Intrusion Prevention System Using Unique Application Indentification

Rupali Singh, Siddharth Lavania, Dr.Pankaj Chaturvedi, Namrata Dhanda

Abstract—In this paper, after analyzing the advantages and disadvantages of various Intrusion prevention systems, we are proposing a new system in which all the advantages has been considered to remove the drawbacks given by different IPS's. We have proposed a centralized on line system to deal with global vulnerabilities activities due to intrusion. IPS clients will be having the combination of unique MAC address and IP Address of the network clients.

Index Terms— Distributed Denial of Services, Intrusion Prevention System, IPS Clients, IPS Centralized Server, MAC Address, Multi-Tier Architecture, Network Security

1 Introduction

The current improvements in modern technology have enabled the use of computer systems and programs in conducting business and in gathering and sharing information in corporations and academic institutions using the Internet. Today, Government make use of networks for e-Governance, banks make use of networks to perform its financial operations, hospitals have the records of their patients in databases, Judges are maintaining records of their court proceedings, cases and amendments of laws and many companies has been presented on the Internet, so that any user with Internet access is able to choose the product that customers desires and buy it online. The data that is handled in this type of businesses should be saved from attacks.

Nowadays, guarantee of secure communication is as important as the traditional computer and information security assurance. Information in transit (as messages) must be protected from unauthorized release and modification, and the connection itself must be established and maintained securely. Prevention of illegitimate traffic is one of the goals of communication security and seeks to prevent an eavesdropper from gaining any meaningful information about network users' behavior or objectives by observing the legitimate traffic on the network. To protect the enterprise, security managers have deployed a variety of technologies**.**

While these technologies are useful for defending corporate assets, they have limitations. For example, firewalls may be configured to block certain types of traffic, but attackers still find ways to exploit legitimate traffic types to mount their attacks. Intrusion prevention presents its own difficulties. Intrusion prevention systems (IPS's), mostly, prevent attacks that fit an established pattern or "signature." This leaves the network vulnerable to new, undocumented attack strategies. IPS's also tend to yield a large number of false positives – thereby wasting staff time and eventually causing a real attack to be ignored. Other types of anomaly recognition systems are similarly prone to generating false positives, since they trigger alerts whether a deviation has an innocuous or a malicious cause. Finally, intrusion prevention and anomaly systems are reactive; the action against an attack is taken as it occurs by resetting TCP connections or requesting a firewall rule change, which are mostly not fast enough to prevent the attack.

2 Background and Overview

2.1 Phases of Attacks

It is not an easy task to provide security and prevent attacks. In order to protect digital information and other network assets, thinking methodology and behavior of the attacker can help to find out a way to prevent them.

All successful intrusions share the following characteristic phases [3]:

- Reconnaissance
- Assessment and Strategy
- Exploitation / Invasion
- Maintaining Access
- Operations

Attackers place different priorities on each stage. In essence, the more time spent on one step ensures better results in the following steps. Also, each phase is conducted in such a way as to ease the way for the next step, and lower the chance of getting caught.

2.2 Reconnaisance, Assesment and Strategy

Reconnaissance, or Recon, is the act of scoping out a target. This information gathering stage is the most important step an attacker takes, and all key information is considered. The Assessment and Strategy stage is the sorting of the gathered data to piece together an idea of what the hacker is attacking [5].

Recon can go undetected for considerable lengths of time and the Assessment and Strategy stage is often completely undetectable, as it is usually done without contact with the target.

2.3 Intrusion Detection system

A second layer in the perimeter defense is intrusion detection systems (IDSs). The audits of security existed before the intrusion detection. Audit is the process of generating, storing and revising events of a system chronologically. IDS is the evolved version of the traditional audits [10]. The term audit, in Latin "audire" (to hear), is defined as "to examine the economic management of a company in order to verify if it is adjusted to the established rules by law or custom" [11]. Intrusion detection is the process of monitoring and searching networks of computers and systems for security policy violations [12]. Intrusion Detection Systems (IDSs) are software or hardware products that automate this monitoring and analysis process. An IDS inspects all inbound and outbound network activity, system logs and events, and identifies suspicious patterns or events that may indicate a network or system attack from someone attempting to break into or compromise a system [13].

