J Inf Process Syst, Vol.12, No.2, pp.226~233, June 2016
http://dx.doi.org/10.3745/JIPS.03.0049

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Mitigating Threats and Security Metrics in Cloud Computing

Jayaprakash Kar* and Manoj Ranjan Mishra**

Abstract

Cloud computing is a distributed computing model that has lot of drawbacks and faces difficulties. Many new innovative and emerging techniques take advantage of its features. In this paper, we explore the security threats to and Risk Assessments for cloud computing, attack mitigation frameworks, and the risk-based dynamic access control for cloud computing. Common security threats to cloud computing have been explored and these threats are addressed through acceptable measures via governance and effective risk management using a tailored Security Risk Approach. Most existing Threat and Risk Assessment (TRA) schemes for cloud services use a converse thinking approach to develop theoretical solutions for minimizing the risk of security breaches at a minimal cost. In our study, we propose an improved Attack-Defense Tree mechanism designated as iADTree, for solving the TRA problem in cloud computing environments.

Keywords

Dynamic Access Control, Risk Assessment, Security Intelligence

1. Introduction

Cloud computing is constantly attracting interests from a broad spectrum of users and organizations. On one hand, users see cloud computing as the integration of computing and communication capabilities, which provide avenues for better information processing with a greater ease of accessibility and flexibility. The cloud service provider (CSP) must assess the operational risks of different cloud computing applications and then select the particular applications that meet the user's service requirements while simultaneously ensuring that their data remains secure. However, cloud computing services are exposed to multiple, changeable threats from malicious attackers. In practice, cloud computing services are secured by various information security technologies and the residual risk to the network is evaluated by means of a Threat Risk Assessment (TRA) process [1]. The TRA issue typically involves collecting sufficient system vulnerabilities from multiple information assets to determine a set of feasible defensive strategies given the constraint on both the attack cost (i.e., the attack difficulty) and the defense cost (i.e., the security cost). Accordingly, we propose an improved Attack-Defense Tree system (iADTree) for solving the TRA problem in the context of cloud computing applications [2].

Manuscript received January 29, 2015; accepted September 7, 2015.
Corresponding Author: Jayaprakash Kar (jgopabandhu@kau.edu.sa)
* Dept. of Information Systems, Faculty of Computing & Information Technology, Information Security Research Group, King Abdulaziz University, Jeddah, Saudi Arabia (jgopabandhu@kau.edu.sa)
** School of Computer Application, KIIT University, Bhubaneswar, India (mrmishrafca@kiit.ac.in)

Dynamic access control models, such as those based on risk and context, have been developed to deal with the problems of highly dynamic environments. Also, these models are able to deal with exceptional access requests when a normally unauthorized user must be granted access to perform a critical action. This is known as "breaking the glass." In this paper, we present a model for dynamic risk-based access control for cloud computing. The system manages the users' access to cloud resources using the aggregation of risk metrics that are defined in risk policies, which are created by the owners of the resources. This combination provides great flexibility for access control for both the users and the CSPs [3].

2. Common Threats and Risks

2.1 Distributed Denial of Service (DDoS)

DDoS is widely considered to be an ongoing problem. Multiple machines launching an attack on infrastructure to the point of derailing existing services prompted researchers to address a new tactic of detecting, mitigating, and filtering at the TCP/IP layer. However, in cloud computing, communication and information transaction processes operate at the application layer. Therefore, securing this layer is considered to be the major motivation for many researchers. Web services are prone to these attacks. XML messages are sent to the Web server to prevent legitimate access to the system. Fortunately, H-Dos are less known, but it is used as to intentionally flood HTTP messages via an attack in order to derail legitimate web traffic. The combination of these two attacks is known as HX-DDoS [4,5].

2.2 Multi-Tenancy Security Threats

The fundamental security issue with multi-tenancy is clients using cloud computing by employing single and the same computer hardware to share and process information. This presents a number of challenges in terms of compliance, security, and privacy. Moreover, the lack of user network isolation makes cloud computing vulnerable to threats, as does the lack of efficient bandwidth and traffic isolation, since malicious tenants may launch attacks at other tenants in the same cloud data center. Existing approaches to access control of the clouds do not scale well to multi-tenancy requirements because they are based merely on individual user IDs.

