Security Challenges and Solutions in Cloud Computing

Eystein Mathisen
Bodø Graduate School of Business
University of Nordland
N-8049 Bodø, Norway
Email: Eystein.Mathisen@uin.no

***Abstract*—This paper provides a brief introduction to the cloud computing platform and the services it provides. In particular, we intend to discuss some of the key security issues that cloud computing are bound to be confronted with, as well as current implementations that provides a solution to these vulnerabilities. In this paper we have discussed policy, software- and hardware security.**

***Index Terms*—Cloud computing, security, policy, virtualization.**

I. Introduction

The purpose of this paper is to provide an overview of the services offered by cloud computing and some of the most important security issues related to these services.

Although there exist many definitions of the concept of cloud computing [1] [2] [3], a general consensus in both the computing industry and the academia is that cloud computing provides on demand resources and services across the Internet. In addition, this form of computing allows developers to write applications and run them in the cloud itself [4]. There are three types of services that are offered in the cloud today: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These services can be used independently, but they also work hand-in-hand.

Infrastructure provides the hardware where virtual machines are installed. These virtual machines are provided with different operating systems where different software can be installed. Platform (as a Service) provides a higher level environment where developers can write custom applications. Software (as a Service) is an application created and hosted on the Internet.

A. Infrastructure as a Service (IaaS)

Infrastructure as a Service is a way of providing a computer infrastructure to a company, and this product is usually in the form of *platform virtualization*. Some companies buy their own server(s) to host the company's website and services. This server solution can be very expensive and, usually, the company must hire additional manpower to maintain it. The number of requests made to the company server can vary, as well as the idle time of the server. If the server has a high idle percentage, the company could have acquired a smaller server. In the case that the company's popularity increased over night and experienced a rapid increase in demand, the server could fail due to capacity problems. Clearly, this is something that ha a negative impact on the reputation of the company. To prevent such events you can buy a dedicated server or a webhosting package. These packages have a monthly fee you have to pay, and are not dependent on the activity on the server or webpages. So, even if no one is using your services or browsing your webpages, you have to pay the monthly fee.

With Infrastructure as a Service (IaaS) you only pay for what you use, so even if you have a small company or a large one, this would be the perfect "package" for your company. To get a better understanding of how IaaS work, you need a basic understanding of virtual servers, and what the differences between dedicated and virtual servers are. This is discussed in chapter II-B1.

B. Platform as a Service (PaaS)

As the number of the services that is made available in the cloud increases, it is apparent that a platform has to be developed to effectively leverage these services. Platform as a Service (PaaS) is the delivery of an architecture or framework where cloud computing services can prosper. This platform not only provides a place where applications can be stored and deployed, but also an IDE that supports a complete life cycle for developing applications that can be easily made available on the Internet. With PaaS, the cost and complexity of evaluating, buying, configuring, and managing all of the hardware and software needed to develop an application is drastically lowered. This is because the development tools (IDE, GUI Tools, database connectivity, etc.) and delivery tools (hosting, metering, storage, etc.) are made available inside the cloud itself. In this context, the advantage of PaaS is realted to the fact that a customers is not required to invest in expensive hardware or software to develop or make use of the applications offered in the cloud [5].

C. Software as a Service (SaaS)

Software as a Service (SaaS) is a way of providing users with software through the Internet. The combination of using the Internet together with software servies have existed for some time, although the term describing this phenomenon have been rather diffuse until recent years. Some of the most

ISBN: 978-1-4577-0872-5 (c) 2011 IEEE

common uses of these services include email clients (Hotmail, Gmail, etc,), anti-virus scans (Symantec, McAfee, Kaspersky, etc) and word processors (Google Docs, Adobe Buzzword, etc). These applications in it self are not directly a collection of SaaSs, but the services they offer are.

SaaS should not be seen upon as a way of creating software or its underlying architecture. SaaS is more of a business model, which establishes a new way of delivering software. It is about delivering web-based software over the Internet, where the user runs the application in a browser and only pays for the use of the software instead of owning it [6].

The definition of SaaS according to Gartner [7] reads:

> "*SaaS is software that is owned, delivered and managed remotely by one or more providers. the provider delivers an application based on a single set of common code and data definition, which are consumed in a one-to-many model by all contracted customers, at any time, on a pay-for-use basis, or as a subscription based on usage metrics.*"

By using this economical approach to software acquiring, clients can avoid paying large amounts of money on software packages and licenses. The concept of SaaS avoid the known problems of desktop software; system compatibilities, installation difficulties, manual updating, etc. The customer-focused and customer-driven approach is appealing to customers and therefore also to companies [6].

