INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

TO SECURE CLOUD COMPUTING ASSESS NETWORK PATH VULNERABILITIES

PROF. SWAPNIL V.KHEDKAR[1], PROF. S. A. DHAWALE[2], PROF. O. A. JAISINGHANI[3]

Information Technology, Computer Science, SGBAU University Amravati, Maharashtra, India

Accepted Date: 05/03/2015; Published Date: 01/05/2015

Abstract: Cloud storage enables users to remotely store and retrieve their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. Cloud storage system enables storing of data in the cloud server efficiently and makes the user to work with the data without any trouble of the resources. Cloud computing is highly promising technology because of its unlimited resource provisioning and data storage services which help us in managing the data as per requirements. In recent times cloud computing based delivery model has been proven to reduce enterprise IT costs and complexities. In contrast to traditional enterprise IT solution, the cloud computing model moves the application software and data to remote servers in large datacenters, which raise many security challenges. One of the critical challenges is the inability to characterize the cloud network's impact on the cloud security and performance guarantees. In this paper, we analyse the degree of security provided by the network to data sharing applications deployed in cloud environments that span administrative and network domains. Our analysis is based on examining the security level of network applications on routers which lie between cloud subscriber and cloud provider. Our preliminary results confirm that the majority of the routers are plagued by insecure network protocols, leading to vulnerable routers. These results confirm our hypothesis that the security of the network infrastructure needs to be upgraded to assure the protection of information exchange between the cloud subscriber and cloud provider

Keyword: Network Measurement, Cloud Network, Planet lab, Router

Corresponding Author: PROF. SWAPNIL V.KHEDKAR

Access Online On:

www.ijpret.com

How to Cite This Article:

Prof. Swapnil V. Khedkar, IJPRET, 2015; Volume 3 (9): 1886-1896

PAPER-QR CODE

INTRODUCTION

Cloud computing has grown from being a promising business concept to one of the fastest growing segments of the IT industry. So, cloud environment always remains vulnerable to attacks. The framework serves as an excellent platform for making cloud services intrusion tolerant. The feasibility of the framework has been tested by making cloud's Infrastructure as a Service (IaaS) and Data Storage Service intrusion tolerant. The proposed framework has been validated by integrating Intrusion Tolerance via Threshold Cryptography (ITTC) mechanism in the simulated cloud's IaaS. Cloud computing is an emerging technology used by commercial organizations to run a variety of network applications and cloud-based services [1] [2].The network applications are typically hosted on servers managed by cloud providers to provide service to cloud subscribers. The networking applications, such as, Web services, instant messaging, financial applications, and gaming, typically involve the exchange of sensitive information. The security of these applications depends on the availability of a trustworthy underlying network between the cloud provider and cloud subscriber. The underlying network between the subscriber and provider has largely focused on providing basic connectivity to customer VMs, with basic firewall capabilities available at each server. Several key network security capabilities for protection of data exchanged between the subscriber and provider are not available. This untrustworthy network can compromise sensitive and high value information transmitted by the applications. For example, a set of routers on a path between the cloud provider and subscriber could be vulnerable to attacks, which could lead to search queries to be snooped, IM message's to be modified and financial transactions to be compromised. Dissatisfied cloud subscribers could choose alternate cloud providers, which will result in a significant loss in revenues. Thus, there is an urgent need to assess the level of security and privacy mechanisms provided by the underlying network to protect the authenticity, integrity and confidentiality of the information flowing between the cloud subscribers and providers. The network traffic between the cloud subscriber and cloud providers flows through the network of core routers. The security of the network traffic hinges on the security level of the core routers in the path from the cloud subscriber to each of the cloud providers. Assessing the security level of each individual router in the path will provide the cloud subscribers a mechanism to evaluate the security of the network paths to each cloud provider. The cloud subscriber will choose to conduct business with the cloud provider, whose information traverses the most secure network route. Cloud security issues have recently gained traction in the research community, where the focus has primarily been Workshop on Clouds, Unsecured cloud servers have been proven to be crippled with novel denial-of-service attacks [4]. However, while such threats to cloud servers are widely understood, it is less well appreciated

