Attack Identification in Peer to Peer Network based on Chaotic Analysis

Vidhyalakshmi. R,
Student,
Department of Computer Science and Engineering,
Dhanalakshmi Srinivasan College of Engineering and Technology, Mamallapuram.

Pon. Arivanantham,
Associate Professor,
Department of Computer Science and Engineering,
Dhanalakshmi Srinivasan College of Engineering and Technology, Mamallapuram.

***Abstract*— Distributed denial-of-service (DDoS) attacks remain a major security problem, the mitigation is very hard especially when it comes to highly distributed botnet, which detect malicious activities like (attacks, infections, etc... As the number and size of the Network and Internet traffic increase, the need for the intrusion detection grows in step to reduce the overhead required for the intrusion detection and diagnosis, it has made many public servers increasingly vulnerable to unauthorized accesses and also attack of intrusions. Hence implementation of an intrusion prevention system (IPS) or intrusion detection system (IDS) can detect such DDoS attacks ,as they are located very close to the victim. Collect network packets and allow flow of information in real-time. Use chaos Theory to analyze it and then proposed a novel network anomaly detection algorithm (NADA) to detect the abnormal traffic. Chaotic analysis is used to detect the various DDOS attacks, which include mimicking DDoS. This algorithm can detect an anomaly caused DDoS flooding attacks.**

Index Terms*— *ANAMOLY DETECTION, LYAPUNOV EXPONENT, ENTROPY

1. INTRODUCTION

The main objective of the project is to improve the network security. As the network usage increases day by day, the number of threats posed by intruders and hackers increases. To overcome these threats and provide a safe network that overcomes these threats have to produce an advanced safety technique. So this project proposes an hybrid architecture that implements both peer to peer and Firecol techniques for safe network that cannot be easily shut down or hijacked by the hackers. One of the exclusive scope of the proposed system is the ability to track and capture the various patterns of the threatening situation by the system which makes sure that the organizational network is 100% safe from any probability of attacks from the specific attacker, thereby assuring the best of the intrusion prevention techniques.

In the field of networking, the area of network security consists of the provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources.

2. RELATED WORKS

The exponential growth of computer/network attacks are becoming more and more difficult to identify the need for better and more efficient intrusion detection systems increases in step. The main problem with current intrusion detection systems is high rate of false alarms. The design and implementation of a load balancing between the traffic coming from clients and the traffic originated from the attackers is not implemented.

3. PROPOSED SYSTEM

The proposed System, which it has “Invite the Attacks” with confidentially.
Use of this method provides effective solution to increase the security and reliability of the network. The process of forwarding requests to the Balancer detects traffic as an attack on the server; it is then directed to an alternative server.

Conventional detection and forensics methodology can then be used to gather information on the intruder who will be unaware that they are not using “real” server. By using the proxy in the system, can able to protect the system by identifying the attack present in that information which was sending by the user. Here the type of attack will be blacklisted for the future usage.By identifying the attack, the user will not be allowed to send the data to another user.Until the attack gets removed, the proxy will not allow the user to send the data.

In the System Architecture Client/Intruder can send files either with or without virus are sniffed by Network Sniffer and routes the packets to Router for filtration. Later router sends the packet for classifying types of attack to the Attack Classifier. Here based on the behavior of the Client/Intruder, it creates dynamic list of attacks to Firecol Schema. Using Rule Creation techniques, it blacklists the IP address of intruder to block them reaching server. If it founds the files without virus, allows client for grant access to server otherwise show access denied to the intruder.

