IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

Network Security Architecture with Active and Dynamic Response Selection

Resmi .A.M [1], Dr. R. Manickachezian [2]

Ph. D Research Scholar, Dept of Computer Science, NGM College, (Autonomous), Pollachi, Coimbatore, Tamil Nadu[1]

Associate Professor: Dept. of Computer Science, NGM College (Autonomous), Pollachi, Coimbatore, Tamil Nadu[2]

Abstract: In the past decade, several network attacks have become recognized in the field of networking. This situation necessitates serious care and considerations to address its extensive impact. To conquer and defeat the effects of network attacks and vulnerabilities, an appropriate intrusion prevention system, intrusion detection system and an effective dynamic intrusion response system are essential. This paper presents an Intrusion Response System (IRS) framework based on real time implementation parameters. Moreover, this paper investigates the essential response design parameters for IRS to reduce attacks in real time and obtain a robust and effective outcome. Different IRS design parameters are broadly discussed in this paper.

Keywords: Network Intrusion, Intrusion Response System, Alert Correlation, Intrusion Detection System, Content Delivery Networks.

I. INTRODUCTION

In the recent years, network security needs more consideration and focuses against security threats. Currently, people have become increasingly technology dependent and adopted for several new technological habits. Excessive use of computer networks developed a number of security episodes, which includes integrity, threats to confidentiality, and data availability. Data integrity and availability in computer networks should have enough security against intrusions[1].

The intrusion is a kind of interruptions by using several types of attacks such as Denial of Service (DoS) attacks, spoofing attacks, application layer attacks and many. There is a need for complete security mechanism, which helps to enforce the security policies. Those policies will defeat intrusions.

Security systems like firewalls, cryptography, and authentication access control mechanisms are used as the base line of defense against security threats [2][3]. But, these anti threat applications are failed to sense internal intrusions and inadequately provide security countermeasures and responses. So, a variety of types of intrusion systems are invented. For such inventions, Intrusion Detection Systems (IDSs) is the base. The invented or originated systems are intrusion prevention systems and intrusion response systems. These set of inventions are developed to detect, prevent, and respond to intrusions effectively [4]. In general IDS is a collection of software or hardware resources that can analyze, spot, distinguish and report intrusions to the users. But IDS, IPS and IRS requires high-performance systems and are difficult to manage in analyzing and spotting intrusions. This is more tedious in advanced and distributed network systems. Thus, a security countermeasure that constantly scrutinizes the performance of the network. From the observed data, the system effectively identifies and handles potential episodes. This type of countermeasures are knows as IRS (Intrusion Response Systems).

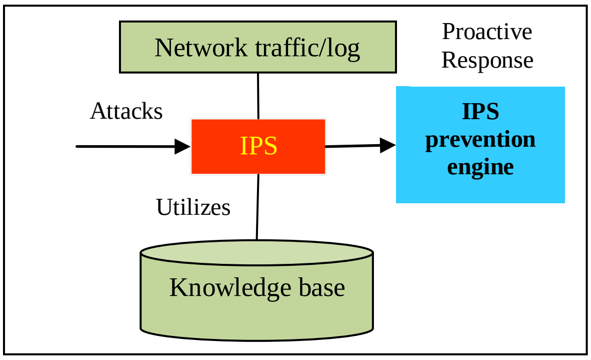

Fig 1.0 Intrusion Prevention System Process

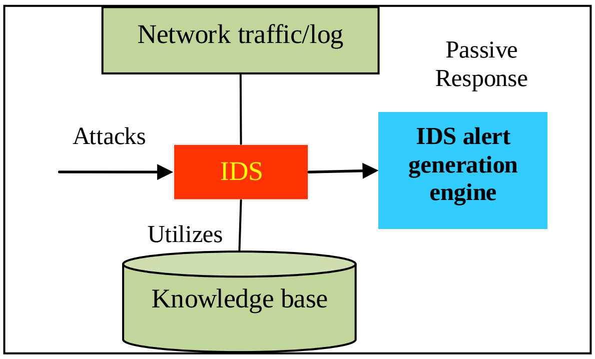

Fig 2.0 Intrusion Detection System Process

Fig. 1.0, fig 2.0 and fig 3.0 illustrate the basic functionality of IPS, IDS and IRS respectively. Here, the IPS is a proactive response engine, which eliminates and protects data from security threats.