that the underlying network infrastructure itself is subject to constant attack as well. Attackers have repeatedly demonstrated their ability to compromise routers, through combinations of social engineering and exploitation of weak passwords or latent software vulnerabilities [5], [6]. Recently, an underground market has emerged for trading access to over 5000 compromised routers [6]. Once a router is compromised, CISCO and Juniper vendors provide command-line interfaces, which can drop and delay cloud information, send copies of cloud data to an adversary, or ”divert” cloud data through an adversary and back. Cisco routers have been demonstrated to be compromised via simple software vulnerabilities [7]. In an annual survey of the Internet network security operations community, once a router’s software vulnerabilities are exposed, an Attacker may manipulate the router to selectively drop, modify, or re-route cloud information. In this paper, we assess the security level of the network between the cloud provider and cloud subscriber based on the data collected from routers in the core network. Our work is motivated by the observation that the performance of the majority of data-sharing applications deployed on cloud infrastructures will depend on the secure underlying networks. The data collected from the routers helps in the assessment of software and protocol vulnerabilities. We will also assess the impact of the vulnerabilities of routers on the performance of data-sharing applications in the cloud. To the best of our knowledge, there has been little work on the security implications for data-sharing applications due to software and protocol vulnerabilities in routers.

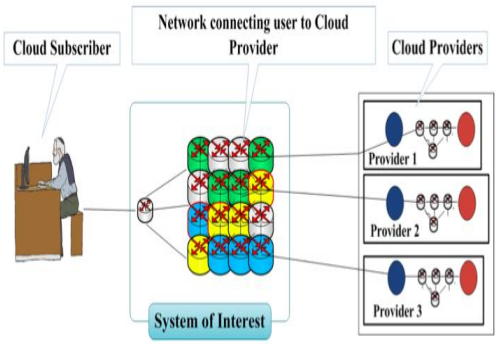

Fig: 1 Subscriber and Provider

RELATED WORK

1. Cloud providers have started to enhance their current network operations in order to provide better service to cloud subscribers. But most of these enhancements are primarily targeted at a small set of functionalities. For example, to cloud providers, Amazon and

Azure, are now providing network related add-on services such as traffic isolation, custom addressing, traffic load balancing across clustered VMs, and content distribution services using their distributed platforms. For example, Amazon extended its VPN services to include secure connectivity to isolated virtual instances with the ability to segment them into subnets and specify private address ranges and more flexible network Access Control Lists [9]. Also, Microsoft Windows Azure virtual network provides services for customers to integrate on-premise applications [10]. Recently, there has been an influx of virtual cloud appliances, which are network related services provided by third-party providers. Some of these services include security capabilities like, intrusion prevention [11], custom addressing and encrypted communications [12], [13]. Recently, the research community has advanced its view of the network requirements and challenges in supporting diverse applications in the cloud [14], [13]. Cloud NaaS (Cloud Networking-as-a-Service) is a networking framework that extends the self-service provisioning model of the cloud beyond virtual servers and storage to include a rich set of accompanying network services [14]. Cloud NaaS mitigates the current limited control available to cloud subscribers to configure the network, by providing them access to services like, network isolation, custom addressing, service differentiation, intrusion detection, and caching. Recent research efforts have reported increasing number of vulnerabilities in routers. Experimental results have demonstrated how routers are generally less secure than general Purpose computers and are often trivial to exploit. For example, the impact of hypothetical malnets exploiting vulnerable Routers has been described by several researchers [14], [15]. Similarly, the public availability of proof of concept Cisco IOS exploits and shell code [16], [17], have allowed adversaries to scan and exploit routers to develop botnets for DDOS attacks. A **botnet** is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks. This can be as mundane as keeping control of an Internet Relay Chat (IRC) channel, or it could be used to send spam email or participate in distributed denial-of-service attacks. Also, recent appearance of tutorials and simple to use tools to control specific routers indicate the transition of these techniques from research circles to the general black-hat community [18]. Our router port vulnerability process demonstrates that trivially exploitable routers exist between the cloud provider and subscriber for adversarial attacks to be feasible. Our preliminary research results also demonstrate that there are enough insecure open ports on routers which can be compromised on a large scale by technically unsophisticated attackers. For the remainder of this paper, the term router is used as shorthand for router ports. Figure 2 shows a router connects LAN or WAN to the internet with the help of router. Router helps to subscriber and provider to detect these

