An MMO based Approach to Detect and Prevent Intrusion

Vasima Khan
Computer Science & Engg.
All Saint Inst. Of Tech
Bhopal, M.P, India

Kiran Pandey
Department of CSE
All Saint Inst. of Tech
Bhopal, M.P, India

ABSTRACT
Due to quick advances in network and communication engineering, fast development of open source Internet network tools and technologies, per hour ratio of the exchange of privacy or confidentiality of the data in the form simple or complex files over the network, the Government's planning or any confidential amendment information, or any other important evidence of the agreement or deal If all these has been attacked or stolen by the malicious as a intention of tampering, will results catastrophic penalty for the society. So that the cost of securing such information is worthless as compared to the valuable information is the modern concept and current trends for research in the field of network protection technology [1]. Most of the IDS and IPS are based on two fundamental mechanisms; Misuse detection or signature based detection [2]. Signature based systems are simple to create and efficient to operate, but are only effective against known types of attack that has fixed pattern while Anomaly detection mechanisms, on the other hand, create a profile of typical behavior for a user and raise an alert when a user attempts an activity that does not fit his/her profile. This approach tends to be highly complete in that it can detect a previously unknown attack pattern, but it requires significant effort to develop algorithms that can create accurate user profiles. In this paper a behavioral based anomaly detector solution has been proposed based on the idea inferred from [2] and [4]. The novel thing about the proposed technique is the idea of MMO (Means, Motive and Opportunity) which speedup the detection rate and enhanced the capability of catching unknown attacks by applying anomaly on them. Proposed system has been applied on real-time traffic (flows) and obtained results found much more satisfactory. For sniffing real time traffic ourmon monitoring tool has been deployed on ubuntu 13.04.

General Terms
Intrusion Detection System, Anomaly Detection.

Keywords
Anomaly, Anomaly Detection, Intrusion, ICMP Flood, IDS, IPS, IDPS, MMO, ourmon, TCP SYN, Ubuntu, Worms.

1. INTRODUCTION
Due to quick advances in network and communication engineering, fast development of open source Internet network tools and technologies, per hour ratio of the exchange of privacy or confidentiality of the data in the form simple or complex files over the network, the Government's planning or any confidential amendment information, or any other important evidence of the agreement or deal If all these has been attacked or stolen by the malicious as a intention of tampering, will results catastrophic penalty for the society. So that the cost of securing such information is worthless as compared to the valuable information is the modern concept and current trends for research in the field of network protection technology [1]. Therefore, information or network security is defined as a practice of protecting data from illegitimate access, utilize, exposé, demolition, alteration, or disruption. It is concerned with ensuring that information related risks are assessed, appropriate controls are implemented to manage those risks, and that the adequacy of those controls is monitored on a regular basis.

Four fundamental pillars of security are CAIA means Confidentiality, Authenticity, Integrity and Availability makes our system protected. But a Hackers goal is to exploit. Modern attacking techniques are so keen to their target without revealing their identity until the attack has been deployed on to the target system. Signatures are failing here due to rapid growth in IT fields only balanced anomaly detection will work to identify the unknown attacks. Another thing is to carried out the dataset which has been taken as a testing input will change every day, security never relies on the old dataset or traffic. There must be need of real time traffic. There is a urgent need of security which will insight into flowing data (traffic).

Another biggest challenge is DoS (Denial of Service) attack which makes legitimated user handicapped for their resources (computing or network). SYN flood is the transport layer specialization of the DoS.

Transport can also transport another harmful traffic known as TCP WORMS. In all such attacking condition signature based is failed only proper behavior comparative technique will work i.e. anomaly detection applied on real time traffic statistically.

In this section we have discuss the fundamental terminology and background related to network or Information security, we also present an idea of intrusion and its different types of method to detection and prevention along with the architecture of IDPS with their types.

According to [2], Intrusion is an active chronological sequence of concomitant events that intentionally try to cause damage, making system unusable, accessing illegitimate information, or act upon such information. This definition refers to both successful and unsuccessful attempts.

Free dictionary define, the act or an instance of intruding; an unwelcome visit, interjection, etc. an intrusion on one's privacy.

English Test.net defines the act of entering without warrant or invitation; encroachment called intrusion.

KDD '99 [3] has categorized five types of intrusions such as normal, probe, denial of service, user-to-root and remote-to-local.