DOI10.17148/IJARCCE.2017.63183

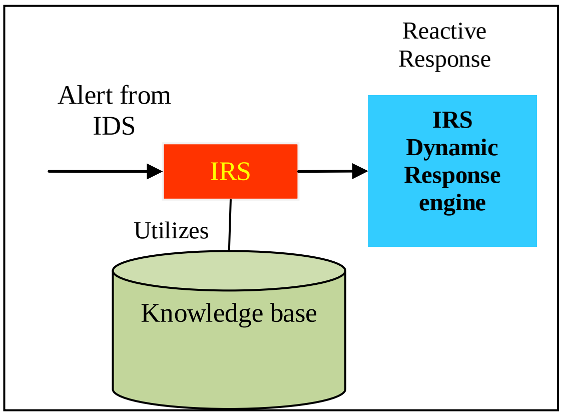

Fig 3.0 Intrusion Response System Process

And the IDS create alarm at the time of intrusion, so it is known as passive response engine. And finally the IRS is a reactive response system, which selects dynamic response according to the IDS alert. The majority of existing schemes ignores the importance of dynamic response factors at the time of response selection process. Hence, most existing schemes produce imprecise and erroneous results by generating many false alarms at the time of IRS process.

Several researches have been conducted on IRS design and selection. But, most existing IRS designs employ a static approach in selecting an optimum response for intrusion alerts generated by the IDSs [5]. Instead of dynamic response, several existing [6] [7] only used static response strategies. This includes the static risk threshold metric, damage reduction metric, IDS confidence metric and severity metric. And this system is faced several difficulties at the time of real time detection scenarios and created many false alarms too. So this paper is aimed to develop a new intrusion response system with effective parameters. The newly developed IRS is designed for the dynamic countermeasure selection with minimum false rates.

II. INTRUSION RESPONSE SYSTEMS

IDS have some limitations that the system only detects and warns the user about the intrusion in the network. There is no action is taken on the detected attacks. So there is a need to handle such attacks in the network. In order to provide a better response to the detected attack, IPS is generated. When comparing with IDS IPS can take preventive actions before occurring intrusions. And it only generates an alarm at the time of detection [8]. However, when comparing with any type of security system in the network, the complete prevention of intrusions is unfeasible in current scenario. Therefore, the constraint of both IDS and IPS was addressed by adding the response components in the IDS. IRS is a new era in the research field. The investigation on IRS is considerably less concentration than IDS process.

Fig. 4.0 illustrates the basic functionality of IRS. Here, the IDS is activated when some intrusions need to be detected in the network. IRS is always activated on the basis of IDS result.

When IDSs obtain any new attack, the response component generates responses on the basis of the detected attack from IDS.

