2013 13th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing

Security Risk Assessment of Cloud Carrier

Swetha Reddy Lenkala and Sachin Shetty
College of Engineering
Tennessee State University
Nashville,USA
Email: slenkala@tnstate.edu, sshetty@tnstate.edu

Kaiqi Xiong
College of Computing and Information Sciences
Rochester Institute of Technology
Rochester, USA
kxxics@rit.edu

Abstract—**Cloud computing based delivery model has been adopted by end-users and enterprises to reduce enterprise IT costs and complexities. The ability to offload user software and data to cloud datacenters has raised many security and privacy concerns over the cloud computing model. Significant research efforts have focused on hypervisor security and low-layer operating system implementations in cloud datacenters. Unfortunately, the role of a cloud carrier on the security and privacy of user software and data has not been well studied. A cloud carrier represents the wide area network that provides the connectivity and transport of cloud services between cloud consumers and cloud providers. In this paper, we present a risk assessment framework to study the security risk of the cloud carrier between cloud users and two cloud providers. The risk assessment framework leverages the National Vulnerability Database (NVD) to examine the security vulnerabilities of operating systems of routers within the cloud carrier. This framework provides the quantifiable security metrics of each cloud carrier, which enables cloud users to select quality of security services among cloud providers. Such security metric information is very useful in the Service Level Agreement (SLA) negotiation between a cloud user and a cloud provider. It can be also used to build a tool for verifying the commitment of an SLA. Furthermore, we implement this framework on Amazon Web Services and Windows Azure, respectively. Our experiments show that the security risks of cloud carriers on these two commercial clouds are significantly different. This finding provides guidance for a network provider to improve the security of cloud carriers.**

I. Introduction

Cloud computing is a fast emerging and popular technology which is being used by many commercial and academic organizations for computation and storage of network applications. Commercial cloud providers such as Amazon Web Services [1], Windows Azure Platform [2], Google App Engine [3], Rackspace [4], provide a variety of services ranging from infrastructure to software. Several researchers have studied the security of the Virtual Machine and low-layer operating system implementation in cloud datacenters. But there is a lack of the study to assess the security of the cloud carrier. Cloud carrier is the intermediary which provides connectivity and transport of cloud services between the cloud provider and the cloud user [8]. The study of the cloud carrier is important as the cloud users have no control over the network through which the data transports. The cloud carrier comprises of the intra-cloud network and wide-area delivery network. The intra-cloud network represents the network infrastructure inside a cloud provider's datacenters to connect the virtual instances of an application among themselves and with the shared cloud provided services [25]. The wide-area delivery network provides users access to cloud services from geographically dispersed datacenters [25]. In this paper, we focus on the security risk analysis of the wide-area delivery network within the cloud carrier. Similar analysis for the intra-cloud network will be carried out as part of future work.

The security of the data that is being transported depends on the availability of a secure cloud carrier connecting the user to the provider. Other than basic firewall capabilities, there are no other major security capabilities for protecting the data traversing between the cloud users and the providers. This may result in the unreliable cloud carrier which can compromise the security and integrity of the sensitive data that is being transmitted. If the user is offloading sensitive data through the cloud carrier, this data may be snooped, stolen or compromised. This results in the dissatisfied cloud users because the cloud carrier is out of the control of the cloud user. The risks of the cloud carrier have to be quantified to empower the user to choose the cloud provider which best suits their needs. The quantified security metrics also can be included in the service level agreements of the cloud provider so that the user can be aware of what is being promised to him for the price he is willing to pay.

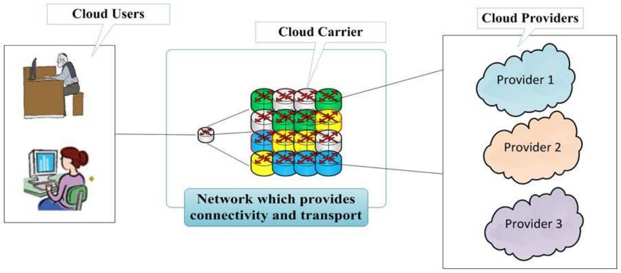

Fig. 1. Cloud Carrier

The vulnerabilities of the operating systems on the routers along the cloud carrier determine its security risk. Several studies have shown that the routers are easily exploitable compared to the computers. For example, a set of routers on a path between the cloud provider and subscriber could be vulnerable to adversarial attacks, which could lead to search queries to be snooped, IM message's to be modified, and

978-0-7695-4996-5/13 $26.00 © 2013 IEEE
DOI 10.1109/CCGrid.2013.28

financial transactions to be compromised [10], [11]. Once a router's OS vulnerabilities are exposed, an attacker may manipulate the router to selectively drop, modify, or re-route cloud information. Thus, there is an urgent need to assess the level of security mechanisms provided by the cloud carrier to protect the authenticity, integrity and confidentiality of the information flowing between the cloud subscribers and providers.

