Cloud Computing Security Case Studies and Research

Chimere Barron, Huiming Yu and Justin Zhan

***Abstract*-Cloud computing is an emerging technological paradigm that provides a flexible and scalable information technology infrastructure to enable business agility. There are different vulnerabilities in cloud computing and various threats to cloud computing. We have investigated several real-world cases where companies' cloud was infiltrated by attacks. In this paper several types of attacks are discussed, real-world cases are studied, and the solutions that providers developed are presented. Our current research will also be discussed.**

***Index Terms*-cloud computing security, real-world cases, security case studies, algorithms**

I. INTRODUCTION

Cloud computing has become the newest rave in the computing industry. Its ability to save business's cost by eliminating the need to purchase huge amounts of software and/or software licenses for every employee, reducing the need for advanced hardware, eliminating the need for companies to rent physical space to store servers and databases, and shifting the workload from local computers that has appealed to cloud computing providers such as Amazon, Google, IBM, Yahoo, Microsoft, etc. [17, 18].

There is no fixed definition for cloud computing, but it is the general term used for computing that involves delivering hosted services over the internet. Cloud services offer three distinct amenities - it is sold on demand (typically by the minute or hour), it is elastic (a user can have as much or as little of a service as needed at any given time), and the service is fully managed by the provider. These services are categorized as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) [17]. Infrastructure as a Service provides low-level services which can be booted with a user-defined hard disk image such as Amazon EC2. In Platform as a Service, the cloud provider offers an API which can be used by an application developer to create applications on the provider's platform. Examples of PaaS include Force.com, GoogleApps, etc. With Software as a Service, the vendor supplies the software product and interacts with users through a front-end portal; web-based office applications like Google Docs or Calendar are examples of SaaS [18].

Cloud computing offers numerous advantages, therefore hackers are also interested in it. Various attacks such as social engineering attack, XML signature wrapping attack, malware injection, data manipulation, account hijacking, traffic flooding, and wireless local area network attack pose a great risk to cloud computing systems. There have been many instances where companies have fallen victims to cloud computing being hacked [1, 2, 3, 7, 10, 12, 14].

We have examined cloud computing providers that were compromised, how the attack was completed, and solutions the company developed to make sure the incident can never be repeated in the future. In section II, the guest and provider sides of cloud computing will be discussed. The details of these real-world cases will be presented in section III. In section IV our current research will be discussed. The conclusion and future work will be given in section V.

II. GUEST AND PROVIDER SIDES OF CLOUD COMPUTING

When companies, governments or organizations decide to make the shift to cloud computing security is a main consideration. Cloud computing consists of guest and provider sides. The guest side is the end users who use the cloud. It provides the end users with the ability to choose cloud services and environment. It is the interface that clients see after they enter credentials and have the ability to use the services provided by the cloud. The guest side may consist of different users, laptops, tablets, cell phones, various computers and enterprise centers. The provider side of cloud computing is the service providers which consists of application servers, service platforms, runtime environment, and datacenters etc. An application server can be WebSphere Application Server that is a Java EE, EJB supported technology-based application platform. Service platforms provide capabilities to users to build, deploy and manage robust, agile and reusable SOA business applications and services. A datacenter can provide huge capacity to store users' data and keep them secure. Figure 1 is an example that shows the basic layout of the guest side and provider side of cloud computing [2]. The guest side is the enterprise portion and the provider side is the service provider portion.

Manuscript received March 23, 2013; revised April 15, 2013. This work was partially supported by National Science Foundation under the award numbers 0909980, 0830686, 1247663, 1238767, and 1137443.

Chimere Barron is with the Department of Computer Science, North Carolina A&T State University, Greensboro, NC 27411 USA (e-mail: cvbarrn1@gmail.com).

Huiming Yu is with the Department of Computer Science, North Carolina A&T State University, Greensboro, NC 27411 USA (e-mail: cshmyu@ncat.edu).

Justin Zhang is with the Department of Computer Science, North Carolina A&T State University, Greensboro, NC 27411 USA (e-mail: zzhan@ncat.edu).

