Exploring Vulnerabilities in Cloud Computing

Kajetan Cieplinski 1678329	**Aikaterini Chelioti** 1581991	**Thomas James Williams** 1690225
Ehsun Hanif 1617402	**Eleni Katsi** 2088699	**Xiao Zhang** 2020567

Abstract

Cloud Computing has become an integral part of our lives and we benefit from this technology almost every day, be it for storing data, such as documents, or providing various computational resources for businesses, such as Amazon Web Services and Google Cloud Services. But, as with great power comes great responsibility, protecting stored data or resources and tools is very much a necessity. With this report, we aim to analyse papers pertaining to security vulnerabilities in Cloud Computing and why they pose a major point of consideration for any company that relies on the Cloud.

Cloud service models

a) Definition of Cloud Computing

Kangchan Lee **[1]** defines Cloud Computing as “a model for enabling service users ubiquitous, convenient and on-demand network access to a shared pool of configurable computing resources”. Cloud computing involves multiple computational machines working in conjunction to provide services over the Internet. There are three elementary layers of Cloud Computing: **i)** the Infrastructure-as-a-Service (IaaS) layer, the least abstract layer, **ii)** the Platform-as-a-Service layer (PaaS), and **iii)** the Software-as-a-Service (SaaS) layer the most abstract layer. Each of these layers serves a distinct purpose, not just from a technical standpoint but also from a financial one. For example, the IaaS layer aims to reduce hardware costs, while all of the layers are capable of reducing capital and operational expenditures.

IaaS

The Infrastructure-as-a-Service layer provides the most basic *infrastructure* elements, such as memory, CPUs and storage. A prime example of such a service is the Amazon Elastic Compute Cloud **[2]**, a service that provides virtual machines of various capabilities, which can be used online while running inside Amazon’s data centers.

PaaS

The Platform-as-a-Service layer supplies platform-oriented services which enable the use of hosting environments customized to a specific requirement. An example of this would be the Google App Engine. It can be used to deploy and dynamically scale Python and Java-based Web applications.

SaaS

The Software-as-a-Service layer presents the user with ready-to-use applications catering to specific needs, such as Dropbox which enables users to save a multitude of files on the Cloud, from text documents to large multimedia files.

b) Foundations of Cloud Computing

In order to properly discuss Cloud Computing, it is insufficient to only talk about the models that are used to create them; we also need to address the technologies that are used to access them. These include server-enabled fat clients, which are capable of a lot of functionality separate from the server, and Web browser-based thin clients, which are heavily dependent on the server's applications.

When talking about Cloud Computing security vulnerabilities, the following two specifications inevitably arise:

WS-Security and SOAP

Web Services Security is perhaps the most important specification for addressing security in Web Services. It is an extension to the SOAP messaging system, and enforces privacy and integrity on exchanged messages. SOAP itself is a messaging protocol specification for exchanging web service information in computer networks. It has three main characteristics, *extensibility* (allows for extensions such as WS-Security), *neutrality* (can operate over any protocol such as HTTP, UDP, etc.), and *independence* (allows for any programming model).

WS-Security defines a SOAP Header and three main mechanisms: the signing of SOAP messages (to guarantee integrity), the encryption of SOAP messages (to guarantee confidentiality), and the attachment of security tokens (to verify the user's identity). It allows for the application of XML Signature in SOAP messages.

XML Signature enable us to digital sign XML Fragments, providing integrity or proof of authenticity. The signing process works in the following way:

1. For each part of the message to be signed, a *Reference* element is created. This part of the message is then hashed.
2. The result is added into the *DigestValue* element and a reference to the signed part is entered into the URI attribute.
3. Finally the *SignedInfo* element is canonicalized and signed.
4. The result of the signing operation is placed in the *SignatureValue* element and the *Signature* element is added to the security header.

TLS

The Transport Layer Security, according to Rescorla and Modadugu **[3]**, is an extensively implemented protocol for securing network traffic such as Web Traffic and e-mail protocols such as IMAP and POP. As with every other case, TLS is also very important in terms of Cloud Computing. Any weakness in TLS implicitly constitutes a weakness in the Cloud system using it. The TLS protocol comprises two parts: **i)** the *TLS Handshake*, in which algorithms and keys are negotiated and (if need be) the server and client are authenticated, and **ii)** the *Record Layer* which encrypts/decrypts TCP data streams using the aforementioned exchanged information.

