Asian Journal of Applied Science and Technology (AJAST)
(Open Access Quarterly International Journal) Volume 2, Issue 1, Pages 34-43, 2018

Prevent Attacks in the Network and Scrutinizes Threshold for Authenticating Message Communication

K.Lavanya[1], M.Subhashini[2], S.Deepadharani[3], S.Thangamalar[4], K.Megalakshmi[5], Dr.M.Ramesh Kumar[6]

[1,2,3,4,5] *UG Students, Department of Computer Science and Engineering, VSB College of Engineering Technical Campus, Coimbatore, Tamilnadu, India.*
[6]*Associate Professor, Department of Computer Science and Engineering, VSB College of Engineering Technical Campus, Coimbatore, Tamilnadu, India.*

Article Received: 21 September 2017 *Article Accepted: 23 December2017* *Article Published: 07 January 2018*

ABSTRACT

Cloud security is an important issue and particularly, attackers can explore vulnerabilities of a cloud system and compromise virtual machines to deploy further large-scale Distributed Denial-of-Service (DDoS). Within the cloud system, the detection of zombie exploration attacks is difficult because cloud users may install vulnerable applications on their virtual machines. To prevent this, a multiphase distributed vulnerability detection, measurement, and countermeasure selection mechanism called NICE is built on attack graph-based analytical models and reconfigurable virtual network-based countermeasures. In this work, we use Counter Attack Authentication Metrics model is used to prevent the vulnerable attacks such as DDOS and intrusion. This can also prevent attacks in the network and scrutinizes threshold for authenticating message communication. For validating the authorizing users and isolating the attackers from the network of cloud, attack graph model is proposed. The system and security evaluations demonstrate the efficiency and effectiveness of the proposed solution.

Keywords: DDOS, NICE, Network Cloud and Graph.

1. INTRODUCTION

A network is two or more computers linked together in order to share data. From a security stand point, the problem with networks is that unauthorized individuals might also be able to access that data. Network security is a term that encompasses your overall system for keeping your network as impenetrable as possible, be it hardware, software, or company policies. Network security starts with authenticating the user, commonly with a username and a password. Since this requires just one detail authenticating the user name—i.e. the password, which is something the user 'knows'— this is sometimes termed one-factor authentication. With two-factor authentication, something the user 'has' is also used (e.g. a security token or 'dongle', an ATM card, or a mobile phone); and with three-factor authentication, something the user 'is' is also used (e.g. a fingerprint or retinal scan).

1.1. Various Issues in Network Security

1. Authentication
2. Confidentiality
3. Integrity
4. Denial of Service

1.2. Security

Computer security is a growing problem that becomes increasingly important every year as more communication and business is conducted over the Internet. The threats are coming from various sources: Thieves looking to making money through cybercrime, companies looking to steal trade secrets and countries or terrorist groups looking for crucial weaknesses. We need to be more vigilant to protect our important data, and intrusion detection is a major part of this vigilance.

2. TYPES OF ATTACKS

Attacks that could set off an intrusion detection alarm come from various sources, typically referred to as malware or malicious software. Trojan horses, worms, rootkits and even some spyware are all forms of malware that could allow someone to access your PC illegally.

2.1 False Positives

A false positive occurs when a legitimate application or "normal" computer process sets off an alarm indicating intrusion detection. Typically, this occurs if the application or process does something not recognized by the IDS. Once the false positive is confirmed, a company's IT department and the IDS manufacturer can take steps to correct the problem. False positives force companies to spend time and money troubleshooting the problem--time and money that could be better spent on legitimate threats.

2.2 Denial of Service Attack

Denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

A DOS is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. There are two general forms of DoS attacks: those that crash services and those that flood services.

2.3 Leeching

In computing and specifically Internet, a leech is one who benefits, usually deliberately, from others' information or effort but does not offer anything in return, or makes only token offerings in an attempt to avoid being called a leech. Depending on context, leeching does not necessarily refer to illegal use of computer resources, but often instead to greedy use according to etiquette: to wit, using too much of what is freely given without contributing a reasonable amount back to the community that provides it.

