EXPLORE
iJET International
Journal of Engineering & Technology
CENTRE OF PROFESSIONAL RESEARCH PUBLICATIONS
ISSN 2049-3444

Prepared for the Cloud

Nigel McKelvey, Eamonn Houston-Callaghan
Letterkenny Institute of Technology, Port Road, Letterkenny, Co Donegal, Ireland

ABSTRACT

Cloud computing is currently a hyped word in IT. This paper examines the capabilities and vulnerabilities of the cloud. In particular, it examines the security issues that exist in the cloud that businesses are concerned about when moving to the cloud. Steps have been taken to standardise the cloud and provide consumers with confidence in the service. The purpose of this paper is to examine some of these security issues and provide suggested alterations to the curriculum for secure programming modules in order to resolve or reduce the impact of the issues on the client.

Keywords: *Cloud, security, CABLE, Botcloud, legal*

1. THE CLOUD AS A WEAPON

Cloud computing is not just appealing to enterprises. It also offers hackers a whole new playground that is full of potential. Hackers will always find new ways of committing fraud. Consider what the cloud has to offer. For an enterprise, they get access to a vast amount of resources should they require it. Traditional distributed denial of service attacks (DDoS) that try and flood a server and take it down will end up failing, as the cloud will provide more servers if requires. A DDos will obviously raise a company's expenditure, as it would cost them money to gain more servers. This does not satisfy the hacker however. Ironically, they have used the cloud as a weapon to not only get around this problem, but also create new problems for companies.

By renting a basic service from a cloud provider, a hacker has access to as much computing power as he or she desires. Already this has been used for spamming and DDoS that has brought down many websites in just seconds. Many of these attacks are going unnoticed, as cloud vendors wish to keep any negative effects of the cloud quite (Pacella R, 2011). However hackers have created a new way of hacking systems. They use the cloud as a weapon to succeed in their attempts to hack businesses and organisations. One such weapon that highlights the potential danger of the cloud, are BotClouds.

BotClouds are an evolved version of Botnets. In the past, hackers would have to slowly build up an army as such of computers and wait for the right time to use it to unleash spam and DDos attacks on servers. A cloud Botnet can be easily be purchased and created in an instant. Aron (2011) describes how a handful of colleagues in University of Technology in the Netherlands were able to create a BotCloud of 20 computers from a provider and use it to attack their own server. Within 10 seconds, the server was brought down. Whilst the idea seems somewhat fictional, BotClouds is a worrying trend that will only grow if cloud vendors do not take action to try and prevent it. Computing will always remain a battle between hackers and authorities. The cloud is just the latest playing field for the battle to commence. With the growing popularity of cloud, it seems likely the cloud will be continue to present opportunists with the chance of committing fraud. This issue will remain in the hands of the provider to deal with, unless of coarse the company is running their own cloud. One issue that remains the responsibility of the consumer, regardless of how their cloud is deployed, is legality.

2. LEGAL ISSUES

Consumers of cloud services must remember that they are solely responsible for their data in the cloud and "cannot shift blame to their cloud service provider if things go wrong" Ashford (2011). The legal risks of cloud computing are often overlooked by consumers. An organisation can not use the cloud to defend any cases that they face. As (Rosenbaum D, 2011) quipped, "The cloud ate my evidence" will not be a valid answer in court. The first line of defence to combat any legal issues is the service level agreement (SLA). Once a company has selected a cloud provider, they must form a contractual agreement with them, the SLA. The SLA will outline the cost of service, what service the cloud will provide etc. It is important for any company to ensure the SLA meets their needs and also provides a clear understanding of any events that could lead to legality issues, such as outages or closure of the cloud. The SLA is an import agreement not just for legal issues, but also for any of the other risks of the cloud. Companies should learn from previous experiences that could arise in the cloud. The two main areas that legal issues revolve around are Audibility and Data Location.

Legal issues in the cloud will continue to develop in the coming years. In IT in particular, the law is always behind and struggles to keep up with the rapid change. Currently, there is very little, if any, law on the use of cloud computing. For now, companies will have to ensure they are covered as best possible from potential legal issues. As mentioned earlier, companies must ensure their cloud service provider has taken every action to prevent such incidents from happening. As well as that, the cloud should provide a plan to respond to any of these incidents, should they arise. However, trusting the service provider is ultimately the crux of cloud computing. This has lead to the development of potential solutions to resolving the issues themselves by the clients themselves.

3. RESOLVING ISSUES WITH CLOUD

How do can you resolve issues that are not in your control? Consumers often look at the provider when issues in the cloud arise. While it is fair to say that the providers have a responsibility to provide a secure service, clients must first ensure that the application they wish to host on the cloud is secure. Deploying an unsecured application to any server, whether it is in house or cloud, would create problems. While this may seem very obvious, it is an important point nonetheless to make. Vulnerabilities in software cost money when compromised. Microsoft recently reported in their intelligence report that application vulnerabilities accounts for 71.5 percent of all vulnerabilities disclosed (Microsoft, 2011). A typical opinion is that Java is a secure programming language that was developed to overcome security issues of preceding languages, such as C++. While this may be true, the Java language is not fully secure. Security vulnerabilities exist in common packages that are used in the majority of web applications today (Livshits and Lam, 2005). That is not to dismiss the use of the Java language, as its easy to code security features has made it a very popular programming language for many businesses today.. While Java is a secure language, that does not exempt it from malicious attacks such as SQL Injections and cross-site scripting. Logical programming errors can also create vulnerabilities (Livshits and Lam, 2005). Java is only secure if it is securely written, which is fundamental in the development of any software artefact. This involves ensuring that the correct access control is set for classes and methods and ensuring that classes are not immutable.