2.3 Side-Channel Attacks

Side-channel attacks pose a great risk to multi-tenancy environments. They are based on information obtained from bandwidth monitoring. They typically occur due to a lack of authorization mechanisms for sharing physical resources.

3. iADTree Mechanism for TRA in Cloud Computing Environments

This section describes the iADTree mechanism that we are proposing for identifying the attacker's profile, estimating the attack and defense costs associated with each attack path, and selecting the appropriate safeguards to minimize the risk of security breaches. For large-scale open networks

identifying the attack profile, predicting the likelihood of a successful attack, and estimating the cost of appropriate countermeasures represents a significant challenge. The aim in solving the TRA problem is to identify a feasible set of defense solutions that are subject to certain constraints (e.g., a limitation on the defense cost). Our iADTree mechanism recognizes two basic types of events: attack events and defense events. Attack events are sub-classified as either detection events or attack events, while defense events are sub-classified as either deception events (e.g., deploying honeypots in the network) or countermeasure events (e.g., deploying fireworks or intrusion detection systems in the network). In solving the TRA problem, the defender must estimate the probability of a successful attack at each node in the iADTree. The success probability at the root node (goal) can be estimated by FTA formula. To protect the system, a defender must identify the threat profile and potential attack events by traversing each of the possible attack paths in the tree. In practice, a defender generally selects the smallest set of countermeasures possible to protect against the maximum number of attack events [3].

3.1 Solving the TRA Problem Using the iADTree

This section describes using the proposed iADTree mechanism in solving the TRA problem. In describing the TRA process, it is assumed that the attack profile is expressed in the form of an attack tree (AT), and the TRA problem is solved using a four-phase procedure.

- Phase I (Asset definition): This phase classifies all of the IT assets in the organization in terms of their value and vulnerability (as quantified by their CVSS scores).
- Phase II (Threat assessment): This phase identifies the profile of the suspected attack and evaluates the corresponding success probability and loss impact.

    1. Collect malware: Dionaea, a honeypot, is used to capture the suspected malware.
    2. Signature analyses: The possible attack profile is examined using TaiWan Malware Analysis Net (TWMAN). The signature analysis process commences by placing the suspected malware into the queue at the server site. Once the suspect malware starts running, the system loops continuously for 10 minutes in order to allow the infection process to take place. Once time is up, a copy of the RAM image is placed in the root of the system drive and the server then reboots. In addition, the TFTP service on the TRUMAN server modifies the client's boot state. When the client boots up, it saves a complete image of the local system partition in the server and then restores itself to a clean baseline image. For handset devices, the virus signature is then examined using a Droidbox. The Droidbox signature extraction process is carried out according to the three steps listed below:

        - Step 1: Download the suspected app (.apk) to the Droidbox platform.
        - Step 2: Commence recording the system activities and network connections.
        - Step 3: Perform signature analysis.

- Phase III (Risk assessment): In evaluating the effectiveness of the iADTree solving the TRA problem for cloud computing services, a set of performance metrics are applied at each node. Let the threat i be composed of n basic attack actions, which are represented by n child nodes (j = 1, …, n) in the iADTree. The probabilistic analysis metrics are defined in terms of both the AND-

gate and OR-gate formulas of the FTA and are used to compute the Return On Attack (ROA) and Return On Investment (ROI) values for each leaf node in the tree in such a way that the risk and ROA of the top item can be determined.

- Phase IV (Recommendations assessment): Generally speaking, the decision to launch a system attack depends on the perceived tradeoff between the ROA and the attack cost. Having decided to launch an attack, the attacker may adopt various offensive strategies (OSs) in response to the countermeasures put in place by the defender. In practice, a defender may adopt one of three different defensive strategies in order to secure the network [2], which are as listed below:

  a. Defensive Strategy I: Select the countermeasures that reduce the residual risk with the minimal defense cost (i.e., max ROI).
  b. Defensive Strategy II: Select the countermeasures that defend against the maximum number of attacks (events) with the minimal defense cost.
  c. Defensive Strategy III: Select the countermeasures that handle the maximum number of attack paths (i.e., mini-cuts) with the minimal defense cost.