In this paper, we propose a framework to assess the security risk of the cloud carrier by analyzing the OS vulnerabilities of the routers. Our work is motivated by the observation that the security of the majority of data-sharing applications deployed on cloud infrastructures will depend on the secure cloud carrier. The data collected from the core routers in the wide-area delivery network will provide information on OS vulnerabilities. In our proposed framework, OS vulnerabilities of routers are converted to confidentiality, integrity and availability security risks by leveraging information provided by NVD [5]. Quantifying security risk will provide a holistic view of the security and privacy provided by the cloud carrier and enables the user to prioritize the requirements to choose the cloud provider that suits their needs. By using this framework, we calculate the risks of the cloud carrier connecting one data center in Amazon Web Services and one data center in Windows Azure Platform by accessing them from various PlanetLab [7] nodes which are geographically distributed across the United States. This framework can be extended to more data centers in several other cloud providers. To the best of our knowledge, there has been little work on the security implications for data-sharing applications due to OS vulnerabilities in routers on the cloud carrier.

II. Related Work

Cloud security issues have recently gained traction in the research community where the focus has primarily been on protecting servers on cloud providers(securing the low level operating systems or virtual machine implementations). Unsecured cloud servers have been proven to be crippled with novel denial-of-service attacks [9]. 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. Recent studies [10] have shown that several open and malicious ports in the routers are vulnerable to adversarial attacks. Their study shows that the malicious ports in the routers make them vulnerable but they do not propose a method to assess the vulnerabilities. Another study [11] shows that 24,000 routers around Manhattan can be compromised in less than 2 hours.

Several approaches have been used to assess the risks of the network by identifying the vulnerabilities the systems. However, not much research has been done on the implication of router vulnerabilities on the security of the cloud carrier connecting the cloud user and provider. Common Vulnerability Scoring System [12] metrics have been extensively used by the researchers to identify the vulnerabilities of the systems and estimate risks.

Ranking of the attacks was done by categorizing the vulnerabilities based on the date of discovery into past, present and recent and assigning weights to the categories [13]. A visualization tool is built by proposing new set of security metrics [14] by collecting the vulnerabilities using the network scanning tool, Nessus and NVD. The risk level is estimated for Target of Evaluation (ToE) [15] using the CVSS metrics to calculate misuse frequency and misuse impact. Based on the impact, service levels are assigned to the vulnerabilities and Markov analysis is used to get the transition between various operational service levels and thus the risk level is estimated. NVD was also used to predict the occurrence of a yet to be discovered vulnerability [17] in a software system using data mining techniques and various machine learning algorithms. Safety and Mission Critical systems have also used CVSS [18] to estimate the risks using a Bayesian Belief Network which uses frequency and impact. Another approach defines the life cycle of vulnerability [16] and its various state transitions. From the discovery of the vulnerability to the exploitation, various stages are identified and explained. The risk calculation is based on the stochastic model in which Markov analysis is used to approximate the behaviour of the system. The risk estimation uses impact related metrics from the CVSS [16]. The authors have implemented this model for estimating the risk posed by known unpatched vulnerabilities in a software system.

III. Security Risk Assessment Framework

In this section, we provide the security risk assessment framework for the wide-area delivery network within the cloud carrier based on the stochastic model for quantitative security risk estimation using vulnerability lifecycle and CVSS metrics [16]. The network and telecommunication access devices in the wide-area delivery network are predominantly core routers managed by network service providers. NVD is used to identify the vulnerabilities of these core routers. For each vulnerability, we compute the three security risks, Confidentiality Risk, Integrity Risk and Availability Risk by using the CVSS metrics provided by the NVD. Based on the risks obtained for the vulnerability, we calculate the risks for the routers in the cloud carrier.

Risk is the potential that something will go wrong [19]. In other words, risks is the possibility of the occurrence of a harmful event. Risk can be formally defined as a function of the likelihood of the adverse event happening and the impact of the adverse event [20]. So we define the risk as

$$\begin{aligned}\text{Risk} = {} & \text{Probability of the occurrence of adverse event} \\ & *\text{Impact of the adverse event} \qquad (1)\end{aligned}$$

Using the risk definition in (1) and the life cycle of the vulnerability model [16], we propose a security risk assessment framework to calculate the risks posed by the vulnerabilities in core routers. Figure 2 depicts the stochastic model describing the life cycle of a vulnerability [16]. The vulnerability life cycle begins with State 0 in which the vulnerability is not yet discovered. State 1 is next state when the vulnerability is discovered but it is yet to be disclosed. When the vulnerability is disclosed with the release and application of the patch, it is said to be in State 2. State 4 represents scenario wherein the vulnerability is disclosed without a patch. At State 5, the vulnerability is disclosed with the patch, but the patch is not applied. In State 3, the vulnerability is being exploited. The stochastic model is used to explain the life cycle of the vulnerability and the state transitions. There are 11 possible transitions between the states. The combined risk of a vulnerability being exploited is the probability of the vulnerability being in State 3. Let us denote the probability of the vulnerability being in State 3 as $Pr3$. Markov chain can be used to calculate the $Pr3$ for the vulnerability. The initial probability for each vulnerability at State 0 is given by $X1 = [100000]$. The matrix that represents all the state transitions M is shown below.

