2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks

A Layered Security Approach for Cloud Computing Infrastructure

Mehmet Yildiz[¥], Jemal Abawajy[£], Tuncay Ercan[§] and Andrew Bernoth[¥]
[¥]Global Technology Services, IBM Australia, Melbourne, Australia
{myildiz, bernoth@au1.ibm.com}
[§]Department of Computer Engineering, Yasar University, Izmir, Turkey
tuncay.ercan@yasar.edu.tr
[£]School of Engineering and Information Technology, Deakin University, Geelong, Australia
jemal.abawajy@deakin.edu.au

Abstract - *This paper introduces a practical security model based on key security considerations by looking at a number of infrastructure aspects of Cloud Computing such as SaaS, Utility, Web, Platform and Managed Services, Service commerce platforms and Internet Integration which was introduced with a concise literature review. The purpose of this paper is to offer a macro level solution for identified common infrastructure security requirements. This model with a number of emerged patterns can be applied to infrastructure aspect of Cloud Computing as a proposed shared security approach in system development life cycle focusing on the plan-built-run scope.*

Key words: Cloud computing, Grid computing, Utility computing, Dynamic infrastructure, Security, Virtualization, Service Oriented Architectures.

1. INTRODUCTION

Cloud computing is a class of the next generation highly scalable distributed computing platform in which computing resources are offered 'as a service' leveraging virtualization and Internet technologies. Cloud-based services include software-as-a-service (SaaS) and platform as a service (PaaS). Amazon's Elastic Compute Cloud (EC2) [24] and IBM's Blue Cloud [23] are examples of cloud computing services. These cloud service providers allow users to instantiate cloud services on demand and thus purchase precisely the capacity they require when they require based on pay-per-use or subscription-based model.

Cloud computing is receiving traction with businesses and has become increasingly popular for hosting data and deploying software and services. Fig. 1 shows Cloud computing in trends as reported in Google trends. It is obvious that cloud computing (blue line) has outpaced Grid computing (red line). The attractive part of the cloud computing is that it enables customers a way to increase capacity or add capabilities on the fly without upfront investment in new infrastructure, personnel training, or software licensing drastically boost their infrastructure resources, all at negligible cost.

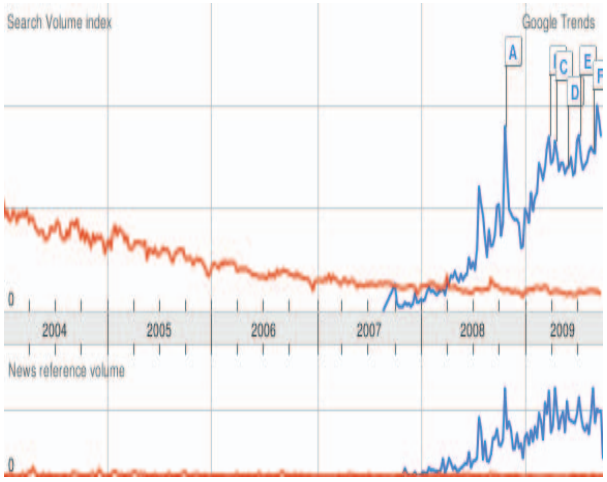

Figure 1. Cloud computing in Google trends

Although cloud computing provides a number of advantages that include economies of scale, dynamic provisioning, increased flexibility and low capital expenditures, it also introduces a range of new security risks [22]. As cloud computing brings with it new deployment and associated adversarial models and vulnerabilities, it is imperative that security takes center stage. This is especially true as cloud computing services are being used for e-commerce applications, medical record services, and back-office business applications, all of which require strong confidentiality guarantees. Thus, to take full advantage of the power of cloud computing, end users need comprehensive security solutions to attain assurance of the cloud's treatment of security issues.

This paper introduces a practical security model based on key security considerations by looking at a number of infrastructure aspects of cloud computing. The paper offers a macro level solution for identified common infrastructure security requirements. This model with a number of emerged patterns can be applied to infrastructure aspect of cloud computing as a

978-0-7695-3908-9/09 $26.00 © 2009 IEEE
DOI 10.1109/I-SPAN.2009.157

proposed shared security approach in system development life cycle focusing on the plan-built-run scope.

The rest of the paper is organized as follows. In Section 2, we identify security concerns arising in cloud computing environments and present related work. A policy-based and layer infrastructure security is discussed in Section 3. We also present a dynamic infrastructure security model.