TLS becomes rather important when discussing *phishing* attacks, which came to the academic limelight in 2004. In a phishing attack, the attacker deceives a victim into accessing a fake web page, through forged emails or attacks on the Domain Name System (DNS). Once the user is successfully tricked into believing the web page to be genuine, they might proceed to provide personal details to the attacker. Furthermore, they might be coaxed into entering financial details, such as credit card numbers, or their email/password pair to 'login' to the fake service presented on the web page. Once the attacker has gained access to these data, he has a number of options, including the possibility to financially damage the user.

Cloud Computing Security Issues

a) Data Breaches

Malicious Insider

A business may choose to migrate all their applications and data to a Cloud Computing platform in order to gain financial advantages or any advantages over red-tape. But during that process, it is quite possible for the organization's data set and applications to be compromised.

The paper outlines three types of insider threats. These are: **i)** the rogue administrator, who has the privileges to steal unrestricted files, brute-force passwords and illicitly download user data, **ii)** insiders who exploit cloud vulnerabilities to gain unauthorised access to sensitive information, and finally **iii)** insiders who use the Cloud to carry out their own personal nefarious activities. These attacks are extremely hard to trace even with forensic analysis because the attacker already has clearance to use the Cloud system.

Here is an example of insider threats. There is a BalaBit survey of 200 IT professionals. From this survey, almost half of them said they have bypassed the IT policy. Also they may made some exception roles in the firewall. What's worse is, 29 percents of respondents admitted to taking home company data and 25 per cent have looked into confidential files.Most worrying, is the fact that 15 per cent have already deleted or modified system log files (in order to hide or destroy evidence). By this way, it means insider threats might be more serious than expectation.**[9]**

Online Cyber Theft

A Cloud system makes for an ideal target for hackers wishing to steal users' information, as it is capable of high data storage. Stolen data can be used in many ways, such as in the creation of fake bank accounts to carry out fraudulent activities. For example, hackers stole personal information through Amazon's Elastic Compute Cloud by first creating a fake account and then using a virtual machine to initiate an attack on Sony's PlayStation Network **[4]**. According to the survey and analysis of global companies in 2011, there are 37 percent of cases of data breach is about malicious attacks. These cases cost $222 on average by record.**[10]** It is well known that online retailer Zappos was also the victim of this kind of case.**[11]**

b) Cloud Security Attacks

Malware Injection

One plausible attack on a Cloud environment is a *Malware Injection* attack. In this scenario, the attacker's goal is to inject a malicious service implementation or virtual machine into the Cloud environment. This injected malware can eavesdrop on the user's communication with the Cloud, modify data, or alter the functionality of the Cloud.

This attack requires the user to implement their own malicious (SaaS or PaaS) service or virtual machine instance (IaaS) and add it to the Cloud system. The attacker can then trick the Cloud into treating the new service implementation instance as a valid instance of the specific service the attacker wishes to compromise. Once this process succeeds, all user communication is redirected to the malicious service implementation and the attacker's code is executed.

The Cloud system can neutralize the attack by performing a service instance integrity check before using a service instance for incoming requests. It is still possible for the attacker to inject his malicious code but now he would have to bypass the integrity check to embed a malicious instance into the Cloud system.

SQL injection

SQL injection is the most common mode of malware injection. It attempts to exploit SQL servers running applications which are communicating with a database. Attackers embed malicious SQL statements in the web application in order to gain access to the data. The contents of the database can then be viewed, modified and otherwise damaged by the attacker. According to Te-Shun Chou, SQL injections were used to plant unauthorized code on 209 pages promoting the PlayStation network games like "SingStar Pop" and "God of War".

Cross-site scripting attack

Another kind of malware injection is the cross-site scripting attack. A hacker plants malicious scripts into a victim's web browser by means of a web application. The scripts then run in the victim's browser. An example consequence of this attack is the theft of the victimised user's session cookies when logging onto web pages they frequent. According to Te-Shun Chou, researchers in Germany have successfully demonstrated a XSS attack against Amazon AWS cloud computing platform. The vulnerability in Amazon's store allowed the team to hijack an AWS session and access to all customer data which included authentication data, tokens, and even plain text passwords.

