Current Issues on Cloud Computing Security and Management

Pedro Artur Figueiredo Vitti, Daniel Ricardo dos Santos, Carlos Becker Westphall, Carla Merkle Westphall, Kleber Magno Maciel Vieira

Networks and Management Laboratory

Federal University of Santa Catarina

Outline

1. INTRODUCTION
2. RELATED WORKS
3. SECURITY CONCERNS IN CLOUD COMPUTING
4. CLOUD MONITORING
5. SECURITY CONCERNS IN SLA
6. CLOUD SECURITY MONITORING
7. CASE STUDY

Outline

8. KEY LESSONS LEARNED
9. CONCLUSIONS AND FUTURE WORKS
10. SOME REFERENCES

1. INTRODUCTION

- Numerous threats and vulnerabilities that become more important as the use of the cloud increases, as well as, concerns with stored data and its availability, confidentiality and integrity.
- Need for monitoring tools and services, which provide a way for administrators to define and evaluate security metrics for their systems.

1. INTRODUCTION

- We propose a cloud computing security monitoring tool based on our previous works on both security and management for cloud computing.
- Features of cloud computing such as virtualization, multi-tenancy and ubiquitous access provide a viable solution to service provisioning problems.

1. INTRODUCTION

- What are the new risks associated with the cloud and what other risks become more critical?
- We provide some background in security concerns in cloud computing, briefly describe a previous implementation of a monitoring tool for the cloud, show how security information can be summarized and treated under a management perspective.

2. RELATED WORKS

- Uriarte and Westphall [4] proposed a monitoring architecture devised for private Cloud that considers the knowledge requirements of autonomic systems.
- Fernades et al. [5] surveys the works on cloud security issues, addressesing key topics: vulnerabilities, threats, and attacks, and proposes a taxonomy for their classification.

2. RELATED WORKS

- Cloud Security Alliance [6] has identified the top nine cloud computing threats. The report shows a consensus among industry experts.
- Mukhtarov et al. [7] proposed a cloud network security monitoring, which is based on flow measurements and implements an algorithm that detects and responds to network anomalies.

3. SECURITY CONCERNS IN CLOUDS

- Each cloud technology presents some kind of known vulnerability: Web Services, Service Oriented Architecture (SOA), Representational State Transfer (REST) and Application Programming Interfaces (API), virtualizarion, network infrastructure... [8].
- The usual three basic issues of security: availability, integrity and confidentiality are still fundamental in the cloud.

3. SECURITY CONCERNS IN CLOUDS

- Multi-tenant characteristic: one single vulnerable service in a virtual machine, exploitation of many services hosted in the same physical machine.
- Web applications and web services: susceptible to a lot of easily deployed attacks such as SQL injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) and session hijacking.

3. SECURITY CONCERNS IN CLOUDS

- Another important topic in cloud security is Identity and Access Management, because now data owners and data providers are not in the same trusted domain [9].
- The main security management issues of a Cloud Service Provider (CSP) are: availability management, access control management, vulnerability management, patch and configuration management, countermeasures, and cloud usage and access monitoring [10].

3. SECURITY CONCERNS IN CLOUDS

- The cloud is an easy target for an intruder trying to use its abundant resources maliciously, and the IDS also has to be distributed, to be able to monitor each node [11].
- Distributed Denial of Service (DDoS) attacks can have a much broader impact on the cloud, since now many services may be hosted in the same machine. DDoS is a problem that is still not very well handled.

3. SECURITY CONCERNS IN CLOUDS

- To maintain data security a provider must include, at least: an encryption schema, an access control system, and a backup plan [12].
- When moving to the cloud it is important that a prospective customer knows to what risks its data are being exposed. Some of the key points considered in this migration are presented in [13, 20, and 21].

