Blocking Distributed Denial of Service Flooding Attacks with Dynamic Path Detectors

Dr. E. Punarselvam[1], Mrs. P. Bhuvaneshwari[2], B. S. Mohanapriya[3], Sandra Kumar[4], V. Saranya[5],R.Sneha[6]
[1].Professor & Head of the department,
[2] .Assistant Professor ,
[3,4,5&6]. Final Year Students
Department of Information Technology, Muthayammal Engineering College (Autonomous),
Rasipuram-637 408, Namakkal (Dt), Tamil Nadu.

***Abstract*:-The Path identifiers are used in existing approaches are static, which makes it easy for the attackers to launch the distributed denial of service flooding attacks. To address this issue, design and implement the framework by using dynamic path identifier (D-PID).By using D-PID, to implement and evaluate the result with different types of modules. The first module can access the user for viewing the authenticated process after registered. Then the second module can access after the registration process that the users can compare the path information by using correlation factors among nodes. Then the third module has to select the system to transfer the data key automatically enabled and decrypted. Then the stub monitoring process will initiate automatic to find the behavioural distance and evaluating the distance. In the fourth module, the D-PID can trace back the path of every data. The result will give the users and admin to report in the next module. These are the results to make it easily using network.**

Keywords: Distributed Denial-of-Service (DDoS), Inter-domain Routing, path identifiers, Security.

1. INTRODUCTION

Today's network environment is full of dangerous attackers, hackers, crackers, and spammers. Authentication, authorization and auditing are the most important issues of security on data communication. An authentication system must provide adequate security for its intended environment, otherwise it fails to meet its primary goal. Security has become an inseparable issue as information technology is ruling the world. As a result of the astonishingly rapid advancement of various kinds of Internet technologies, more information are transmitted to all parts of the world from everywhere through the net. Some of the objects transmitted online may be important secret images, and in such cases the senders have to take information security issues into consideration before they can trustingly enjoy the speed and convenience that nothing in this world but the Internet can offer. Intrusion Detection Systems, also known as Intrusion Detection and Prevention Systems, are the appliances that monitor malicious activities in a network, log information about such activities, take steps to stop them, and finally report them. Intrusion detection systems help in sending an alarm against any malicious activity in the network, drop the packets, and reset the connection to save the IP address from any blockage. A good network security system helps business reduce the risk of falling victim of data theft and sabotage. Network security helps protect your workstations from harmful spyware. It also ensures that shared data is kept secure. Huge traffic can cause stability problems and may lead to vulnerabilities in the system

2. IMPLEMENTATION

D-PID is the art of detecting inappropriate, incorrect, or anomalous activity. It also evaluates suspicious activity that occurs in corporate network. Intrusion detection system is the process of detecting and identifying unauthorized or unusual activity on the system. The external intruders are unauthorized users of the machines they attack.

Internal intruders have permission to access the system, but not some portions of it. Furthermore internal intruders divide into intruders who masquerade as another user, those with legitimate access to sensitive data and the most dangerous type, the clandestine intruders who have the power to turn off audit control for themselves.

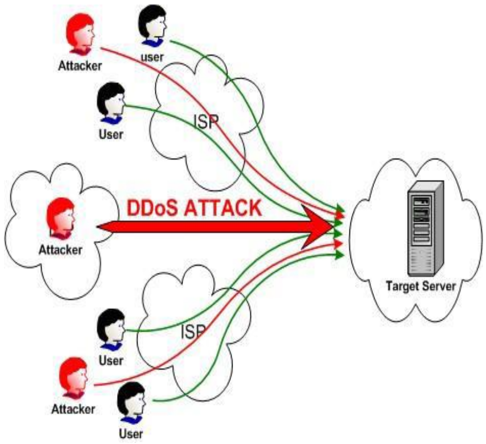

Fig 2.1 DDos Attack

3.SYSTEM ARCHITECTURE

To trace back the source of the DDOS attacks in the internet is extremely hard. It is one of the extraordinary challenge to trackback the DDOS attacks, that attackers generate huge amount of requests to victims through compromised computers(zombies), in order to denying normal services or degrading the quality of services. Recent survey shows that than 70 internet operators in the world demonstrated that DDOS attack are increasing dramatically and individual attacks are more strong and sophisticated. IP trace back means the capability of identifying the actual source of any packet across the internet; with the help of IP trace back schemes identify the zombies from which the DDOS attack packets entered the internet.