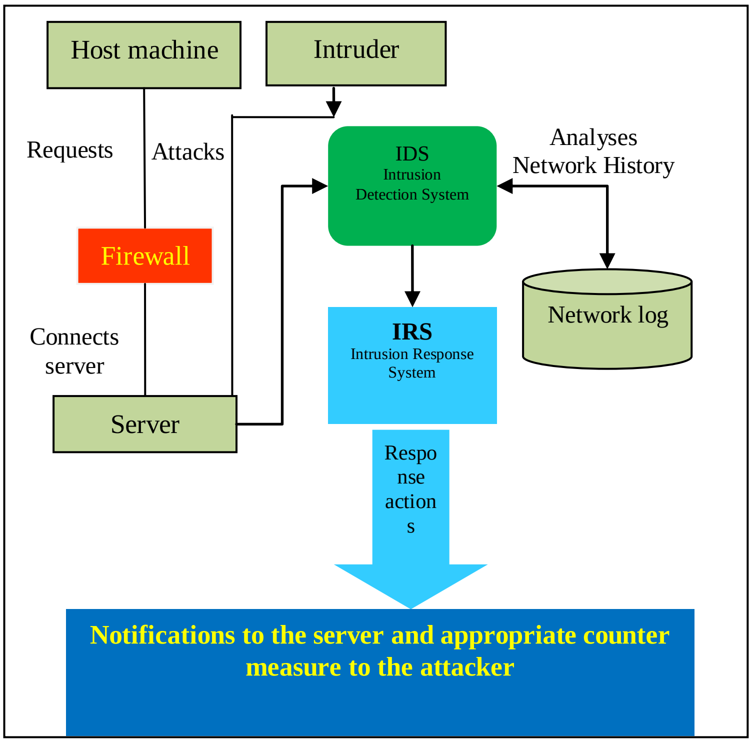

Fig 4.0 Intrusion Response System Basic Process

DOI10.17148/IJARCCE.2017.63183

IRS is defined as a security countermeasure [9] that is performed when an intrusive behavior occurs.

IRSs are classified into three approaches. This segmentation is based on the degree or level of automation: the Type of IRS is notification, manual and automated response systems.

a. Notification Response Systems: IDS with notification response was developed by Vigna in [10]. The existing IRSs [11] [12] with notification systems that mainly provide information about intrusions by email messages, console alerts and alarms. From the generated notifications, the system administrators select the best reactive countermeasure and responds to the detected intrusions [13].but this approach is infeasible and the attacker can block the notifications, which sent through email. Moreover, these approaches create a time gap between the detection and response process. This is considered as a major challenge and opens an opportunity for intruders. Notification response systems cannot prevent attacks or return the system to a safe mode.

b. Manual Response Systems: The notification system is ineffective and incompetent in the distributed systems, because it generates alerts based on the attacks, which are detected by the IDS. To overcome the issues of notification response system, a manual response system was developed. The authority in this type of system applies a prefixed set of responses. These responses are based on the symptoms of attacks in the network. This approach is highly automated, when compared with the notification system approach [14] [15]. In [16] author found a problem of detecting delay between intrusion detection and time occur when the system administrators initiate a response. Protecting the system against Dos and DDoS, is impracticable when this system is implemented in the IRS.

c. Automated Response Systems: Notification and manual response system in the IRS approaches are inadequate and unable to respond to high-speed attacks such as DoS and DDoS. Because those approaches are in active. Due to several issues in the above mentioned approaches, highly automated response systems are needed. In [17] [18] authors proposed to decrease the size of the vulnerability in the network by deploying immediate and automated response system.

III. INTRUSION RESPONSE SYSTEMS DESIGN

This paper introduces a new IRS engine with fast and dynamic response system with various considerations. There is a need of tremendous focus and concentration for IRS design. Because the weak feature of IRS may result in high number of false alarms and less accuracy in detection. The paper utilizes the some defense strategies against intrusions. For every episode of IDS, the response will be selected. While designing such response system there are several challenging task are emerged. The following are the challenging tasks, which should be carefully planned.

a. Data Sets: The main challenge in the designing IRS is the lack of publically available datasets for generating a proper response engine. The dataset collection creates a major risk. It requires the researchers should posses more knowledge on public datasets to evaluate various frameworks and algorithms. This paper utilizes a systematic dataset for alert response, which are given for sample.

Response engine dataset selection = {
DS1: KILL the PROCESS, DS2: LOCK the USER,
DS3: REMOVE ALL USERS, DS4: SESSION QUIT,DS5: QUIT}
Level1 = {Round1 (DS1, DS2, DS4), Round2 (DS5)}
Level2 = {Round1 (DS1, DS3, DS4), Round2 (DS5)}

b. Alert Correlation: To monitor attacks different IDS and IRS are embedded. In specifically, in the distributed network the size of IRS is huge. So alert correlation is the next major task of IRS. A correlation module, which must be installed on every host for cooperative detection and response process. It aggregates similar alerts based on the predefined situation condition.