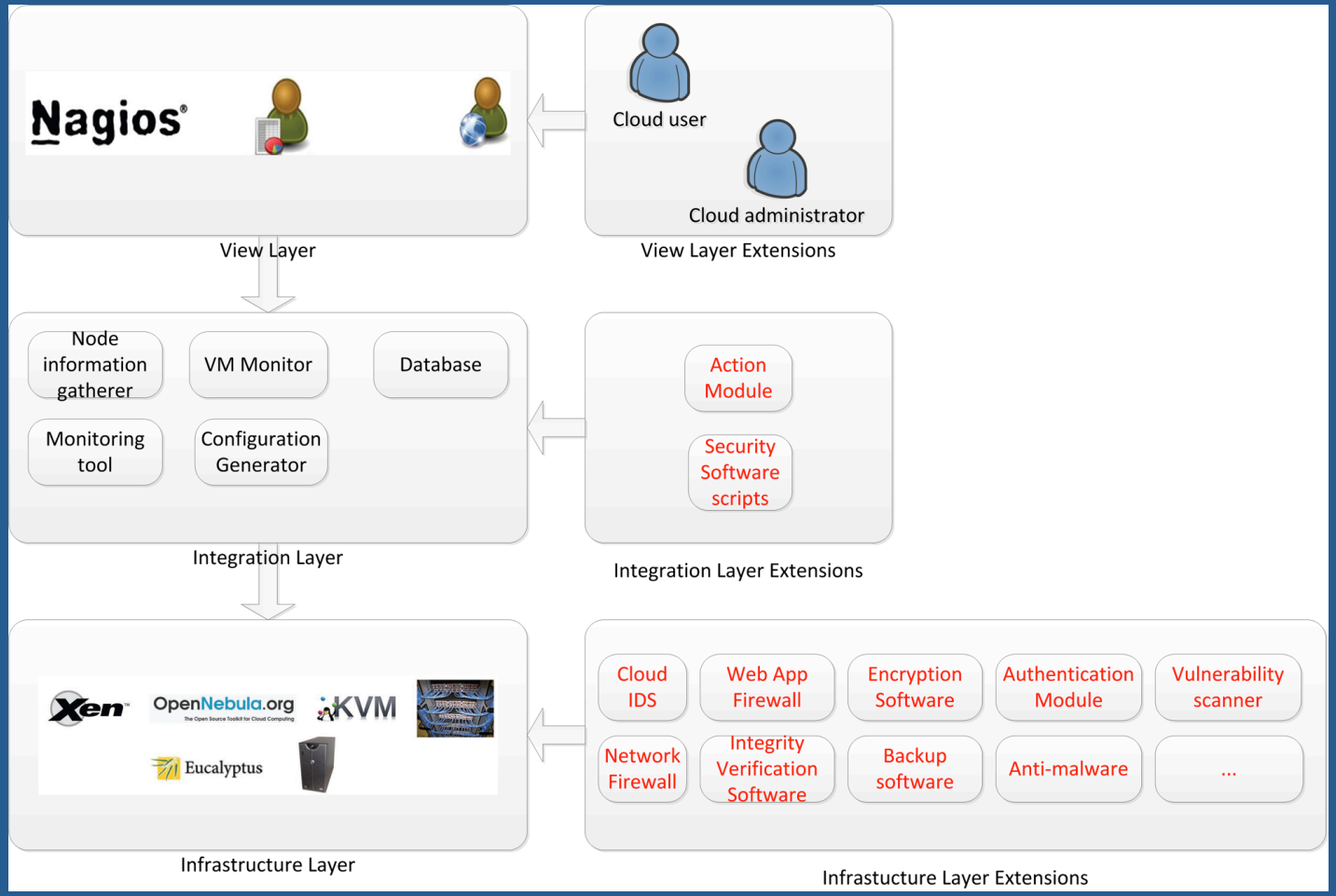
3. SECURITY CONCERNS IN CLOUDS

- Legal compliance is fundamental when dealing with cloud computing. In the cloud world, it is possible that data cross many jurisdiction borders.
- Availability and confidentiality are critical to the telecommunications business and if services are being deployed in a public cloud without a proper SLA [15].

4. CLOUD MONITORING

- Our team has previously proposed and implemented an open-source cloud monitoring architecture and tool called the Private Cloud Monitoring System (PCMONS) [14].
- The architecture of the system is divided in three layers: Infrastructure; Integration; and view.

4. CLOUD MONITORING



5. SECURITY CONCERNS IN SLA

- Providers must have ways to ensure their clients that their data is safe and must do so by monitoring and enhancing security metrics.
- SLAs may also be used in the definition, monitoring and evaluation of security metrics, in the form of Security SLAs, or Sec-SLAs [15].