Most of the IDS and IPS are based on two fundamental mechanisms; Misuse detection or signature based detection [2]. It defines a set of "unacceptable" behaviors and raise alerts when system behavior matches this set. Such systems are simple to create and efficient to operate, but are only effective against known types of attack that has fixed pattern. SNORT is well known IDS based on misuse concept. Moreover, it is difficult to maintain an up-to-date knowledge base of acceptable behaviors and thus this mechanism is ineffective against unknown or unusual attack patters. Anomaly detection mechanisms, on the other hand, create a profile of typical behavior for a user and raise an alert when a user attempts an activity that does not fit his/her profile. This approach tends to be highly complete in that it can detect a previously unknown attack pattern, but it requires significant effort to develop algorithms that can create accurate user profiles.

This article proposed a cost effective solutions based on behavioral anomaly mechanism by calculating MMO metrics idea inferred jointly from [2] and [4].

The novel thing about the proposed technique is quickness against intrusion. Proposed system has been applied on real-time traffic (flows) and obtained results found much more satisfactory. For sniffing real time traffic ourmon monitoring tool has been deployed on ubuntu 13.04.

Rest of the paper is organized as follow, section 2 give brief details about the types of anomalies and their methods of detection used in IDPS, section 3 briefly insights and discusses the about the current related work in the field of IDPS using anomaly detection, section 4 explains the working of proposed solution and the algorithm used, section 5 presents the experimentation and results obtained using proposed solution and finally section 6 outlines the conclusion.

2. TYPES OF ANOMALIES

Generally there are two types of anomalous behavior have been studied – Host and Network based Anomaly [5].

A. **Host Based Anomalies–** In this category all action which can try to access of the host machine in unauthorized way to be the intent of modification by executing suspicious commands. Such anomalies calculation pact while monitoring the operating system call traces. Usually intrusions are determined (found) as a cumulative chain of anomalous actions (system logs) signs. Resulting to an malicious program, illegal behavior and policy exploitation. .

B. **Network Based Anomalies–** These types of anomalies came with the network traffic or flows. Major conventional protocols works as a carrier for the network anomalies. Various tools have been applied to detect network anomalies like Nmap and Netflow tcpdump, wireshark, or ourmon.

2.1 Network Protocols Anomaly

Our previous research article addresses the anomalies of the network [5]. Author of [6] has discusses various types of anomalies related to the network flows resulting severe damage in network as well as system. Few of interest them are following –

2.1.1 UDP flood

It is a types of Denial of Service (DoS) attack exploit by sending a excessive number of UDP packets to the target machine consequently remote (target) system check the UDP protocols packets for the data and found that there is no useful information inside. After detecting such victims activity on UDP flow remote machine sends the ICMP unreachable message as a responsive and preventive mechanism that makes machine unreachable in front of legitimated machine too. If the number of UDP packets are too much cause machine down.

Proposed wok used statistical approach [2] [5] to identify UDP flooding attack. For this two metrics (indicator) for UDP flood attack has been identified:

a**. TotalBytes:** total volume of flows in bytes.

b**. TotalPackets:** total packets in incoming traffic.

2.1.2 ICMP Flood

Other types of DoS are ping flooding or ICMP flooding. To launch this attacker transmit a huge number of ICMP Echo Request (ping) packets with huge and varying in size to targeted machines. ICMP flooding is a heir of the Ping-of-Death (PoD) attack, attempting to send an extra-large ping packet to the target server or machine to get down the destination system owing to the system's be deficient to handle huge ping packets.

For Example: for windows

Ping –l 4096 192.168.1.1

Where –l option used to specify the size of the ping packets to send to targeted IP address i.e. 192.168.1.1. In this example the size of the packet is 4096 bytes instead of default size (32 bytes).

This attacks used by attackers to consumed or disrupt the targeted machines bandwidth and make them down.

Analogous to UDP flood, ICMP attack also generate a massive amount of data towards the destination [5]. Therefore similar metrics ***TotalBytes and TotalPackets*** is sufficient to compute and detect such types of attack. Indeed applying the same metrics creates vagueness to discriminate ICMP from UDP flood attack. For tenacity another metric for monitoring the ***total number of ICMP or UDP*** has been define to watch ongoing traffic into the network.