2. BACKGROUND AND RELATED WORK

Many of the previous work in the field of cloud computing have been in the areas of its technological architecture and features, differences from other similar technologies and security issues. Regardless of what technology is being used, people generally look for the most important criterion which is security to adopt it while many other smart environments like utility computing, smart data centers, pervasive computing, automation, virtualization and intelligent networks already penetrate into our daily life [3]. Cloud computing builds different services in business, education and government sectors and becomes a new term together with the latest networking, web and software services [4]. Cloud computing inherits the advancements and limitations in other computing research areas aforementioned above.

In cloud computing environment, overall security issues can be evaluated from the points of service providers and the clients. While the providers focus on the continuity of their services against configuration updates for performance and QoS, spam and virus threats and proper customer accountability, clients mainly look for the security of their data and the reliability of the provider. The basic features of cloud computing are presented and compared with the computational resources used in Grid Computing [5] together with the required security architecture [6] incorporated firewalls, intrusion detection/prevention systems, antivirus, authentication, authorization, access control, encryption and other services. Although Cloud Computing maintains their own software services, it brings serious responsibility to service providers to ensure the security of business applications.

Customers who are the most important element of cloud computing are the end users with the fixed or mobile device browsers. Web services platform is the largest implementation methodology and requires a robust security policy. Reference [7] presents a framework for designing security aspects in Service Oriented Architectures (SOAs) and Web services. With the development of web services application, some issues of web services security are increasingly prominent. XML based policies [8] [9] were proposed as the core of web services security technology. Using different web applications covered by the cloud service providers requires certain security of qualifications. A Role-Based Access (RBAC) model for authorization using secure web services [10], a context based dynamic role based access control model (CDACM) for web services [11] and proxy-based security architecture that provides authentication and authorization [12] are proposed for the management and the enhancement of security goals in web services. Reference [13] also proposes a formal model on policy-based access control framework for autonomic systems.

Cloud also provides data storage in its web space for the customers. Even though the storage of user data on remote servers is not new, current emphasis on the expansion of cloud computing is whether it has drawbacks for ensuring data privacy, confidentiality and reliability. The General File System (GFS) introduced in [14] integrates different storage spaces and promises the data security. The privacy challenges that software engineers face are assessed and key design principles are suggested in [15].

System and web administrators who served in the cloud service providers want to ensure that their web services meet the security requirements of their information systems. A methodology for decision support system (DSS) proposed in [16] presents a systematic assessment model based on the Common Criteria for Information Technology Security Evaluation and helps Information System managers in making the right decision for security issues.

Cloud providers allow users to access information and business processes with specialized permissions. This means the open flow of information and trust relationship between the cloud and the client. The trust management models with their limitations are defined and compared in [17] [18] and [19].

There are some other additional security trends which present efficient solutions for the security of SaaS applications. Therefore, security requirements strongly influence the architectural design of Information Technology (IT) services like non-functional requirements. Reference [20] proposes a method that combines security and software engineering approaches to set up proper security architecture in the organizations.

3. POLICY BASED AND LAYERED INFRASTRUCTURE SECURITY

Defining a structured policy based security system has proven to ease the creation and use of a cloud computing environment. Policies are required to be defined for each actor in the cloud computing environment. Administrators will be required for network, system and storage components. Then additionally separate policies are required within each instance of a cloud computing virtual system.

Defining the security policy of which actor can define cloud systems and the connectivity of these systems reduces the churn during service creation. Initial deployments of cloud computing followed a traditional change management process including items such as impact assessment and vulnerability scanning before allowing they new virtual system to go live. It was soon realized this defeated one of the primary requirements of cloud computing that of speed of deployment. Therefore each image passed a set of stringent controls before being placed in the cloud options. These included vulnerability assessments, vastly streamlining the ability to deliver a cloud system in a timely manner.

Since each sub-system will require downtime for upgrades or replacements as systems improve and systems will need to be added as the cloud service matures. The change management process had to be altered to allow capacity management to install new physical resources, systems, network, and security, according to capacity forecasts. This necessitated an actor to work with capacity planners and provide authorization to deploy new equipment.

Each organization subscribing to the cloud computing service will also require policy based security. Typically a minimum of two policy types were required, these defined actors as:

- A cloud service administrators or developer
- The organization's end users.

