenticate him. The user 24 must have *something you know* used together with *something you have*. For example, when a user logins to a web page he writes his static password (*something you know*), and a series of random numbers from an authentication device (*something you have*). [5]

The most common implementation of this is when a person withdraws money from an ATM. The user has a bank card that he puts in to the machine, and a PIN code must then be entered before withdrawal is possible. [5]

In most online implementations over the Internet, the static password is a PIN code that you enter into an authenticating device, which will then generate a OTP. The only thing sent over the Internet to authenticate the user is the OTP, which will be of no use of a sniffing attacker.

4.2 Encryption standard used

[14]AES (Advanced Encryption Standard) and RC4 are two encryption ciphers that are used in a variety of applications. A common example where you would see both ciphers employed is in wireless routers. Although you would not explicitly see RC4 as an encryption mechanism there, both WEP and TKIP implement the RC4 cipher. Whereas AES is relatively new and very complex, RC4 is very old and is very simple.

The most significant difference between the two would probably be their type. AES is a block cipher that operates on discrete blocks of data using a fixed key and a formula while RC4 is a stream cipher that does not have a discrete block size. Instead, it uses a key stream of pseudorandom bits that is combined to the data using an exclusive OR (XOR) operation. You can use block ciphers as stream ciphers and vice versa, so the separation is not very distinct. But it is quite well known that RC4 is not very effective when used as a block cipher.

A good example of the weaknesses of RC4 is the implementation of WEP. WEP has been completely rendered insecure and can even be broken within a couple of minutes with tools that you can find readily available online. Although TKIP addresses some of the issues that have plagued WEP, it is not considered to be as secure as AES is. For this reason, it is advisable to use AES in any situation unless hardware limitations prevent you from doing so.

The primary reason why RC4 is very popular is the fact that it is simple and it can be very fast. This is already being mitigated since AES implementations in hardware are becoming very popular as it provides speed advantages over software implementations.

Lastly, RC4 is trademarked since it was initially a trade secret, which led to some people coming up of inventive ways to call the leaked description way back in 1994; like ARCFOUR and ARC4 (Alleged RC4). On the other hand, AES is publicly available and can be freely used without hitting any legal problem.

Summary:

1. AES is a very new and complex encryption standard while RC4 is rather old and simple.
2. AES is a block cipher while RC4 is a stream cipher.
3. AES is extremely secure while RC4 is not so.
4. RC4 is very fast compared to AES.
5. RC4 is trademarked while AES is not

Over the recent years, three factor authentications have also been introduced. This kind of authentication also needs “something you are”, like a fingerprint or a voice print, together with the password and the physical token. [6]

Two factor authentications together with OTP is much safer than static passwords, when looked at from an access attack perspective, such as sniffing, password cracking and social engineering. However, it cannot protect against two common attacks [7]:

Man-in-the-middle attack an attacker sets up a fake website, resembling a legitimate site that the user surfs to in order to log in. The user generates the OTP and sends it to the fake website controlled by the attacker, which can now use this password to login to the real web site.

Trojan attack A Trojan is installed on the user's computer, allowing a hacker to “piggyback” on the session established when the user logins to a website.

These two attacks are best solved by educate users in how to spot web pages with false certificates and how to protect your computer and keep anti-virus software up to date. That is out of the scope of this paper.

One of the methods that can be used to come over this problem is using mOTP but with some modification as follows:

1. Unique user name
2. 4-digit PIN
3. Init-secret number of mobile

Following figure describes the procedure how it will work:

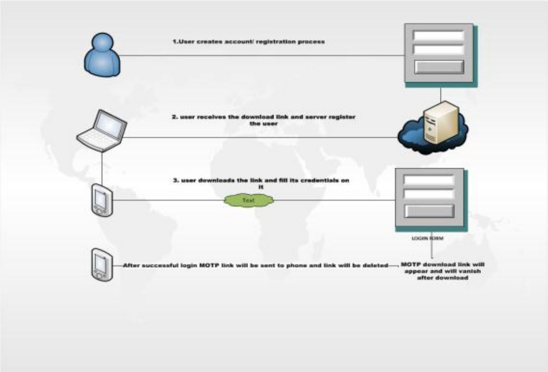

1.User creates account/ registration process
2. user receives the download link and server register the user
3. user downloads the link and fill its credentials on it
Text
LOGIN FORM
After successful login MOTP link will be sent to phone and link will be deleted
MOTP download link will appear and will vanish after download