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

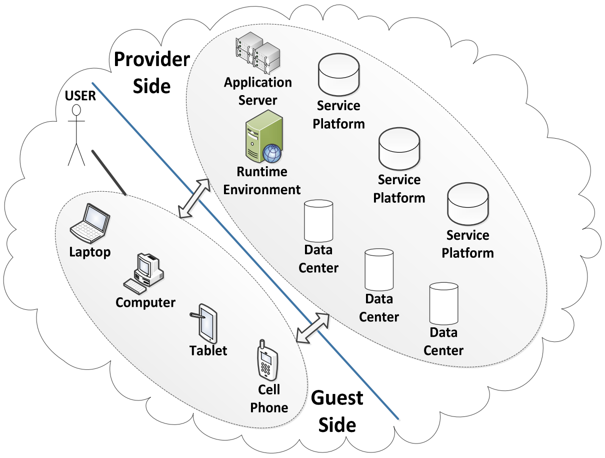

Figure 1. Guest and Provider Sides of Cloud Computing

Cloud computing providers must keep users' privacy and assure the information stored on the cloud is always secure. The Service-Level Agreement (SLA) between cloud providers and customers specifies details of the service. A typical cloud SLA specifies service objectives such as 99.9% uptime, compensation to the user [15]. The Cloud Security Alliance (CSA) offer certification to cloud providers that meet the criteria. The CSA's Trusted Cloud Initiative program was created to help cloud service providers develop industry-recommended, secure interoperable identity, access and compliance management configuration and practices [1].

III. SECURITY CASE STUDIES

Multiple real-world cases where cloud computing were compromised and the ways the company mitigated the incident will be discussed. For each case the attack type will be briefly described, the details of the case will be presented and the prevention methods will be discussed.

A. **XML Signature Wrapping Attack**

Wrapping attacks aim at injecting a faked element into the message structure so that a valid signature covers the unmodified element while the faked one is processed by the application logic. As a result, an attacker can perform an arbitrary Web Service request while authenticating as a legitimate user [4, 6].

In 2011, researchers lead by Dr. Jorg Schwenk from Ruhr-University Bochum found a cryptographic hole in Amazon's EC2 and S3 services. The flaw was located in the web services security protocol and enabled attackers to trick servers into authorizing digitally signed SOAP messages that have been altered. The attackers hijacked control interfaces used to manage cloud computing resources, which would allow attackers to create, modify, and delete machine images, and change administrative passwords and settings [5].

A proposed solution is to use the SOAP message during message passing from the web server to the web browser. A redundant bit (STAMP bit) will be added onto the signature value when it is appended in the SOAP header. This bit will be transmitted when the message is interfered with by a third party during the transfer. When the message reaches its destination the STAMP bit is checked. If the STAMP BIT has been changed, then a new signature value is generated by the browser and the new value is sent back to the server as recorded to modify the authenticity checking [5].

B. Malware Injection

In a malware-injection attack an adversary attempts to inject malicious code into a system. This attack can appear in the form of code, scripts, active content, and/or other software. When an instance of a legitimate user is ready to run in the cloud server, the respective service accepts the instance for computation in the cloud. The only checking done is to determine if the instance matches a legitimate existing service. However, the integrity of the instance is not checked. By penetrating the instance and duplicating it as if it is a valid service, the malware activity succeeds in the cloud.

Case one occurred in May 2009. The United States Treasury Department moved four public websites offline for the Bureau of Engraving and Printing after discovering malicious code was added to the parent side [10]. The third-party cloud service provider hosting the company's website was victim to an intrusion attack. As a result numerous websites (BEP and non-BEP) were affected. Roger Thompson, chief research officer for Anti-Virus Guard (AVG) Technologies, discovered malicious code was injected into the affected pages. Hackers added a tiny snippet of a virtually undetectable iFrame HTML code that redirected visitors to a Ukrainian website. IFrame (Inline Frame) is an HTML document embedded inside another HTML document on a website. From there, a variety of web-based attacks were launched using an easy-to-purchase malicious toolkit called the Eleonore Exploit Pack [10].

To prevent this type of attack server operators need to check for and exploit iFrame code. Firefox users should install NoScript and set "Plugins | Forbid iFrame" option. Window users should make sure they have installed all security updates and have an active anti-malware guard running.

Case two occurred in June 2011. The cyber criminals from Brazil who first launched their attacks as spam/phishing campaigns, where users were sent spoofed emails with links that took them to one of the malicious domains, created some major problems in Amazon Web Services [3]. The attackers installed a variety of malicious files on the victims' machines. One component acted as a rootkit (a type of malicious software that is activated each time a user's system boots up) and attempted to disable installed anti-malware applications. Additional components that were downloaded during the attack attempted to retrieve login information from a list of nine Brazilian banks and two other international banks, steal digital certificates from eTokens stored on the machine, and collect unique data about the PC itself that is used by some banks as part of an authentication routine [3].