Flexibility in allowing organizations to define their own actors and related security policies assisted in the growth of the cloud services.

Security needed to evolve from protecting the edge of the network from unauthorized access into a layered security approach. Users were becoming more aware of computing and want the flexibility to initiate compute processes on their workstation to enable them to complete their task quickly.

3.1 Network layer

While the network layer had traditionally provided security at layer-3 and layer-4. Experience soon showed that other services were being run on previously approved ports" simply to bypass the approval process to enable a new service.

Within cloud computing it was clear that layer-7 aware security needed to be installed in the network. Today many different systems are used to provide this security need, An Intrusion Prevention Device (IPS) was placed in line and provided analyses of traffic against potential intrusion attempts.

The cloud environment was configured to drop packets based on a known signature, whereas alert on packets identified by the heuristic engine. The network security actors were then engaged to provide monitoring and updates in a timely basis. Again the network security actors needed to know who to alert given a certain class of intrusion event.

Working closely with the cloud on-boarding process each client on the cloud environment could then define a security contact. Similarly, an approved client system administrator could advise the network security actors of an expected change in system activity. For example a retail client with a promotional offer only available in a given time period was seen to increase network activity well past historical usage. Prior knowledge of this event allowed the network security actors to confirm the heuristic traffic alerts for that time period were within the expected usage.

3.2 Process hosting layer (Servers)

Virtualization of systems can result in competitors using separate virtual machines on the same physical hardware. While larger computing systems, e.g., mainframes, have been capable of providing secure separation, the cost of these platforms was not always acceptable to the SaaS providers. This is where lower cost equipment was introduced to the equation with emerging virtualization capabilities.

Most of the mainstream virtualization systems have now achieved security certification by one of the authorized labs. It is still a major decision point in deploying a virtual environment.

Another issue at the process hosting layer is the ability to move processing and data from one physical system to another. Change is inevitable whether it is hardware, firmware or software upgrades. The provider of cloud compute services must be able to seamlessly migrate such processing from one system to another, allowing the users to continue working without interruption.

Coexisting different sectors also proved problematic. When manufacturing sector have a quieter time is not always the same as the retail sector client. This created issues in applying security patches, to shared equipment.

3.3 Storage layer

Whether for data backup or storage for processing, the cloud enables the mixing of cloud user's data. The storage and backup systems needed to provide sufficient security to ensure cloud user data is not compromised. It is unacceptable for one user to be able to access another user's data or backup.

Most commercial grade storage systems allow for this separation today. Similarly, any off-site backup must ensure security. One of the most prevalent options today is to enable data encryption on movable media such as tapes. As with all encryption facilities the encryption keys must be stored in a secure manner. Facilities exist to escrow parts of the encryption key

among multiple escrow agencies. This separates the encryption key so no single agency has the entire key.

3.4 Systems management layer

In any managed environment security at the systems management layer is an area of concern. This is no different in cloud computing, perhaps even more important. Various teams around the globe (or within the borders of your cloud) virtualization of systems is also touching on virtualization of the network. More systems are including network equipment which then leads to the separation of duties. Should the network team have access to the systems management platform to provide network management? Should the system operators have the responsibility of controlling the network equipment?

Typically we have seen a separation of duties with combined change management. While this expands the number of users with management access it does allow for teams to specialize in their fields. Specialization is desired in the cloud environment to ensure the best configurations are available to all end-users.

3.5 Application layer

Since application is a separate domain and a comprehensive area from security perspective, the application layer is excluded in this paper. However, it will be presented in a different paper by the same team related to this model to complete the security model.

4. DYNAMIC INFRASTRUCTURE SECURITY MODEL

Figure 2 illustrates a dynamic security model which we propose to use for the solutions of cloud computing infrastructure [21]. This model emerged through practical experience of authors in developing solutions for utility based and service oriented projects in a number of large scale global initiatives. This model is based on 8 aspects. It includes 4 layers: Network, Storage, Servers and Applications. It includes one enterprise level principles at the highest level and a systems management aspect. It also includes two kinds of dynamic security types: horizontal and vertical.

The horizontal type is specific to each layer end to end. For example, horizontal dynamic security policy for storage does only cover the security objects related to storage. The vertical type is designed to cover the interfaces between layers. For example some security objects between servers and storage may be partially belong to each layer. The vertical dynamic policies ensure that any common object or exceptions are covered.