Fig. 1 basic scheme for authentication

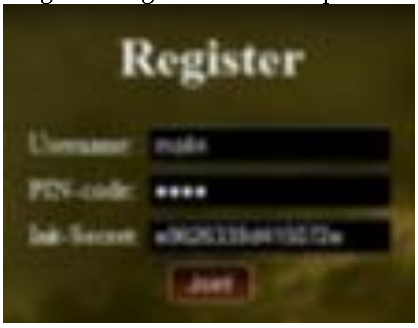
Pros

1. No crucial login information is sent over the network.
2. If the encrypted username and PIN-code is cracked it will not matter, since a hacker cant login without the correct Init-secret. And todays best encryptions (AES, RC4) have not been cracked yet.
3. The Init-secret will be safe inside an application. If someone tries to manipulate the application along the way it can be detected by hash-function.
4. No configurations needed for the client, the application is ready-to-go.
5. Application downloaded and installed directly to the mobile phone, no need for user to connect the phone to the computer first.
6. Extra security by requiring authentication to the download page.
7. The download page can be deleted after 1 download, that way only one copy of the application/Init-secret will exist.
8. Extra security by using two devices. If the client's computer is compromised and the traffic is being monitored by an attacker, perhaps your mobile phone will be safe.

Cons

1. Harder to implement, more work for the server.

2. If the process is not automated it can take a long time to get the server response.



Register

Username: [illegible]

PIN-code: ****

Init-Secret: [illegible]

However, there are problems with this solution. All of this information will be sent over an insecure network where someone might sniff the packet. Even if the packet is encrypted through TLS/HTTPS, there is a possibility that a hacker can decrypt the information and get full access to the user's account, especially since he don't have any time limit and can decrypt the packet offline. One more point, even though all the packets will be encrypted, the user will not be protected against Man-in-the-middle attacks, that can direct the user to a page with a fake certificate where the attacker can gather all of the information that the user provide during the registration part. [23]

To protect against Man-in-the-middle attacks, people need education on how to spot a fake certificate, and is out of the scope of this thesis.

In order to provide a safe method to registrar to a service, these guidelines must be followed:

1. The Init-Secret can NEVER at ANY point travel over the network.

2. Since this is a cloud provider that customers will access through a web browser, the registration should be simple and at low or no cost.

3. The registration customers should be able to do the whole registration process over the Internet, not like the banks' system where the users go to the local office to get the authentication device. That will not be flexible and possible for a cloud solution.

5. Conclusion

After implementing the practical solution of mobile authentication and RC4 encryption in a real life system, it is concluded that this system satisfies the criteria’s.

1. *Provide better password solution for login procedures than the insecure method of static passwords.*

2. *Provide better two-factor OTP authentication solution than those being used today.*

3. *Have an easy-to-understand registration system, which at the same time doesn't compromise the security.*

4. *Use an encryption algorithm that is secure but also fast, to be able to serve the vast amount of cloud users.*

5. *Offer a solution that is free of charge in order to attract more customers to the cloud services.*

6. *In overall, the security solution for cloud services must be easy to use, but also be very secure in order to protect the customers' data and gain the trust of the customers.*

Acknowledgments

Thanks to the experts who have contributed towards completion of my research.

References

[1] Amazon EC2, http://aws.amazon.com/ec2/

[2] Google App Engine, http://code.google.com/appengine/

[3] http://docs.google.com/ Google Apps

[4] *"Safer Authentication with a One-Time Password Solution "*, D. Griffin, MSDN Magazine, Issues. Published May 2008

[5] *"A Two-Factor Mobile Authentication Scheme for Secure Financial Transactions"*, R. Di Pietro & G. Me & M. A. Strangio, ICMB 2005. International Conference. 11-13 July (2005), 28

[6] http://searchsecurity.techtarget.com/sDefinition/0,, sid14_gci992919,00.html Accessed 05/11/2010

[7] *"Impersonation Attacks on Software-Only Two-Factor Authentication Schemes"*, T. Kwon, Communications Letters, IEEE Aug 2002. V6, page(s): 358

[8] *"Performance Analysis of Advanced Encryption Standard (AES)"*, Y. X. Guizani & S. Bo Sun Hsiao-Hwa Chen Ruhai Wang, Global Telecommunications Conference, 2006. GLOBECOM '06. IEEE .page(s): 1

[9] *"An improved RC4 stream cipher"*, J. Xie & X. Pan, Computer Application and System Modeling (ICCASM), 2010 International Conference. 22-24 Oct. 2010. Page: V7-156

[10] *"2-clickAuth – Optical Challenge-Response Authentication"*, A. Vapen, D. Byers, N. Shahmehri, 2010 International Conference on Availability, Reliability and Security

[11] *"Cryptography and Security Services: Mechanisms and applications"*, M. Mogollon, Cybertech Publishing, New York, 2007

[12] http://zxing.appspot.com/generator/ Last Accessed 21/10/2011

[13] http://www.doityourself.com/video/Hacking-and-decrypting-SSL-and-TLS-traffic-27836970, 15/10/2011

[14] http://www.differencebetween.net/technology/internet/difference-between-aes-and-rc4/