International Journal of Engineering Innovation & Research
Volume 1, Issue 6, ISSN : 2277 – 5668

The New Trend of Security in Cloud Computing

Xiangdong Li
Computer Systems Technology, NYC College of Technology, CUNY, New York, USA
xli@citytech.cuny.edu

***Abstract* – The use of services of cloud computing has been growing widely in industry, organizations and institutions recently, due to its tempting benefits, for example, the scalability, efficiency, flexibility and lower cost. The security issues have been studied and analyzed extensively. In order to understand the risk issues existing in today's cloud, we discuss the new trend of security of cloud in this paper. The preventing methods are also discussed.**

***Key words* – Cloud computing, services, security.**

I. INTRODUCTION

The virtualization and high-speed Internet have boosted the transformation of compute environments and the computer resources into the cloud. The cloud computing has been attracting more and more industry companies and organizations due to its apparent and prompt evidence of benefits tired to the efficiency, scalability, flexibility and lower cost. The global revenue on public IT cloud services is predicted to grow at a rate of 27.6% annually from 2010 ($21.5 billion) to 2015 ($72.9 billion) [1].

The traditional three cloud service models are *Infrastructure as a Service* (IaaS), *Platform as a Service* (PaaS) and *Software as a Service* (SaaS). Recently several new models are defined due to the growing use of their specific services, for example, *Disaster Recovery as a Service* (DRaaS), *Storage as a Service*, *Security as a Service*, etc. The three common deployment models are: *Private cloud*, where the entire cloud infrastructure is used only for one customer; *Public cloud*, where the cloud infrastructure is for general public or a large industry group; and *Hybrid cloud*, where the cloud infrastructure contains different type of cloud deployments [2]. The choice of these deployment models depends on the customers' requirements. For example, an organization may adapt the hybrid cloud for its business applications, such as disaster recovery (DR) plan, data mining, or backup/storage solutions. The data is stored in a private cloud where it keeps the highest security level, and the data processes take place in the public cloud. Actually, a large number of companies test their IT developments and implementations in public cloud before they can be migrated into the private cloud for production purposes [3]. In the following we briefly introduce two new cloud services: *Disaster Recovery as a Service* and *Security as a Service*.

1.1 Disaster Recovery as a Service (DRaaS)

Today many industry companies and organizations are moving their disaster recovery (DR) to cloud, where the efficient cloud computing services can be used to make the disaster recovery easier and less expensive. With the hybrid cloud model, the backup or recovery takes place locally because of the needs for the fast backup speed. After that, a copy of backup is sent to the cloud. Such, it provides a fast recovery with local resources and the cloud is used for the offsite data for disaster recovery. In addition, the DRaaS can be designed and implemented to automatically start the recovery process with no or little human interaction. Another benefit from DRaaS is the lower cost, compared to the dedicated infrastructure used for each customer, where the DRaaS vendors can provide multiple services to many customers from the same server racks. Today in the cloud market there are more than 100 cloud vendors who provide pure DRaaS and DR heavy-weighted services. There exist some new challenges in DRaaS model. The biggest concern is the requirement for the high bandwidth when the customers have heavy transactional apps, that the DRaaS copies the applications and virtual machine images in the cloud, it is frustrating to constantly keep those apps and VM images updated [3].

1.2 Security as a Service (SaaS)

Most industry companies, governmental organizations and institutions cannot afford the cost to build sophisticated secure systems with fully updated technology; many of them just keep the minimal staffs with limited budgets to meet the minimal governmental requirement of regulatory compliance. The benefits of cloud *Security as a Service* for the enterprises include the cost reduction and IT updated expertise. Today the cloud vendors proposed the model of *Security as a Service* to offer the security expertise for large amount of users to meet their business requirements. The cloud-based services include Encryption, Identify management, Configuration and Vulnerability management.