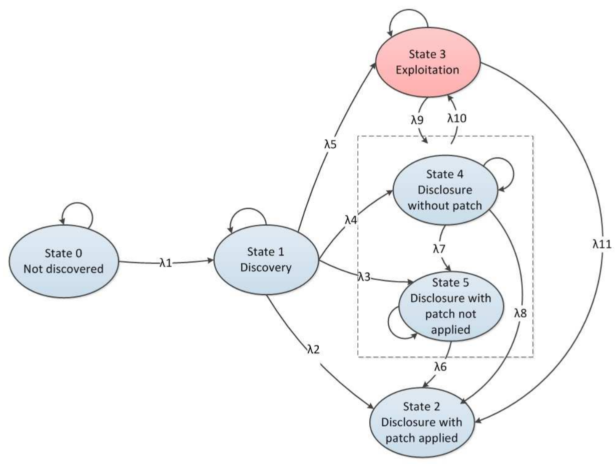

Fig. 2. Life cycle of vulnerability (reproduced from [16])

$$\begin{matrix}
(1-\lambda_1) & \lambda_1 & 0 & 0 & 0 & 0 \\
0 & (1-\lambda_2-\lambda_3-\lambda_4-\lambda_5) & \lambda_2 & \lambda_5 & \lambda_4 & \lambda_3 \\
0 & 0 & 0 & 0 & 0 & \\
0 & 0 & \lambda_1 & (1-\lambda_{10}-\lambda_{11}) & 0 & \lambda_{10} \\
0 & 0 & \lambda_8 & 0 & (1-\lambda_7-\lambda_8) & \lambda_7 \\
0 & 0 & \lambda_6 & \lambda_9 & 0 & (1-\lambda_6-\lambda_9)
\end{matrix}$$

Based on state transition matrix *M* and the initial probabilities $X1$, the state probabilities after two steps, $X3$, is obtained as follows:

$$X3 = X1 * M^2 \qquad (2)$$

$Pr3$ is the third element of the matrix $X3$ and represents the combined risk of a vulnerability being exploited. By applying the risk formula from (1), we can define the risk for the vulnerability i

$$Risk_i = Pr3_i * Impactofexploitation_i \qquad (3)$$

We calculate Confidentiality risk, Integrity risk and Availability risk based on (3). We used Confidentiality Impact value of the vulnerability which was obtained from NVD database as the impact of exploitation for the Confidentiality Risk calculation. Similarly we used the Integrity Impact for Integrity Risk calculation and Availability Impact for Availability Risk calculation. The risk equations for a vulnerability are listed as follows

$$\begin{aligned}
CRV_i &= Pr3_i * ConfidentialityImpact_i \\
IRV_i &= Pr3_i * IntegrityImpact_i \\
ARV_i &= Pr3_i * AvailabilityImpact_i \qquad (4)
\end{aligned}$$

where CRV is the Confidentiality risk of the Vulnerability, IRV is the Integrity risk of the Vulnerability and ARV is the Availability risk of the Vulnerability. Based on these equations, we calculate the risk of the routers and then the cloud carrier.

The total risk for router is the sum of the risks of the individual vulnerabilities which have been mapped to it. So the risks of a router with n vulnerabilities mapped to it is given by the following equations.

$$\begin{aligned}
CRR &= \sum_{i=1}^{n} CRV_i \\
IRR &= \sum_{i=1}^{n} IRV_i \\
ARR &= \sum_{i=1}^{n} ARV_i \qquad (5)
\end{aligned}$$

where CRR is the Confidentiality risk of the Router,IRR is the Integrity risk of the Router and ARR is the Availability risk of the Router.

The total risk for a network path in the cloud carrier is the sum of the risks of the routers which are in the path. So the risks of a path with m routers is given by the following equations.

$$\begin{aligned}
CRP &= \sum_{j=1}^{m} CRR_j \\
IRP &= \sum_{j=1}^{m} IRR_j \\
ARP &= \sum_{j=1}^{m} ARR_j \qquad (6)
\end{aligned}$$

where CRP is the Confidentiality risk of the path, IRP is the Integrity risk of the path and ARR is the Availability risk of the path.

IV. Implementation of the Framework

In this section, we present the implementation the framework presented in the previous section. The vulnerabilities in routers originate from unsecure OS. To detect these vulnerabilities, the first step is to scan the routers and perform OS fingerprinting. The fingerprinting process will provide insight into various level of OS vulnerabilities on routers at any given time. The implementation of the framework can be broken down into three sequential phases - Router Data Collection, Vulnerability Identification, Risk Calculation and Comparison. We calculate the risks of the cloud carriers for geographically distributed cloud users connected to one data center each in two cloud providers - Amazon Web Services and Windows Azure Platform. PlanetLab nodes hosted on university campuses across the United States were chosen to mimic cloud users. We categorize the routers in the cloud carrier in three groups - High Risk, Medium Risk and Low Risk. We compare the two cloud providers based on the number of routers in each group.