6. CLOUD SECURITY MONITORING

- We now propose an extension to the PCMONS architecture and tool to enable security monitoring for cloud computing.
- We also present the security metrics which we consider adequate to be monitored in a cloud infrastructure and which provide a good picture of security as a whole in this environment.

6. CLOUD SECURITY MONITORING

- The tool uses data and logs gathered from security software available in the monitored systems, such as IDSs, anti-malware software, file system integrity verification software, backup software, and web application firewalls.
- The entities involved in the definition, configuration and administration of the security SLAs and metrics are:

6. CLOUD SECURITY MONITORING

- Cloud users; Cloud administrators; and Security applications.
- Data Security Metrics, Access Control Metrics and Server Security Metrics are shown in Table I, Table II, and Table III, respectively.
- If a virtual machine has had a huge number of failed access attempts in the last hours we may want to lock any further access.

6. CLOUD SECURITY MONITORING

TABLE I. DATA SECURITY METRICS

Metric	Description
Encrypted Data?	Indicates whether the data stored in the VM is encrypted
Encryption Algorithm	The algorithm used in the encryption/decryption process
Last backup	The date and time when the last backup was performed
Last integrity check	The date and time when the last file system integrity check was performed

6. CLOUD SECURITY MONITORING

TABLE II. ACCESS CONTROL METRICS

Metric	Description
Valid Accesses	The number of valid access attempts in the last 24 hours
Failed access attempts	The number of failed access attempts in the last 24 hours
Password change interval	The frequency with which users must change passwords in the VM's operating system

6. CLOUD SECURITY MONITORING

TABLE III. SERVER SECURITY METRICS

Metric	Description
Malware	Number of malware detected in the last anti-malware scan
Last malware scan	The date and time of the last malware scan in the VM
Vulnerabilities	Number of vulnerabilities found in the last scan
Last vulnerability scan	The date and time of the last vulnerability scan in the VM
Availability	Percentage of the time in which the VM is online

7. CASE STUDY

- We have implemented the metrics presented in Tables I-III and gathered the data generated in a case study.
- The following software were used to gather the security information: dm-crypt (encryption), rsync (backup), tripwire (filesystem integrity), ssh (remote access), clamAV (anti-malware), tiger (vulnerability assessment) and uptime (availability).

7. CASE STUDY

oneadmin i-322 stratus	AVAILABILITY	OK	2014-08-14 15:58:51	4d 1h 16m 40s	1/4	99.93%
	CIPHER	OK	2014-08-14 15:58:51	4d 1h 16m 40s	1/4	AES
	SSH_VALID	OK	2014-08-14 15:58:51	4d 1h 16m 40s	1/4	25
	IS_ENCRYPTED	OK	2014-08-14 15:58:51	4d 1h 16m 40s	1/4	yes
	LAST_BACKUP	OK	2014-08-14 15:58:51	4d 1h 16m 40s	1/4	2014-08-14 18:30:48
	LAST_INTEGRITY	OK	2014-08-14 15:58:51	4d 1h 16m 40s	1/4	2014-08-14 10:23:50
	LAST_MALWARE_SCAN	OK	2014-08-14 15:58:51	4d 1h 16m 40s	1/4	2014-08-14 10:02:42
	VULNERABILITIES	CRITICAL	2014-08-14 15:58:51	4d 1h 16m 40s	1/4	111
	MALWARE_FOUND	CRITICAL	2014-08-14 15:58:51	4d 1h 16m 40s	1/4	5
	PASSWORD_INTERVAL	OK	2014-08-14 15:58:51	4d 1h 16m 40s	1/4	180 days
	SSH_FAIL	WARNING	2014-08-14 15:58:51	4d 1h 16m 40s	1/4	545

7. CASE STUDY

- It represents how the metrics are shown in Nagios and it is possible to see the vision that a network administrator has of a single machine.
- The metrics HTTP CONNECTIONS, LOAD, PING, RAM and SSH are from the previous version of PCMONS and are not strictly related to security, but they are show combined.

8. KEY LESSONS LEARNED

- The tool helps network and security administrator perceive violations to Sec-SLAs and actively respond to threats.
- The major piece of technology used to provide security in the cloud is cryptography.
- Data leakage and data loss are possibly the greatest concerns of cloud users.
- Backup and recovery are also fundamental tools to ensure the availability of customer data.