vulnerabilities. The vulnerabilities in routers originate from unsecure software and protocols.

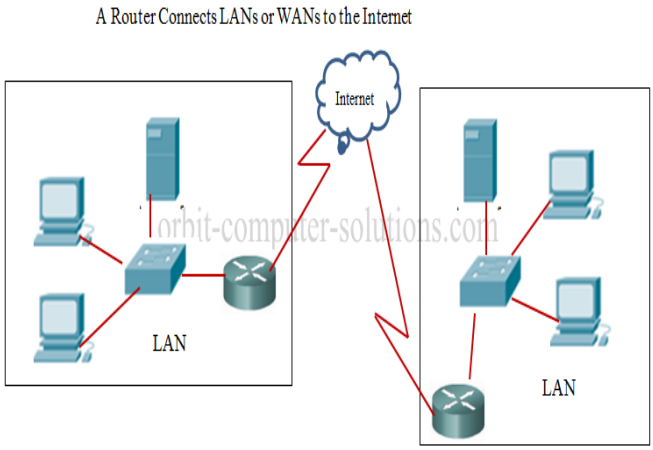

Fig: 2 Routers

ROUTER VULNERABILITY ASSESSMENT APPROACH

In this section, we present our router vulnerability assessment approach. The vulnerabilities in routers originate from unsecure software and protocols. To detect these vulnerabilities, the first step is to characterize the network port information for the routers. The network port characterization will provide insight into the number of secure ports, number of insecure ports, and number of open and closed ports at any given time. The network port characterization process can be broken down into three sequential phases: collection, recognizance, and categorization. *Collection*: First, we collected the IP addresses of a target set of spatially diverse routers within United States through full mesh trace route probing from Planet lab [19] nodes, supplemental data from the iPlane [20] project, and careful alias resolution. Our data collection experiment minimise the network traffic patterns between university campus based cloud providers and cloud subscribers. We assume that the university campus based cloud providers and subscribers will 5549 share routers similar to those that exist between the Planet lab nodes. In our experiment, we exclusively chose Planet lab nodes hosted on university campuses. *Recognizance*: Second, a popular network scanner tool, nmap was used to scan these IP addresses for secure, insecure and open ports. The results of the nmap scan were stored in a SQL database.

Vulnerability Analysis: Finally, the routers were categorized based on three security levels described by our vulnerability assessment approach. The three security levels categorized the routers based on the presence of malicious ports, insecure ports, and secure ports Figure 3 shows that vulnerability analysis done by three technique penetration testing, vulnerability assessment and network assessment. Penetration testing learns how serious your risk and how to mitigate them. Vulnerability assessment drill down to find security risk. Network assessment evaluate their network.

