Current Threats, Vulnerabilities, Exploits and Recommended Controls to Secure Information in the Cloud

Roy Portas

***Abstract*—The abstract goes here.**

I. Introduction

The Cloud is becoming a larger part of business each year, even companies such as Microsoft who in the past have been focussed on local software applications (such as Windows and Office) is transitioning parts of Office and Windows into the cloud.

With the popularity of the cloud increasing, so are the threats against it. User database breaches on large companies such as Twitter and LinkedIn [1] are becoming more frequent and as those services grow, so will the potential for a hack against them.

II. What is the Cloud?

The Cloud is a term used to refer to a collection of servers on the internet. These servers are owned by companies who rent out the system's resources to customers as 'services'. Most cloud computing companies provide a variety of services, such as database storage (e.g. Amazon RDS [2]), computational power (e.g. Google Compute Engine [3]) and networking (e.g. Google CVN [4]).

These services can be divided into three categories [5]:

- Software as a Service (SaaS)
  SaaS is software applications ran on cloud servers. A company that uses this service only has very limited access to the underlying server, as it is designed to easily host an software application.
- Platform as a Service (PaaS)
  PaaS allows more freedom than Saas, a Paas system generally grants a company control over the database system, networking and the server side software [6]. More control also allows tighter security control, since applications like the database system is now in the domain of the developers.
- Infrastructure as a Service (IaaS)
  IaaS grants the most freedom to the company, as an IaaS system is a complete virtual server. The company has complete control over the entire operating system and allows the developers to freely implement security as required.

IaaS offers the most freedom to the company, thus the most customization of security. Because of this, IaaS services will be the focus of this report.

III. Threats against the Cloud

Most client facing cloud servers are public on the internet, this brings a variety of security concerns. For an IaaS system, these threats can be divided into a few categories.

A. Data Breach

A data breach is one of the most common threats against a server. A data breach is when an attacker accesses sensitive information. This information can come in many forms, such as user accounts and health records.

The Privacy Act 1988 states that Australian businesses are required to ”take reasonable steps to protect the personal information they hold” [7]. Meaning that a data breach can lead to serious consequences for both the business and the customers.

Examples of data breaches include the breach of 100 million LinkedIn user accounts [1] and the breach of 32 million Twitter accounts [8]. This resulted in many users having their accounts defaced.

Data breaches can have serious impacts on customers, thus is a significant threat to a cloud service.

B. Service Hijacking

Service hijacking is similar to identity theft. Service hijacking involves intercepting the login details for a user and gaining access to the service by using the intercepted details. When logged in to the service, the attacker can access the user's information and modify it.

An example of this is hijacking an email account to send spam. Service hijacking is a serious problem to the user as an attacker could potential retrieve all data they store on their account.

C. Denial of Service

A denial of service attack (DoS) is when an attacker sends fake traffic to a server in an attempt to overload it. When a legitimate user connects to the site, the request will fail since the server is busy processing the fake requests [9].

DoS attacks are some of the most frequent, since they are relatively easy to do. Examples of DoS attacks include the recent Census hack [10], where a DoS attack prevented users submitting the census form.

IV. Vulnerabilities

A. *Ease of Use*

Users enjoy a system which is accessible and easy to use. So much so that usability is a large part when designing user facing applications. In order to make the experience more seemless, websites adopt various techniques to streamline the process. For example Single Sign On and persistant log ins. These methods may streamline a user's experience, however thos leads to security vulnerabilties [11].

- Single Sign On
  Single sign on provides a uniform method of authenicating with a service. This method allows users to remember only one password, however if that password is compromised an attacker could get access many accounts at once [12].
- Persistant login
  Persistant login allows user's sessions to be saved to allow user's to access the service later without having to reenter their password. [13]. However if an attacker gains physical access to a device, they can access the all of the user's services without needing to log in.

Overall these methods allow user's easier access to a service, they also provide easy access to an attacker. Thus this vulnerability could open the doors to a possible service hijack threat.