2.4 Distributed Denial ofServices

The DDoS field is evolving quickly, and it is becoming increasingly hard to grasp a global view of the problem. This study strives to introduce some structure to the DDoS field by proposing a classification of DDoS attacks and DDoS defense systems. [19] This study has not been done to propose or advocate any specific DDoS defense mechanism. Some sections might point out vulnerabilities of certain defense systems, but our purpose is not to criticize but to draw attention to these problems.

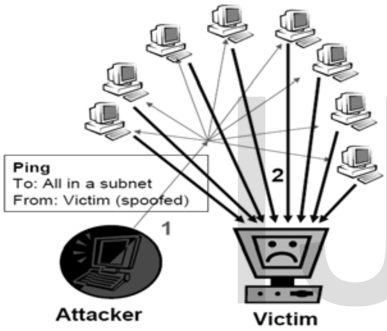

Fig. 1: A Type of DDoS Attack e.g. "Ping of Death

The main purpose of this study [19] is to provide a clear and thorough coverage of the area of DDoS attacks. In principle, this study attempts to aid the DDoS research on the issues related to the field of attack mechanisms. The study is based on a comprehensive literature review, which spans an area of source codes and analyses of DDoS attack tools. The prime objectives of this research can be summarized to the following:

- Analyse the details of DDoS attack mechanisms and the principles DDoS attacks rely,
- Present the novel classification of DDoS attack mechanisms,
- Discuss a few of the possible evolutions of the DDoS attack mechanisms.

3 Literature Survey

The main purpose of this study [19] is to provide a clear and thorough coverage of the area of DDoS attacks. In principle, this study attempts to aid the DDoS research on the issues related to the field of attack mechanisms. The study is based on a comprehensive literature review, which spans an area of source codes and analyses of DDoS attack tools. The prime objectives of this research can be summarized to the following:

- Analyse the details of DDoS attack mechanisms and the principles DDoS attacks rely,
- Present the novel classification of DDoS attack mechanisms,
- Discuss a few of the possible evolutions of the DDoS attack mechanisms.

4 Proposed Intrusion prevention system

We have noticed that the authentication check is always checked by Login_id and Password mechanism which is quite vulnerable. We have proposed a Centralized online system to deal with global vulnerabilities activities due to Intrusion. We have introduced a new concept in which the IPS clients will be having a unique Application Identification i.e. App_Id, which will be combined with MAC address and IP Address of the network clients. The major Functional requirements of an IPS are like real time operations, high performance, scalability, reliability, availability, detection accuracy, low latency, data analysis capability, patch updates and modular design.

In our case the proposed Intrusion Prevention System will be working on an IPS Server in a distributed Client Server architecture.

Tier 1	Tier 2	Tier 3
Graphical User Interface	Intrusion Prevention System	IPS Clients

Table.1: Proposed Architecture of Multi-Tier IPS

The proposed Intrusion Prevention System will be Three-tier architecture. A Graphical User Interface will be on Tier-1, Intrusion Prevention System will be on Tier-2 as a centralized server, IPS Clients will be there on Tier-3 distributed over network.

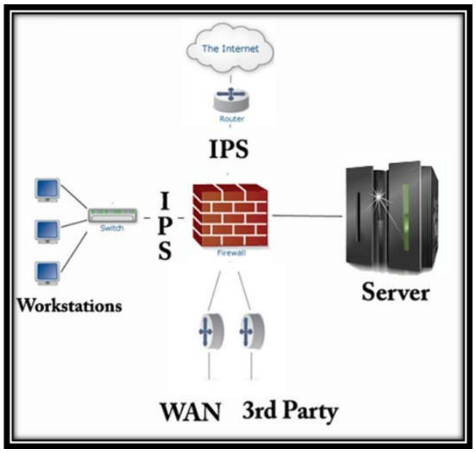

Fig. 2 :Block diagram of Proposed IPS System

A graphical user interface is required to interact with the IPS. This Web-based User Interface can be used remotely and can analyze the information stored on the IPS Server. Through this User Interface we can manage security policies, digital signatures and requests coming by IPS clients. All the user interfaces are using connection to our IPS centralized Server to perform all management operations.