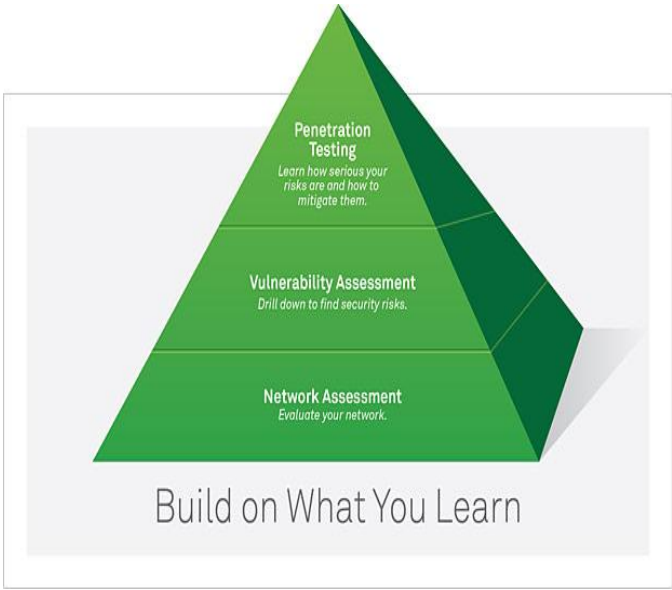

Fig: 3 Vulnerability Assessments

A. Collection

The first step in our vulnerability assessment approach is to identify the routers. To limit the number of scans, we decided to focus on routers within the United States. To identify the router IP addresses, we used two sets of datasets. The first dataset was obtained by probing spatially diverse set of Planet lab nodes. To evaluate our vulnerability assessment, we procured a large set of IP addresses of routers with as much spatial diversity as possible within the continental United States. We collected the IP addresses of the routers by performing full mesh trace route probing between spatially diverse set of Planet lab nodes. There were 200 planet lab nodes in the United States and the full mesh trace route probing between these nodes generated a very large set of router IP addresses with high spatial diversity. Similar trace route probes between Planet lab hosting sites are available from the iPlane project. iPlane is a

scalable service providing accurate predictions of Internet path performance for emerging overlay services.

B. Recognizance

The objective of the recognizance process is to identify vulnerabilities in routers by procuring the details for open ports. The router port information can be procured by the network scanner Nmap. Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. Nmap was used to query known malicious, secure and insecure ports on the routers. To query the port information, the default TCP ping mechanism in Nmap sends a TCP packet with the ACK flag set. The set of ports to query was provided with the command to avoid scanning all 65535 ports on the router. Upon receiving this packet, the router firewall will look up in its state table to see if the packet is part of a previously established connection. Once it finds that this is a rogue TCP packet, it will promptly discard the packet, preventing us from discovering the port on the host. Firewalls that do not perform state ful inspection but

Have a specific rule set will only pass the TCP ping through to authorize routers. To mitigate this problem, the SYN flag was set instead of the ACK flag. The results from the Nmap scan were inserted into a SQL database for categorization of security levels.

C. Vulnerability analysis

Our vulnerability analysis step will detect the vulnerabilities associated with the router ports. In addition, this step will provide the insight into the degree of risk to the routers due to presence of vulnerable router ports. The ports were categorized into three groups: Malicious and Insecure ports, Semi-Secure ports and secure ports. The malicious and insecure group is comprised of ports which have been reported to be target of Trojan attacks or ports which can be trivially exploited. These include ports which have attracted Trojan traffic and insecure ports like TELNET, FTP and SMTP. The semi-secure group comprised of open non-malicious ports which are non-trivially exploitable. These ports include SMB, SSH and FINGER. Finally, the secure group comprises of mostly closed and encrypted ports (which assure confidentiality, authentication and integrity of messages).