B. *Malicious Employees*

Another possible vulnerability are malicious employees. Generally companies spend considerable resources securing information systems from the outside, however generally they lack the same level of security within the company. This can include giving employees incorrect permissions on file systems and not securing rooms that contain sensitive documents.

This is a significant issue, as a malicious employee could take user's records from a database and leak password. This would cause damage to both the business and the user's of the system.

C. *Virtual Machine Escape*

Virtual machine escaping is a newer vulnerability that has only really emerged with the popularity of cloud services [14].

Virtual machine escaping only occurs on servers that run virtual machines, such AWS [2]. These virtual servers are used by companies to host their websites. If a user of the system can find a way to escape the virtual environment and somehow access another user's environment, they would have complete access to all the files. This is called virtual machine escaping and has already affected some large cloud services providers [15].

This type of vulnerability has potential to cause a lot of damage to many companies, as there could be dozens of virtual machines owned by different companies on a single server. Thus an attacker could compromise many companies at once.

D. *Insecure Cryptography*

Crytography is at the heart of web security. It provides a way of securing communication between the server and clients. This is important as the internet is not a secure communication channel [16], meaning that anyone can intercept messages between the client and server. Thus when communicating over the internet, its important to encrypt sensitive information to ensure it cannot be intercepted by third parties.

For this reason, it is vital to ensure the algorithms used to encrypt the data is secure. However this is difficult, as researchers are always attempting to find new ways to break cryptography algorithms. An example of this is MD5, which was a popular hashing algorithm used on many webpages. When MD5 was created in 1992 it was secure, however over time security researchers have found many security vulnerabilities [17], allowing attackers to easily break the hashing algorithm to break into password databases.

Insecure cryptography is a serious vulnerability to a company and has the potential to cause a lot of damage. Failure to secure cryptography can lead to a data breach and other threats.

V. Threat Mitigation

Cloud services contain valuable information, information which should be protected from attackers. There are common methods of preventing and mitigating the vulnerabilities mentioned earlier. Below is a list of the common prevention methods:

A. *DDOS Prevention*

The most freqeuent attack against companies are DDOSs, with 2016 breaking the record of daily attacks with 1272 attacks on a single day [18]. For this reason DDOS mitigation is important. In order to prevent DDOS attacks, the system needs a way to differentiate between normal traffic and attacks. A common method of doing this is using a statistical model to determine outliers (DDOS traffic) [19].

Once the DDOS traffic is identified, the system needs a way to mitigate the traffic. Generally this involves blocking lists of IP addresses used by the attacker. There are many methods to generate this list, generally they involve using a statistical algorithm to determine if traffic from a source IP is a DDOS attack or general traffic [20]. Some companies, such as Cloud Flare https://cloudflare.com, provide DDOS protection as a service. A company simply needs to change the nameservers to CloudFlare's nameservers and they handle the rest.

B. *Data Breaches*

Data breaches are also a significant threat to companies. According to the ITRC, in 2016 28,574,795 records were stolen through 638 individual attacks [21]. There are many methods to prevent data breaches, one such method [22] involves:

- Use a username and password based login
- Lock the user out of the system after a few failed attempts
- Use one-time passwords when possible

- Use secure encryption algorithms, like Elliptic curve cryptography [23]

VI. Conclusion

References

[1] LinkedIn, "An Update on LinkedIn Member Passwords Compromised," 2012. [Online]. Available: http://blog.linkedin.com/2012/06/06/linkedin-member-passwords-compromised/

[2] AWS, "Amazon Relational Database Service (RDS) AWS," 2016. [Online]. Available: //aws.amazon.com/rds/

[3] Google, "Compute Engine - IaaS," 2016. [Online]. Available: https://cloud.google.com/compute/

[4] ——, "Virtual Network - Your Private Cloud Network," 2016. [Online]. Available: https://cloud.google.com/virtual-network/