A. Router Data Collection

We chose one data center each from two commercial cloud providers Amazon Web Services and Windows Azure Platform for the implementation. Each cloud provider has various data centers which host the applications that provide the cloud services. These data centers are geographically distributed across the country and sometimes across the world. We created an account in both cloud providers. For Amazon Web Services, we uploaded a file in CloudFront and obtained the IP address of the data center in which the file was stored at that point of time. For Windows Azure Platform, we created Windows Azure project and deployed it to the Cloud Service in Windows Azure Platform. Next, we obtained the IP address of the data center at which hosts our project at that point of time. The data collection process is illustrated in Figure 3. PlanetLab nodes hosted by academic institutions in United States were used to access the data centers of cloud providers. We identified the PlanetLab nodes which are geographically located in the United States and hosted by academic institutions based on the IP geolocation data obtained from the Maxmind [6] database. The PlanetLab nodes were chosen based on their ability to respond to ping probes. The responsive nodes were used in our research to access the two data centers of the cloud providers. We access the data centers from each PlanetLab node once and identify the IP addresses of the routers. We collected the IP addresses of the routers by performing traceroute probing between the Planetlab nodes and the two data centers. There were 200 planetlab nodes in the United States and the traceroute probing between these nodes and cloud providers generated a very large set of router IP addresses on the cloud carrier with high spatial diversity. Next, an active OS fingerprinting tool, Xprobe2 [21], was deployed to identify the operating system of the routers on the cloud carrier. Xprobe2's signature database uses fuzzy logic for remote OS fingerprinting. This helps Xprobe2 to overcome many problems that the other active fingerprinting tools face. Xprobe2 largely uses ICMP based tests for remote OS detection. Xprobe2 provides various options to for customizing the scans. Xprobe2 takes the IP address of the remote host as a parameter and scans the host based on the options specified by the user. Xprobe2 is installed in the local computer and a shell script is written to scan all the routers that have been identified using traceroute probes..

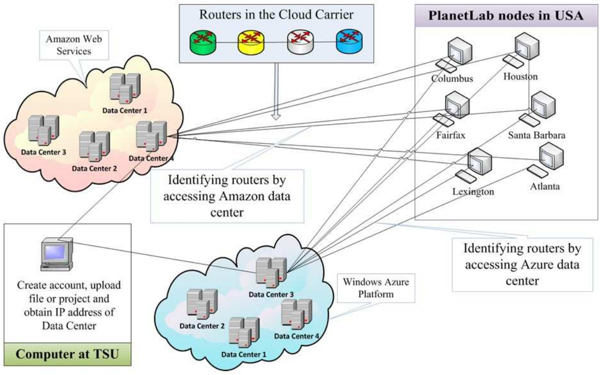

Fig. 3. Router Data collection

B. Vulnerability Identification

NVD is used to identify the vulnerabilities of the routers. To fully understand the use of NVD in the calculation of risks, it is necessary to understand the concepts of CVSS and Common Vulnerabilities and Exposures (CVE) [22]. CVSS provides an open framework to estimate and quantify the software vulnerabilities of various vendors. Before CVSS there was no common platform to identify the vulnerabilities and vendors used their own methods for scoring the vulnerabilities. National Infrastructure Assurance Council (NIAC) [23] launched CVSS in 2005. Several major organizations such as CERT, IBM and Cisco were involved in the development of CVSS. These organizations also use these metrics to prioritize the response to the vulnerabilities they encounter in their day to day activities. CVSS is currently maintained by the Forum of Incident Response and Security teams (FIRST).

CVE is a dictionary that assigns unique identifiers for all the security vulnerabilities that are publicly known. CVE is used as the industry standard for vulnerability and exposures names. Once vulnerability is discovered, it is assigned a unique CVE Identifier (e.g.: CVE-2012-0015), brief description and references such as advisories or vulnerability reports. CVE was quickly adopted by organizations and its use is widespread so much so that the organizations are producing ”CVE Compatible” products and services.

The NVD is the repository which provides CVSS scores for all CVE vulnerabilities. It was created by the government of United States to help the Department of Homeland Security to warn public about common computer vulnerabilities. It

TABLE I
CATEGORIZATION OF VULNERABILITIES

Exploit	Impact	(λ1, λ2, λ3, λ4, λ5, λ6, λ7, λ8, λ9, λ10, λ11)
High	High	(0.7, 0.1, 0.05, 0.05, 0.75, 0.3, 0.1, 0.3, 0.4, 0.1, 0.3)
High	Low	(0.5, 0.05, 0.1, 0.1, 0.65, 0.4, 0.1, 0.25, 0.3, 0.2, 0.3)
Low	High	(0.6, 0.3, 0.1, 0.1, 0.4, 0.2, 0.1, 0.3, 0.3, 0.2, 0.2)
Low	Low	(0.8, 0.1, 0.2, 0.3, 0.2, 0.1, 0.3, 0.4, 0.2, 0.3, 0.4)

is maintained by the National Institute of Standards and Technology (NIST) [24]. The NVD website provides XML feeds for all the CVE vulnerabilities with CVSS metrics for all the years from 2002 to present (2012) which can be downloaded. The data obtained from NVD is used to identify the vulnerabilities of the routers based on the operating system version running on them. The CVSS metrics obtained from the NVD are used to calculate the risks.