PRELIMINARY RESULTS

In this section, we provide the experimental setup for assessing the vulnerabilities of routers. As described in the earlier section, the collection step was implemented by performing a mesh trace route probing between all Planet lab nodes. The trace route probes were performed using the Paris trace route tool [23], using it once in UDP mode and a second time in ICMP mode in order to discover as many routers as possible [24]. The trace route probes between mesh of Planet lab nodes were performed multiple times to collect as many router IP addresses as possible. Using these two data sets, we were able to discover 196,125 unique router IPv4 addresses. Out of these router IPv4 addresses, we eliminated 100,000 addresses as they were unresponsive to ping probes. Another problem with trace route-based studies is IP interface disambiguation, also known as alias resolution. Interfaces on a given Internet router are typically assigned separate IP addresses; identifying which addresses correspond to the same physical router is the challenge in alias resolution. To de-alias our data set, we used the alias database published by the iPlane project. This database builds on prior work in alias resolution, including the methods used by the Rocket fuel project [25]. Upon de-aliasing our set of router IP addresses, we identified 56,287 routers. To implement the recognizance step, we deployed the Nmap tool on a group of planet lab nodes to query the router's port status. The total lists of router IP addresses were divided equally among 20 planet lab nodes which were available for the evaluation process. Each planet lab node was assigned 2500 IP addresses to analyse. As described in the previous section, the scans were performed using the default TCP ping Nmap Mechanism. To avoid overwriting of the router with scan messages, each TCP ping Nmap probe was sent with the - T polite option. TCP Connect scan was used to avoid any stealth scanning. These scan results were parsed and placed into a SQL database for vulnerability analysis. Finally, to implement the vulnerability assessment step, we employed the K-means algorithm, an unsupervised clustering method [27]. The filtered IP addresses with no open ports were clustered at the highest security level (Cluster 3). The IP addresses with open malicious and insecure ports open were clustered in the least secure cluster (Cluster 1). IP addresses that had non-trivially exploitable ports open were placed into the 5550 Medium security level, Cluster 2. The non-trivially exploitable ports are ssh, finger, dcom-scm, profile, and microsoft-ds Some of the insecure or trivially exploitable ports were FTP, Telnet, SMTP, netbios-ns, netbios-dgm, netbios-ssn, and blackjack. The malicious ports were identified from known ports which shown evidence of receiving trojan traffic [28] Our preliminary results indicate that large number of routers has trivially exploitable and malicious ports open. If these routers were in the network path between the cloud provider and subscriber,

They present an easier option for adversaries to steal or modify the subscriber or provider's traffic.

ETHICAL CONSIDERATIONS

The methodology underlying our vulnerability assessment approach of our project is straightforward. However, the process of gathering real-world data to assess vulnerability of networking devices has often raised an ethical debate. Unplanned port scanning of a remote networking device can onetime manifest in an adversarial attack. At the same time, it is extremely difficult to assess the security level of routers without the quantifiable evidence of the problems. In a recent position paper on the ethics of security vulnerability research [26], this line of proactive vulnerability research serves an important social function and is neither unethical nor illegal with respect to US law. Bound by the ethics principal of the duty not to harm, we have ensured that our experimental data collection process does not interfere with the normal operations of the networks we monitor. Our data collector has been designed to use minimal external resources in order to accurately collect the port information from the routers. We scanned the target networks in 24 blocks in non-sequential order in order to minimize the number of incoming TCP requests destined to any individual organization. No router was unnecessarily probed multiple times during a single scan. Every network probe used the appropriate Nmap options to avoid stealth scanning and overwhelming of networks. The data collector's outbound packet-rate was monitored in order not to overwhelm any in-path networking devices.

CONCLUSION AND FUTURE WORK

In this paper, we conducted a preliminary assessment of the security level of routers which exist between university campus based cloud providers and cloud subscribers. We collected the router IP addresses from Planet lab and performed the security level assessment using nmap. Out of 56,817 routers, we found that 69 % of the routers were found to be vulnerable to adversarial attacks due to open malicious and insecure ports. The security level of routers will help cloud subscribers choose the cloud providers which lie at the edge of the most secure network path. Our long term research objective is to leverage the vulnerability assessment process to generate quantifiable cloud network security metrics. These metrics can be part of a cloud SLA, which will provide cloud subscribers a mechanism to evaluate the security strength of the network path to the cloud provider. We plan to combine clustering and classification techniques to accurately assign security level to new router IP addresses. We will extend the security analysis to include protocol, OS, and software versions and encryption strength of

secure ports. We realize that the cloud subscriber would like to choose a network path which not only provides the best security, but also fast response time. With the availability of router security metrics, we also plan to investigate resource allocation solutions to aid the cloud subscriber in determining the network path which provides the best security and fast response time.

