COMP 7360 Individual assignment [2] 10%

Discussion Question:

3. Choose one of the following cloud services categories: SaaS, IaaS, PaaS. Do some Internet research that focuses the security issues associated with the selected cloud service category. Summarize the major security risks associated with the cloud service category and identify mechanisms that can be used to address these risks.

Topic: implementation of the security issues on the SaaS model of Gmail service

Student Number: ____ 15451682_____

Student Name: _____CHEUNG Saiho_____

Program: _____MSc AIS_____

In the 21 century, the cloud computing is a big impact to the traditional data center infrastructure and enterprise network design. Most of internet service providers (ISPs) have provided the different level of cloud computing services to the enterprises, academic sectors and organizations, this service is dependent on the subscription price model. It can be reduced the cost of IT infrastructure investment and minimal management capability by these companies.

According to the National Institute of Standards and Technology (NIST) has defined the three levels of the cloud computing service model, Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). (Mell & Grance 2011) The IaaS is focused on providing the infrastructure level of cloud computing service for customers, it has only the fundamental computer resources to allocate in the cloud platform, such as number of CPU, RAM, HDD capacity and network bandwidth etc. Customers should evaluate the computer hardware resources what their business needs. For example, PCCW Ltd. business cloud computing service. The PaaS is focused on deploying the application which is created by the customers, so the vendor has provided the software development tool, program API libraries and configuration setting for the software debugging. The customers can produce an application hosting environment for using this service model. For example, Google App engine, Microsoft SQL Azure. The SaaS is focused on providing vendor's application service to the customers, they can use the mobile devices or web browser to access it. For example, Google e-mail service and YouTube. (Liu et al. 2011)

For the SaaS model, the cloud platform is dedicated to deploy the specify software or web service for customers, they do not spend the amount of money to purchase the computer hardware and software, it is including a group of servers, various of network devices, software license fee, technical supporting and annual maintenance fee. (Soofi et al. 2014) For example, HKBU student e-mail service, this service has provided by Gmail portal instead of depend on HKBU IT service department. The department does not need to purchase any physical servers, routers and a set of software related which provides e-mail service. The HKBU has signed the service contract to the Google company when it has needed to pay an annual subscription fee to rent the e-mail service for all students in the campus. Actually, the Gmail portal must have hosted more than one the university of student e-mail service.

Certainly, the Gmail e-mail management system is stored a huge amount of student information and e-mail record, so students can allow to login anywhere and receive e-mail from other people via internet. Therefore, many hackers can attack it through the public network, the system may be infected the e-mail attachment by the virus or spyware by the hackers. It is a very important network security issues for cloud computing service. Moreover, the SaaS provider must ensure that the user's application setting and data cannot allow to access the other users illegal, the hackers can use the network zombie program or worm to interrupt the system service or steal some personal information in other applications, such as Google cloud drive, Google calendar. It has involved the data security issue in the cloud computing system. (Takabi et al. 2010) On the other hand, the cloud computing system architecture has typically provided a wide range of web service to different kind of companies or organizations. The SaaS provider has responsibility to propose the planning of system recovery when the system would be collapsed by human error or natural disaster. This is the most important issue of system availability when the provider should concern, otherwise it is a big disaster that all client data would be lost.

The Google Company should consider the five keys of security issues for the cloud e-mail service, such as network security, system authentication, web application security, data security and system availability. (Subashini & Kavitha 2011) There have proposed the five development process and solutions to enhance security level for this service which is shown as below:

A. Data security

For the data security issue, it is the most important topic in the SaaS model. As many enterprises sensitive data is stored in the cloud storage when the web applications can use the data, it is not similar to the traditional on-premise software deployment model. In the traditional way, these enterprises have developed the standalone security system to protect the data for themselves. It is including the data of security control policies and system user access permission in their company servers. however, the cloud system is needed to manage so many security policies and access permission of difference users in different enterprises. It is very complicated and easy to have the conflict of system access right. (Almorsy et al. 2010)

The Gmail e-mail management system is separated to their own system which is according the company or academic institute, it seems like HKBU email system, the system is classified the two part of student and staff in the top of one network domain system. these two e-mail system should have depended the management site and domain security policies. The students' e-mail administrator cannot manipulate the staff e-mail system, the administrator can only manipulate student e-mail accounts and set usage quota in management site via VPN connection.

B. Network security

In the SaaS service model, most of enterprises sensitive data should be stored and processed in the cloud computing platform, it must ensure that the data transmission has a high security channel from the endpoint of cloud systems. Therefore, the secure service layer (SSL) protocol is the best solution which is encrypting the data transferred in the OSI application layer. There can be prevented so many network attacks by hackers, such as packet sniffing, man-in-middle and IP spoofing. On the other hand, the SaaS model is not similar to the traditional server model, it has so many different applications for running in the cloud machine. Actually, it cannot block the unused service ports from the firewall which is based on OSI network layer. (G & S 2013)

The Gmail e-mail system has enabled SSL to encrypt user's data in the web browser when student login the email system on the web. This system is only open three service ports, such as web, incoming e-mail service and outgoing email service. Thus, the students can send or receive your e-mail on the mobile apps or browser.