II. Security issues

In most cases it seems that solutions offered in the cloud can be a major advantage to any company who decides to make use of it. But what happens if the provider fails in securing a customer's data? Are there any reasons that companies and individuals should be concerned for the data they send into the clouds? In this chapter we discuss some of the security issues that are related to the implementation of cloud computing solutions, and what some of the providers are doing to mitigate them.

A. Policies

There are a number of important factors that need to be taken into consideration when employing a policy for ensuring security between a cloud hosting provider and a customer (company).

1) Inside threats: Even with the most advanced firewalls and computer security available your computer system will still be vulnerable to inside threats. If your employees can not be trusted, neither can your overall security. It is important for any company to maintain a good sense of supervision and management (governance). External customers may store data sensitive to their business at your cloud hosting site. If any of your employees manage to misuse this data, your cloud computing company will build a bad reputation regarding the level of security offered and certainly loose current and future customers.

One of the world's largest technology companies, Google has invested heavily into the cloud space, and the company recognizes the value of having a reputation for security as a key determinant of success. According to a Google spokesperson, "... security is built into the DNA of our products ..." and "... Google practices a defense-in-depth security strategy, by architecting security into our people, process and technologies" [8].

2) Access control: Cloud computing offer services that may be critical for their users and therefore need to exhibit a high level of availablilty at all times. What is just as important is to keep the data stored at cloud hosting sites accessible only to the users who owns the data. Even though an external customer would most likely want their data to be available for their users only, it is inevitable that the system administrators controlling the cloud hosting sites has access as well. Creating and maintaining a solid confidence between provider and customer is of great importance, in the same way a cloud computing provider need to be able to trust the system administrators working for them.

Authentication and authorization through the use of roles and password-protecting is probably the most common way to maintain access control when using web-browsers to access cloud computing sites. A more efficient way to ensure adequate security is to facilitate an additional authentication factor outside of the browser (in addition to username/password). This is essentially multi-factor authentication, but available options today are rather limited when considering requirements of scalability and usability [9]. An example of this put into use is BankID, which has been developed by the banks in Norway for use by private persons, authorities and companies. In short, BankID is an electronic ID and service that offers secure electronic identification and signatures on Internet [10].

3) System portability: A major future concern for cloud computing customers is vendor lock-in. There are no current cloud computing standards for elements and processes such as APIs, the storage of server images for disaster recovery, and data import and export. If a company is dissatisfied with one cloud computing service - or if the vendor goes out of business - the firm cannot easily and inexpensively transfer these services to another provider or bring it back in-house. Instead, the company would have to reformat its data and applications, and transfer them to a new provider, a potentially complex and costly process. Furthermore, if the company brings the service in-house, it would have to hire employees with the skill necessary to work with technology [11].

In the future it will be important to settle on open standards, in order to avoid problems such as vendor lock-in and incompatibility. One of the largest initiatives surrounding open standards have been made through the Open Cloud Manifesto [26], although some of the largest companies with interest cloud computing have reluctant to follow through with such standards as they find them overly restrictive [8].

B. Software security

Software security is an important aspect since software are programs written by all kinds of people, and some are actually free. Free software are usually open source software, so you

ISBN: 978-1-4577-0872-5 (c) 2011 IEEE

as a developer or a hacker can access the code and find bugs. One consequence of this is that users always should run the latest versions of their programs and services.

1) Virtualization technology: Basically, virtualization allows abstraction and isolation of lower level functionalities and underlying hardware. This technology refers to the service running on the host operating system that makes virtualization possible. There are several virtualization products available, for instance Xen, OpenVZ or VMware to mention some. Which one you choose is up to you. If you are going to use the open source product such as Eucalyptus [12] - a software infrastructure for implementing cloud computing - you have to use Xen on all you nodes. Some virtualization products require that your CPU supports virtualization (Intel VT and AMD-V) such as KVM [13]. There are a number of security issues related to the use of different virtualization products such as Xen [14] [15] [16]. The technique most commonly used is to modify the hypervisor on the host operating system, and modifying it in a way so that the attacker can access it directly and the hacker can install a rootkit on it. To protect against this, you should always have an up to date version of your virtualization product and check on your product's website about vulnerabilities and how to patch them. When using virtualization technologies you also get security, since each virtual server are isolated from each other [2].

2) Host operating system: You need a host operating system that is easy to use, install and maintain. It is extremely important that this operating system is as secure as it can be and always up to date, since this is one of the "holy grails" for a computer hacker. If a hacker controls the host operating system, he or she also controls all the guest operating systems on that computer.

To protect your company's host operating systems, you should choose a minimal operating system that is stripped for all unnecessary services. Keep in mind that this is one of the most important parts of your cloud, so the advice is to keep it up to date at all times.