Major cloud vendors provide the encryption service which can be easily integrated with compliance like FIPS-140-2, PCI DSS and HIPAA-HITECH. Cloud-based identity management service provides specialization in putting disparate authentication protocols together into one management framework. They are also integrated with customers' internal authentication resources, for example, Microsoft Active Directory. This allows for a much-needed single sign-on methodeioquy for users of cloud-based resources. It can also enable standardized account configuration, including complex password control, aging and intruder-lockout status for strong authentication [9]. The cloud-based security configuration and vulnerability management provide full configuration management, including monitoring the patches, service configurations and firewalling settings. It analyzes the vulnerabilities that may exist in the configuration. These cloud-based configuration services allow a single configuration to be extended to apply in all registered servers, regardless of the difference of hosting location or the types of operating systems [9].

Similarly, the use of Security as a Service contains risks. The main concern is that if an organization adapts the

Security as a Service, it may reduce the need for in-house staffs and grant cloud vendor with some level of access to its network or data, in order to let the cloud vendor provide specific activities or inspection, for example, to monitor the system logs, network traffic, and database accesses.

II. VARIOUS THREATS IN CLOUD

The cloud computing is based on the use of Internet. To protect the network connections to the internet-based assets has become more important. All the websites are vulnerable to various attacks; most of the attacks are Denial of Service (DoS) or Distributed DoS (DDoS). In addition, various network attacks can cause the cloud servers unreachable. Today, the top threats in the cloud can be cataloged as: abuse of cloud computing; vulnerable application programming interfaces; malicious insiders; unknown risk profile; shared technology vulnerabilities; data loss or leaks; account, service and traffic hijacking; etc [10].

To evaluate the potential risks in cloud and manage these risks, the security in the following fields should be considered and analyzed. *Cloud Access Devices*: If the cloud users are allowed to use various devices, personally or from business, to access the cloud services, this extremely makes it hard to control the risks from the user access device; *Cloud Platform*: The cloud services are built on various platforms, physically and virtualized, this requires a security solution to protect the virtualization layer and other special malware protections; *Identity and Access Management*: if a business moves to cloud, its security maintaining, auditing and reporting may not be under its control; *Security and Compliance Management*: the vulnerability, compliance, security patch management and the incident, configuration, capacity, availability management may be more complicated in the cloud; *Security Impact*: the function of the cloud security attributes, for example, the consumers, service delivery and service governance, should be clearly defined. Below we describe several Layer-2 level and router-level attacks which commonly happen in the network of cloud computing and make the cloud services unreachable. We also briefly describe their prevention methods.

2.1 VLAN hopping:

It involves a virtual LAN (VLAN) with a trunk port, where the trunk port is used to route traffic for multiple VLANs across the same physical link, usually between the switches. The Dynamic Trunk Protocol (DTP) is a process that is used to synchronize the trunking mode on the link's ends to replace the human intervention on both sides. The DTP is set as "Auto" by default; other options are "On", "Off", "Desirable" and "Non-Negotiate". A hacker can launch the attack by spoofing the trunk port, like the way a station spoofs a switch. The station is now a member of all the VLANs. The attack only successes if the trunking protocol is set as "Desirable". Technically, the attacker sends double encapsulated 802.1Q frames; the switch only de-capsulates one and the other frame is proceeded to the victim. To prevent VLAN Hopping, first, disable the auto-trunking and unused ports (or put them on an unused VLAN); second, do not use VLAN 1 and set all user-ports as non-trunkable [4].

2.2 ARP spoofing attack:

It involves the process of sending forged ARP replies to a target station. An ARP Spoofing attack can lead to other types of attacks, such as sniffing and MAC flooding attacks. The sniffing attack is that a hacker gets in the middle of communication between other stations and he is able to sniff out the data being transmitted. The hacker then may get the control on the data being transmitted on the network before it reaches its destination. The MAC Flooding attack allows any host on the same LAN to intercept any data packet from the network, no matter what their destination MAC address are. The hacker may intentionally send spoofed ARP replies to a switch constantly and such it can overload the switch and cause the MAC Flooding attack. To prevent against ARP Spoofing attacks, first, restrict the user accesses to the LAN; second, monitor the LAN for multiple occurrences on any MAC address. Another possible way to prevent the data is to encrypt the data. For example, using HTTPS, VPN or SSH. These methods are commonly used in the cloud computing. The implementation of port security that restricts the access by limiting and identifying the MAC addresses allowed to access the port is also a good prevention method. To utilize static entries in the ARP cache [5] or to use a stateful ARP with a cache that contains the information of previous requests [6] may be effective.