For the horizontal policies, each layer, based on its detailed security elements, can be configured with policies from lowest to the highest in terms of security hardening. For example a hardened policy can be categorized as level 1 in the lowest part of the scale and level 10 in the highest end based on the sensitivity of the specific layer for a specific business solution. Usually network is the most sensitive component in cloud computing projects due to myriad of virtual connections and external interfaces providing the required business connectivity.

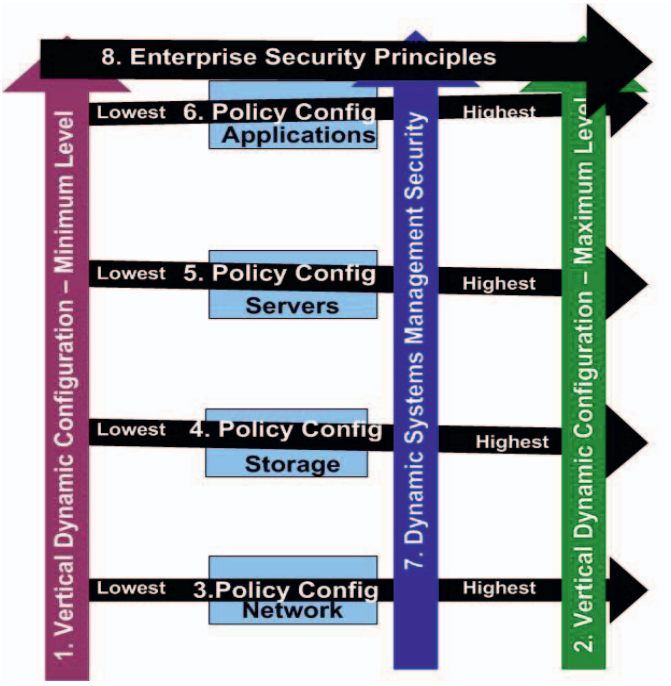

Figure 2. Dynamic System Security Model

Dynamic configurations are designed using security objects. A security object is an infrastructure component requiring protection in a specific security context. For example wireless connectivity between two nodes is a security object. User authentication to access to a service is also another security object.

Linkage and integration of security objects are essential to maintain required level of security in cloud computing. Simply put, a system is as strong as its weakest point.

The dynamic security model is not only designed to cater needs of production environments but also to support other environments in the life cycle of a cloud computing project. Using such a dynamic model from development, test, support and production environments make it cost effective and also produce good results for required security.

The implementation of a dynamic configuration requires automation of tools and processes. There are already a number of useful tools automating the infrastructure security available in the market. Based on parameters provided by the changing business requirements, these tools can customize the security solutions scaling both vertically and horizontally for the

required security levels in all system life cycle environments.

5. CONCLUSION

A well established dynamic security model for the infrastructure of cloud computing solution is essential. The dynamic model introduced in this paper offers a horizontally and vertically configurable and policy based security approach. This paper focuses on the infrastructure scope covered within the domains of network, servers, storage and systems management. These domains protected using both horizontal and vertical policies. Application security is excluded and beyond the scope of this paper. Applying dynamic security policies using automated tools and processes contribute to the security of cloud computing in a positive manner in terms of cost, systems management and end user satisfaction for large scale projects in enterprises.

6. REFERENCES

[1]. B. Hayes, "Cloud computing", Communications of the ACM, vol. 51, no. 7, pp. 9-11, July 2008. Retrieved July,04 from http://bit-player.org/bph-publications/CACM-2008-07-Hayes-cloud.pdf.

[2]. J. Newton, "Are SaaS & Cloud Computing Interchangeable Terms?", Feb 16, 2009, retrieved from http://www.daniweb.com/blogs/entry3993.html.

[3]. C. Klein, G. Kaefer, "From smart homes to smart cities: Opportunities and challenges from an industrial perspective", Next Generation Teletraffic and Wired/Wireless Advanced Networking, Proceedings, Lecture Notes in Computer Science, vol.5174, p.260, 2008.

[4]. M.A. Vouk, "Cloud computing, issues, research and implementation", 30th International Conference on Information Technology Interface, 23-26 June, pp.31-40.

[5]. F.M. Aymerich, G. Fenu, S. Surcis, "An approach to cloud computing network", 1st International Conference on the Applications of Digital Information and Web Technologies, Ostrava, Czech Republic, Aug 4-6, 2008, pp.120-125.