Algorithm: Active Attack Correlation
Steps:

```
1. Get alert S from IRS
2. If(s is a new alert) then
3. Create node N in the alert graph hierarchy (AGH)
4. Locate the alert in the hierarchy
5. Verify the alert s with the parameters P
   a. For each alert(si verifies P)
   b. If the parameter P satisfied
   c. Calculate priority P for Node N in H.
6. For all alert s containing p do
   a. If s is the last element in H then
   b.  Append s in H based on the priority P.
7. End for
8. End
```

Fig 5.0 Active Attack Correlation Process

The fig 5.0 shows the active attack correlation and alert priority calculation steps in the IRS. The IRS engine collects the valid attack alerts and store as a hierarchy based architecture. This type of architecture provides the fast data collection and organization. And it provides the best and appropriate response after perceiving the attack type.

c. Risk Assessment: The several existing studies consider individual topics in design issues under IRS Such as, risk assessment and improving quality of services. This is another important feature helps to mitigate several attacks. This risk assessment process gives the severity of the received alert from the IRS.

d. Managing False Alarm:even though there are several studies concentrated on the false alarms, the uncertainty of data may produce unexpected false alarms.

So an effective mechanism in IRS that can handle the false alarms generated by IDS should be developed. So applying the effective hybrid techniques in IRS increases the accuracy of detection and response selection. For this, this paper utilizes post feedback techniques are used to rate the given response is better or not.

Performance Analysis:

The IRS has been analyzed with sample set of IDS data. As per the analysis the following table represents the performance of IRS for multiple IDS and IPS.

Table 1.0 Time Analysis Table for Every Activity in IRS

IRS Activity	Time Taken for multiple IRS (ms)
Alert correlation	**134**
Alert risk assessment	**120**
Priority calculation	**90**
Response	**120**
Report and update hierarchy	**300**
Total	**754**

The table 1.0 shows the performance results of the IRS engine on the basis of activity time. The total time taken for all actions of IRS i.e. totally 5 activities is 754 milli seconds for multiple IRS. The minimum time taken by the engine is for calculating alert priority and response selection priority. This time is reduced by applying top-k algorithm for popular and suitable response selection. After receiving the report, the response will be performed. The response time is approximately 120 milli seconds. This is the maximum time specified for multiple IDS and IRS system engines.

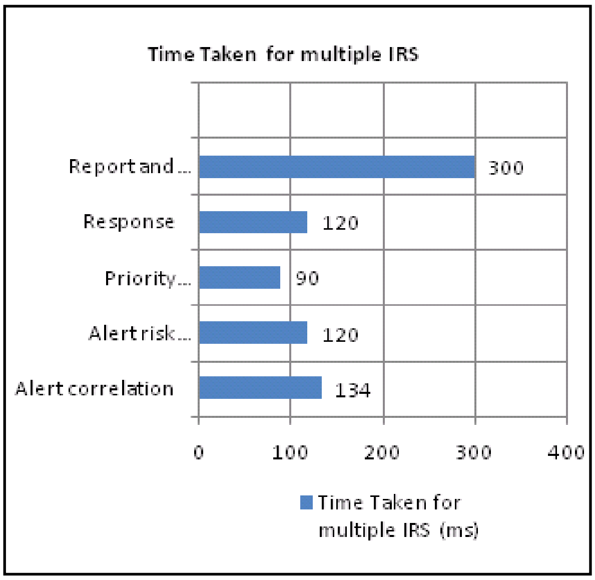

Fig 6.0 Time Analysis Chart

The fig 6.0 shows the time analysis chart, which is generated from the table 1.0.The system finally performs the analysis to show the accuracy of the IRS system. Accuracy refers to the proportion of valid alerts an accurate type in total alerts, namely the situation TP and TN, thus the accuracy is

$$\text{Accuracy}= \frac{\mathbf{TP + TN}}{\mathbf{TP=TN+FP+FN}} \ \mathbf{*100\ \%}$$

Formula 1.0 Accuracy Calculation Formula

The formula 1.0is an accuracy calculation formula is applied in order to find the accuracy of the IRS alert. This helps us to detect the total number of false alarm in the IRS system. This accuracy calculation is performed after every iteration of IRS steps.