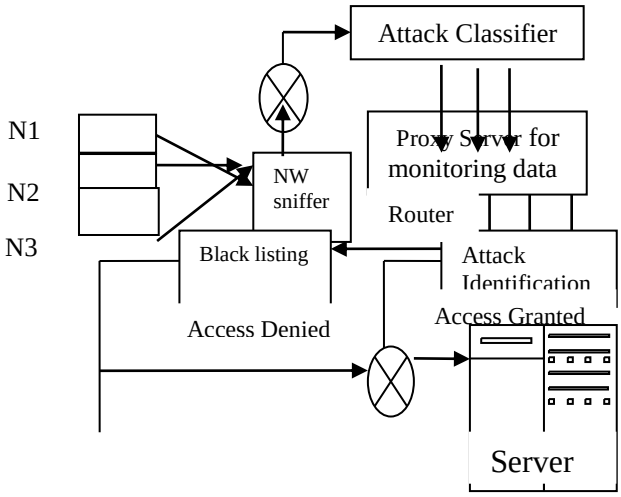

fig 1.1Architecture Diagram

3.1 SENDER/TRANSMITTER

Sender can be either host or network based, as all interaction is typically performed over a network connection. Secure Direct is an attempt to address this problem by providing a fully automated response to specific network intrusions; it can eliminate the need for human decision making, and thus mitigate slow human response times. Therefore To define a time stamp for each connection. Each time a packet is received on a connection its time stamp is updated.

3.2 NETWORK SNIFFER

Sniffer is a powerful network analysis tool that can intercept, log and sometimes parse traffic passing over a network or part of a network. A Sniffer is a piece of software that grabs all of the traffic flowing into and out of a computer attached to a network . Network Sniffer consists of a well-integrated set of functions that can resolve network problems. Sniffing is a very effective method for hackers and attackers since it is usually a passive attack and therefore more stealthy and more difficult to detect.

3.3. ROUTER

Router is a device that forwards data packets along networks and also it is connected to atleast two networks, commonly a LAN or WANs or two LANs and its ISP network. Routers are located at the gateways like places where two or more networks got connected. Routers uses headers and forwarding tables to determine the best path for forwarding the packets, and they also use protocols such as ICMP to communicate with each other and to configure the best route between any two hosts. Very little filtering of data is done through routers.

3.4 ATTACK CLASSIFIER

Attack classifier's is used to divert the attention of the attacker from the real network, in a way that the main information resources are not compromised. To build attacker profiles in order to identify their preferred attack methods similar to criminal profiles used by law enforcement agencies in order to identify a criminals modus operand. To identify new vulnerabilities and risks of various operating system, environments and programs which are not thoroughly identified at the moment.

3.6 FIRECOL SCHEMA

Honey pot schema which is powered by intelligence along with the design of attack classifier. The output generated by the classifier generates a dynamic list of attacks, which are then queued in the proposed Firecol architecture built with neural network to understand various approach of behaviour and patterns of the attacker. The network administrator collects all such relevant information over the network itself allowing the inbound network connection from the attacker to do so. The system creates a hybrid framework to prevent the probability of vulnerable and hostile situation over the network even before the attack event is performed by the attacker.

3.7 RULE CREATION

In the dynamic rule creation mechanism very easily a suspicious intruder and intrusions can be detected based on the behaviour and context blacklisting of the resource/host/IP/network can be done without much overheads. These rules are used to differentiate normal network connection from anomalous connections refer to the probability of intrusions.

3.8 NETWORK INTRUSION DETECTION SYSTEMS (NIDS)

It monitors the packets on the network wire and tries to discover an intruder by matching the attack pattern to a database of known attack patterns.

3.9 BLACK LISTING

In computing, a blacklist or block list is a basic access control mechanism that allows access to everyone, except for the members of the black list (i.e. list of denied accesses). The opposite is a whitelist, which allow nobody, except members of the white list. As sort of a middle ground, a greylist contains entries which are temporarily blocked or temporarily allowed. Greylist items are reviewed or further tested for inclusion in a blacklist or whitelist.An organization may keep a blacklist of software or websites in its computer system. Titles on the list would be banned and everything else would be allowed.

4.CONCLUSION

In this research work proposed a system where the network administrator will observe and analysis various types of attacking tendencies originating from variable source in network. The process basically understand the pattern and behaviour of the hostile circumstances over the network and then it creates the profiles of the attackers based on this pattern analysis, which will protect the network system of the organization by blacklisting the origination of the resource profiling over the network itself thereby assuring the organizational network to be the most secure one in any future probability of network threats from those attackers.