2.4. Cloud Service

Cloud computing presents a number of management challenges. Companies using public clouds do not have ownership of the equipment hosting the cloud environment, and because the environment is not contained within their own networks, public cloud customers don’t have full visibility or control. Users of public cloud services must also integrate with an architecture defined by the cloud provider, using its specific parameters for working with cloud components. Integration includes tying into the cloud APIs for configuring IP addresses, subnets, firewalls and data service functions for storage. Because control of these functions is based on the cloud

Provider's infrastructure and services, public cloud users must integrate with the cloud infrastructure management. Capacity management is a challenge for both public and private cloud environments because end users have the ability to deploy applications using self-service portals. Applications of all sizes may appear in the environment, consume an unpredictable amount of resources, then disappear at any time.

2.4.1 Chargeback - or, pricing resource use on a granular basis—is a challenge for both public and private cloud environments. Chargeback is a challenge for public cloud service providers because they must price their services competitively while still creating profit. Users of public cloud services may find chargeback challenging because it is difficult for IT groups to assess actual resource costs on a granular basis due to overlapping resources within an organization that may be paid for by an individual business unit, such as electrical power. For private cloud operators, chargeback is fairly straightforward, but the challenge lies in guessing how to allocate resources as closely as possible to actual resource usage to achieve the greatest operational efficiency. Exceeding budgets can be a risk.

Which combine public and private cloud services, sometimes with traditional infrastructure elements, present their own set of management challenges. These include security concerns if sensitive data lands on public cloud servers, budget concerns around overuse of storage or bandwidth and proliferation of mismanaged images. Managing the information flow in a hybrid cloud environment is also a significant challenge. Hybrid cloud environments also typically include a complex mix of policies, permissions and limits that must be managed consistently across both public and private cloud.

2.4.2 Cloud Clients

Users access cloud computing using networked client devices, such as desktop computers, laptops, tablets and Smartphone. Some of these devices - cloud clients - rely on cloud computing for all or a majority of their applications so as to be essentially useless without it. Many cloud applications do not require specific software on the client and instead use a web browser to interact with the cloud application. With Ajax and HTML5 these Web user interfaces can achieve a similar, or even better, look and feel to native applications.

2.4.3 Deployment models

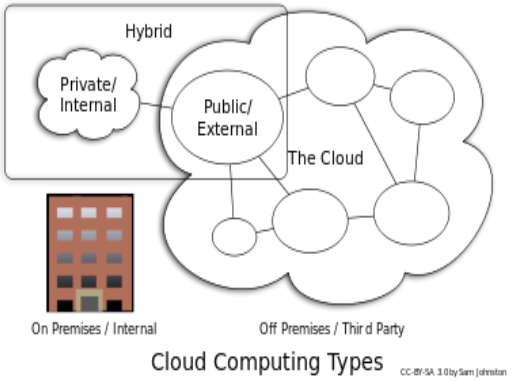

Figure 2.1 Cloud Computing Types

3. CLOUD ARCHITECTURE

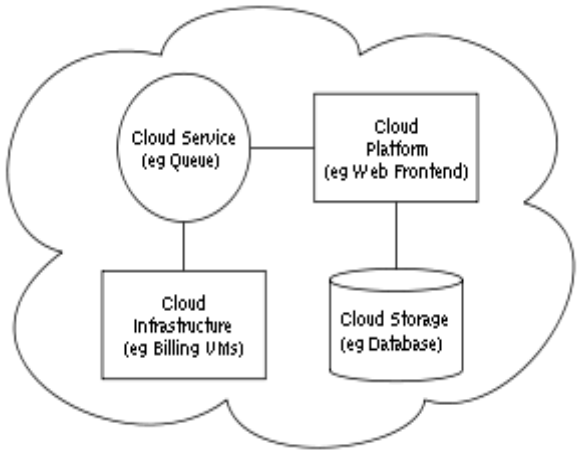

Figure 3.1 Cloud Architecture

Cloud architecture, the systems architecture of the software systems involved in the delivery of cloud computing, typically involves multiple cloud components communicating with each other over a loose coupling mechanism such as a messaging queue. Elastic provision implies intelligence in the use of tight or loose coupling as applied to mechanisms such as these and others.