2.1.3 TCP SYN Attack

In network communication, Transmission Control Layer ensures end to end and connection oriented services. For achieving this TCP adopt the idea of 3 way handshaking. Attackers takes the advantages of this flaw (make connection using SYN transmission). Attackers send excess number of SYN packet to the host machine telling to make connection, then host replies with SYN+ACK messages to the sender but

attacker didn't reply to this and send SYN again resulting host machine is busying to handle large numbers of SYN packet i.e. SYN FLOOD attack [2,5].

TCP SYN FLOOD is a type of DoS attack launched from transport layer and it has different behavior than above two attacks relies on values SYN and ACK bit of TCP protocol. That means **TotalBytes or TotalPackets** alone is not sufficient to determine SYN anomaly so that another new metrics are required as mentioned below-

DestSocket: It is a number of flows with similar volume (e.g. SYN) to the same target socket.

Detection of SYN attack- Following metrics has been applied to detect TCP SYN attack in aggregate as mentioned in [5]-

a. The number of TCP flows per minute

b. The average number of packets in each TCP flow per minute

c. The average number of bytes in each TCP flow per minute

d. The number of unique IP addresses seen per minute.

2.1.4 Port scan

This type of attack has been launched with the help of port scanner software to search a network host for open ports. A port scanner is often used by network administrators to check the security of their networks, and it also used by hackers to compromise the system security. Many exploits rely upon port scans, for example to find open ports and send large quantities of data in an attempt to trigger a condition known as buffer overflow, or to send some specific port data packets with malicious purposes.

So again new metrics is required to catch port scanning attack to check anomalous traffic behavior:

DPort*:* number of flows that have a similar volume, same source and destination address, but to different ports.

Dport finds port scanning activity with the help of above mentioned three metrics.

2.1.5 DNS Reflector Attack

According to article [5]t to launch this type of attack, the attacker sends a excess request (flood) of DNS with a hoax d IP address (the one of the victim) to one or more DNS servers which outcome as a DNS flooding responses being sent to the victim. If an adequate amount DNS response is found in traffic this can lead to a denial of service.

To determine the DNS reflector attacks the behavior DNS request rate has been monitored per minute or per 30 sec in flows from the same (spoofed) IP address to a DNS server inside the network or another method is to filtering hosts which receive an high number of UDP flows abnormally with source port 53. False positives will be occur if legitimate host (user) sending a large number of DNS requests in a short duration of time.

Most commonly used Ports are 21, 25, 53, 110, 135, 139 and 445 these are the well known port and offer important services for the network, for example port 110 and 25 is use for email in which plays a vital role in today's business communication [7], while port 53 is important because it is the reference center for mapping IP address to DNS, if it is attacked the whole network will be in catastrophic [8]. Moreover these ports are the most popular target for attack activity especially for worm virus and port scanning.

3. Related Work

Author [4] has focuses on the insider threat and proposed a behavioral based solution to identify the suspicious one using the anomaly detection technique. To captured anomalous host activity author proposed a novel MMO based statistical technique to identify suspicious activities in the host. According to author MMO means: Means, Motive and Opportunity.

Correctness is the major designing criteria especially in the field of security; article [8] talking about the accuracy of the IDS and IDPS and their impacts and application in real time traffic with the way of metrics to validate the intrusion caught or misses. Author has discusses the significance of the FALSE positive and negative metrics of the IDS.

According to author, false positives and false negatives happen to every intrusion detection and intrusion prevention system. In this author [8] proposes a mechanism for false positive/negative assessment with multiple IDSs/IPSs to collect FP and FN cases from real-world traffic and statistically analyze these cases.

Author of [9] has introduced this article as a security need in current fast communication era and their enhancement paradigm has been proposed to strengthen security tools and methods.

In the article [10], author has discusses the method of modern attack launching through penetration testing to attack generation and proposed a anomaly based mechanism to defend from this. According to author [10], Intrusion detection systems, which aim to protect our IT infrastructure are not reliable. In this article author has explained the concept of IDS and their purpose in detail with their methods to be operated.

The author [11] has presented a method anomaly detection approach based on using immunological cooperative ways to find out network anomalies. Author has talking about the AIS and way its work as security measure in the design of modern IDPS technology.

In article [12], author has addresses the seriousness of the Denial of Service (DoS) attack and proposed a HTTTP request based anomaly method to identify the DOS attack by analyzing the TCP SYN field.