The centralized Intrusion Prevention System server will be a Software System implemented on a Server computer. It is made to manage all the Security service policies, Network Attack events, to maintain log information and Protocols. It will be a centralized server in order to service distributed IPS clients all over the network. The IPS administrators can easily manage Centralized management of policies and logs to insure best network security scenario for a large distributed organization.

Following are the components of centralized IPS system

- Configuration module
- Forensic module
- Update module
- Data collection module
- Response module

The role of IPS Clients is to monitor the network for network attacks and inform the IPS server. These IPS Clients will be network software components. They can work in both active and passive modes to insure the security in coordination with Centralized IPS Server. The primary task of IPS Clients is to detect suspicious and anomalous network traffic based on specific rules defined in rule bases of IPS. If the Clients are running in-line, it can also take a predefined action against malicious traffic.

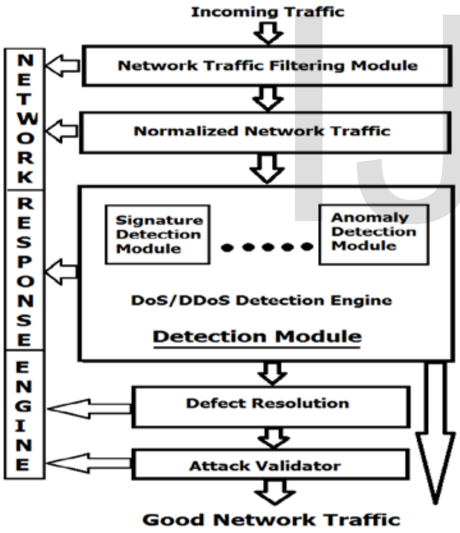

Fig. 3: Working of Proposed IPS System

Procedure of Proposed Intrusion Prevention System

Step 1: Client sends a HttpRequest to IPS

Step 2: IPS registers the Application Id of Client App

Step 3: Then a Random Captcha mechanism starts.

Step 4: If Client enters wrong Captcha, the App_Id is recorded and in response a tougher captcha is generated, sensing a DDoS attack.

Step 5: At the maximum 3 try has to be given to the Client Application.

Step 6: On failure the App Id, Mac Add and IP Add will be blocked.

5 Conclusion

Distributed denial of service attacks is a complex and serious problem and consequently, numerous approaches have been proposed to counter them. The multitude of current attack and defense mechanisms obscures the global view of the DDoS problem. It is important to recognize and understand trends in attack technology in order to effectively and appropriately evolve defense and response strategies.

This paper includes the various approaches to the already existing problems of the IPS technology. The proposed architecture would get around most of the problems but, there may be other approaches which may be better. Thus, future work on IPSs is required to perform more detailed analysis on the existing and upcoming problems. Another future work may be to test the IPS developed in this thesis with in a real network to find out deficiencies. Thus, new researches to eliminate them can be performed. Also, testing of the IPS model in this thesis with different rule set to determine the effect of rules on performance can be another future work. Later, this system and the IPS implementation developed in this thesis can be combined to form a better IPS architecture. Though we have tried our best efforts to make an Intrusion Prevention System with the best of features but still the future scope always exists.

Acknowledgment

The authors wish to thank **Dr. Manuj Darbari**, Associate Professor, Dept of Information Technology, BBD University, Lucknow, for his valuable guidance and suggestions throughout thi research work. This work was impossible without him.

References

[1] Oliver J., Leahy Dermot M., Tynan J., Mark Smith, Sean G. Doherty, “Firewall technology”, Digital Technical Journal, (2), 1997.

[2] NIST Special Publication (SP) 800-61, Computer Security Incident Handling Guide, which is available at http://csrc.nist.gov/publications/nistpubs/.