3.1. Service Modes

Cloud computing providers offer their services according to several fundamental models: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) where IaaS is the most basic and each higher model abstracts from the details of the lower models. Other key components in anything as a service (XaaS) are described in a comprehensive taxonomy model published in 2009. Strategy-as-a-Service, Collaboration-as-a-Service, Business Process-as-a-Service, Database-as-a-Service, etc. In 2012, network as a service (NaaS) and communication as a service (CaaS) were officially included by ITU (International Telecommunication Union) as part of the basic cloud computing models, recognized service categories of a telecommunication-centric cloud ecosystem.

Infrastructure as a service (IaaS)

In the most basic cloud-service model, providers of IaaS offer computers - physical or virtual machines - and other resources. IaaS clouds often offer additional resources such as a virtual-machine disk image library, raw (block) and file-based storage, firewalls, load balancers, IP addresses, virtual local area networks (VLANs), and software bundles. IaaS-cloud providers supply these resources on-demand from their large pools installed in data centers. For wide-area connectivity, customers can use either the Internet or carrier clouds.

To deploy their applications, cloud users install operating-system images and their application software on the cloud infrastructure. In this model, the cloud user patches and maintains the operating systems and the application software. Cloud providers typically bill IaaS services on a utility computing basis cost reflects the amount of resources allocated and consumed.

Platform as a service (PaaS)

In the PaaS model, cloud providers deliver a computing platform, typically including operating system, programming language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers. With some PaaS offers, the underlying computer and storage resources scale automatically to match application demand so that the cloud user does not have to allocate resources manually. The latter has also been proposed by an architecture aiming to facilitate real-time in cloud environments.

CAAM is used to prevent the vulnerable attacks such as DDOS and intrusion already thrived in the network. This also prevents attacks like Leeching that occurs due to the usage of infrastructure as a service in cloud. In this model, we prevent attacks in the network and scrutinizes threshold for authenticating message communication. For validating the authorized users and isolating the attackers from the network of cloud we propose CAAM.

4. ARCHITECTURAL REPRESENTATION

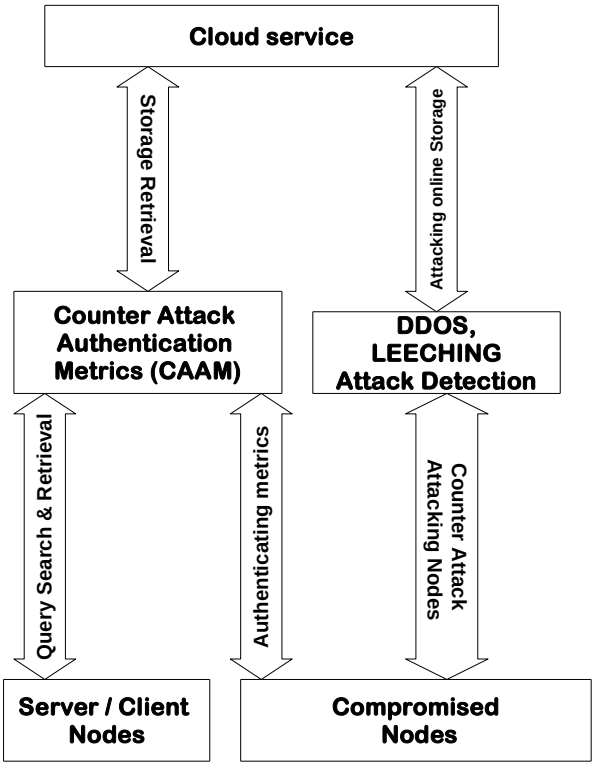

Figure 4.1 Architectural Representation

Within the cloud service, the CAMM was introduced which will check for Authentication based details. It checks for registered user clients for their authenticity and user metrics for having check over client/server system which might be attached system. This will prevent the counter Attack attacking Nodes in the DDOS and Leeching in the cloud service. The cloud service used for query search and storage retrieval. Cloud users may install vulnerable applications on their virtual machines. In Attack Graph Model, every detected vulnerability is added to its corresponding Virtual Memory entry in the database.