REFERENCES

1. S. Palumbo. Is iaas moving beyond just cloud fluff? August2010.http://www.businesswire.com/news/home/20100823005929/en.
2. C. Pettey. Gartner identifies the top 10 strategic chnologies for 2010.October 2009. http://www.gartner.com/it/page.jsp?id=1210613.
3. G. Wang and T. S. E. Ng. The impact of virtualization on network performance of amazon EC2 data center. In INFOCOM'10: Proceedings of the 29th conference on Information communications, pages 1163– 1171, Piscataway, NJ, USA, 2010. IEEE Press
4. H. Liu, A New Form of DOS Attack in a Cloud and Its Avoidance Mechanism, in Proceedings of the 2010 ACM workshop on Cloud computing security workshop, ser. CCSW 10. ACM, 2010, pp. 6576.
5. X. Ao, Report on DIMACS Workshop on Large-Scale Internet Attacks, http://dimacs.rutgers.edu/Workshops/Attacks/internet-attack-9- 03.pdf, Sept. 2003.
6. R. Thomas, ISP Security BOF, NANOG 28, http://www.nanog.org/mtg-306/pdf/thomas.pdf, June 2003.
7. A. Mizrak, S. Savage and K. Marzullo, Detecting Compromised Routers via Packet Forwarding Behavior, IEEE Network, March 2008.
8. D. McPherson and C. Labovitz, Worldwide Infrastructure Security Report, Sept. 2006, http://www.arbornetworks.com/sp/security/report.php 5551
9. AmazonVirtual Private Cloud. http://aws.amazon.com/vpc/.
10. WindowsAzurePlatform.http://www.microsoft.com/windowsazure/.
11. CohesiveFT:VPN-Cubed. http://www.cohesiveft.com/vpncubed/.
12. T. Benson, A. Akella, A. Shaikh and S. Sahu, CloudNaaS: A Cloud Networking Platform for Enterprise Applications, SOCC 2011, Cascais, Portugal
13. J. Chase, et. al. Cloud Network Infrastructure as a Service: An Exercise in Multi-Domain Orchestration. In submission
14. P. Akritidis, W. Y. Chin, V. T. Lam, S. Sidiroglou, and K. G. Anagnostakis. Proximity breeds danger: Emerging threats in metro-area wireless networks. In In Proceedings of the 16 th USENIX Security Symposium, 2007.

15. Patrick Traynor, Kevin R. B. Butler, William Enck, Patrick McDaniel, and Kevin Borders. malnets: large-scale malicious networks ia compromised wireless access points. Security and Communication Networks, 2010.
16. Felix ”FX” Linder. Cisco Vulnerabilities. In BlackHat USA, 2003.
17. Michael Lynn. Cisco IOS Shellcode, 2005. In BlackHat USA.
18. The End of Your Internet: Malware for Home Routers, 2008.http://data.nicenamecrew.com/papers/malwareforrouter/paper.txt.
19. A. Bavier, M. Bowman, B. Chun, D. Culler, S. Karlin, S. Muir, L. Peterson, T. Roscoe, T. Spalink, and M. Wawrzoniak, Operating System Support for Planetary-Scale Network Services, in USENIX NSDI , March 2004.
20. H. Madhyastha, T. Isdal, M. Piatek, C. Dixon, T. Anderson, A. Krishnamurthy, and A. Venkataramani, iPlane: An Information Plane for Distributed Services,” in USENIX OSDI, 2006.
21. B. Augustin, X. Cuvellier, B. Orgogozo, F. Viger, T. Friedman, M. Latapy, C. Magnien, and R. Teixeira, Avoiding traceroute anomalies with Paris traceroute, in Proceedings of ACM IMC ’06, October 2006.