A number of IP trace back approaches have been suggested to identify attackers. Among them two major methods for IP trace back, Probabilistic packet marking (PPM) and deterministic (DDPM). Both of these require routers to inject marks into individual packets. And also provides some limitations such as scalability, huge demands on storage space and vulnerability to packet pollution. Both PPM and DPM also require duplicate on the existing routing software which is extremely hard. IP traceback using information theoretical parameters, and there is no packet marking in the proposed strategy; we, therefore, can avoid the inherited shortcomings of the packet marking mechanisms. To categorize packets that are passing through a router into flows, which are defined by the upstream router where a packet came from, and the destination address of the packet.

During non-attack periods, routers are required to observe and record entropy variations of local flows.Entropy variation or entropy variation interchangeably. Once a DDoS attack has been identified, the victim initiates the following pushback process to identify the locations of zombies: the victim first identifies which of its upstream routers are in the attack tree based on the flow entropy variations it has accumulated, and then submits requests to the related immediate upstream routers. The upstream routers identify where the attack flows came from based on their local entropy variations that they have monitored.

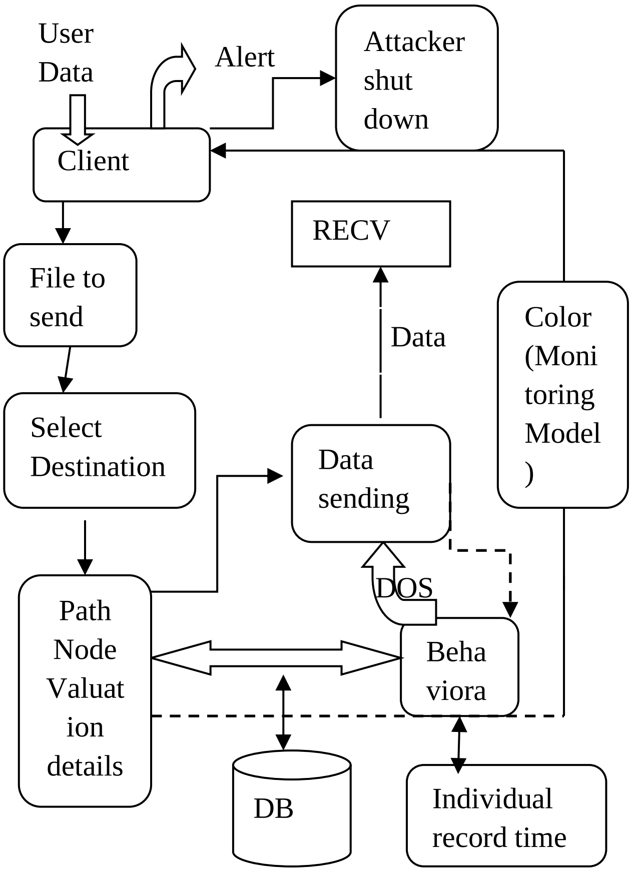

Fig 3.1 System Architecture

4. EXISTING SYSTEM

These mechanisms release the protected online servers from monitoring attacks and ensure that the servers can dedicate themselves to provide quality services with minimum delay in response. Moreover, network-based detection systems are loosely coupled with operating systems running on the host machines which they are protecting. As a result, the configurations of network based detection systems are less complicated than that of host-based detection systems.

Network-based detection systems can be classified into two main categories, namely misuse based detection systems and anomaly-based detection systems. Misuse-based detection systems detect attacks by monitoring network activities and looking for matches with the existing attack signatures. Owing to the principle of anomaly based detection, which monitors and flags any network activities presenting significant deviation from legitimate traffic profiles as suspicious objects, anomaly-based detection techniques show more promising in detecting zero-day intrusions that exploit previous unknown system vulnerabilities. These systems commonly suffer from high false positive rates because the correlations between features/attributes are intrinsically neglected or the techniques do not manage to fully exploit these correlations.