[3] Johansson, Karsten. “Offensive Operations Model”. KSAJ Inc. August 2001.[http://www.penetrationtest.com/]

[4] ForeScout Technologies, Inc. January 2004. [http://www.forescout.com/

[5] Johansson, Karsten. “Offensive Operations Model”. KSAJ Inc. August 2001.[http://www.penetrationtest.com/]

[6] Pfleeger, P. Charles. “Security in Computing”. Prentice Hall PTR. SecondEdition. p 3. 1997

[7] Shay, William A. “Firewall”. University of Wisconsin-Green Bay. 2000

[8] Yakomba Yavwa. “The Firewall Technology”. May 2, 2000

[9] Check Point Software Technologies Ltd. “Stateful Firewall Technology - Products and Solutions”. 2000. [http://www.checkpoint.com/products/technology]

[10] Espasa Calpe. “Dictionary of the Spanish tongue”. 1994

[11] Bace, R. “Intrusion Detection”. Macmillan Technical Publishing. 2000

[12] Jupitermedia. “Intrusion Detection System”. Last modified: December 13,2002. [http://www.webopedia.com/tem/I/intrusion_detection_system.html]

[13] Bace, Rebecca and Mell, Peter. “Intrusion Detection Systems”. NIST Special Publication. August 2001

[14] Spitzner, Lance. “Honeypots: Definitions and Value of Honeypots”. Last

Modified: 29 May, 2003. [http://www.tracking-hackers.com/papers/honeypots.html]

[15] TechTarget.“Honeypot”.Last updated on: September 24, 2003. [http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci551721,00.html]

[16] Honeypots.net. “Honeypots, Honeynets”. Page last modified on 21 November 2003. [http://www.honeypots.org/]

[17] CERT Coordination Center, “Denial of Service Attacks,” <http://www.cert.org/tech_tips/denial_of_ service.html>, Jun 2001.

[18] Blitznet, <http://www.packetstormsecurity.org/ distributed/blitznet.tgz>, 1999.

[19] DOSnet.c, <http://www.packetstormsecurity.org/ distributed/DOSnet.c>, 2002.

[20] Distributed DNS Flooder v0.1b (ddnsf), <http://www.packetstormsecurity.org/distributed/ddnsf.tar.gz>, 2001.

[21] Lavania, S., Darbari, M., Ahuja, N. J., & Shukla, P. K. (2012). Application of Evolutionary Algorithm in Managing the Trade-Off between Complexity of Software and its Deliverables. International Review on Computers & Software, 7(6).

[22] Dhanda, N., Darbari, M., & Ahuja, N. J. (2012). Development of Multi Agent Activity Theory e-Learning (MATeL) Framework Focusing on Indian Scenario. International Review on Computers & Software, 7(4).

[23] Siddiqui, I. A., Darbari, M., & Bansal, S. (2012). Application of Activity Theory and Particle Swarm Optimization Technique in Cooperative Software Development. International Review on Computers & Software, 7(5).

[24] Yagyasen, D., Darbari, M., Shukla, P. K., & Singh, V. K. (2013). Diversity and convergence issues in evolutionary multiobjective optimization: application to agriculture science. IERI Procedia, 5, 81-86.

[25] Darbari, M., Asthana, R., Ahmed, H., & Ahuja, N. J. (2011). Enhancing the capability of N-dimension self-organizing petrinet using neuro-genetic approach. International Journal of Computer Science Issues (IJCSI), 8(3).

[26] Srivastava, A. K., Darbari, M., Ahmed, H., & Asthana, R. (2010). Capacity Requirement Planning Using Petri Dynamics. International Review on Computers & Software, 5(6).

[27] Darbari, M., Singh, V. K., Asthana, R., Prakash, S., & Kendra, D. (2010). N-Dimensional Self Organizing Petrinets for Urban Traffic Modeling. IJCSI.

[28] Sahai, P., & Darbari, M. (2014). Adaptive e-learning using Granulerised Agent Framework. International Journal of Scientific & Engineering Research, 5(2).

[29] Lavania S, Darbari M, Ahuja NJ, Siddqui IA. Application of computational intelligence in measuring the elasticity between software complexity and deliverability. Advance Computing Conference (IACC), 2014 IEEE International, 1415-1418.