A proposed solution is to utilize the File Allocation Table (FAT) system architecture. The FAT table identifies the code or application that a customer is going to run. It checks with the previous instances that have already executed from the customer's machine to determine the validity and integrity of the new instance. A secure and unbreakable hypervisor would be needed on the provider's end. The hypervisor would be responsible for scheduling all instances, but not before checking the integrity of the instance from the FAT table of the customer's virtual machine.

C. Social Engineering Attack

A social engineering attack is an intrusion that relies heavily on human interaction and often tricking other people to break normal security procedures [9]. It can happen in cloud computing.

In August 2012, hackers used a social engineering attack to completely destroy technical writer Mat Honan's digital life by remotely deleting the information from his iPad, MacBook, and iPod [12]. The heart of the story revealed the dangerous blind spot between the identity verification systems used by Amazon and Apple. The hackers found the victim's @me.com address online which informed them that there was an associated AppleID account [12]. The hacker called Amazon customer service wanting to add a credit card number to the victim's account. The representative asked the hacker for the name, billing address, and an associated email address (all information the hacker found on the internet) on the victim's account. Once the hacker answered these questions successfully the representative added the new credit card onto the account. Once ending the call, the hacker called Amazon customer service back and explained to the representative that he had lost access to his account. The Amazon representative asked the hacker for his billing address and a credit card associated with the account; the hacker used the new credit card information he provided from the previous phone call. Once the hacker gave the representative the information they added a new email address to the victim's account. Upon logging onto Amazon's website the hacker requested a password reset the email address he just created. The hacker now had access to the victim's Amazon account and credit card information on file. The hacker then called Apple technical support and requested a password reset on the victim's @me.com email account. The hacker could not answer any of the victim's account security questions, but Apple offered him another option. The Apple representative only needed a billing address and the last four digits of the victim's credit card and issued the hacker a temporary password. Once the hacker had access to the victim's Apple iCloud account all the information from the victim's iPad, MacBook, and iPod account was remotely erased [12].

Apple confirmed that it temporarily disabled its customers' ability to reset an AppleID password over the phone. Instead, customers have to use Apple's online "iForgot" system. In the process they will work on a much stronger authentication method that proves customers are who they say they are. Amazon customer service representatives will no longer change account settings like credit card or email addresses by phone [12].

D. Account Hijacking

Account hijacking is usually carried out with stolen credentials. Using the stolen credentials, attackers can access sensitive information and compromise the confidentiality, integrity, and availability of the services offered [1]. Examples of such attacks include: eavesdropping on transactions/sensitive activities, manipulation of data, returning falsified information, and redirection to illegitimate sites [1].

In July 2012, the hacker group, UGNazi, exploited a major flaw in Google's gmail password recovery process and AT&T's voicemail system which in turned allowed the group to access the CEO of CloudFare's personal gmail account [13]. The hacker deceived AT&T'S system into redirecting the victim's cell phone to a fraudulent voicemail box. The hacker visited gmail and initiated the account recovery feature for the victim's personal email address. A voicemail message was recorded on the compromised voicemail box to sound like someone was answering the phone. A call was placed to the victim from Google, but the victim did not recognize the number and let the call go to voicemail. Google's system was tricked by the fraudulent voicemail and a temporary PIN was left (which allowed the password to be reset) in the voicemail. The hacker logged into the victim's gmail account and added his email address to the 'account recovery control' feature. The victim's linked Cloudfare account received an email informing him that the recent password was changed. The victim initiated the account recovery process and changed the password back. An email is sent to the hacker informing him that the victim changed passwords, but immediately the hacker changed the password. Both users continue going back and forth to get control over the account. Soon, the hacker is able to remove the victim's mobile phone and email addresses authorized for account recovery preventing the victim from resetting the gmail password. The team at CloudFare is called to investigate the situation [13].

A flaw in Google's account recovery system allowed two-factor authentication setup on the victim's Cloudfare account to be bypassed and the hacker now had access to the account. The victim's administrative privileges were used by the hacker to change passwords on other administrative accounts. Cloudfare's operations team suspended the victim's account, reset all CloudFare employee email passwords, and cleared all web mail sessions, which terminated the hacker's access to the email system [13].

Google fixed the flaw in the Google Enterprise Application account recovery process by no longer allowing a user to get around two-factor authentication. CloudFlare has stopped emailing blind copies of password resets and other transactional messages to administrative accounts [19].

Another case occurred in July 2012. Dropbox, the cloud storage service, confirmed that hackers used usernames and passwords stolen from third-party sites to access Dropbox users' accounts. It was altered after users complained about Spam they were receiving to email address used only for the Dropbox accounts. One stolen password was used to access an employee account that contains a file that included user email addressed. The company believed users who use the same password on multiple websites make it easier for hackers to access their accounts on other websites [7].