The XML files that contain the CVE vulnerabilities were downloaded from the NVD website. The vulnerabilities for each year are stored in a separate file. We downloaded the files for all the available years 2002 to 2012. The XML file has several attributes that describe the nature and specifics of the CVE vulnerability. For our research we do not need all these attributes. So we chose the following attributes - CVE identifier, CVSS score, CVSS vector, CVSS exploit score, CVSS impact score, vendor, product name, versions affected and description. We obtained the values of Confidentiality Impact, Integrity Impact and Availability Impact using the Access Vector and Base Equation (formula version 2.10) [12]. If vulnerability is rejected by the CVE as it is a duplicate of another, an attribute reject is added to the XML node. When we import the data into the database, we do not import the vulnerabilities that have a reject attribute. The vulnerabilities obtained from NVD are mapped to the routers based on the operating system that is running on them.

C. Risk Computation and Comparison

Before calculating the risks, we categorized the vulnerabilities based on the CVSS exploit score and CVSS impact score. This classification is important as the probability of a vulnerability being exploited is based on exploit score and impact score. All the vulnerabilities that have CVSS exploit score that is less than or equal to 5.0 were categorized as "Low exploit", greater than 5.0 are categorized as "High exploit". The same criterion was used for CVSS impact score to categorize them to "Low impact" and "High impact". This categorization classifies the vulnerabilities to four groups - High exploit and High impact, High exploit and Low impact, Low exploit and High impact, Low exploit and Low impact. We defined the state transition probabilities for each group as shown in Table 1 by predicting the behavior of the system based upon the knowledge of the system that we have.

The *Pr3* value for four sets of values were calculated as shown in Table 2.

TABLE II
Pr3 VALUES

Exploit	Impact	*Pr3*
High	High	0.525
High	Low	0.325
Low	High	0.240
Low	Low	0.160

We matched the operating system that was identified using Xprobe2 with the prodname, vendor and version attributes of the vulnerability, to identify the router vulnerabilities. Then we calculated Confidentiality Risk, Integrity Risk and Availability Risk for the vulnerabilities by using equations (4), (5) and (6). Then we calculated the risks for the routers and network paths in the cloud carrier.

We normalized the risks obtained for the paths in the Cloud Carrier. The paths were divided into three groups based on the normalized risks values High Risk ($\geq$ 0.5), Medium Risk ($\geq$ 0.3 and $<$ 0.5) and Low Risk ($<$ 0.3). The number of paths in each category was compared for the two cloud providers.

V. EXPERIMENTAL RESULTS

In this section, we provide the experimental setup for assessing the vulnerabilities of routers on the cloud carrier. As described in the earlier section, the router data collection step was implemented by probing one datacenter in Amazon Web Services and Windows Azure Platform from Planetlab nodes. Each datacenter was sent traceroute probes from 159 PlanetLab nodes. To avoid any legal issues we decided not to use the names of cloud providers when discussing the results, but refer to them as cloud A and cloud B. We compare the normalized values of Confidentiality Risk, Integrity Risk and Availability Risk of the cloud carrier for the two cloud providers. We then compared the security risk for the cloud providers by categorizing the routers of the cloud carrier based on geographical location of the PlanetLab node from which the data center was accessed.

A. Risk Assessment

Figure 4 shows the comparison of Confidentiality risk of the cloud carrier for the two cloud providers. We see that the high risk and medium risk groups are dominated by cloud B where as the low risk group is dominated by cloud A. We see a similar trend when we compare the Integrity risk as shown in Figure 5. The Availability risk also follows the same trend as shown in Figure 6.

B. Regionwise comparison of risks

Of the 159 nodes which were used to access the data centers, 38 nodes belonged to the Northeast region, 37 belonged to the Midwest region, 34 belonged to the West region and 50 belonged to the South region. Figure 6 shows the regionwise distribution of PlanetLab nodes. Figure 7 shows the