Wrapping Attack

SOAP messages are vulnerable to a malware injection attack known as an *XML Signature Wrapping Element* attack. The SOAP Message Body contains a request made by the sender along with their signature. In a typical SOAP message, the signature information is stored in the SOAP Header along with a pointer to the 'Id' attribute. An attacker can intercept the message and modify it thus: he inserts a wrapping element in the Header in which he places the original body. He then creates a new body which contains the operation the attacker wants to effect. The resulting message still has the sender's valid signature on it (albeit at a different location within the message), and the malicious operation is allowed to be executed.

A solution to such an attack, known as the *inline approach*, was proposed in Rahaman, Marten and Shaad **[5]**. This solution relied on embedding *SOAP Account information* into the SOAP message to protect the sender's digital signature from malicious alteration, however it was later proven to be ineffective by Gajek, Liao, and Schwenk **[6]** who also proposed alternative possibilities to fixing the wrapping element attack.

Abuse of Cloud Computational Resources & Flooding Attacks

One of the primary advantages of Cloud Computing is the ability to *lease* server hardware to clients. This is done in the form of virtual machines running on the Cloud's data servers. The higher a company's need for computational power, the more Virtual Machines and other resources are made available to it.

a) Direct Denial of Service

While such flexibility in terms of computing resources is rather amenable to users, this arrangement has severe security flaws. An attacker only need to *flood* the Cloud system with nonsensical requests. In response, the system will allocate progressively more resources (for example, more virtual machines) to attempt to cater to all the incoming requests. Even though such a reaction might seem capable of dealing with the attacker's malicious intent, it is in fact *aiding* the attacker by allowing him to eventually perform a complete Denial of Service attack on the service, as the server will ultimately run out of resources to process the barrage of requests.

b) Indirect Denial of Service

However, the damage caused by a direct Denial of Service attack on a service is unfortunately not limited to that service. The server will use up all of its hardware resources to cater to the flooded service, thus depriving other services running on the same server of their much needed computational power. As such, all services on the server and the server itself will inevitably shut down. Depending on its sophistication the Cloud system even might, upon witnessing one server becoming defunct, *evacuate* this server's services to other servers. The affected services will therefore overrun these other servers with requests as well, thus propagating the Denial of Service attack across the entire Cloud.

c) Accounting and Accountability

Such flooding attacks also have less technical implications. Users of a Cloud Computing service are usually charged based on their *usage* of the system, their usage being interpreted as the amount of resources allocated and workload caused. A flooding attack imposes tremendous workloads on the Cloud, and with the attacker himself usually being indeterminable, the user is tasked with paying the bill for their 'usage' of the Cloud Computing services.

Countermeasures

a) Security Policy Enhancement

Implementation of security policies mitigates the risk of computational power being abused. Well-specified regulations can also help network administrators to manage the cloud system more effectively. Amazon abides by this strategy by defining a clear user policy which isolates (even terminates) any offensive instances whenever it receives a complaint regarding spam or malware coming through Amazon EC2.

b) Access Management

Access control mechanisms can ensure that only authorized users have access to data. This is achieved by continuously monitoring traffic on the Cloud system. Intrusion detection systems and firewalls are commonly used for restricting access from untrusted resources and for monitoring malicious requests. The Security Assertion Markup Language (SAML) and eXtensible Access Control Markup Language (XACML) can be used to restrict access to the Cloud system itself.

c) Data Protection

Various security tools are available in order to stop data breaches. One method, detailed by Stolfo, Salem and Keromytis **[7]**, makes use of *User Behaviour Profiling* and *Decoys*. User Behaviour Profiling is used to monitor how, when and with what frequency a user accesses

their information on the cloud. An example of this is receiving an email from Google to let you know that there has been a login attempt to your account from another part of the world. As this login behaviour is out of the norm, you are notified by email to confirm whether the login was legitimate. Decoys can come in the form of fake documents or bogus information, which serve as a means for detecting unauthorised access to information.
By combining the two techniques, it is possible to detect unauthorised Cloud access with reasonable accuracy.

d) Security Techniques Implementation

Te-Shun Chou also discussed solutions to several attacks mentioned prior. He suggests that malware injection attacks can be prevented with a File Allocation Table (FAT) architecture. Using a FAT table the Cloud system can identify, in advance, the instance that the customer is going to run. The integrity/validity of this new instance can be determined by comparing it with the previous ones that have already been executed from the customers' machine.

As a second solution, the Cloud system can store a hash value for the original service instance. This integrity check between the new service instance's image and the original can help identify the malicious instances.