In order to prevent a repeat attack, Dropbox has implemented two-factor authentication into the company's security controls. Two-factor authentication (also called strong authentication) is defined as a user entering in two of the following three properties to prove his/her identity: something the user knows (e.g, password, PIN), something the user has (e.g., ATM card) and/or something the user is (e.g., biometric characteristic, such as a fingerprint) [16]. The company launched new automated mechanisms to identify suspicious activities and a new page to show all logins.

E. Traffic Flooding

Traffic flooding attacks bring a network or service down by flooding it with large amounts of traffic. Traffic flooding attacks occur when a network or service becomes so weighed down with packets initiating incomplete connection requests it cannot process genuine connection requests. Eventually, the host's memory buffer becomes full and no further connections can be made, and the result is a Denial of Service.

In May 2011, LastPass, a cloud-based password storage and management company, announced a possible successful hack against its servers. There were no reports of any data leakage, but the company insisted that customer's take a few measures to ensure that their information is safe. Security experts discovered unusual behavior in the database servers that had more traffic going out compared to incoming data. The company presumed this was hacking activity related to siphoning stored login credentials and other sensitive user data. Master passwords (passwords that protect lists of passwords to access other websites and online services in the cloud) were immediately changed to protect customers from possible data leakage. [8].

To prevent this problem from happening again Lastpass enhanced its encryption algorithms used in protecting customers' data and introduced additional measures to secure sensitive data on its servers [8].

F. **Wireless Local Area Network Attack**

In a wireless local area network attack a hacker breaks into an authorized user's wireless local area network to perform attacks such as man-in-the-middle, accidental association, identify theft, denial of service, network injection attacks, etc.

In January 2011, German security researcher Thomas Roth used cloud computing to crack wireless networks that relied on pre-shared passphrases, such as those found in homes and small businesses. The results of the attack revealed that wireless computing that relies on the pre-shared key (WPA-PSK) system for protection is fundamentally insecure. Roth's program was run on Amazon's Elastic Cloud Computing (EC2) system. Using the massive power of Amazon's cloud the program was able to run through 400,000 possible passwords per second. It would typically cost tens of thousands of dollars to purchase the computers to run the program, but Roth claims that a typical password can be guessed by EC2 and his software in about six minutes [11]. The type of EC2 computers used in the attack costs $.28 cents per minute, so $1.68 is all it took to hack into a wireless network.

WPA-PSK is believed to be secure because the computing power needed to run through all the possibilities of passphrases is huge. But cloud computing provides this kind computing power today, and is very inexpensive [11]. It is suggested that up to 20 characters are enough to create a passphrase that cannot be cracked, but the more characters included, the stronger the passphrase will be. A good variety of symbols, letters, and numbers should be included in the passphrase and it should be changed regularly. Dictionary words and letter substitution (i.e "n1c3" instead of "nice") should be avoided [11].

IV. OUR CURRENT RESEARCH

One of the severe types of attacks, that interrupt cloud computing normal functions, is a SYN flood attack which is simply a type of Denial of Service. An attacker sends a succession of SYN requests to a victim system in an attempt to consume system resources and make the system unresponsive to legitimate traffic. There are a number of existing countermeasures against SYN flood attacks such as Filtering, SYN Cache, SYN Cookies, Firewalls and Proxies, Reducing SYN-RECEIVED Time, etc. [20]

In cloud computing all servers work in a service specific manner with internal communication among them. When a server is overloaded or has reached the threshold, it transfers some of its jobs to similar service-specific server to offload tasks. If an adversary successfully attacks one server with SYN flood and causes the denial-of-service, the victim server will transfer upcoming tasks to other servers in order to offload jobs. Thus, the same thing will occur on other servers and the attacker is successful in engaging the whole cloud system by just interrupting the usual processing of one server, in essence flooding the cloud.

Based on the characteristics of cloud computing we are developing an approach to effectively detect and prevent SYN flood attacks. The first part of this approach is to design an algorithm to discover the malicious packets. The detecting algorithm will check some parameters of incoming IP packets to decide to filter an incoming packet out or not. The second part is to develop an algorithm to stop SYN flood to spread over cloud computing. Once a server is overloaded the preventing algorithm will check current situation, compare with normal cases, then decide it is SYN flood or normal overloaded work. If it is SYN flood it will keep the victim server from transferring upcoming jobs to other servers. These algorithms will run on the hypervisor of the provider side.

