Implementing Intrusion Management as Security-as-a-Service from Cloud

Deepak H. Sharma
Department of Computer Engineering,
K. J. Somaiya College of Engineering, Mumbai
deepaksharma@somaiya.edu

Dr. C A. Dhote
Department of Information Technology,
P. R. M. I. T & R,
Amravati
vikasdhote@rediffmail.com

Manish M. Potey
Department of Computer Engineering,
K. J. Somaiya College of Engineering, Mumbai
manishpotey@somaiya.edu

Abstract— **In Security-as-a-service model the objective is to provide security as one of the cloud services. In this model the security is provided from the cloud in place of on-premise implementation. The Intrusion Management comprises of methods for intrusion detection, intrusion prevention and response to intrusions. In physical environments Intrusion management methods have already matured. However, due to growth of cloud computing, virtualization and multi-tenant resource sharing there are new targets for intrusion due to their complex structure. There are several issues related to intrusion detection and prevention in a cloud environment, and even in a traditional environment with intrusion management service to be delivered as a service from the cloud. This paper provides implementation framework for cloud-based intrusion management from the cloud as a service. The management is easy and efficient through Web-based console anywhere, anytime. The Intrusion Management-SecaaS implemented as the cloud service can benefit the user with all the advantages offered by Security-as-a-service (SecaaS). The proof of concept (POC) prototype of Intrusion Management IM - SecaaS is implemented and evaluated successfully.**

Keywords—Cloud Computing, Security-as-a-Service, Intrusion Management-Security-as-a-Service.

I. INTRODUCTION

In Security-as-a-service model the objective is to provide security as one of the cloud services. In this model the security is provided from the cloud in place of on-premise implementation. The security-as-a-service model helps enhance the capability of existing on-premise solutions by working with them in a hybrid manner. The Intrusion Management comprises of methods for intrusion detection, intrusion prevention and giving responses for intrusion attempts. In physical environments Intrusion management mechanisms have already matured. However, due to the growth of cloud computing, virtualization and multi-tenant resource sharing there are several new targets for intrusion. The intrusion risk increases also due to the complexity of the system. There are many issues related to intrusion detection and prevention in a cloud environment, and even in a traditional environment with intrusion management service to be delivered as a service from the cloud. The primary purpose of intrusion Management is to monitor the clients' organization infrastructure at important points to find out malicious activity intended at interruption, interception, modification of data, applications, and systems. The objective is also to respond in such a way to block the intrusion, reduce it, or continue normal operations in the event of attack. An effective intrusion service should combine prevention, detection and response management mechanism for control and reporting. It should have interface to the rest of the security architecture. For delivering these capabilities from the cloud often requires various administrative associations, raised user rights, and an end to end transactional access between hosted elements. There is also a need of a central control and reporting of all incidents [1].

An Intrusion Management-Security-as-a-service (IM-SecaaS) framework is proposed in this paper. In particular this IM-SecaaS is an on-demand portable, and available pay-per-use cost model. The paper discusses issues related to security provided as cloud service. This paper addresses the following issues in separate sections. Section II discusses related work. Section III describes the scope and main components of POC framework prototype implementation of IM-SecaaS in public cloud. Section IV evaluates the prototype IM-SecaaS. Finally, Section V concludes the paper and discusses future work.

II. RELATED WORK

The easiest way to implement IM-SecaaS is directly forwarding the traffic to the cloud-based Intrusion detection services. This can be done by transparently forwarding traffic from clients' network firewall or proxy that supports forwarding to an upstream proxy. Intrusion detection is a combination of inspection of network traffic using various methods, detection of signatures, and other anomaly based algorithms. According to guidelines in CSA implementation guidance [1], the main functional areas covered for Intrusion management are:

- Intrusion Detection through:
  - Inspection of Network Traffic, Behavioral Analysis, and Analysis of traffic flow,
  - OS, Virtualization Layer, and Events at Host Process,
  - Events at Application Layer, and
  - Techniques of Correlation and other Capabilities at Distributed and Cloud level.