4.1 Server and Client Establishment

In this module a server & client systems is created. In Server and client systems a network structure is formed between them for further communications. It provides a strong security so that no one can hack any message communication. Thus we create more client systems in which some system are secured.

Here we create a single server and multiple client systems which have intermediate communications between each other. Server will send more requests and client will respond for all the requests simultaneously. Thus they can easily pass messages between server and client and the message communications between clients to client is also possible.

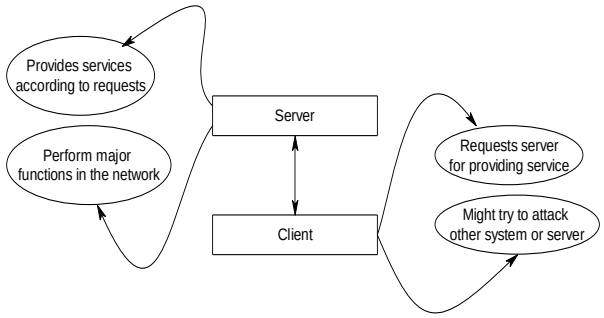

Figure 4.2 Servers and Client Establishment

4.2. Cloud Storage Creation

Cloud Service was connected with the server and the client. Server accesses the Cloud Service and make request according to the service and send to the client. Cloud Service can be created by connecting systems with each other were one cloud service is connected with other cloud service and thus acquired cloud computing network. It provides Infrastructure as a service environment which affords networking connection in cloud infrastructure. The Cloud Service has a secured Cloud Storage Service. Database can be accessed through online in Cloud storage area.

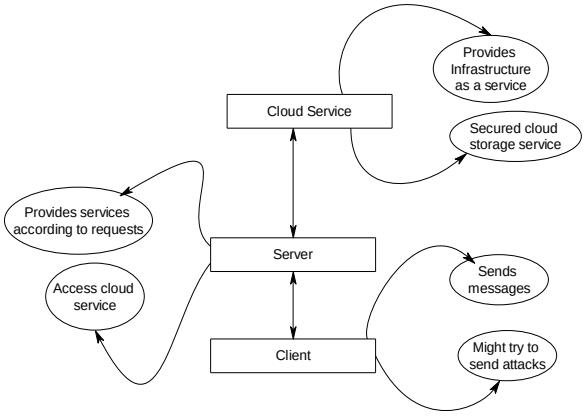

Figure 4.3 Cloud Storage Creation

4.3 Propose Counter Attack Authentication Metrics

Our proposed CAAM is generated which provides a check for authenticated message communication in the network of cloud. Attack graph model is connected with the server and client who provide transaction. Attack graph based detection authenticates client and service registration. It manipulates metrics for checking based on transactions made. It also prevents attacks that are vulnerable in the network and proposes all prevention measures before any attack