8. KEY LESSONS LEARNED

- SLAs are fundamental to provide customers with the needed guarantees.
- Definition of requirements and the monitoring of security metrics remain an important open research topic.
- The major decisions in this work were related to the security metrics and the software used to provide the necessary security data.

8. KEY LESSONS LEARNED

- The idea of analyzing logs to obtain security data is classical in information security and it seemed like a natural approach to our challenges.
- To read, parse and present the data we chose to use the Python programming language because it already formed the base of PCMONS (Private Cloud Monitoring System).

8. KEY LESSONS LEARNED

- Setting up a reliable testing environment was also extremely important to the success of the project.
- An important feature of this extension of PCMONS is that it can run over OpenNebula, OpenStack and CloudStack.
- The use of scripting languages in the development process, such as Python and Bash Script allowed us to define the metrics.

9. CONCLUSION AND FUTURE WORK

This work described:

- A few of our previous works in the field of Cloud Computing and how to bring them all together in order to develop a cloud security monitoring architecture; and

- The design and implementation of a cloud security monitoring tool, and how it can gather data from many security sources inside VMs and the network.

9. CONCLUSION AND FUTURE WORK

As future work:

- We can point to the definition and implementation of new metrics and a better integration with existing Security SLAs; and
- It would be important to study the integration of the security monitoring model with other active research fields in cloud security, such as Identity and Access Management and Intrusion Detection Systems.

10. REFERENCES

References indicated in this presentation:

- [4] R. B. Uriarte and C. B. Westphall, "Panoptes: A monitoring architecture and framework for supporting autonomic clouds," in IEEE Network Operations and Management Symposium, 2014.
- [5] D. Fernandes et al., "Security issues in cloud environments: a survey," International Journal of Information Security, 2014.

10. REFERENCES

References indicated in this presentation:

- [6] T. T. W. Group et al., "The notorious nine: cloud computing top threats in 2013," Cloud Security Alliance, 2013.
- [7] M. Mukhtarov et al., "Cloud network security monitoring and response system," CLOUD COMPUTING 2012 (The Third International Conference on Cloud Computing, GRIDs, and Virtualization).

10. REFERENCES

References indicated in this presentation:

- [8] B. Grobauer, et al., "Understanding cloud computing vulnerabilities," Security Privacy, IEEE, vol. 9, no. 2, March-April 2011.
- [9] X. Tan and B. Ai, "The issues of cloud computing security in high-speed railway," in Electronic and Mechanical Engineering and Information Technology (EMEIT), 2011 International Conference on, vol. 8, 2011.

10. REFERENCES

References indicated in this presentation:

- [10] F. Sabahi, "Cloud computing security threats and responses," in Communication Software and Networks (ICCSN), IEEE 3rd International Conference on, 2011.
- [11] K. Vieira, et al., "Intrusion detection for grid and cloud computing," IEEE IT Professional, vol. 12, no. 4, 2010.

10. REFERENCES

References indicated in this presentation:

- [12] L. Kaufman, "Data security in the world of cloud computing," Security Privacy, IEEE, vol. 7, no. 4, 2009.
- [13] S. Chaves et al., "Customer security concerns in cloud computing," in ICN, The Tenth Inter- national Conference on Networks, 2011.

10. REFERENCES

References indicated in this presentation:

- [14] S. A. Chaves, R. B. Uriarte, and C. B. Westphall, "Toward an architecture for monitoring private clouds,," Communications Magazine, IEEE, vol. 49, n. 12, 2011.
- [15] S. A. Chaves, C. B. Westphall, and F. Lamin, "Sla perspective in security management for cloud computing," in Networking and Services (ICNS), 2010 Sixth International Conference on, 2010.

10. REFERENCES

References indicated in this presentation:

- [20] D. R. dos Santos, C. M. Westphall, and C. B. Westphall, "A dynamic risk-based access control architecture for cloud computing," in IEEE Network Operations and Management Symposium (NOMS), 2014.
- [21] P. F. SIlva et al., "An architecture for risk analysis in cloud," in ICNS, The Tenth International Conference on Networking and Services, 2014.