3) Guest operating system: Each customer in your cloud can create, modify and delete their virtual private servers (VPS). One of the benefits of using virtualization is that you can choose what kind of operating system you want. This is something that results in many different operating systems on a single physical machine, and it is easy for a hacker to find vulnerability in one of the operating systems. Each customer is responsible for their own virtual machines, so they have to update and patch the operating system and all the software on their own. This is something, along with default configurations, that lead to security holes that can be exploited by an attacker. Another issue with the guest operating systems is that the customers usually uses a *httpd* such as Apache, with an open and free website solution such as Wordpress [17]. Recently, it has been noted that Wordpress have experienced a number of security exploits [18]. There is no easy way of protecting your customers from themselves, but you can inform them about the importance of having an up to date operating system and the latest version of the services and products (e.g. Wordpress [17]). Another benefit from using virtualization is that all the operating systems are isolated from one and another, so if a virtual private server is hacked, then none of the other VPSs will be affected by this.

4) Data encryption: The company that hosts your VPS can access your company's data, since they have full access to the host operating system. To protect your company's data you should enable encryption on all your data, including your swap-partition [4]. Transferring data is also very critical, since other can listen to the network and intercept information that is being transferred. To protect against this, you should encrypt your data stream using SSH-tunneling or VPN [19].

C. Physical security

To maintain a satisfying level of software and policy security it is important to have a strong physical security in place. Without physical security your hardware components may be attacked by people or natural disasters, regardless of the level of internal software and policy security.

1) Backup: To begin with, relying totally on the cloud service providers to keep a backup of critical data can be considered rather foolish. It is still critical that a company or an individual keeps an offline backup of all their files. Although cloud providers offer geographic redundancy on data on the Internet to enable high availability, one still has to be prepared for the unexpected. What if a company suddenly is forced to switch provider because the provider goes out of business, or because the provider's service level has degraded? For the customers, it is important that issues or scenarios such as these are brought up before signing any legal contract.

Up to this point, the providers' point of view regarding backup strategies is unclear. Either a backup plan is provided automatically for each customer, or they can use the plans provided elsewhere in the cloud such as Amazon's S3 (Simple Storage Service) [20]. In this case, a customer chooses which data should be backed up as well as the appropriate level of data mirroring.

It is also possible for a cloud provider to make use of Continuous Data Protection (CDP) [21]. This is common in online project planning solutions where every version saved by a user is stored as a copy in the server allowing for restoration of data at any given point in time.

Cloud computing makes use of virtualization because of cost efficiency and better resource utilization. In this case, a customer is given an instance or a part of a virtual machine. This instance is saved as an image file, and can easily be copied for backup purposes.

For both providers and customers, it is important that the issue of data portability is disclosed to avoid vendor lock-ins. Apart from that, with the use of virtualization, it is possible for a customer's data to commingle with other data from other customers. Here, it is important that logical segregation of data is validated.

2) Server location: There are many factors that must be considered when it comes to the security of the physical machines. Depending on the number of servers to be protected,

ISBN: 978-1-4577-0872-5 (c) 2011 IEEE

the room should provide adequate space. This room should be isolated. Its floors should have anti-static finishing, and should not have windows for security, sound and environmental reasons.

The room should make use of racks with seismic bracings, and should be properly grounded. A fire suppression system should be installed, as well as cooling systems to avoid the machines from overheating.

All entrances to the room should be properly secured and alarmed where appropriate. Not only does this room need security for illegal access, it should also have alarms related to the functioning of the A/C system.

Emergency or backup power should also be in place, and a separate emergency power shutdown for this room should be highly considered.

3) Firewall: Any cloud computing service providers should provide a complete firewall solution to their clients. This is the case for AmazonÂ´s Elastic Compute Cloud (EC2) [22]. A mandatory inbound firewall is configured to default deny mode and a must customer explicitly open a port to allow incoming traffic. This traffic may be restricted by protocol, by service port, and by IP address.

The control of the firewall remains in the EC2 system and not on the host (instance). For a customer to be able to change settings for his instance, a customer's x.509 certificate [23] and key is required. This setting allows for another layer of security.

Amazon also encourages their customers to apply additional per-instance filters with host-based firewalls such as IP tables. This mechanism allows for the restriction of both inbound and outbound traffic on each instance. EC2's firewall can also be configured to different classes of instances to have different rules.

One of the most important tasks of a firewall is to protect against *ddos* and *dos attacks*, since everyone can connect to the cloud. Cloud computing companies are very vulnerable to these type of attacks, as they can shut down services they offer to their customers [24].

One way to ddos a server is by using packet flooding ddos attacks. A simple way to defeat this type of attack is to check whether the source ip-address is invalid. Another protection that firewalls should offer is reverse firewall. This is used to prevent an attacker to create a connection from your VPS to an external server [25].

III. Conclusion

Cloud computing is a large and complex field which includes hardware, software and the security surrounding it. In the end, the success or failure of cloud computing services is related to whether or not users feel confident that a cloud solution that holds their software, data and processes, offers services that are highly reliable and available, as well as secure and safe, and that privacy is protected.