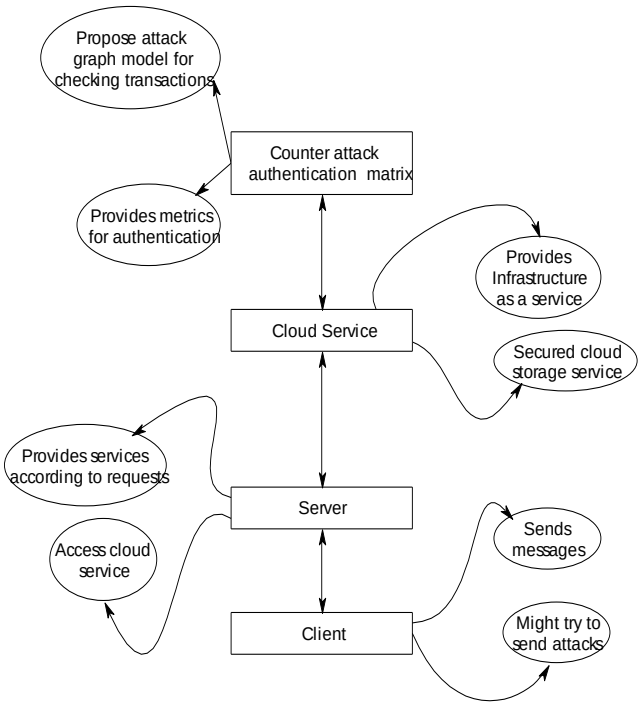

Figure 4.4 Proposed Counter Attack Authentication Metrics

4.4 Attack Prevention

The existing network attacks such as intrusion , DDOS and the upcoming attacks through the Cloud network such as leeching will be detected and prevented by the proposed model thus by eliminating those attacking nodes from the network. It takes prevention measures for forthcoming attacks like DDOS, Leeching, and intrusion attacks. Then give counter attacks to the nodes that try to attack the cloud infrastructure.

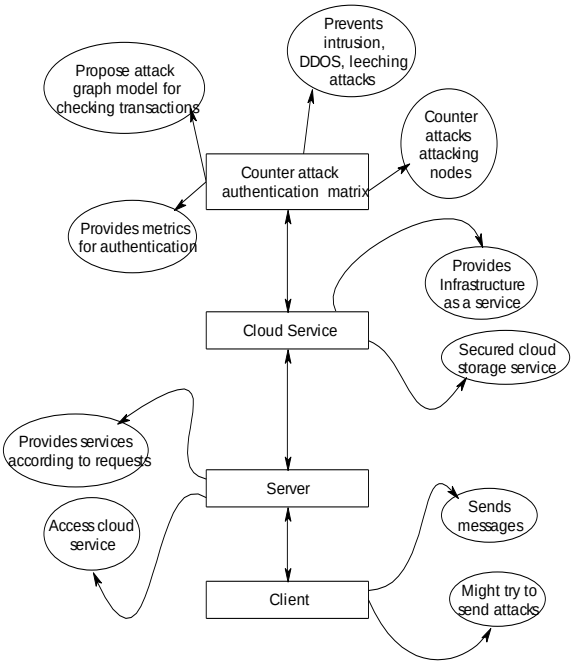

Figure 4.5 Attack Prevention

5. DATA FLOW DIAGRAM

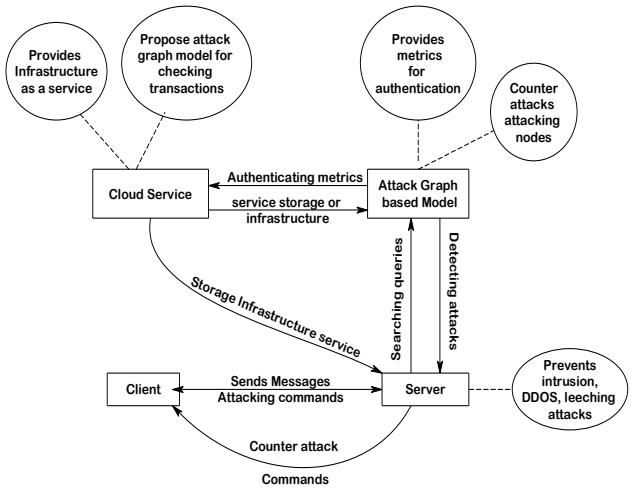

Figure 5.1 Data Flow Diagram

6. CONCLUSION

Herewith we confer results by using Attack Graph model to prevent the vulnerable attacks such as DDOS and intrusion already thrived in the network and also prevents attacks like Leeching that can occur due to usage of infrastructure as a service in cloud. In this model, we prevent attacks in the network and scrutinizes threshold for authenticating message communication. Scrutinizes message communication in all centralized and decentralized networks. For validating the authorized users and isolating the attackers from the network of cloud we propose CAMM will check for authentication based details. It checks for registered user clients for their authenticity and uses metrics for having check over clients systems which might be attacked system. Some attackers use their system to intrude in the network and might try to Denial of service or intrusion; there is a possibility for leeching attack also. All these attacks will be detected by checking with these metrics. Thus these found attacks will be terminated and those attackers will be given counter attacks through this metrics model.