Table 2.0 Accuracy of IRS

Iterations	Accuracy (%)
Iteration 1	**89**
Iteration 2	**91**
Iteration 3	**93**
Iteration 4	**94**
Iteration 5	**97**

The table 2.0 shows the performance results based on the detection and response selection accuracy of the IRS engine. The maximum percentage of accuracy can be gained after 4 iterations. Here each iteration refers the set of alerts and its priority based selection process.

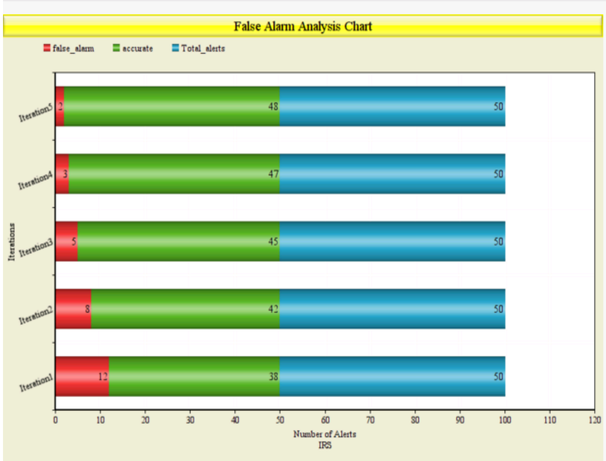

Fig: 7.0 False Alarm Analysis Chart

Detection and identification of alerts and response selection process is much considerable. So after every activity the accuracy has been calculated. Fig 7.0 shows the false alarm in the IRS system, which shows it reduced to 2 when the iteration reaches 5.

- True positive (TP): the count of alerts detected when it is highly accurate.
- True negative (TN): the count of alerts detected when it is actually not an attack.
- False positive (FP): The count of alerts detected as false when it is actually true one, namely false alarm.

- False negative (FN): The count of alerts detected as true one when it is actually not, which can be detected by IRS system.

Nowadays, intrusion detection and response selection process requires high detection rate and low false alarm rate, thus the research compares accuracy, detection rate and false alarm rate, and lists the performance results with numerous iteration.

IV. CONCLUSION

To meet the contemporary issues and threats in Network Security, a novel IRS design is introduced. Before developing the new IRS, which is necessary to analyze and determine optimal factors and requirements for best IRS development. So this paper discussed about the basic process of IDS and IRS with real time challenges. This improved with the intension of reducing attack severity and number of attacks. This paper presents drawbacks of existing IDSs in terms of detection capacity, design factors, and response selection. Additionally, the design specification and functionality of existing IRSs also discussed. Finally, new design parameters with a set of algorithms are proposed for designing a good IRS engine. The main contribution of this paper is to enhance the IRS with different factor considerations. The challenges encountered at the time of designing a better IRS are also discussed. At last the results are discussed in terms of time and accuracy.