4. Access Management

The cloud computing paradigm has been successful because of its scalability and reduced costs, but some researcher claim that in order to use its full potential, a step must be taken toward cloud federations.

It is comprised of services from different providers aggregated in a set that supports three basic interoperability features: resource migration, resource redundancy, and the combination of complementary resources or services. Several proposals and architectures for cloud federations have been discussed in the research related to this topic but they all share the same idea of aggregating sets of clouds through the use of standard protocols, which allows them to interact with and utilize each other's resources. This is also known as multi-clouds or clouds of clouds. The main benefits of this model are an increase in scalability, availability, and reduced costs, because providers can outsource their resources. It is also expected that the migration of resources improves interoperability among clouds, avoiding problems such as vendor lock-in.

4.1 Identity and Access Management

Identity and Access Management includes the processes related to the identification, authentication, authorization, and accountability of users in computer systems. Authorization or access control is the process through which the system ensures that access requests are validated with well-defined rules. Those rules are known as policies and the way that these policies are defined and managed constitutes an access control model. In Federated Identity Management (FIM), digital identities are shared amongst users, identity providers (IdPs), and service providers (SPs). A federation is an association comprised of any number of SPs and IdPs. Trust is implicit in this definition, where every participant is expected to trust the others in what is known as a Circle of Trust (CoT). The main problems with the

FIM approach are the need for negotiating the CoT, which can hinder dynamic collaboration, and the use of an extensive number of protocols and standards, which reduces interoperability. These problems lead to a reduced scalability in practical applications.

At this point, it is important to make a distinction between cloud federations and identity federations. Cloud federations share resources amongst different CSPs, while identity federations share identity information amongst different domains. The trust requirements and assumptions are not the same in each case. An access control system considers subjects trying to execute actions on resources and is comprised of policies, which describe what is permitted in the system, and mechanisms for enforcing the policies. Access control systems are categorized into different models. The most traditional models are Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Risk-Based Access Control (RBAC).

4.2 Risk-Based Access Control

Traditional access control models rely on static authorization (i.e., every access decision is pre-established based on the policies). The idea behind dynamic access control systems is that every access request must be analyzed in its context and must take into account not only the policies, but also contextual information such as security risks, operational needs, and the benefits of the action for the system and the users. Dynamic access control models are characterized by the use of a function that evaluates each access request in real time. Features that can be taken into account by this function include risk, need, benefit, trust, and context. The dynamic nature of access control is captured in these models because access decisions may vary according to the contextual information evaluated at the time of the request. Risk is the potential damage that can arise from a process and is usually represented by the probability of the occurrence of an undesired event multiplied by its impact. Risk metrics are a way to quantify the assets, threats, and vulnerabilities of a system. Also, risk is different from uncertainty, because risk can be measured and managed. Risk-based access control systems perform a risk analysis on access requests to reach an access decision. This analysis can be qualitative or quantitative and automatically attributes a numeric value to each risk.

4.3 Architectures for Access Control Systems

Traditional access control models, which are currently implemented in most cloud solutions, are not enough to ensure the security of these environments when it is necessary to have a greater flexibility to enable efficient information sharing in critical situations. The main reference architecture for access control is presented in RFC2904, which defines the four components for an access control system: the Policy Retrieval Point (PRP), where policies are stored and retrieved; the Policy Information Point (PIP), where information that is useful for access decisions are retrieved; the Policy Decision Point (PDP), where policies are evaluated and access decisions are achieved; and the Policy Enforcement Point (PEP), which protects sensitive resources and forwards access requests to the PDP. XACML is a standard for access policies, requests, responses, and the reference architecture for access control systems. It is based on RFC2904, but renames the PRP to Policy Administration Point (PAP).