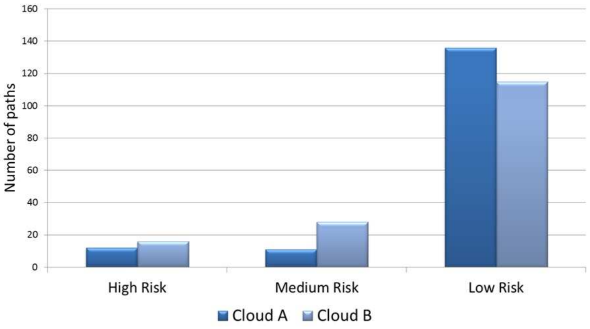

Fig. 4. Comparison of Confidentiality Risk

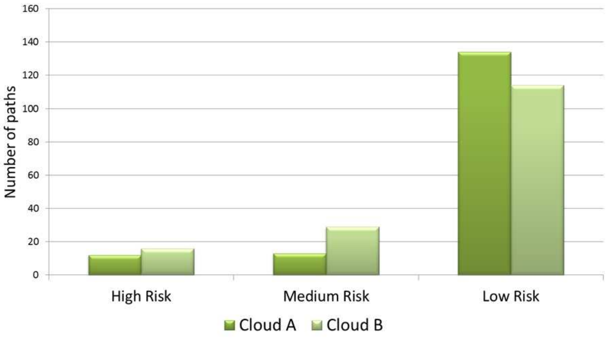

Fig. 5. Comparison of Integrity Risk

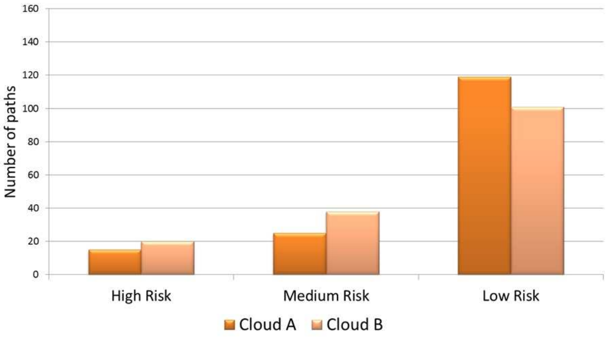

Fig. 6. Comparison of Availability Risk

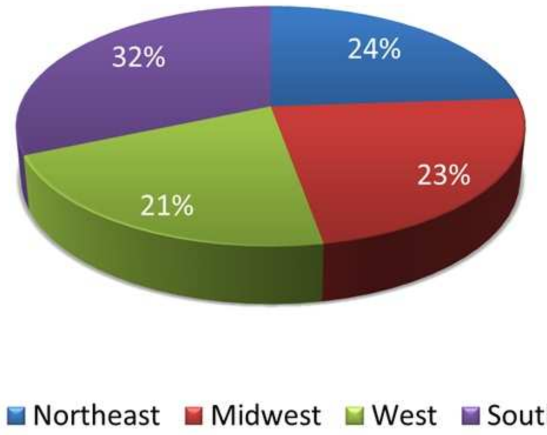

Fig. 7. Regionwise distributions of PlanetLab nodes

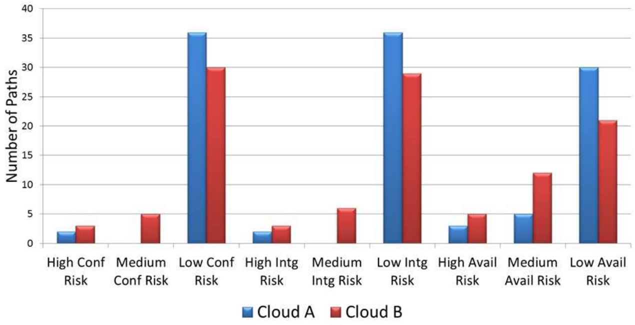

Fig. 8. Comparison of risks for cloud users in the Northeast region

comparison of network paths in cloud carrier for the two cloud providers in the Northeast region. Each network path comprises of unique set of core routers between one PlanetLab node and the datacenter. Upon examining , we can conclude that in the Northeast region, Cloud B dominates the High Risk and Medium Risk categories whereas Cloud A dominates the Low Risk category for all the three risks.

Figure 8 shows the comparison of paths in cloud carrier for the two cloud providers in the Midwest region. Upon examining, we can conclude that the trend in Midwest is similar to that of Northeast. Cloud B dominates the High Risk and Medium Risk categories whereas Cloud A dominates the Low Risk category for all the three risks. Figure 9 shows the comparison of paths in cloud carrier for the two cloud

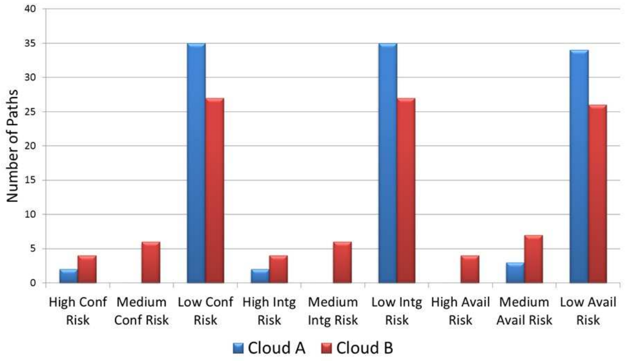

Fig. 9. Comparison of risks for cloud users in the Midwest region

providers in the West region. The risk distribution in the West is different from the Northeast and Midwest regions. We notice that in the West region, Cloud A and Cloud B have equal paths in the High category for Confidentiality and Integrity Risks whereas Cloud A dominates the High category for the Availability Risk. We also notice that in the Medium Risk category Cloud A dominates Cloud B and in the Low Risk category Cloud B dominates for all the three risks. Figure 10 shows the comparison of paths in cloud carrier for the two cloud providers in the South region. Upon examining the data shown in the graph, we can conclude that in the South region, Cloud B dominates the High Risk and Medium Risk categories whereas Cloud A dominates the Low Risk category for all the three risks. The region wise comparison of the data shows that Cloud B dominates the high risk category in 3 regions Northeast, Midwest and South whereas in the West Cloud A dominates the High Risk category.