C. System authentication

In fact, most of academic institutions and enterprises have used the directory service system when they are storing the employee personal information in the central database system, such as Lightweight Directory Access Protocol (LDAP) and Microsoft Active Directory Service. It has implemented the single sign on service for the system, there can login or use the different kinds of system services in the single user account. (Zissis & Lekkas 2012) Therefore, this service can enhance system integration and easy to

remember the login system account for users.

In the SaaS service model, it has provided more than one web service to the users. HKBU students can use one single computer account to login all the system services which are provided by the university. For example, the Gmail system must synchronize with the student data of directory system service in HKBU when it has manipulated the student records.

D. Web application security

As the SaaS service model is focused on providing the web application service for clients, the vendor need to ensure that these application versions is very stable and complete system. It should avoid to deliver the application of beta version and has not any restricted software testing to open the public. The web applications should keep track of update in the latest version and system patch frequently. In addition, there should be installed the anti-virus software and intrusion detection system (IDS) by the cloud system. The anti-virus software can detect all incoming files, whether are infected by a virus or spyware, the IDS can detect network traffic and monitor the index of system workload. If it finds some abnormal case or malicious activity, the system alarm is triggered to acknowledge the system administrators. (Chen & Zhao 2012)

Certainly, the Gmail system is not allowed to attach any execute file and execute any program file on it, such as Javascript. Moreover, the web e-mail system has implemented the powerful virus scanning engine, it can prevent the verity of computer virus, Trojan horse and spyware when they have hidden in the uploaded by students.

E. Availability and system backup

For the service availability and system backup strategy, it is a key of the most important development process in a SaaS model. As the cloud computing architecture is typically a distribution network system, there have so many different types of web service running on the system when this system is served several hundred thousand of people to access it simultaneously. Thus, the system must be enabled to implement a server farm instead of a single server, this server farm contains a large group of servers to process all user requests through the internet. It should be implemented a load balance function by the network manager. (Overview & Considerations 2010)This function can distribute these requests for each server, which is according to network bandwidth and server processing power in different data centers. Besides the network manager must have planned the mirror site and system backup schedule for each data centers.

The Gmail system is facilitated the data center in Hong Kong Cyberport, the mirror site is located in London and New York. Due to these are big city, high speed network support, lack of natural disaster and mature political environment. In addition, the system is typically produced the full backup in a weekend, the incremental backup is produced in daily. The data transmission must be encrypted to transfer the other sites via a fiber network, it can ensure that the data would be safety and recovery anytime.

For these above security issues, there have discussed and provided some solutions how to enhance the security level on the Gmail system, it is typical provided the web service in the SaaS model.

Bibliography:

Almorsy, M., Grundy, J. & Müller, I., 2010. An analysis of the cloud computing security problem. *17th Asia-Pacific Software Engineering Conference (APSEC 2010) Cloud Workshop,Sydney, Australia*, (December), p.7. Available at: http://researchbank.swinburne.edu.au/vital/access/services/Download/swin:20103/SOURCE2.

Chen, D. & Zhao, H., 2012. Data Security and Privacy Protection Issues in Cloud Computing. *2012 International Conference on Computer Science and Electronics Engineering (ICCSEE)*, 1(973), pp.647–651. Available at: files/443/Chen and Zhao - 2012 - Data Security and Privacy Protection Issues in Clo.html.

G, S. & S, M., 2013. Securing Software as a Service Model of Cloud Computing: Issues and Solutions. *International Journal on Cloud Computing: Services and Architecture*, 3(4), pp.1–11. Available at: http://www.airccse.org/journal/ijccsa/papers/3413ijccsa01.pdf.

Liu, F. et al., 2011. NIST Cloud Computing Reference Architecture Recommendations of the National Institute of Standards and. *NIST Special Publication 500-292*, 292(9), p.35. Available at: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505.

Mell, P. & Grance, T., 2011. The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology. *National Institute of Standards and Technology, Information Technology Laboratory*, 145, p.7. Available at: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Overview, A. & Considerations, B., 2010. Software- as- a- Service (SaaS) on AWS Business and Architecture Overview. *Amazon Web Services*, (September), pp.1–11.

Soofi, A.A. et al., 2014. Security Issues in SaaS Delivery Model of Cloud Computing. , 3(3), pp.15–21.

Subashini, S. & Kavitha, V., 2011. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34(1), pp.1–11. Available at: http://dx.doi.org/10.1016/j.jnca.2010.07.006.

Takabi, H., Joshi, J.B.D. & Ahn, G.J., 2010. Security and privacy challenges in cloud computing environments. *IEEE Security and Privacy*, 8(6), pp.24–31.

Zissis, D. & Lekkas, D., 2012. Addressing cloud computing security issues. *Future Generation Computer Systems*, 28(3), pp.583–592. Available at: http://dx.doi.org/10.1016/j.future.2010.12.006.