4. Proposed MMO based IDPS

Our proposed solution is to automatic discovery of intrusions into computer systems is central issue to stop unauthorized activity. Implementing intrusion detection systems on networks and hosts requires a broad perceptive of computer security. Most of the IDS and IPS are based on two fundamental mechanisms; Misuse detection or signature based detection. It defines a set of "unacceptable" behaviors and raise alerts when system behavior matches this set. The common attempts can be easily detected by Signature based IDS and the defense can be provided against such type of attack by either matching string pattern or signature. But in the prevailing scenario where there are new intrusions/ attempts reported almost every day, the existing signature-based detection proves futile [5].

Our proposed work is based on two articles [2] and [4], the reason behind choosing these two is following-

a. The author of [4] presents a new approach "BANDIT (Behavioral Anomaly Detection for Insider Threat)" to detect illegitimate insider attacker or threat using the concept of behavioral detection also term as anomaly detection. Author uses three metrics to detect insider threat- Motive, Means, and Opportunity.

We want to expand and apply authors idea to detect outside attack came from network traffic due to insider attack has less probability of exploit rather than outside.

But the idea of three metrics MMO will be applied to the outside threat detection.

b. Author of [2] has integrated the idea of agents in anomaly detection for faster reaction against intruder activity. The idea of this article, our proposed work utilized is anomaly detection technique and real time network is interesting one. Authors future will be considered in our proposed work i.e. prevention methods to ensure zero attacks on the system.

4.1 Proposed Algorithm

c. Our proposed algorithm is integration of [2] and [4], the big difference between base papers with proposed algorithm is network based malicious detection and prevention on applying modify BANDIT algorithm.

d. Its work as follow-

a. Motive: Capture network traffic (flows) for -

(1). number of flows per minute
(2). number of packets per minute
(3). number of bytes per minute
(4). average number of packets per flow per minute
(5). average number of bytes per flow per minute
(6). number of unique IP addresses seen per minute
(7). number of L2 layer flows
(8). number TCP packets, port and their control bits(R/S/F) per minute flows
(9). number of ICMP flows
(10). number of UDP flows
(11). DNS statistics
(12). HTTP flows (for detecting Trojan)

b. Means:

Calculate the mean, Max and Average for all protocols traffic (IP, TCP, UDP, DNS etc.) being captured

c. Opportunity:

Calculate TCP Work Weight, TCP Worm Weight, TCP Error Weight and UDP Work metric.

Then determine a threshold value say Tv calculated as the mean value over the last 20 minutes plus/minus five times its standard deviation.

Calculation of TCP control bit weight is using following rules:

a. TCP work weight:

IP source: $(syn + fin + reset)/total\_pkts$

b. TCP worm weight:

IP src: $syn - fin > n$

Where n number of control bits. We have fixed its value to *18.

c. TCP error weight:

IP src: $(syn - fin) * (reset + ICMP\_error$

d. UDP work metric:

IP src: $(UDPs - UDPr) * (ICMP_{errors})$

e. HTTP per minute flows

After that all these five metrics have compared with threshold (Tv) and check the deviation (in ADE) if found call to raise alarm and starts prevention mechanism.

Briefly summarized the proposed system is to develop an IDPS based on anomaly approach to detect novel attacks [2], using MMO concept given by [4].

5. Experimentation and Result Discussion

For experimentation the ubuntu 13.04 has been used on which ourmon monitoring system has been deployed for capturing real time traffic (flows), then MMO [4] concept has been designed in which following results has been obtained.

5.1 SYN FLOOD

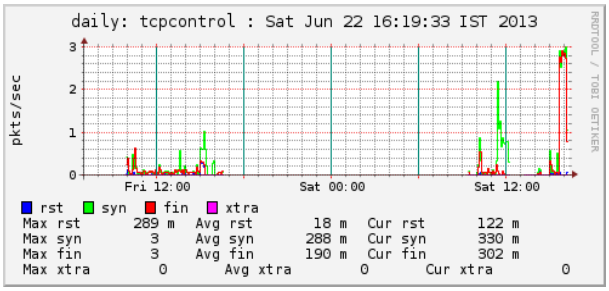

Fig 4.1: TCP SYN COUNT (Control bit)