[5] IBM, "IBM - What is cloud computing?" Jan. 2016. [Online]. Available: https://www.ibm.com/cloud-computing/what-is-cloud-computing

[6] Interoute, "What is PaaS?" 2016. [Online]. Available: http://www.interoute.com/what-paas

[7] Office of the Australia Information Commissioner, "Rights and responsibilities - Office of the Australian Information Commissioner (OAIC)," 2016. [Online]. Available: https://www.oaic.gov.au/privacy-law/rights-and-responsibilities

[8] LeakedSource, "LeakedSource Analysis of Twitter.com Leak," 2016. [Online]. Available: https://www.leakedsource.com/blog/twitter

[9] Department of Homeland Security, "Understanding Denial-of-Service Attacks | US-CERT," 2009. [Online]. Available: https://www.us-cert.gov/ncas/tips/ST04-015

[10] ABC, "ABS blames overseas hacking attack for census night shambles," Aug. 2016. [Online]. Available: http://www.abc.net.au/news/2016-08-10/australian-bureau-of-statistics-says-census-website-hacked/7712216

[11] Z. Javaid and I. Ijaz, "Secure user authentication in cloud computing," in *2013 5th International Conference on Information Communication Technologies (ICICT)*, Dec. 2013, pp. 1–5.

[12] H. K. Lu, "Keeping Your API Keys in a Safe," in *2014 IEEE 7th International Conference on Cloud Computing*, Jun. 2014, pp. 962–965.

[13] L. F. B. Soares, D. A. B. Fernandes, M. M. Freire, and P. R. M. Incio, "Secure user authentication in cloud computing management interfaces," in *2013 IEEE 32nd International Performance Computing and Communications Conference (IPCCC)*, Dec. 2013, pp. 1–2.

[14] M. Ramachandran and V. Chang, "Recommendations and Best Practices for Cloud Enterprise Security," in *2014 IEEE 6th International Conference on Cloud Computing Technology and Science (CloudCom)*, Dec. 2014, pp. 983–988.

[15] CloudStrike, "VENOM Vulnerability," 2016. [Online]. Available: http://venom.crowdstrike.com/

[16] V. K. Nisha, L. Aliyar, and A. Ali, "An overview of cryptographic solutions to web security," in *2010 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, Dec. 2010, pp. 1–5.

[17] P. Ora and P. R. Pal, "Data security and integrity in cloud computing based on RSA partial homomorphic and MD5 cryptography," in *2015 International Conference on Computer, Communication and Control (IC4)*, Sep. 2015, pp. 1–6.

[18] Kaspersky, "Kaspersky DDoS Intelligence Report for Q1 2016 - Securelist," 2016. [Online]. Available: https://securelist.com/analysis/quarterly-malware-reports/74550/kaspersky-ddos-intelligence-report-for-q1-2016/

[19] N. Hoque, D. K. Bhattacharyya, and J. K. Kalita, "Botnet in DDoS Attacks: Trends and Challenges," *IEEE Communications Surveys Tutorials*, vol. 17, no. 4, pp. 2242–2270, 2015.

[20] S. Yu, Y. Tian, S. Guo, and D. O. Wu, "Can We Beat DDoS Attacks in Clouds?" *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 9, pp. 2245–2254, Sep. 2014.

[21] K. Barney, "2016 Data Breaches," 2016. [Online]. Available: http://www.idtheftcenter.org/2016databreaches.html

[22] N. P. Doe and S. V, "Secure service to prevent data breaches in cloud," in *2014 International Conference on Computer Communication and Informatics (ICCCI)*, Jan. 2014, pp. 1–6.

[23] Y. Rahulamathavan, M. Rajarajan, O. F. Rana, M. S. Awan, P. Burnap, and S. K. Das, "Assessing Data Breach Risk in Cloud Systems," in *2015 IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom)*, Nov. 2015, pp. 363–370.