In this paper we have discussed the most vital parts to ensure a secure environment. This includes a basic view on security policies, hardware and software security. We can probably expect a high degree of cloud computing in the future. This will again bring it to attention to hackers as a potential target, as you will find a large amount of resources stored at these cloud hosting sites.

Another important issue for the future is the use of open standards to avoid problems such as vendor lock-in and incompatibility. Furthermore, there are no security standards specific to cloud computing. Security is often addressed too late when adopting cloud computing technologies. Nevertheless, you can usefully apply conventional security concepts. One of the largest initiatives surrounding open standards have been made through the Open Cloud Manifesto [26], although some of the largest companies with interest in cloud computing have been reluctant to follow through with such a standard as they find it restrictive.

References

[1] Erdogmus, H.: Cloud Computing: Does Nirvana Hide behind the Nebula? IEEE Software. **26** (2) (2009) 4–6.

[2] Vaquero,L.M., Rodero-Merino, L., Caceres, J., Lindner, M.: A Break in the Clouds: Towards a Cloud Definition. ACM SIGCOMM Computer Communication Review. **39**(1) (2009).

[3] Hayes, B.: Cloud computing. Communications of the ACM. **51** (7) (2008).

[4] Grossman,R.L.,: A quick introduction to Clouds. Open Data Group. Technical Report No. 1, 2008.

[5] The CTO forum: PaaS can help foster innovation. http://www.thectoforum.com/index.php?option=com_content&task=view&id=237&Itemid=53, December 2008.

[6] Hoogvliet, M.T.: SaaS Interface Design. Designing web-based software for business purposes. thesis in Communication and Multimedia Design, Rotterdam University (HRO), The Netherlands. (2008)

[7] Gartner: Market Trends: Software as a Service, Worldwide, 2007-2012. September 2008.

[8] ComputerWeekly.com: Top Five Cloud Computing Security. http://www.computerweekly.com/Articles/2009/04/24/235782/top-five-cloud-computing-security-issues.htm#6,April 2009

[9] Chou, D.: Cloud Computing and User Authentication. http://blogs.msdn.com/dachou/archive/2008/08/19/cloud-computing-and-user-authentication.aspx, August 2008

[10] BankID: What is BankID? http://www.bankid.no/index.db2?id=4481, 2005

[11] Leavitt, N.: Is Cloud Computing Really Ready for Prime Time? IEEE Computer. **42**(1) (2009).

[12] Eucalyptus: http://open.eucalyptus.com/. Accessed May 2009.

[13] KVM. Kernel-Based Virtual Machine: http://www.linux-kvm.org. Accessed May 2009.

[14] Black Hat USA: Subverting the Xen hypervisor. http://blackhat.com/html/bh-usa-08/bh-usa-08-speakers.html#Wojtczuk, 2008.

[15] Black Hat USA: Detecting and Preventing the Xen Hypervisor Subversions. http://blackhat.com/html/bh-usa-08/bh-usa-08-speakers.html#Rutkowska, 2008.

[16] Black Hat USA: Bluepilling the Xen Hypervisor. http://blackhat.com/html/bh-usa-08/bh-usa-08-speakers.html#Tereshkin, 2008.

[17] WordPress.org: http://wordpress.org. Accessed May 2009.

[18] MILWORM: Wordpress vulnerabilities. http://milw0rm.com/search.php?dong=wordpress. Accessed May 2009.

[19] Vouk M.A.: Cloud Computing - issues, Research and Implementation Journal of Computing and Information Technology. CIT 16, **4** (2008) 235–246.

[20] Amazon Web Services: Amazon Simple Storage Service (Amazon S3). http://aws.amazon.com/s3/. Accessed May 2009.

[21] SearchStorage.com Definitions. http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci1015407,00.html. Accessed May 2009.

ISBN: 978-1-4577-0872-5 (c) 2011 IEEE

[22] Amazon Web Services: Overview of Security Processes. White Paper. September 2008. http://s3.amazonaws.com/aws_blog/AWS_Security_Whitepaper_2008_09.pdf
[23] IETF.org: RFC 4158. Internet X.509 Public Key Infrastructure: Certification Path Building. http://tools.ietf.org/html/rfc4158. (2005)
[24] Mansfield-Devine, S.: Danger in the clouds. Network security. December 2008.
[25] Cs3 Inc.:The Reverse Firewall: Defeating DDoS Attacks Emerging from Local Area Networks.
http://www.cs3-inc.com/rfw.html. Accessed May 2009.
[26] Open Cloud Manifesto: http://www.opencloudmanifesto.org/. Accessed May 2009.

ISBN: 978-1-4577-0872-5 (c) 2011 IEEE