5. Systems for Security Metrics

The system for security metrics is comprised of the following phases:

1. The generation of attack and service dependency graphs based on the data about the network topology.
2. Consideration of the malefactor's skills and the position and generation of the profile attack graphs.
3. Analysis of system events to monitor the current security situation.
4. Calculation of metrics based on this data.

SCAP, produced by the National Institute of Standard and Technologies (NIST), includes a collection of specifications intended to standardize the way the security software solutions communicate software security flaws and configuration information. SCAP contains the following standards: Common Configuration Enumeration (CCE), which specifies features of the configurations that negatively influence on security; Common Platform Enumeration (CPE); Common Vulnerabilities and Exposures (CVE); and the Common Vulnerabilities Scoring System (CVSS), which allows for characteristics of hosts to be defined, as they are used for the generation of an attack graph. On the basis of these considered aspects, we can arrange security metrics in our framework by levels [4]. The metrics of the higher levels are defined on the basis of the metrics of the lower levels, except for the system level metrics, which are specified on each level via metrics of the appropriate level, as defined below.

- Topological level: The administrator can calculate the metrics of this level, on the basis of system topology. We considered the following examples of metrics of this level: the vulnerability level of the host, the criticality level of the host, and the vulnerability of the host to zero-day attacks.
- Attack graph level: In this level we considered information from the attack graph for the generation of metrics. The metrics of this level are attack likelihood and attack impact (in this case the impact is defined only by target criticality and attack severity). When representing the attack graph to the user we can highlight the most critical attack paths (from the risk level point of view, i.e., the combination of attack probability and attack impact).
- Malefactor level: On the basis of the metrics of this level, the dependency from the malefactor profile is introduced (including his/her position and skills). This allows for the profile attack graph, which includes attacks that can be implemented by the appropriate malefactor, to be represented.
- Events level: When the security evaluator works in real time, it allows for monitoring the attack deployment and malefactor profile according to incoming events. When new events occur we can represent the current position of the malefactor (host and access rights) on the attack graph and possible attack paths (all possible paths and the most probable) [6,7].
- System level: The common security level of the system and the attack surface are defined on this level. One more common metric that can be used on this level is the resistance to zero-day attacks. We outlined three risk assessment techniques based on the considerations mentioned above, which are as follows:

    a. Express risk assessment technique.
    b. Performance-based (dynamic) technique.
    c. Technique based on historical data.

The express risk assessment technique is used for evaluation the express risks. It is a static technique that incorporates qualitative and quantitative approaches to the risk assessment and allows for the common security level of the system to be defined [8].

6. Attack Mitigation Frameworks

Cloud computing technology is used to rent resources under three types of models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). All three types of resources are accessible through a web-based control panel using a standard web browser. The control panel provides an interface to the cloud resources. For example, in IaaS model virtual machines with specific computing power and storage capacity, software instances are created to share the infrastructure. Similarly, other models also create respective software instances as per customer request. We referred to the IaaS instances, the PaaS instances, and the SaaS instances using the generic Software Instances (SIs) [1]. The overall multi-tenant risks for IaaS, PaaS, and SaaS can be reduced and controlled, and in some cases, eliminated by effective isolation. This consequently allows CSPs to offer potentially premium for a comprehensive segregated infrastructure. This expensive countermeasure, however, has the effect of eliminating the business case for adapting cloud computing in the first place. Arguably, if every risk-averse tenant demands their own physical and secure infrastructure, then the CSP essentially becomes a co-location provider and can offer little beyond the low-margin benefits of shared physical space to their clients [9]. The ADT method is designated as the iADTree for solving the TRA problem in the context of cloud computing applications [10]. It enables the identification of the countermeasures, which achieve an acceptable tradeoff between the residual risk and the corresponding defense cost. In evaluating the performance of different defensive strategies four metrics were considered: ROA at the root, the risk at the root, the attack cost, and the ROI. The development of access control systems for cloud computing is of great importance because these systems are fundamental to enabling the security of these environments [11].