5.2 TCP WORM

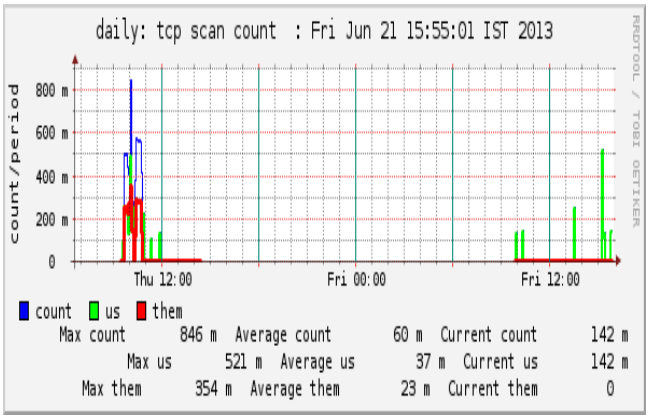

Fig 4.2: TCP SYN COUNT (Control bit)

5.3 WORMS CAPTURED

Table 4.1 Number of worms captured by Proposed System

Malicious IP Address	Dated Caught
172.16.14.96	Wed_Jun_19_10:41:04_IST_2013
103.21.127.130	Wed_Jun_19_11:05:35_IST_2013

74.125.236.139	Wed_Jun__5_12:30:36_IST_2013
172.16.1.1	Wed_Jun_12_14:49:36_IST_2013

6. CONCLUSION

This paper has discussed the types of anomalies and anomalies and ways to detect them. To overcome theses deficiency of existing methods of security a new MMO Anomaly based IDPS approach has been proposed which provides a cost effective solutions than any hardware and software based IDPS. Proposed system has provides a solution that has low false rate and high detection capability.

7. REFERENCES

[1] Lin Keming "A Network Invasion Model Based on Information Feedback", Elsevier, SciVerse Science Direct, Procedia Engineering 15 (2011) 5498 – 5502.

[2] Rathore, J.S., Saurav, P. and Verma, B. "AgentOuro: A Novelty Based Intrusion Detection and Prevention System", IEEE, Fourth International Conference on Computational Intelligence and Communication Networks (CICN), 2012.

[3] KDD09. INTRUSION DETECTOR LEARNING [EB/OL]. .http://kdd.ics.uci.edu/databases/kddcup99/task.html, 2010-09-19.

[4] Vincent H. Berk, George Cybenko, Ian Gregorio-de Souza, and John P. Murphy "Managing Malicious Insider Risk through BANDIT", IEEE, 45th Hawaii International Conference on System Sciences, 2012.

[5] Vasima Khan "Anomaly Based Intrusion Detection And Prevention System", International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 3, March – 2013.

[6] Huy Anh Nguyen, Tam Van Nguyen, Dong Il Kim AND Deokjai Choi "Network Traffic Anomalies Detection and Identification with Flow Monitoring", IEEE, 2008.

[7] Mark Ciampa, "Security + Guide to Network Security Fundamentals Second Edition", Canada. Thomson Course Technology, 2003.

[8] Cheng-Yuan Ho, Yuan-Cheng Lai, I-Wei Chen, Fu-Yu Wang, and Wei-Hsuan Tai "Statistical Analysis of False Positives and False Negatives from Real Traffic with Intrusion Detection/Prevention Systems", IEEE Communications Magazine, pp. 146-154, 2012.

[9] Cristian I. Pinzón, Juan F. De Paz, Martí Navarroc, Javier Bajo, Vicente Julián and Juan. M. Corchado "Real-time CBR-agent with a mixture of experts in the reuse stage to classify and detect DoS attacks", Science Direct Elsevier, Applied Soft Computing 11 (2011) pp. 4384–4398, 2011.

[10] Hilmi Günes¸Kayacık, A. Nur Zincir-Heywood and Malcolm I. Heywood "Can a good offense be a good defense? Vulnerability testing of anomaly detectors through an artificial arms race", Elsevier, Science Direct, Applied Soft Computing 11 (2011) pp. 4366–4383, 2011.

[11] Tarek S. Sobh and Wael M. Mostafa "A cooperative immunological approach for detecting network anomaly", Elsevier Science Direct, Applied Soft Computing 11 (2011) pp. 1275–1283, 2011.

[12] S. Venkatesan , M.S. Saleem Basha, C. Chellappan, Anurika Vaish and P. Dhavachelva "Analysis of accounting models to detect duplicate requests in web service", Elsevier Science Direct, Journal of King Saud University – Computer and Information Sciences (2012.