4.1. Limitations

- Lot of misbehave users and security violation
- Router failures
- Lacks scalability
- Data corruption
- Poor security
- Defacing &packet loss

5. PROPOSED SYSTEM

An alternative approach based on novel Hidden Markov Model (HMM) for computing behavioural distance, and present the design, implementation, and evaluation of a novel architecture using HMM-based behavioural distance to detect attacks. An HMM models a doubly stochastic process; there is an underlying stochastic process that is not observable (it is “hidden”) but that influences another that produces a sequence of observable symbols. When applied to our problem of computing behavioral distance, the observed symbols are process behaviors, and the hidden states correspond to aggregate tasks performed by the processes (e.g., read from a file). An interesting and important observation is that since these hidden tasks should be the same, it should be possible to reliably correlate the simultaneous observable behaviours of the two processes when no attack is occurring, and to notice an increased behavioural distance when an attack succeeds on one of them. Perhaps surprisingly, our technique uses a single HMM to model both processes simultaneously, in contrast to traditional uses of HMMs for anomaly detection, where an HMM models a single process.

5.1 ADVANTAGES

- Faster authentication
- No defacing by abusers
- Data packet security and maintain the domain reliability
- Easily abusers will blocked and rise alarm
- Trace backing system helps to prevent data corruption

6. METHODOLOGY

6.1 Node authentication of individual ensuring

This module contains the user and the administrator authentications. The admin will have permission to view the entire processes done by the user. The user can only view the authenticated process after getting registered to the approach. User can view their personal information and the data which sent by him. In the server module have the static and secure login to enter and starts the server to receive the data.

6.2 Network info with path node correlation

The network has divided by workgroups. This module will help us to get the connected and the active systems in the network. After getting login to our process, this module will get the connected systems and shows to the users. The user can select the system to deliver their data by file transfer. The disconnected and the shutdown systems are not visible in the list. After that users can compare the path info by using correlation factors among nodes. Every node update their own table about correlation factors and that will circulate entire network

6.3 Data Transfer

The user has to select the system to transfer the data and the file to be transferred. The selected file will be encrypted for secured transfer. When the data received by the desired path of destination, the key automatically enabled and decrypted. When the user starts the process, the stub monitoring will initiate automatically to find behavioural distance and the evolutionary distances.

6.4 Color Monitoring and verification

In our process, we have to monitor the client data, which are sent to the receiver with a certain path. After the intruder affects the current data, there is no use of reports. So here, we trace back the path of every data. Tracing the path of the data from one end to another end helps to find path deviations. The Monitoring stub will Report to the client side, when the data information path getting differ from the desired paths by comparing the distance and time intervals.

6.5 Admin and Reports

All the data transactions and intruder information are forward to the administrator. The administrator can view all the reports and monitor the network paths. The whole histories of data are maintained by the administrator. So that, the administrator can able to make the denial of service of the intruder from the reports module.

7. RESULTS AND DISCUSSION

Home Page

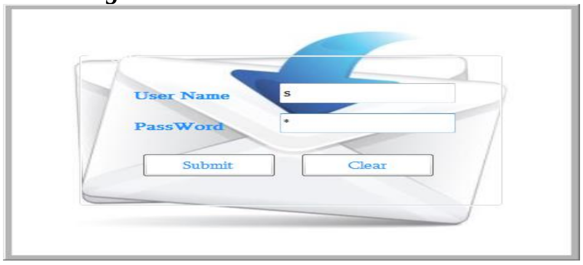
User Name: s
PassWord: *

Fig 7.1 Home Page

User Login Details

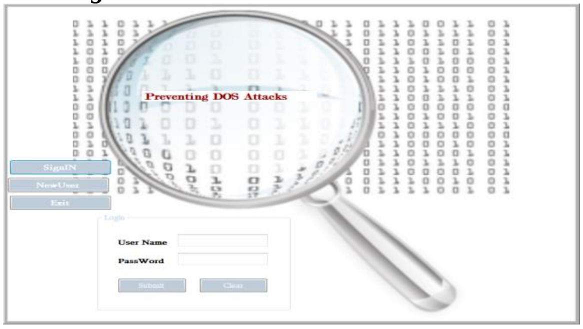

Fig 7.2 User Login Page

Monitoring Details

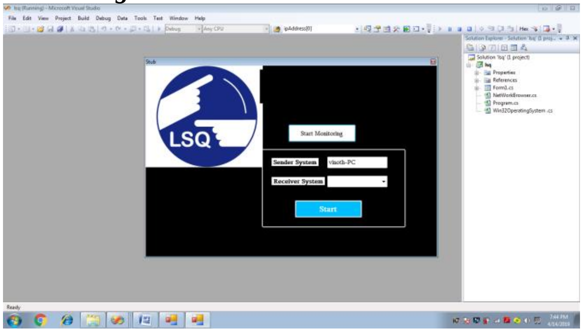
Sender System: vinoth-PC
Receiver System:

Fig 7.3 Stub Monitoring

Data Path Jammer

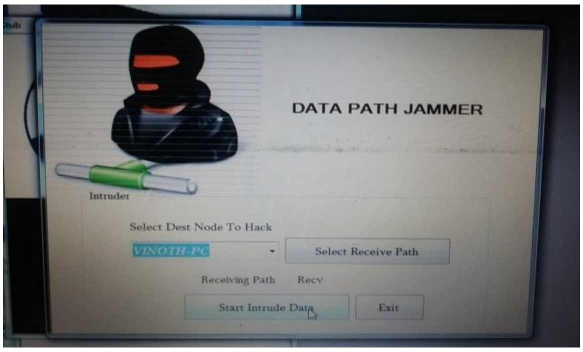
Select Dest Node To Hack: VINOTH-PC

Fig 7.4 Intruder

8. CONCLUSION

Project presented the design, implementation and evaluation of D-PID, a framework that dynamically changes path identifiers (PIDs) of inter-domain paths in order to prevent DDoS flooding attacks, when PIDs are used as inter domain routing objects. It described the design details of D-PID and implemented it in a 42-node prototype to verify its feasibility and effectiveness. It presented numerical results from running experiments on the prototype. The results show that the time spent in negotiating and distributing PIDs are quite small (in the order of ms) and D-PID is effective in preventing DDoS attacks. The results show that D-PID significantly increases the cost in launching DDoS attacks while incurs little overheads, since the extra number of GET messages is trivial when the retransmission period is 300 seconds, and the PID update rate is significantly less than the update rate of IP prefixes in the current Internet. The latter technique facilitates our system to be able to distinguish both known and unknown DoS attacks from legitimate network traffic

9. FUTURE ENHANCEMENTS

In future test D-PID based detection system using real world data and employ more sophisticated classification techniques to further alleviate the false positive rate.

10. REFERENCES

[1] Duan, X. Yuan, and J.Chandrashekar, “Controlling IP spoofing through interdomain packet filters,” IEEE Trans. Depend. Sec. Comput., vol. 5, no. 1, pp. 22–36, Jan. 2008.

[2] J. Francois, I. Aib, and R. Boutaba, “FireCol: A collaborative protection network for the detection of flooding DDoS attacks,” IEEE/ACM Trans. Netw., vol. 20, no. 6, pp. 1828–1841, Dec. 2012.

[3] P. Ferguson and D. Senie, “Network ingress filtering: Defeating denial of service attacks that employ IP source address spoofing,” IETF RFC 2827, May 2000.

[4] OVH Hosting Suffers 1Tbps DDoS Attack: Largest Internet Has Ever Seen,accessed on December 25, 2016.

[5] K. Park and H. Lee, “On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law Internets,” ACM SIGCOMM Comput. Commun. Rev., vol. 31, no. 4, pp. 15–26, Aug. 2001.

[6] C. Snoeren et al., “Hash-based IP traceback,” In ACM SIGCOMM Comput. Commun. Rev., vol. 31, no. 4, pp. 3–14, Aug. 2001.

[7] S. Savage,D. Wetherall, A. Karlin, and T. Anderson, “Practical network support for IP traceback,” ACM SIGCOMM Comput. Commun. Rev., vol. 30, no. 4, pp. 295–306, Aug. 2000.

[8] H. Wang, C. Jin, and K. G. Shin, “Defense against spoofed IP traffic using hop-count filtering,” IEEE/ACM Trans. Netw., vol. 15, no. 1, pp. 40–53, Feb. 2007.

[9] Yaar, A. Perrig, and D. Song, “StackPi: New packet marking and filtering mechanisms for DDoS and IP spoofing defense,” IEEE J. Sel. Areas Commun., vol. 24, no. 10, pp. 1853–1863, Oct. 2006.

[10] S. T. Zargar, J. Joshi, and D. Tipper, “A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks,” IEEE Commun. Surveys