[6]. K. Sloan, "Security in a virtualised world", Network Security, Aug 2009, vol.2009, Issue.8, pp.15-18.

[7]. X. Larrucea, R. Alonso, "Modelling and deploying security policies", WEBIST 2009: Proceedings of the 5th International Conference on Web Information Systems and Technologies, pp.411-414, 2009.

[8]. Y.S. Gu, B.J. Zhang, J.Y. Zhu, "Research on web services security based on XML signature and XML encryption", Advancing Knowledge Discovery And Data Mining Technologies, Proceedings, 2nd International Workshop on Knowledge Discovery Data Mining, Moscow, Russia, Jan 23-25, 2009, pp.448-450.

[9]. M.M. Molla, P. Madiraju, S. Malladi, S.I. Ahamed, "An XML based access control architecture for pervasive computing", IEEE International Conference On Pervasive Computing And Communications (Percom), Galveston, TX, Mar 09-13, 2009, vol.1-2, pp.803-808.

[10]. L. Li, W. Chou, "Rich presence authorization using secure web services", 5th International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE 2008), pp.199-204, 2008.

[11]. C.W. Shang, Z.K. Yang, Q.T. Liu, C.L. Zhao, "A context based dynamic access control model for web service", EUC 2008: Proceedings of the 5th International Conference on Embedded and Ubiquitous Computing, vol.2, pp.339-343, 2008.

[12]. J. Wu, Z.M. Huang, "Proxy-based web service security", 3rd IEEE Asia-Pacific Services Computing Conference(APSCC 2008), Proceedings, Yilan, Taiwan, Dec 09-12, 2008, vol.1-3, pp.1282-1288.

[13]. H. Koshutanski, F. Massacci, "Interactive access control for autonomic systems: from theory to implementation", ACM Transactions on Autonomous and Adaptive Systems, vol.3, issue.3, no.9, Aug 2008.

[14]. H.C. Chao, T.J. Liu, K.H. Chen, C.R. Dow, "A seamless and reliable distributed network file system utilizing webspace", 10th IEEE International Symposium on Web Site Evolution (WSE 2008), Proceedings, Beijing, Peoples R. China, Oct 3-4, 2008, pp.65-68.

[15]. S. Pearson, "Taking account of privacy when designing cloud computing services", ICSE Workshop on Software Engineering Challenges of Cloud Computing, CLOUD'09, pp.44-52, May 2009.

[16]. K.M. Khan, "Selecting web services with security compliances: A managerial perspective", 11th Pacific Asia Conference on Information Systems, Auckland, New Zealand, Jul 03-06, 2007, section.1-6, pp.910-916.

[17]. R. He, J.W. Niu, M. Yuan, J.P. Hu, "A novel cloud-based trust model for pervasive computing", Proceedings of the 4th International Conference on Computer and Information Technology, pp.693-700, 2004.

[18]. P. Felix, C. Ribeiro, "A scalable and flexible web services authentication model", Proceedings of the 2007 ACM Workshop on Secure Web Services (SWS'07), ACM Workshop on Secure Web Services Fairfax, VA, Nov 02, 2007, pp.66-72.

[19]. A. Nagarajan, V. Varadharajan, M. Hitchens, "Trust management for trusted computing platforms in web services", Proceedings of the 2007 ACM Workshop on Scalable Trusted Computing (STC'07), ACM Workshop on Scalable Trusted Computing, Alexandria, VA, Nov 02, 2007, pp.58-62

[20]. S. Bode, A. Fischer, W. Kuhnhauser, M. Riebisch, "Software architectural design meets security engineering", 16th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems, pp.109-118, 2009.

[21]. M. Yildiz, "Dynamic System Security Model", 2008, unpublished manustcript.

[22]. Jemal Abawajy, Determining Service Trustworthiness in InterCloud Computing Environments, 10th International Symposium on Pervasive Systems, Algorithms, and Networks (I-SPAN 2009), Kaoshiung, Taiwan.

[23]. IBM Blue Cloud project [URL]. http://www-03.ibm.com/press/us/en/pressrelease/22613.wss/, access on October 2009.

[24]. Amazon Elastic Compute Cloud [URL]. http://aws.amazon.com/ec2, access on Oct. 2009.