Detection and Representation of Threats and Attacks on Portal

Vidyashree H.R[1] Asha[2]
[1]M.tech student, Dept. of CSE [2]Associate professor, Dept of CSE
[1, 2] Dr.A.I.T, Bangalore.

Abstract--- Managed Security Service is the analysis, and interpretation of log data. There is a need for organization investigators in locating internal and external threats/attacks. There is a requirement of software that should reduce the tedious efforts of organization examiners, especially when searching for dangerous attacks which may be a threat to the company. A method is proposed here that uses visualization techniques to represent attack statistics, such as attack location, attack date, when it was solved date, attackers etc. The user interface to this software displays graphical representation of log file about attacks. By viewing attack information graphically, the developed software will reduce the examiner's analysis time and greatly increase the probability of locating attack evidence. The graphical representation of log files rather than traditional text will greatly aid the organizations by reducing the time to identify suspicious attacks and increases the probability of locating the criminal evidence. The purpose of this project is to correlate event data and represent these in a consistent context with the help of a graphical user interface.

The main objective is log extraction, statistics generation and graphical representation. This works by reading the log files generated by the firewalls and storing it to the repositories. Later database is then used to create a statistics page, GIF charts, attackers-map etc.

Keyword: - Managed Security Service, Attacks, Graphical Representation, Log files.

I. INTRODUCTION

Managed Security Services (MSS) team takes care of securing the cloud from malicious attack. Companies can have cloud-based network protection against individual and blended threats without incurring the distraction, expense, and complexity of in-house systems and support staff. It provides services like attack mitigation, anti-malware tools, and Web filtering. Malicious traffic—including viruses, spyware, worms, and service attacks—is malware, and it is a constant threat to a company's network, data, time, and employee productivity. Managed firewalls detect and block suspicious network traffic. Proactive intrusion prevention is prevention against known emerging threat. Managed Security Services increase company productivity by reducing wasted time and resources.

A portal is a web-based gateway which allows users to locate and create relevant content and use the applications they commonly need to be productive. A portal is a single web-based environment from which all of a user's applications can run. These applications are integrated together in a consistent and systematic way. Portals of fetch compelling benefits to today's enterprises: reduced operational costs, improved customer satisfaction, and streamlined business processes.

Portlets are web applications that appear in windows on a page. Portlets are written by developers and can have any functionality a web application has. Many portlets can be added to a single page, allowing convenient access to many applications in one place. Open source solves a lot of the problems inherent in the old Java portal paradigm. Open source projects don't wait around for committees to decide on things; they tend to implement what the users want as fast as possible. There are no barriers to entry with open source; the development tools and the software are made available for free.

Open source products also tend to be lighter weight: you don't need a large, dedicated server to start building your solution. Development goes faster, because developers don't have to learn the entire architecture to be effective. And you don't need a huge initial investment to get started using an open source solution—you can start small (free) and then grow your application and hardware as your needs grow.

II. RELATED WORK

Cloud computing is a new field, some security mechanism are already in place, most which have been adopted from Grid computing area [1] such as Grid Security Infrastructure[2]. Nimbus Cloud-kit adopted Grid Security Infrastructure (GSI), to provide mutual authentication between communicating entities. Once mutual authentication is done, a threat is that an authenticated entity may behave in a malicious way. However, using mutual authentication alone may result in loss of confidentiality, integrity and availability.

Role Based Access Control [3], since it allows easy restriction on which operations user can perform, thus is reducing the probability of an accident by an inexperienced user/malicious user.

Generic Security Management Framework (GSMF) [1], plays a vital role in securing cloud resources from insider. GSMF provides policy management, user activity and trust management which will be essential in developing our model.

Terra [4], is able to prevent owner of the physical host from inspecting and interfering with computation. This mechanism reliably detects whether or not the host is running a platform implementation that the remote party trust. These platforms can effectively secure virtual machine. However many providers run data centres comprising of several hundreds of machines, and customer's virtual machine can be dynamically scheduled to run on any one of them.

Collins [5], propose a model that mainly focuses on the relationship between social context cues and uninhibited verbal/written behaviour in computer-based communication. His work might have been effective but his model focus only on verbal language and does not extend to computer-related behaviour.

C. Meadows [6], proposed a Representation of Protocol Attacks for Risk Assessments, used as the assessment for threat. However, Meadow primarily objective was to model external attack, but paid little attention in modelling insider attack.