2.3 Content Addressable Memory (CAM) Table Overflow:

A switch contains a CAM table (just a memory) with limited size to store the entries of MAC addresses. This attack involves the flooding on switch by using a large amount of invalid source's MAC addresses until the CAM table overflow. When it happens, the switch could not find a port for the MAC address in the CAM table and floods all its ports with incoming data packets. To mitigate the CAM table overflow, the strict administration of dynamic port security at the switch is necessary by blocking the offending MAC or shutting down the switch port.

2.4 Routing Metric Attacks:

This attack is designed to modify the dynamic metrics to change the preferred path as undesirable. If the attack successes, the network becomes with limited connectivity and slower throughput. The Intrusion Detection Systems (IDS) or firewalls are used to detect and prevent this type of attack. The Access Control Lists (ACLs) are effective to filter network router traffic and maintaining uninterrupted flow of data. The IDS can be used to analyze insider attacks and those intrusions which pass the firewall's ACLs.

2.5 Heap and Stack overflow attacks:

A number of critical vulnerabilities were found in series of routers, which can allow remote exploitation of the devices via the Internet [7]. The defects include the heap

and stack overflow attacks. Today, the exploits often take place remotely and lead to a target completely compromised. A buffer overflow in program gives a vulnerability of exploit. An attacker can insert malicious code into the program, and take some control on the target. The primary defense is to write secure programming. A secondary protection relies on security devices "canary-based defenses" to defend against attackers overwriting the return address and "non-executing stack defenses" to make it impossible to execute code on the stack [8].

2.6 Open Shortest Path First (OSPF) Attack:

It involves the OSPF, which determines how data packets are routed or delivered within an autonomous network using the shortest paths. OSPF has some known flaws, for example, it tricks uncompromised routers to propagate false router table updates, known as Link State Advertisements (LSAs), which communicates the router's local routing topology to all other local routers in the same OSPF area. The creating false router tables could create router loops. The compromised router sends the victim router a spoofed LSA mirroring the last one the victim router sent out. It then sends an LSA to another router that appears to be from the first victim router. Initially, the victim router rejects the spoofed LSA and sends a fight-back or a copy of its original/legitimate LSA. When this legitimate LSA reaches the second victim router it notices that it is identical as the spoofed LSA it had earlier received from the compromised router. Such, it rejects the legitimate copy of LSA and broadcast the spoofed LSA, resulting in a false LSA that all other routers will end up accepting as genuine.

2.7 Cross-site Scripting (XSS) Attack:

This is a type of vulnerability in web applications that attackers insert client-side scripts into the web pages. When users visit those web pages, they are then exposed to the XSS attack.

Users' private information and router MAC address through the browser being used will be exposed. When the attacker gets the MAC address, he can simply use Google Location Services to pinpoint the exact physical location of that user. The location information can be used for diverting DNS requests to the attacker's desired locations and launching man-in-the-middle attacks. The two primary XSS attacks are *non-persistent* and *persistent*. The non-persistent XSS attack, known as "reflected XSS", takes place when the vulnerable Web application immediately includes the request to the HTTP response without doing any sanitization. The persistent XSS attack takes place when Web application accepts malicious code, and store it and later distributes it in response to a separate HTTP request. This type of attack is more serious than the non- persistent XSS attack because the codes are injected could affect a large number of users. In order to prevent this attack, several methods should be implemented. The IDS router is used to audit traffic from Internet before it is forwarded to DMZ or the corporate network, and to monitor the incoming traffic before the inbound access list is analyzed. The routing advertisements should not be set by default to accept everything. For example, Cisco routers allow users to define a route map to prevent OSPF routes from being added to the routing table, using a feature called OSPF Route-Map-Based-Filtering. Set the browsers to limit scripting with restrict settings and create white lists for allowed scripts or black lists for blocked scripts.