7. Conclusions

In this paper, we have discussed common threats and risks for cloud computing and presented iADTree mechanisms to identify these attacks. Also, we briefly described the systems for security metrics. Software vulnerabilities in the cloud have different severities and different impacts on security parameters (confidentiality, integrity, and availability), so we used an attack mitigation framework for the cloud and risk-based dynamic access control for cloud computing, which is able to facilitate the collection and utilization of the security intelligence gathered from the cloud environment in order to secure the tenants' resources from attacks. The system of risk assessment metrics was used to calculate in the security evaluator. The most characteristic techniques that allow for the proposed metrics to be evaluated have also been discussed. Cloud computing has a collective infrastructure that can be effectively used to mitigate the attacks if an appropriate defense framework is in place.

References

[1] D. V. Bernardo, "Utilizing security risk approach in managing cloud computing services," in *Proceedings of 2013 16th International Conference on Network-Based Information Systems (NBiS),* Gwangju, Korea, 2013, pp. 119-125.

[2] E. Datta and N. Goyal, "Security attack mitigation framework for the cloud," in *Proceedings of 2014 Annual Reliability and Maintainability Symposium (RAMS)*, Colorado Springs, CO, 2014, pp. 1-6.

[3] D. R. Dos Santos, C. Merkle Westphall, and C. Becker Westphall, "A dynamic risk-based access control architecture for cloud computing," in *Proceedings of 2014 IEEE Network Operations and Management Symposium (NOMS)*, Krakow, Poland, 2014, pp. 1-9.

[4] P. Wang, K. M. Chao, and C. C. Lo, "A novel threat and risk assessment mechanism for security controls in service management," in *Proceedings of 2013 IEEE 10th International Conference on e-Business Engineering (ICEBE),* Coventry, UK, 2013, pp. 337-344.

[5] I. Kotenko and E. Doynikova, "Security metrics for risk assessment of distributed information systems," in *Proceedings of 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS),* Berlin, 2013, pp. 646-650.

[6] J. Kar, "Provably secure online/off-line identity-based signature scheme for wireless sensor network," *IJ Network Security*, vol. 16, no. 1, pp. 29-39, 2014.

[7] M. R. Mishra, J. Kar, and B. Majhi, "Practical deployment of one-pass key establishment protocol on wireless sensor networks," *International Journal of Pure and Applied Mathematics*, vol. 100, no. 4, pp. 531-542, 2015.

[8] J. Kar, "A novel construction of certificateless signcryption scheme for smart card," in *Case Studies in Secure Computing Achievements and Trends.* Boca Raton, FL: Taylor and Francis, 2014, pp. 437-456.

[9] P. K. Manadhata and J. M. Wing, "An attack surface metric," *IEEE Transactions on Software Engineering*, vol. 37, no. 3, pp. 371-386, 2011.

[10] B. Grobauer, T. Walloschek, and E. Stocker, "Understanding cloud computing vulnerabilities," *IEEE Security & Privacy*, vol. 9, no. 2, pp. 50-57, 2011.

[11] D. V. Bernardo, "Security risk assessment: toward a comprehensive practical risk management," *International Journal of Information and Computer Security*, vol. 5, no. 2, pp. 77-104, 2012.

Jayaprakash Kar http://orcid.org/0000-0003-4800-4791

He received M.Sc. and M.Phil in Mathematics from Sambalpur University, M.Tech and Ph.D. in Computer Science from Utkal University, India. Currently he is working as Assistant Professor in Department of Information System, FCIT, King Abdulaziz University, and Kingdom of Saudi Arabia. He is actively associated with Information Security Research Group, King Abdulaziz University. His research interests are on development and design of provably secure cryptographic protocols and primitives using elliptic curve and pairing based cryptography.

Manoj Ranjan Mishra

He has completed B-level course conducted by National Institute of Electronics & Information Technology (NIELIT) (erstwhile DOEACC Society), an Autonomous Scientific Society under the administrative control of Department of Electronics & Information Technology (DeitY), Ministry of Communications and Information Technology, Government of India. He received M.Tech in Computer Science from Utkal University, India. Currently he is working as Assistant Professor at School of Computer Application, KIIT University, Bhubaneswar, India. His research interests are on design and development of cryptographic protocols for low processor devices, network and cloud security.