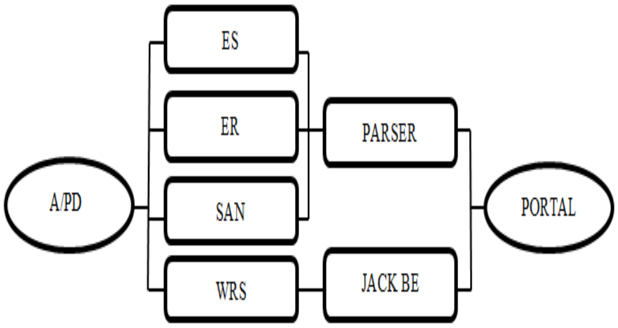
Havlik [7], proposed log to mitigate insider attack but somewhat less defined in this regard. Often, logs are used after something has gone wrong without a clear definition of what one might be searching for. In this case log management fail to detect insider during the time of event.

Fung [8], proposed Collaborative Intrusion Detection Networks, these collaborative systems are surveyed and their robustness against insider attacks is analysed. While technical approaches are essential for detecting insider threats, they often lack support for adding human behaviour to their detection mechanisms. Log management techniques have grown much more capable recently, and the value of application logs has been recognized as a valuable tool in event detection, regulatory compliance and monitoring network performance [9]. The currently drawbacks of log is the cost associated with implementing it. So, drawing inspiration from existing security system used to mitigate insider from misusing resources, we intend to fill gap of securing cloud computing from malicious insider who intentional violate system policy in order to benefit for their interest. We intend to manage user identities, user access and information used by insider. We detect the attack from the external as well as the internal attack and represent them in graphical form. These attacks are also differentiation by the severity of the attack.

III. Design Phase

A. *System Architecture*

This paper describes different methods which are used to represent the threats in a graphical manner which will be easy for the clients to understand the status of their network and to take the necessary actions to avoid the attacks. Below is the basic diagram which explains how the data about the attacks will be fetched from external sources or Arcsight or from SAN repository and used to represent the data graphically.



A/Pd- Arcsight/Public Domain Parser-Java Jaxb Parser San-San Drive Es-External Source Er-External Repository

Fig. 1: Basic Block Diagram

The basic logical that is implemented here is the firewalls will block the attacks and store the details of the attacks in the Arcsight or Public Domain. Then those details about the attacks will be fetched from Arcsight/Public domain and will be stored in the different places like external sources, external repository, SAN drive or REST Web Services .From those repositories data will be fetched and will be converted into required format using JACK BE presto. Then that data will be used to represent the attacks in the graphical form on the portal. Those graphical forms are dashboards, geo-map, stylized table, chartFX.

B. *Dashboard*

The module that is concentrated here is representing the malicious attack into the cloud in the form of graphical representation. This graphical representation is called as dashboard. The corporate world has tried for years to come up with a solution that would tell them if their business needed maintenance or if the temperature of their business was running above normal.

C. *Advantages*

- Dashboards often provide at-a-glance views of KPIs (key performance indicators) relevant to a particular objective or business process.
- Dashboards give signs about a business letting the user know something is wrong or something is right. Dashboards typically are limited to show summaries, key trends, comparisons, and exceptions.
- Dashboard is "An easy to read, often single page, real-time user interface, showing a graphical presentation of the current status (snapshot) and historical trends of an organization’s key performance indicators (KPIs) to enable instantaneous and informed decisions to be made at a glance”.

Dashboards are unique. The design of each dashboard is driven by the business and their needs and culture. a dashboard is a user interface that, somewhat resembling an automobile's dashboard, organizes and presents information in a way that is easy to read. Integration of information from multiple components into a unified display is referred as dashboards. A dashboard is a visual display of the most important information needed to achieve one or more objectives consolidated and arranged on a single screen so the information can be monitored at a glance. A dashboard is a composite view that can presented in the form of chart, gauge, stylized table, geo map, RSS Feeds etc. Chart portlet renders bar charts and line charts on the Portal. The dashboard widgets supported by the MSS Portal fall in one of the following categories: Security posture, incidents trend, threat alerts, vulnerability feeds, security news and custom dashboards.