REFERENCES

[1] Ali A, Ghorbani WL, Mahbod Tavallaee.” Network Intrusion Detection and Prevention: Concepts and Techniques;” 2009 [Accessed on: books.google.com.my/ books?isbn=0387887717]
[2] Kruegel C, Valeur F, Vigna G. “Intrusion detection and correlation challenges and solutions”, vol. 14. Springer Science & Business Media; 2005.
[3] SANS Institute, Dinesh S. “Intrusion prevention systems: security's silver bullet?” Bus Commun Rev 2003;33:36–41.
[4] Anuar NB, Sallehudin H, Gani A, Zakari O. “ Identifying false alarm for network intrusion detection system using hybrid data mining and decision tree”. Malays J Comput Sci 2008;21:101–15..
[5] Mateos V, Villagrá VA, Romero F, Berrocal J. “ Definition of response metrics for an ontology-based Automated Intrusion Response Systems”. Comput Electr Eng 2012;38:1102–14.
[6] Mu C, Li Y. “An intrusion response decision-making model based on hierarchical task network planning.” Expert Syst Appl 2010;37:2465–72
[7] Hubballi N, Suryanarayanan Vinoth. “False alarm minimization techniques in signature-based intrusion detection systems: a survey.” Comput Commun 2014;49:1–17 13:128.
[8] Scarfone K, Mell P. “Guide to intrusion detection and prevention systems (IDPS).” NIST Spec Publ 2007a;800:94.
[9] Chen Y-M, Yang Y. “Policy management for network-based intrusion detection and prevention.” NOMS 2004 IEEE/IFIP: IEEE network operations and management symposium; 2004. p. 219–32.
[10] Vigna Garak.Intrusiondetection: “a brie fhistory and overview”. Computer2002;35 (4):0027–30.
[11] Paxson V.Bro:asystemfordetectingnetworkintrudersinreal-time.ComputNetw 1999;31:2435–63.
[12] Frank Y, Jou FG, Chandru Sargor, Shyhtsun Felix Wu, Cleaveland W Rance. Architecture design of a scalable intrusion detection system for the emerging net- work infrastructure. Technical Report CDRL A005. Releigh (NC, USA): Department of Computer Science, North Carolina State University Releigh; 1997.
[13] Shameli-SendiA,Ezzati-JivanN,JabbarifarM,DagenaisM.” Intrusion response systems: surveyand taxonomy”. IntJComputSci NetwSecur2012;12:1–14.
[14] Tanachaiwiwat S, Hwang K, Chen Y.” Adaptive intrusion response to minimize risk over multiple network attacks”. ACM Trans Inf Syst Secur 2002;19:1–30
[15] Toth T, Kruegel C. “Evaluating the impact of automated intrusion response mechanisms”. In: Proceedings of the 18th annual IEEE computer security applications conference; 2002. p. 301–10
[16] Lee W, Fan W, Miller M, Stolfo SJ, Zadok E. “Toward cost-sensitive modeling for intrusion detection and response”. J Comput Secur 2002;10:5–22.
[17] FooB,WuY-S,MaoY-C,BagchiS,SpaffordE.ADEPTS:adaptiveintrusionresponse using attack graphs in an e-commerce environment. In: Proceedings international conference on dependablesystemsandnetworks, 2005DSN.IEEE;2005. p. 508–17.
[18] WuY-S,FooB,MaoY-BagchiS, Spafford EH.” Automated adaptive intrusion con- tainmentin systems of interacting services.” Comput Netw 2007; 51:1334–60.
[19] Johnson, David E., Frank J. Oles, and Thilo W. Goetz. "Interactive automated response system." U.S. Patent No. 6,567,805. 20 May 2003.

BIOGRAPHIES

Resmi.A.M received MCA from Madurai Kamaraj University, Madurai. She completed her M.Phil Degree from Bharathiar University, Coimbatore. Currently she is doing Ph.D in Computer Science at NGM College, Pollachi. India. She has 10 years of Teaching Experience. She has published 5 papers national level/international conference and journals. Her research interest includes in the areas of Advanced Computer Network, Data Mining and Image Processing.

Dr. R. Manicka Chezian received his M.Sc., degree in Applied Science from P.S.G College of Technology, Coimbatore, India in 1987. He completed his M.S. degree in Software Systems from Birla Institute of Technology and Science, Pilani, Rajasthan, India and Ph.D degree in Computer Science from School of Computer Science and Engineering, Bharathiar University, Coimbatore, India. He served as a Faculty of Maths and Computer Applications at P.S.G College of Technology, Coimbatore from 1987 to 1989. Presently, he has been working as an Associate Professor of Computer Science in N G M College (Autonomous), Pollachi under Bharathiar University, Coimbatore, India since 1989. He has published one-fifty papers in international/national journal and conferences: He is a recipient of many awards like Desha Mithra Award and Best Paper Award. Recently he received the award “Best Computer Science Faculty of the Year 2015” from Association of Scientists, Developers and Faculties. His research focuses on Network Databases, Data Mining, Distributed Computing, Data Compression, Mobile Computing, Real Time Systems and Bio-Informatics.

DOI10.17148/IJARCCE.2017.63183