2.8 Router attacks:

Several attacks on routers: *Disrupting Peering Attack*-- attempt to deny the use of network resources from authorized users of the network. Usually, this attack is not effective from the outside. *Protocol Semantics Peering Attack* -- abuse the semantics of the protocol itself. This attack can reset the routing protocol peering session and disrupt the network services. *Land Attack* -- send a packet to the router with the same IP address and same port number in the source and destination fields, such may cause DOS attacks and degrade the performance of the router. *Smurf Attack* -- send a large amount of IMCP Echo packets to a subnet broadcast address with a spoofed source IP address from that subnet. If a router is positioned, it will forward broadcast requests to other routers on the protected network. It is imperative to consider the following protection for routers: newer versions of software upgrades and patches fix bugs and vulnerabilities; router configuration and commands – exec mode gives limited access to the command set of the router and the access to all the router commands should be reserved; the login-on VM should be disabled if the remote admin is not necessary, because the remote admin without encryption is dangerous and an attack with network sniffer can acquire the router passwords.

III. CONCLUSION

The security becomes highly thornier when the users manage the discipline within a cloud-based architecture. Only about half of cloud users respond that they have in-depth and in-house knowledge of cloud-based security requirements and prefer a hands-on approach to managing security. However, as those firms get deeper and larger with cloud deployments, many of them recognize that there exist big holes in their staff's security expertise, and more than one-third of cloud users admit their security measures are not optimized for cloud environments. With the wide use of cloud application and its services, its security is vitally to be studied and understood. A new research is to consider the possibility of implementing a cloud based Trusted Platform Module (TPM). The structure relies upon the multiple physical TPMs in order to support a larger number of users. The service can offer users the access to a combination of resources, including TPM, cryptographic and user management services.

It's important for a customer to ask a few questions about the security controls when he plans to move to the cloud, as suggested in [11]: Who owns your data? Will your service provider give your data back to you? Will your service provider give your data back to you? What about resource access? Do you have access to user data?

ACKNOWLEDGMENT

This work was partially supported by PSC-CUNY grant 2011.

REFERENCES

[1] F. Gens, M. Adam, D. Bradshaw, M. Eastwood, S.D. Hendrick, C. Ingle, V. Kroa, R.P. Mahowald, S. Matsumoto, C. Morris, R. L. Villars, R. Villate, and N. Wallis, "Worldwide and Regional Public IT Cloud Services 2011-2015 Forecast", in *International Data Corp* (IDC), June 17, 2011.

[2] X. Li, "Cloud Computing: Introduction, Application and Security from Industry Perspectives", in *International Journal of Computer Science and Network Security*, Vol.11 No.5, May 2011.

[3] B. Butler, "Disaster recovery in the cloud: Vendors jump in; enterprises wade", in *Network World*, Sept. 2012.

[4] L. Senecal, "Layer 2 attacks and their mitigation", [Online]. Available: www.cisco.com

[5] C. Abad and R. Bonilla, "An Analysis on the Schemes for Detecting and Preventing ARP Cache Poisoning Attacks", 27th *International Conference on Distributed Computing Systems Workshops* ICDCSW07 (2007)

[6] V. Ramachandran and S. Nandi, "Detecting ARP spoofing: An active technique", in *Information Systems Security*, Vol: 3803, 2005.

[7] L. Constantin, "Hackers reveal critical vulnerabilities in Huawei routers at Defcon", in *ComputerWorld*, July 30, 2012.

[8] D. Wheeler, "Secure programmer: Countering buffer overflows", in *DeveloperWorks*, IBM, 2004.

[9] J. Granneman, "Cloud Security as a Service for secure cloud-based server hosting", in *SearchCloudSecurity*, Oct. 2012.

[10] Cloud Security Alliance, "Top Threats to Cloud Computing V1.0", March 2010, [Online]. Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[11] E. Moyle, "Cloud computing vendor lock-in: Avoiding security pitfalls", in *SerchCloudSecurity*, June 2012.

AUTHOR'S PROFILE

Xiangdong Li

received M.S. in Computer Information Science from CUNY Brooklyn College in 1997, and Ph.D. in physics from the CUNY Graduate School in 2000. Professor Li has five years working experience in the IT industry. He is an associate professor at the Department of Computer Systems Technology in New York City College of Technology, CUNY. He is a faculty member of Ph.D. programs in Computer Science and in Physics at the CUNY Graduate School. His research fields include information security, quantum information and nuclear physics. Professor Li is a member of APS and IEEE.