5.FUTURE WORK

In this work, have described some of the previous efforts to measure IDS, and have outlined some of the difficulties that have been encountered. To believe that a periodic, comprehensive evaluation of IDSs could be valuable for network managers, information security officers and data managers. However, because both normal and attack traffic are so variable from site to site, and because normal and attack traffic evolve over time Solving the problem of high availability and security simultaneously offers the opportunity for more reliability than systems which solve the problems separately, in addition to being easier t6o implement, and offering increased opportunity for recording and data analysis. The integration of these two technologies, however, is a non-trivial task. A fine balance must be achieved between speed and robustness of IDS features – it is equally bad to have the web server crash because an attack was missed, or drop large amounts of traffic due to an overly through IDS becoming a bottleneck. While improving the efficiency of the programming can mitigate this problem to an extent, the trade-off is certain to remain, and choosing the right balance will likely continue to be a difficult task for the system administrator. It is the authors' opinion that this type of system could provide a much needed additional security tool, however, a good deal of streamlining work remains before it could be widely deployed.

REFERENCES

[1] Caimu Tang,Member,IEEE and Dapeng Oliver Wu,Senior Member. (2007),IEEE, ' Distance-Bounding Based Defense Against Relay Attacks in Wireless Network ', IEEE transactions on wireless comunications, vol. 6, NO. 11.

[2] Chieh-Jen Cheng,StudentMember,IEEE, Chao-Ching Wang,Member,IEEE, Wei-Chun Ku,StudentMember,IEEE, Tien-Fu Chen, Member, IEEE, and Jinn-Shyan Wang, Member.(2012). ' A Scalable High-Performance Virus Detection Processor Against a Large Pattern Set for Embedded Network Security ',IEEE trasaction on very large scale integration (VLSI) systems, vol. 20, no. 5.

[3] Fabio Pasqualetti,student Member,IEEE,Florian Dorfler,Student Member and Francesco Bullo,Fellow. (2012) ,' Attack Detection and Identification in Cyber-Physical Systems ' IEEE.

[4] Heather Yu,John Buford and Madjid Merabti,Huawei Technoligies,USA,Avaya Labs,USA and Liverpool John Moores University. (2013),' Improving Messaging Security in Structured in P2P Overlay Networks ',UK.

[5] Johannes Kinder, Stefan Katzenbeisser, Member. (2010) ,' Proactive Detection of Computer Worms Using Model Checking ',IEEE, Christian Schallhart, and Helmut Veith IEEE Transactions on dependable and secure computing, vol.7, no. 4.

[6] Lin Cai and Roberto Rojas-Cessa. (2009),' Bounding Virus Proliferation in P2P Networks with a Diverse-Parameter Trust Management Scheme ',2009 IEEE communications letters, VOL. 13, NO. 10

[7] Qiyan Wang and Nikita Borisov, Department of Computer Science University of Illinois at Urbana-Champaign IL. (2012), ' Octopus: A Secure And Anonymous DHT Lookup ' U.S.A qwang26@illinois.edu,32nd IEEE International Conference on Distributed Computing Systems.

[8] Xiaofei Wang,Yang xu,Junchen Jieng,Olga Ormond,Bin Liu and Xiaojun Wang. (2013) ' StriFA: Stride Finite Automata for High-Speed Regular Expression Matching in Network Intrusion Detection Systems ',IEEE.

[9] Xiang Fan and Yang Xiang School of Management and Information Systems Centre for Intelligent and Networked Systems Central Queensland University Rockhampton, Australia(2010),'Propagation Modeling of Peer-to-Peer Worms ',{x.fan2, y.xiang}@cqu.edu.au,24th IEEE International Conference on Advanced Information Networking and Application.

[10] Xinlei Ma and Yonghong chen,(2014) ' DDos Detection Method Based on Choas Analysis of Network Traffic Entropy ',IEEE comminication letters volume 18.

[11] Zhou Hangxia College of Information Engineering China Jiliang University Hangzhou,(2010),' Mitigating Peer-To-Peer Botnets by Sybil Attack ',China.