978-1-5090-1022-6/16/$31.00 ©2016 IEEE

- Intrusion Response using:
  - Various mechanisms like Automatic, Manual, or Hybrid.
- Intrusion Management Service Infrastructure, including:
  - Detection and Response Architectures,
  - Intrusion Management Service Components,
  - Application, process, and data requirements,
  - Regulatory and Compliance Issues for data privacy

The authors of IDSaaS [2] have discussed Intrusion Detection as a Service (IDSaaS) focusing on security of the infrastructure level of a public cloud. The intrusion detection technology provided is elastic, portable and fully controllable. A prototype of IDSaaS is also described. The implementation of prototype has been done in Amazon web services.

In signature based IDS [3] the focus is on the signature-based IDSaaS, the authors have designed a privacy-preserving intrusion detection mechanism. The process of signature matching hides specific content of network packets. It uses a fingerprint based comparison. The authors have evaluated the proposed mechanism under a cloud scenario and have identified several open problems and issues.

In related paper [4], the authors have proposed a multi-level IDS and log management. It is based on behavior of client for applying IDS effectively to cloud computing systems. The system uses different levels of security strength for users based on the degree of anomaly. Their proposed method provides a way of decreasing the rule set size of IDS and management of user logs.

In DCDIDP [5], the authors have proposed a Distributed, Collaborative, and Data driven Intrusion Detection and Prevention system (DCDIDP). The system's goal is to provide a holistic IDPS for all cloud service providers. The scheme proposes collaboration among peers in a distributed manner at different architectural levels to respond to attacks. A DCDIDP framework is presented with three logical layers: network, host, and global at platform and software levels. The various challenges have been identified in realizing the framework.

Cloud computing architectures based IDS [6] gives a classification of specific and traditional attacks to the cloud computing environment according to their origin and their category. The authors have discussed some existing cloud computing architecture based Intrusion Detection System (IDS), their strengths and weaknesses. They have proposed a new architecture by correcting some weaknesses and integrating certain new concepts.

In SDNIPS [7] the authors have presented a Software Defined Network (SDN) based Intrusion Prevention System solution. It is a full lifecycle solution including detection and prevention in the cloud. A new IDPS architecture is proposed based on Snort based IDS and Open vSwitch (OVS). The authors have compared the SDN based IPS solution with the traditional IPS approach from both mechanism analysis and evaluation.

III. POC IM-SECAAS ARCHITECTURE

According to guidelines in [1], Intrusion detection can be implemented as a combination of various mechanisms like inspection of network traffic using different methods, detection of signatures, anomaly based algorithms, investigation accumulation and information correlation from different sources. The information analyzed is about the systems state, applications running, and various types of user activity. The response to Intrusion is in the form of alerts, manual interventions or automatic handling of events. Intrusion Management also needs an infrastructure where management of all related elements can be done. The algorithms and signature information collection can be centrally located or can be distributed. Various elements of IM-SecaaS architecture are as shown in Figure 1.