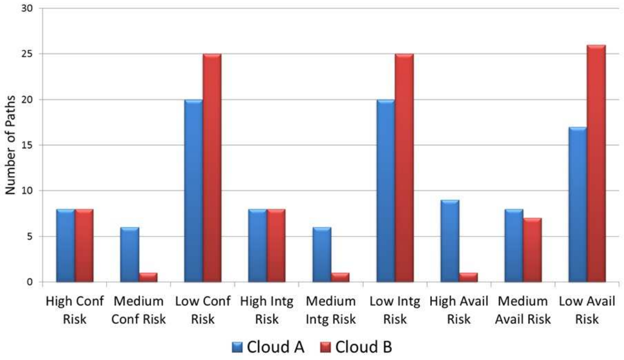

Fig. 10. Comparison of risks for cloud users in the West region

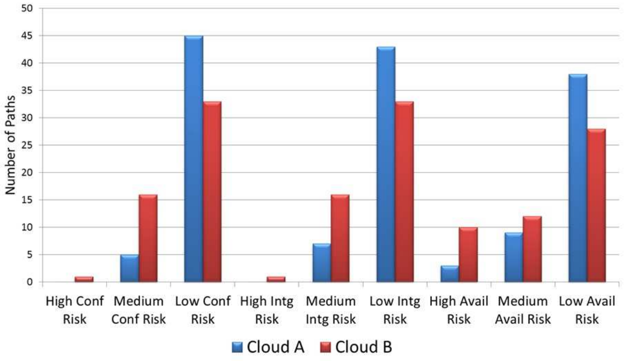

Fig. 11. Comparison of risks for cloud users in the South

C. Sensitivity Analysis

Sensitivity analysis is a technique which is used to determine the variation in output when the dependent variable is changed. This technique is commonly used in risk analysis systems to test the robustness of the model. The effectiveness of the risk assessment framework hinges on the availability of accurate state transition probability estimates. To verify the robustness of the framework, we modified the values of the state transition probabilities in the stochastic model and observed if the modified model had any impact on the risk categories.

Specifically, we increase and decreasing the state transition probabilities by 5%, 10% and 20% respectively. For each modification to the state transition probabilities, we compared Confidentiality Risk, Integrity Risk and Availability Risk metrics for the cloud carrier between the PlanetLab nodes and the two datacenters. From the comparison, we noticed that as the risk metrics were directly proportional to the modification to the state transition probabilities. But, the change in risk metrics did not impact the number of paths in each category.

VI. Ethical Considerations

Our experiments to implement the framework for risk calculation, collect the data from real world routers. This usually raises an ethical debate as scanning remote network devices can sometimes lead to adverse attacks. At the same time, a robust framework for risk assessment is very difficult without collecting data from the real world. Simulation tools cannot replicate the randomness of the real world network traffic. A recent journal article that discusses the ethics of security vulnerability research [26], states that this type of zealous vulnerability research serves important social functions. This approach is neither illegal or unethical under the US laws. While accessing the routers to collect the vulnerability information we have taken utmost care not to disturb the host functions. We used minimum external resources to accurately collect the router information. The target networks in /24 blocks were scanned in a non-sequential order so that no organization is overwhelmed with our probes. We did not scan any router unnecessarily and we specified appropriate Xprobe2 options to avoid stealth scanning.

VII. Conclusion and Future Work

As various cloud providers offer various services, it is important for cloud user to choose the cloud provider which is connected to the most cloud carrier with minimum security risk. In this paper, we proposed a risk assessment framework to assess the security of the cloud carrier between cloud users and cloud providers. Our framework characterizes the security of the cloud carrier, including confidentiality, integrity and availability metrics, and compares these metrics for cloud carriers connected to multiple cloud providers. Our preliminary results benchmark and compare the security of the cloud carrier connected to datacenter governed by two commercial cloud providers. The results show that the security metrics of the cloud carrier connected to different cloud providers can differ significantly, suggesting that a comparison framework of cloud carriers is extremely important. For future work, we want to compare the security metrics for cloud carrier connected to multiple data centers for more than two cloud providers. As router OSs are patched periodically, we plan to repeat the process of assessing vulnerabilities of routers routinely. We would also investigate into a formal method to estimate the state transition probabilities in our risk assessment model.