V. CONCLUSION AND FUTURE WORK

Cloud computing security involves different areas and issues. Many security mechanisms have been developed to prevent various attacks and protect cloud computing systems. Researchers continue to develop new technologies to improve the security of cloud computing. In this paper several real-world cases where companies' clouds were infiltrated by attacks are presented. Social engineering attack, XML signature wrapping attack, malware injection, data manipulation, account hijacking, SYN flood, and wireless local area network attack are discussed. The solutions that the companies developed to prevent similar attacks in the future are discussed.

In order to protect cloud computing technologies of detection, prevention and responding various attacks must be developed. Our current research focuses on detecting and preventing SYN flood in cloud computing. We are developing one detecting algorithm and one preventing algorithm. We will implement and test these algorithms on cloud computing.

ACKNOWLEDGEMENTS

This work was partially supported by National Science Foundation under the award numbers 0909980, 0830686, 1247663, 1238767, and 1137443.

REFERENCES

[1] Cloud Security Alliance, "Top threats to cloud computing", *Cloud Security Alliance*, March 2010.

[2] K. Decker, "What Joni Mitchell might say about cloud computing", 2010. Available: http://decker.com/blog/2010/05/what-joni-mitchell-might-say-about-cloud-computing/

[3] D. Fisher, "Attackers using Amazon cloud to host malware", Available: http://threatpost.com/en_us/blogs/attackers-using-amazon-cloud-host-malware-060611

[4] S. Gajek, M. Jensen, L. Lioa and J. Schneck, "Analysis of signature wrapping attacks and countermeasures", *IEEE International Conference on Web Services*, 2009.

[5] A. Hickey, "Researchers uncover 'massive security flaws' in Amazon cloud", Available: http://www.crn.com/news/cloud/231901911/researchers-uncover-massive-security-flaws-in-amazon-cloud.htm

[6] M. Jensen, C. Meyer, J. Somorovsky, and J. Schwenk, "On the effectiveness of XML schema validation for countering XML signature wrapping attacks", *International Workshop on Securing Services on the Cloud – IWSSC*, 2011.

[7] D. Kerr, "Dropbox confirms it was hackers, offers users help", Available: http://news.cnet.com/8301-1009_3-57483998-83/dropbox-confirms-it-was-hacked-offers-users-help/

[8] Kiril, "LassPass possibly hacked, cloud security concerns on the rise", Available: http://www.cloudtweaks.com/2011/05/lastpass-possibly-hacked-cloud-security-concerns-on-the-rise/

[9] I. Kotenko, M. Stepashkin, and E. Doynikova, "Security analysis of information systems taking into account social engineering attacks", *IEEE 19th International Eurimicro Conference on Parallel, Distributed, and Network-Based Processing*, 2011.

[10] M. Kronfield, "Treasury Dept. has cloud hacked", Available: http://www.gsnmagazine.com/article/20691/treasury_dept_has_cloud_hacked

[11] PC World Staff, "Cloud computing used to hack wireless passwords", Available: www.pcworld.com/article/216434/cloud_computing_used_to_hack_wireless_passwords.html

[12] J. Pepitone, "Hack attack exposes major gap in Amazon and Apple security", Available: http://money.cnn.com/2012/08/07/technology/mat-honan-hacked/index.htm

[13] M. Prince, "The four critical security flaws that resulted in last Friday's hack", Available: http://blog.cloudflare.com/the-four-critical-security-flaws-that-resulte

[14] S. Qaisar and K. Khawaja, "Cloud computing: network/security threats and countermeasures", *Interdisplinary Journal of Contemporary Research In Business* Volume 3, January 2012.

[15] M. Rouse, "Cloud storage SLA", Available: http://searchcloudstorage.techtarget.com/definition/cloud-storage-SLA

[16] M Rouse, "Two-factor authentication", Available: http://searchsecurity.techtarget.com/definition/two-factor-authentication

[17] F. Sabahi, "Cloud computing security management", *2nd International Conference on Engineering Systems Management and Its Applications (ICESMA)*, March 2010.

[18] F. Shaihk and S. Haider, "Security threats in cloud computing", *IEEE 6th International Conference on Internet Technology and Secured Transactions*, December 2011.

[19] L. Tung, "CloudFare boss's Gmail hacked in redirect attack on 4Chan", Available: http://www.cso.com.au/article/426515/cloudflare_boss_gmail_hacked_redirect_attack_4chan/

[20] A. Chonka and J. Abawajy, "Detecting and mitigating HX-DOS attacks against cloud Web services", *15th Int. Conference on Network-Based Information Systems*, 2012.