The Dashboards section of the Liferay Portal contains multiple gadgets containing “mashups” of data from multiple downstream sources and data providers to provide the users with a high-level “single-pane” view of the Portal. Dashboards will provide the following kind of information to users in a summarized or high-level format

- Real-time Usage
- Outstanding Service Requests
- Performance Statistics
- Availability Statistics
- Real-time Outage
- SLA Statistics

The Customer Portal leverages the Service Delivery Dashboard (SDD) to provide on-demand information about the services to the client by the Unisys Service Desk. The SDD is securely integrated with the

Portal via Backend PTA using DES encryption (see details in the section above). The capabilities of SDD are:

- Daily statistical updates relating to Unisys Service Desk performance against agreed service levels,
- The ability to view messages, forecasts and a change calendar related to the services delivered by the organization ,
- Features such as near real-time indicators and the ability to browse open Incidents, Problems and Changes.

Additional dashboard gadgets will be created to represent one or more metrics. The Portal will leverage the Ajax technology for rendering updates to the dashboards in near real-time. Where appropriate, the data in dashboards will be rendered in a graphical representation containing click-to-drill features. The source of data for each of the dashboard gadgets includes the CIS database, RBADB and ODS databases, and the SDD application. The JackBe Presto Server will be the mashup technology used to generate the graphs for the dashboards. The Presto Server exposes individual services as mashlets which are consumed by the Portal.

The following is a summary of the dashboards obtained from the indicated sources:

- RBADB database: Real-time usage data on Secure Cloud offerings
- SDD: Real-time call volume and SLA data
- CIS database: Active Outage information
- ODS database: SLA, OLA and KPI dashboards.

IV. IMPLEMENTATION

A. Geo-map

Geo-map is used to represent the threat that has occurred in the different parts of the world. Information of the threat will be collected and will be represented on the map. The place of attack will be indicated using a bubble marker and an information window which displays an IP address of the victim with the location.

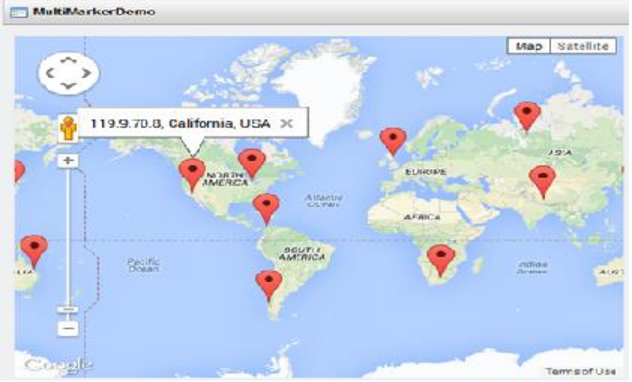


Fig. 2: Geo-map

B. Calendar

Calendar portlet will gives the details about the attack which was occurred on the particular date. The date when the attack has been occurred that date will be highlighted. So, when the clients click on that particular date they will find the complete details about the attack which was occurred on the particular date.

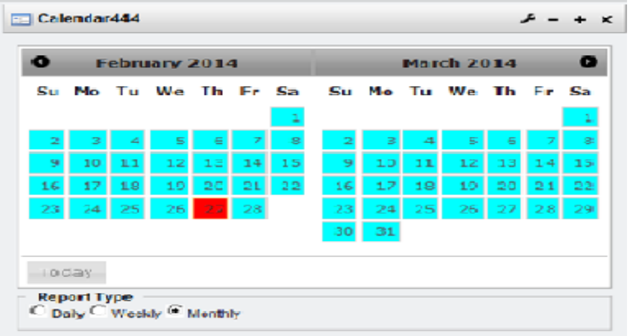
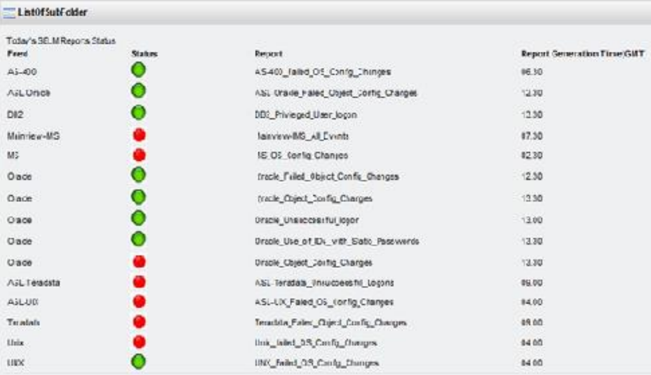


Fig. 3: Calendar

C. Stylized Table

Stylized table is used to represent the details of the attacks. The details of the attack will be put in the form of table and more information can be obtained by downloading the file.