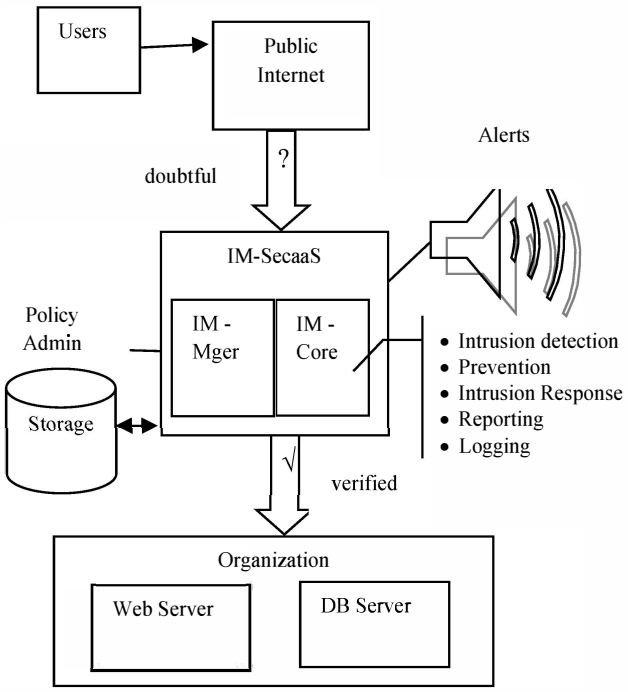

Figure 1: Implementation of POC IM-SecaaS

The architecture of an Intrusion Management Security-as-a-service (IM-SecaaS) mainly involves Intrusion Detection, Intrusion Response, Reporting, and Logging. It detects intrusion attempts by monitoring web traffic before it reaches users' organization's network. The incoming stream is cleaned and then delivered to the organization as shown in Figure-1.

The paper discusses a proof-of-concept prototype of IM-SecaaS which is implemented in a public cloud. For our experimentation purpose a proprietary converged public cloud is used. The IM-SecaaS framework can be applied in all types of cloud implementations. All IM-SecaaS components are implemented in form of virtual machines in the public cloud. The on-demand elasticity, portability, use of security mechanisms from various vendors are some of the characteristics of IM-SecaaS. All these features can be applied by starting the VM instances dynamically on the go.

The focus here is on Intrusion management to be delivered as a cloud service; i.e. security provided through the cloud. The POC system architecture is shown in Figure 1, the main components of the system are IM-SecaaS core – the core functions have been implemented in this module, IM-SecaaS manager – managerial functions like policy administration, and Intelligence have been implemented in this module. On one side of IM-Secaas is public internet from where doubtful traffic comes to the organization and on the other side of IM-SecaaS is the Client Organization. As demonstrated in the figure when traffic reaches IM-Secaas it is in doubtful state. The IM-SecaaS core module cleanses it by applying all policies and then delivers it client organization. A client organization may have different types of protected resources viz. web servers, Database servers etc.

The IM-SecaaS core module has other functionalities like Intrusion detection, prevention, Response, Reporting and Logging. A storage unit as central repository is connected for logging purpose.

The implementation has been done in form of windows OS Virtual machines in a public cloud setup. The IM-SecaaS Core and IM-SecaaS Manager have been implemented in separate Virtual machines. Snort[1], an open source network based intrusion detection system is used in IM-SecaaS core component for the purpose of POC implementation. In actual scenario the Intrusion Detection/ Prevention System (IDPS) from multiple vendors can be used for practical purpose. This type of solution will be more effective than using Intrusion Detection/ Prevention System from single vendor in an on-premise solution.

In this way the entire Intrusion Management functionality can be achieved. It is provided as a Cloud Service to the client on different types of devices (Desktops and Mobiles devices etc.)

IV. EVALUATION OF IM-SECAAS

Several experiments have been conducted to evaluate the effectiveness of our proof-of-concept prototype of IM-SecaaS in public cloud. The evaluation has been done on the basis of discussion given in white paper [9] and our papers [10, 11]. The following criteria have been considered for the evaluation purpose:

- Reliability: the service will be provided in form of multiple web servers running in the cloud environment. The redundancy of servers will lead to high reliability and high availability to the clients. The POC was tested in form of two web servers to provide uninterrupted IM-SecaaS services to the clients.
- Effectiveness: to make the service more effective, the core module handles multiple functionalities like Intrusion detection, prevention, Response, Reporting and Logging.
- Performance: the performance was tested by comparing the average time taken by on-premise Intrusion management w.r.t. IM-SecaaS mechanism. The testing was done by running the IM-SecaaS under various cloud environments. The overall overhead also depends on the traffic in public cloud, but it does not increase by more than 20-25%, which is fairly good given the advantages it offers over legacy systems.
- Flexibility: the solution can work with existing legacy systems as well. The POC implementation uses snort but in actual systems the IDPS from multiple vendors can be actually used to run on VMs. It can provide more flexibility to customers to choose varying functionalities of security as per their need.
- Control: the client can access the service from various devices viz. desktops and handheld mobile devices etc. A central portal is provided through which all the policies can be easily administered.
- Privacy and Security: the IM-SecaaS filters all doubtful inbound traffic before entering clients' organization. This filtering is done based on the policies defined. This ensures the privacy and security of Users' data.
- Cost of ownership: the cost of ownership is borne by the cloud security service provider. The client does not invest in anything in on-premise solution. The client will have to pay only on the basis of pay per use model. Since IM-SecaaS is available as cloud service it is only charged to customer in form of Operational Expenses (OPEX) model.