Acknowledgment

This work is supported in part by NSF RIA grant (HRD-1137466), AFOSR grant FA9550-09-1-0165, DHS SLA grant (2011-ST-062-0000043 and 2011-ST-062-0000046).

References

[1] ”Amazon Web Services.” [Online]. Available: http://aws.amazon.com/

[2] ”Windows Azure Platform.” [Online]. Available: https://www.windowsazure.com/en-us/

[3] ”Google App Engine.” Google, [Online]. Available: https://developers.google.com/appengine/

[4] ”Rackspace.” [Online]. Available: http://www.rackspace.com/

[5] ”National Vulnerability Database.” [Online]. Available: http://nvd.nist.gov/

[6] Maxmind, ”Maxmind - GeoIP Database Installation Instructions.” [Online]. Available: http://www.maxmind.com/en/installation?city=1

[7] PlanetLab, ”An open platform for developing, deploying, and accessing planetaryscale.” [Online]. Available: http://www.planet-lab.org/

[8] F. Liu, J. Tong, J. Mao, R. B. Bohn, J. V. Messina, M. L. Badger and D. M. Leaf, ”NIST Cloud Computing Reference Architecture.” Cloud Computing Program Information Technology Laboratory National Institute of Standards and Technology, 2011. [Online]. Available: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505

[9] H. Liu, ”A new form of DOS attack in a cloud and its avoidance mechanism,” in *CCSW ’10 Proceedings of the 2010 ACM workshop on Cloud computing security workshop* , New York, 2010.

[10] N. Luna, S. Shetty, T. Rogers and K. Xiong, ”Assessing Network Path Vulnerabilities for Secure Cloud Computing,” in *First GENI Research and Educational Experiment Workshop*, Los Angeles, 2012.

[11] P. Akritidis, W. Chin, V. Lam, S. Sidiroglou and K. Anagnostakis, ”Proximity breeds danger: emerging threats in metro-area wireless networks,” in *SS’07 Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium* , Berkeley, 2007.

[12] P. Mell, K. Scarfone and S. Romanosky, ”A Complete Guide to the Common Vulnerability Scoring System Version 2.0,” [Online]. Available: http://www.first.org/cvss/cvss-guide.pdf

[13] J. A. Wang, H. Wang, M. Guo, Z. Linfeng and J. Camargo, ”Ranking Attacks Based on Vulnerability Analysis,” in*43rd International Conference on System Sciences*, Hawaii , 2010.

[14] K. Sun, S. Jajodia, J. Li, Y. Cheng, W. Tang and A. Singhal, ”Automatic Security Analysis Using Security Metrics,” in *MILITARY COMMUNICATIONS CONFERENCE, 2011 - MILCOM 2011*, Baltimore, MD, 2011.

[15] S. H. Houmb and V. N. Franqueira, ”Estimating ToE Risk Level using CVSS,” in *2009 International Conference on Availability, Reliability and Security*, Fukuoka, 2009.

[16] H. Joh and Y. K. Malaiya, ”Defining and Assessing Quantitative Security Risk Measures Using Vulnerability Lifecycle and CVSS Metrics,” in *SAM’11 The 2011 International Conference on Security and Management* , Las Vegas, 2011.

[17] S. Zhang, D. Caragea and X. Ou, ”An Empirical Study on Using the National Vulnerability Database to Predict Software Vulnerabilities,” in *International conference on Database and expert systems applications (DEXA’11)*,Toulouse, France , 2011.

[18] S. Houmb, V. Nunes Leal Franqueira and E. Engum, ”Estimating Impact and Frequency of Risks to Safety and Mission Critical Systems Using CVSS,” in *ISSRE Supplemental Proceedings: 1st Workshop on Dependable Software Engineering*, Seattle, 2008.

[19] B. S. Blanchard and W. J. Fabrycky, Systems Engineering and Analysis, Pearson Prentice Hall, 2006.

[20] G. Stoneburner, A. Goguen and A. Feringa, ”Risk Management Guide for Information Technology Systems,” in *National Institute of Standards and Technology Special Publication*, 2002.

[21] O. Arkin, F. Yarochkin and M. Kydyraliev, ”The Present and Future of Xprobe2 The Next Generation of Active Operating System Fingerprinting.” [Online]. Available: http://www.net-security.org/dl/articles/Present_and_Future_Xprobe2-v1.0.pdf

[22] ”Common Vulnerabilities and Exposures.” [Online]. Available: http://cve.mitre.org/about/index.html

[23] ”National Infrastructure Advisory Council.” [Online]. Available: http://www.dhs.gov/national-infrastructure-advisory-council

[24] ”National Institute of Standards and Technology.” [Online]. Available: http://www.nist.gov/index.html

[25] A. Li, et. al., ”CloudCmp: Comparing Public Cloud Providers,” *Internet Measurement Conference*, 2010.

[26] A. M. Matwyshyn, A. Cui, A. D. Keromytis and S. Stolfo, ”Ethics in Security Vulnerability Research,” *IEEE Security & Privacy*, vol. 8, no. 2, pp. 67 - 72 , 2010.