ListOfSubFolder

Today's SELM Reports Status

Feed	Status	Report	Report Generation Time/GMT
AS-400	🟢	AS400_failed_OS_Config_Changes	06.30
ASL Oracle	🟢	ASL Oracle_Failed_Object_Config_Changes	12.30
DB2	🟢	DB2_Privileged_User_logon	13.30
Mainview-MS	🔴	Mainview-MS_All_Events	07.30
MS	🔴	MS OS Config Changes	02.30
Oracle	🟢	Oracle_Failed_Object_Config_Changes	12.30
Oracle	🟢	Oracle_Object_Config_Changes	13.30
Oracle	🟢	Oracle_Unsuccessful_logon	13.00
Oracle	🟢	Oracle_Use_of_IDs_with_Static_Passwords	13.30
Oracle	🔴	Oracle_Object_Config_Changes	13.30
ASL Teradata	🔴	ASL Teradata_Unsuccessful_Logons	09.00
ASL-UX	🔴	ASL-UX_Failed_OS_Config_Changes	04.00
Teradata	🔴	Teradata_Failed_Object_Config_Changes	09.00
Unix	🔴	Unix_failed_OS_Config_Changes	04.00
UNIX	🟢	UNIX_Failed_OS_Config_Changes	04.00

Fig. 4: Stylized Table

D. Attackers Chart

In Chart the severity of the attack will be represented in the form of bar graph. This gives the complete details about the attack if it had occurred previous. This can be used to secure the system or to avoid the severity of threats on the system.

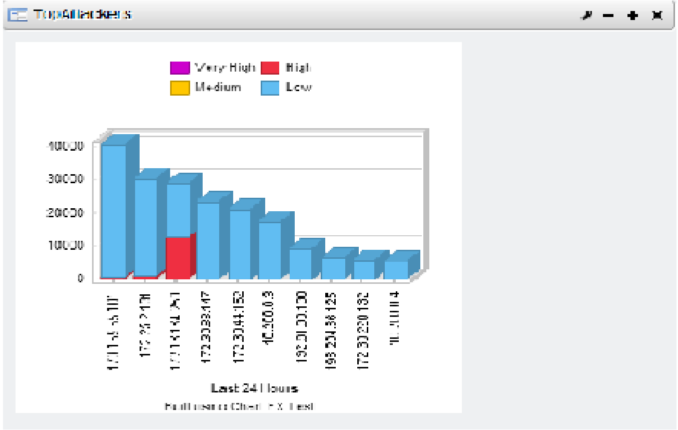


Figure 4: Attackers Chart

V. CONCLUSION

In this paper we are representing the attacks on the network graphically which will help the clients to understand the threats in their networks ant their assets.

REFERENCES

[1] Cristina Basescu, Catalin Leordeanu, Alexandru Costan, Alexandra Carpen-Amarie, Gabriel Antoniu "Managing Data Access on Clouds: A Generic

Framework for Enforcing Security Policies" International Conference on Advanced Information Networking and Applications 2011.

[2] Foster I., Kesselman C., Tsudik G., Tuecke S.(1998) "Security Architecture for Computational Grids" 5th ACM conference on Computer and Communications Security, 1998.

[3] Ahlem Bouchahda, Nhan Le Thanh, Adel Bouhoula, Faten Labbene "Enforcing Access Control to Web Databases" 10th IEEE International Conference on Computer and Information Technology (CIT 2010), 2010.

[4] Nuno Santos Krishna P. Gummadi Rodrigo Rodrigues "Towards Trusted Cloud Computing" MPI-SWS.

[5] Collins, Mauri (1992). "Flaming: The relationship between social context cues and uninhibited verbal behavior in computer-mediated communication". On-line document, papers/flames.html.

[6] C. Meadows. "A Representation of Protocol Attacks for Risk Assessment". In R. N. Wright and P. G. Neumann, editors, DIMACS Series in Discrete Mathematics and Theoretical computer Science: Network Threats, volume38, December 1998.

[7] havlik, J. and Shavlik, M. 2004. Selection, Combination, and "Evaluation of Effective Software Sensors for Detecting Abnormal Computer Usage". Proceedings of ACM Knowledge Discovery and Data Mining 2004 pp. 276-285.

[8] Fung "Collaborative intrusion detection networks and insider attack" journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable vol, 2 ,no. 1, pp. 63-74, 2011 .

[9] Shenk J "Demanding More from Log Management System". SANS Insitute Whitepaper" 2008.

[10] "Advantages of Managed Security Services". Mega Path Whitepaper 2009