7. FUTURE ENHANCEMENT

Future developments include the prevention of Zombie attacks and distributed denial of service attack in cloud storage using Counter attack authentication metrics. Also it prevents attacks such as intrusion, Leeching and scrutinizes message communication in all centralized and decentralized network. The entire detected attacker node will be detached from the network and stored in a database.

REFERENCES

[1] G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee, “BotHunter: Detecting Malware Infection through IDS-driven Dialog Correlation,” Proc. 16th USENIX Security Symp. (SS ’07), pp. 12:1-12:16, January-2004.

[2] G. Gu, J. Zhang, and W. Lee, “BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic,” Proc. 15th Ann. Network and Distributed Sytem Security Symp. (NDSS ’08), December-2004.

[3] NuSMV: A New Symbolic Model Checker,” http://afrodite.itc. it:1024/nusmv. June-2005.

[4] X. Ou, S. Govindavajhala, and A.W. Appel, “MulVAL: A Logic- Based Network Security Analyzer,” Proc. 14th USENIX Security Symp., pp. 113-128, May 2006.

[5] L. Wang, A. Liu, and S. Jajodia, “Using Attack Graphs for Correlating, Hypothesizing, and Predicting Intrusion Alerts,” Computer Comm., vol. 29, no. 15, pp. 2917-2933, June 2006.

[6] P. Mell, K. Scarfone, and S. Romanosky, “Veability Analysis of Network Diversificaton” http://www.first.org/cvss/cvss-guide. html, August 2007.

[7] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J.M. Wing, “A Survey on IDS Alert Processing Technique,” Proc. IEEE Symp. Security and Privacy, pp. 273-284, Dec-2007.

[8] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "OpenFlow: Enabling Innovation in Campus Networks," SIGCOMM Computer Comm. Rev., vol. 38, no. 2, pp. 69-74, February 2008.

[9] A. Roy, D.S. Kim, and K. Trivedi, "Scalable Optimal Countermeasure Selection Using Implicit Enumeration on Attack Countermeasure Trees," Proc. IEEE Int'l Conf. Dependable Systems Networks (DSN '12), October 2008.

[10] E. Keller, J. Szefer, J. Rexford, and R.B. Lee, "NoHype: Virtualized Cloud Infrastructure without the Virtualization," Proc. 37th ACM Ann. Int'l Symp. Computer Architecture (ISCA '10), pp. 350-361, March 2009.

[11] P. Ammann, D. Wijesekera, and S. Kaushik, "the Nepenthes Platform: an efficient approach to collect malware ," Proc. 9th ACM Conf. Computer and Comm. Security (CCS'02), pp. 217-224, Sep 2009.

[12] N. Poolsappasit, R. Dewri, and I. Ray, " NUSMV Scalable Network Vulnerability Analysis," IEEE Trans. Dependable and Secure Computing, vol. 9, no. 1, pp. 61-74,February 2010.

[13] R. Sadoddin and A. Ghorbani, "Alert Correlation Survey: Framework and Techniques," Proc. ACM Int'l Conf. Privacy, Security and Trust: Bridge the Gap between PST Technologies and Business Services (PST '06), pp. 37:1-37:10, July 2010.

[14] A. Roy, D.S. Kim, and K. Trivedi, "Statl: An Attack Language for State-Based Intrusion Detection," Proc. IEEE Int'l Conf. Dependable Systems Networks (DSN '12), November 2010.

[15] Mitre Corporation, "Anomalous Payload Based Network Intrusion Detection," http://cve.mitre.org/, Feb 2011

[16] Open Networking Fundation, "Using Machine Learning Technique to Identify botnet Traffic," ONF White Paper, July 2011.

[17] X. Ou, W.F. Boyer, and M.A. McQueen, "An algorithm for anamoly based botnet detection," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), pp. 336-345, Nov 2011.

[18] N. Poolsappasit, R. Dewri, and I. Ray, "Dynamic Security Risk Management Using Bayesian Attack Graphs," IEEE Trans. Dependable and Secure Computing, vol. 9, no. 1, pp. 61-74, Jan. 2012.