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 prevent user's submitting the census form.

IV. Vulnerabilities

A. Ease of Use

B. Insecure APIs

C. Malicious Employees

D. Virtual Machine Escape

E. Insecure Cryptography

V. 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