A variety of solutions have also been proposed to fix the vulnerabilities found in XML-based technologies. An XML Schema Hardening technique can be adopted to strengthen XML schema declarations. FastXPath, a subset of XPath, is proposed to counter the destructive elements that attackers inject into the structure of the SOAP message.

Results and Summary

The primary purpose of our research and our papers is to raise awareness about security vulnerabilities in the newly-emergent technology of Cloud Computing. The papers serve as a comprehensive listing and description of the most common attacks on the Cloud while they also give an overview of known instances of successful exploitation. Furthermore, they briefly discuss attempts made by other researchers at discovering solutions to the most oppressive attacks.

The information outlined in the papers constitutes a fair word of caution towards all parties involved in using and distributing the Cloud. But the imperfections mentioned can also inform security experts aiming to improve and further fortify the current protocols and techniques used in Cloud Computing.

Limitations and criticism

Although the papers very carefully list several types of Cloud-orientated attacks and mention various instances of them being successfully carried out, they primarily focus on vulnerabilities involving the TLS protocol and Malware Injection. And while they also partially discuss insiders as perpetrators of an attack, they devote very little space to investigate possible issues with hardware resources beyond flooding attacks in virtual machines.

This comes in sharp contrast with Hashizume et al. **[8]**, who mention a number of other considerations, such as the presence of possible covert channels and uncontrolled rollsbacks of a machine's state. In addition, they also identify a number of other weak points that can be exploited by an attacker or direct attacks in Cloud implementations such as resource over-provisioning, ARP spoofing in virtual machine VLANs, and data leakages.

Furthermore, the papers discuss solutions to these Cloud Computing attacks from a purely theoretical standpoint, referencing attempts at fixes documented in other literature. It should also be noted that, although the authors have on occasion suggested countermeasures to the vulnerabilities discussed, they have not proposed any solutions of their own, or demonstrated an implementation of the suggested fixes.

Conclusion

Cloud Computing is a constantly and consistently developing technology. It has plenty of advantages expressed mainly in its ability to give users access to a great number of services and resources. Nevertheless, there are various threats and security issues in Cloud Computing that need to be investigated and addressed lest attackers exploit them to the detriment of the Cloud's users. The papers we discussed, although largely theoretical, are a worthwhile contribution to the world of Cloud security and cyber security as a whole, as they aim to inform the design of the Cloud to guarantee data integrity and user protection.

Citations

1. Lee, K., 2012. Security threats in cloud computing environments. *International journal of security and its applications*, *6*(4), pp.25-32.
2. Cloud, A.E.C., 2011. Amazon web services. *Retrieved November*, *9*(2011), p.2011.
3. Rescorla, E. and Modadugu, N., 2006. Datagram transport layer security.
4. P. Alpeyev, J. Galante, M. Yasu, 2011,
   Amazon.com Server Said To Have Been Used in Sony Attack https://www.bloomberg.com/news/articles/2011-05-13/sony-network-said-to-have-been-invaded-by-hackers-using-amazon-com-server
5. Rahaman, Mohammad Ashiqur, Rits Marten, and Andreas Schaad. "An inline approach for secure soap requests and early validation." *OWASP AppSec Europe* 1 (2006).
6. S. Gajek, L. Liao, J. Schwenk, "Breaking and fixing the inline approach," in SWS '07: Proceedings of the 2007 ACM workshop on Secure web services. New York, NY, USA: ACM, 2007, pp. 37–43.
7. S. J. Stolfo, M. B. Salem, and A. D. Keromytis, "Fog computing: Mitigating Insider Data Theft Attacks in the Cloud," IEEE Symposium on Security and Privacy Workshops, pp. 125-128, San Francisco, CA, 2012.
8. Hashizume, Keiko, et al. "An analysis of security issues for cloud computing." Journal of internet services and applications 4.1 (2013): 5.
9. Natasha Csicsmann (Pennsylvania State University – Altoona, USA), Victoria McIntyre (Pennsylvania State University – Altoona, USA), Patrick Shea (Pennsylvania State University – Altoona, USA) and Syed S. Rizvi (Pennsylvania State University – Altoona, USA)."Cloud Security: Implementing Biometrics to Help Secure the Cloud".
10. Data Breach Trends & Stats, Symantec, 2012. http://www.indefenseofdata.com/data-breach-trendsstats/
11. 2012 Has Delivered Her First Giant Data Breach, January 2012. http://www.infosecisland.com/blogview/19432-2012-Has-Delivered-Her-First-Giant-DataBreach.html