V. CONCLUSION AND FUTURE WORK

In this paper, an IM-SecaaS, in the form of a framework is discussed. It enables the cloud service provider to provide Intrusion management security functionality as a cloud service in public cloud. IM-SecaaS is compatible with prominent cloud features including portability, elasticity, and pay-per-use service. The approach was implemented as a collection of VMs in public cloud to work in the cloud model. This solution can also work along with existing on-premise platform based implementations in a hybrid manner to enhance their security capabilities. With IM-SecaaS, users can detect and prevent any intrusions and secure their protected resources.

In future the system availability, reliability and performance can be enhanced by creating replicas of core VM to distribute the heavy load of traffic and to prevent single point of failure. The additional functionalities related to Intrusion management can be added to make it more effective and efficient.

[1]Snort (version 2.9.5) [online]: Available https://www.snort.org

REFERENCES

[1] CSA SecaaS Implementation guidance : Intrusion Management September 2012

[2] Turki Alharkan, Patrick Martin, 'IDSaaS : Intrusion Detection System as a Service in Public Clouds', The Third International Conference on Cloud Computing, GRIDs and Virtualization 2012

[3] Y. Meng, W. Li, L. F. Kwok and Y. Xiang, "Towards Designing Privacy-Preserving Signature-Based IDS as a Service: A Study and Practice," *Intelligent Networking and Collaborative Systems (INCoS), 2013 5th International Conference on*, Xi'an, 2013, pp. 181-188.

[4] J. H. Lee, M. W. Park, J. H. Eom and T. M. Chung, "Multi-level Intrusion Detection System and log management in Cloud Computing," *Advanced Communication Technology (ICACT), 2011 13th International Conference on*, Seoul, 2011, pp. 552-555.

[5] S. T. Zargar, H. Takabi and J. B. D. Joshi, "DCDIDP: A distributed, collaborative, and data-driven intrusion detection and prevention framework for cloud computing environments," *Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2011 7th International Conference on*, Orlando, FL, 2011, pp. 332-341.

[6] E. N. Saad, K. E. Mahdi and M. Zbakh, "Cloud computing architectures based IDS," *Complex Systems (ICCS), 2012 International Conference on*, Agadir, 2012, pp. 1-6.

[7] T. Xing, Z. Xiong, D. Huang and D. Medhi, "SDNIPS: Enabling Software-Defined Networking based intrusion prevention system in clouds," *10th International Conference on Network and Service Management (CNSM) and Workshop*, Rio de Janeiro, 2014, pp. 308-311.

[8] Tim Mather, Subra Kumaraswamy, and Shahed Latif, 2009, Cloud Security and Privacy. An Enterprise Perspective on Risks and Compliance, O'Reilly Media, 336.

[9] Websense white paper, Seven Criteria for Evaluating Security-as-a- Service Solutions, 2010

[10] Deepak Sharma, Dr. C A. Dhote, Manish Potey, 'Security-as-a-Service from Clouds: A comprehensive Analysis', IJCA Volume 67-Number 3, April 2013

[11] Deepak Sharma, Dr. C A. Dhote, Manish Potey, 'Security-as-a-Service from clouds: A survey' IIJC Vol 1 Issue 4, October 2011.