4. EQUIPPING STUDENTS

Providing students with the necessary skills is essential if gaduates are to be capable of identifying and dealing with these issues/vunerabilities. With regard to developing core secure programming skills, students should be able to implement code that deals with providing appropriate access visibility to classes/methods/variables, be able to facilitate trust boundaries, remove inference from thrown exceptions, understand the dangers of dynamic SQL, have the ability to interpret untrusted code, isolate unrelated code, be familiar with subclass behaviour, implement mutability correctly, code defensibly against partially initialized instances, avoid serialization, implement the Security Manager and comprehend context transformation.

Messages being intercepted and manipulated can have serious repurcussions for a company who deal with Internet Protocols (IP) and network management (Rabah K,2005). Being capable of implementing correct encryption is paramount to any secure programmer.

Producing students with programming skills in these areas will ensure that their future employers will have considerably safer applications. Not implementing these skills into a module at third level would be doing considerable injustice to the students themselves.

Research to date has highlighted an area of interest with regard to teaching computer programming in an online environment. The use of Cognitive Apprenticeship-Based Learning Environment (CABLE) in the teaching of Java programming has been adopted in recent times (Ioana C et al, 2006). The pedagogical model used employs a combination of instructional strategies including directive support, responsive cognitive apprenticeship, collaborative learning, stimulating metacognition (organising, motivating, modifying ones own skills), and using various technologies via the use of online discussion though BlackBoard.

5. CONCLUSION

In conclusion it is important to state that colleges and universities have to develop a curriculum for IT which will facilitate their marketability as well as their functionality in the educational and industrial markets. (Tomas M et al, 2011). Using and incorporating Virtual Learning Environments (VLE) into a curriculum can help catapult a previously mundane module into the 21st Century. Within this "virtual reality", both the facilitator and the students can partake in a variety of curricular and extra-curricular activities (Lawless-Reljic S, 2011). This modern inclusion is a must moving forward when developing a curriculum for IT. A facilitator could easily teach elements of securing programming via this method which would obviously provide the students with instant feedback, thus ensuring bad habits are never started.

The popularity and adoption of the cloud will certainly grow as the leading IT players, such as Apple, Amazon and Microsoft are promoting the benefits of going cloud. Certainly, the potential of cloud can lead to computing becoming a service for everyone. Baker (2007) mentioned the idea of a company, such as Google, becoming the world's primary computer. However, the issue of security is still a major part of the cloud. With every business decision, come the risks. Any company considering the cloud must understand the risks involved. Essentially, the companies are handing over their data without the responsibility associated. Clients are given little protection and until a standardisation enforces better protection, it is up to the client to cover themselves.

The vendor should provide answers to key questions, such as the location, how the data is stored, access control and an emergency plans for when a catastrophe occurs. These questions should be answered in the SLA. If they are not, it would be wise to look at another vendor that will provide the answers.

The main issue with the cloud is trust. Trust is the umbrella that privacy, legality and indeed the adoption of cloud lie beneath. The future of the cloud rests upon the providers. They must build up a trusted service by embracing standardisation, liaising with clients and most importantly, securing the cloud that they deliver.

REFERENCES

[1] Aron J (2011). *Beware of the botcloud*. New Scientist, pages 24–24.

[2] Ashford W (2011). *Securing the cloud*. Computer Weekly, pages 16–20.

[3] Baker S (2007). *Google and the wisdom of the clouds*.URL http://www.msnbc.msn.com /id/ 22261846/.

[4] Ioana C, Wing AU & Yates G. (2006). *The Impact of CABLE on Teaching Computer Programming*. Proceedings of the 2006 conference on Learning by Effective Utilization of Technologies: Facilitating Intercultural Understanding. http://www.unisanet. unisa.edu.au /edpsych/ research/ CABLE2.pdf [Accessed online 3rd April 2012]

[5] Lawless-Reljic S (2011). The Effects of instructor-Avatar Immediacy in Second Life, an Immersive and Interactive 3D Virtual Environment. *Eleed*. Vol. 7. (urn:nbn:de:0009-5-30747).http://eleed. campussource .de / archive /7/3074

[6] Livshits B and Lam M (2005). *Finding Security Vulnerabilites in Java Applications with Static Analysis*. URL http://suif.stanford. edu / papers / usenixsec05. pdf.

[7] Microsoft (2011). *Microsoft Security Intelligence Report*. Technical report. Volume 11.

[8] Pacella R (2011). Hacking the Cloud. *Popular Science*, pages 68–71.

[9] Rabah K (2005). Secure Implementation of Message Digest, Authentication and Digital Signature. *Information Technology Journal* 4 (3): 204-221, ISSN 1812-5638

[10] Rosenbaum D (2011). *Cloud Control*. CFO, pages 31–34.

[11] Tomas M & Castro D (2011). Multidimensional Framework for the Analysis of Innovations at Universities in Catalonia. *Educational Policy*. Vol/Issue: 19 (27). ISSN 1068-2341. Spain