Implementation and Evaluation of Dynamic Path Identifier (D-PID) to prevent Distributed Denial-Of-Service attack

Soumee Maschatak[1], Dhanraj DS[2], Manjunatha T N[3]

[1]Student, Dept. of Computer Science and Engineering, East West Institute of Technology, Bangalore
[2]Associate Professor, Dept. of Computer Science and Engineering, East West Institute of Technology, Bangalore
[3]Assistant Professor, Dept. of Computer Science and Engineering, East West Institute of Technology, Bangalore

Abstract – *PIDs are used as inter-domain routing methods to prevent Distributed Denial-Of-Service attacks. But the PID mechanism used are static, which makes it easy for the attackers to launch the DDOS attack. To overcome this problem, the concept of D-PID was introduced. The main idea behind the DPID is that the PID of an inter-domain path connecting the two domains is kept hidden and it changes dynamically. This paper focuses on the implementation and the evaluation of Dynamic Path Identifiers and its feasibility, effectiveness and cost.*

Key Words: Distributed Denial-Of-Service, Network, Cloud Computing, Decoy Computing, Domains, Dynamic path identifiers.

I. INTRODUCTION

In D-PID, two adjacent domains periodically update the PIDs between them and install the new PIDs into the data plane for packet forwarding. Even if the attacker obtains the PIDs to its target and sends the malicious packets successfully, these PIDs will become invalid after a certain period and the subsequent attacking packets will be discarded by the network. Moreover, if the attacker tries to obtain the new PIDs and keep a DDoS flooding attack going, it not only significantly increases the attacking cost, but also makes it easy to detect the attacker. In particular, our main contributions are twofold.

- On one hand, we propose the D-PID design by addressing the following challenges. First, how and how often should PIDs change while respecting local policies of autonomous systems (ASes)?
- Second, since inter-domain packet forwarding is based on PIDs that change dynamically, it is necessary to maintain legitimate communications while preventing illegal communications when the PIDs To address this challenge, D-PID lets every domain distribute its PIDs to the routers in the domain
- Third, the overheads incurred by changing PIDs should be kept as small as possible. This includes not only the overhead in negotiating PIDs by neighbouring domains, but also the overhead for a domain to distribute the updated PIDs to routers in the domain, and that for transmitting content request messages resent by content consumers. To address this challenge, the PID prefix assigned to an inter-domain path is unique among the PID prefixes assigned by the two domains connected by the inter-domain path

II. IMPLEMENTATION

We have designed a simple project to illustrate and implement the concept of D-PID by designing six pages. The pages and their functionality are as follows –

2.1 General Login Page

2.1.1 Description:

The general login page for admin and user.

2.1.2 Functional requirements:

- Admin can login to this application with valid username, valid password and login type as admin. When click on login button; admin home page should be displayed with links to view user details, view user registration and upload details.
- User can login to this application with valid username and valid password. When click on login button; user home page should be displayed with links to view upload file page, download uploaded details, change password, login access time, user can also view who has attacked his file in view alert page and sign out page.

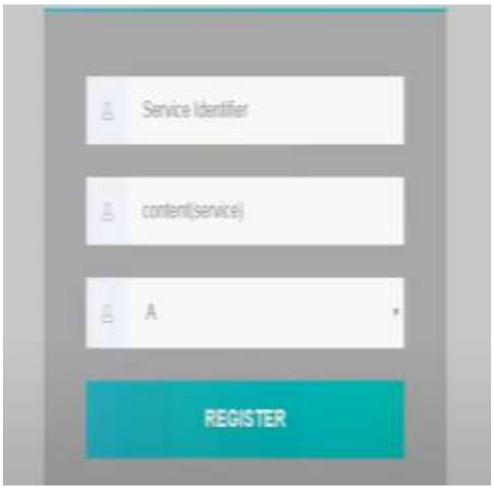


Figure 2.1: Server window page

2.2 Registration

2.2.1 Description:

When User clicks on Signup link in home page; general registration page to register a new user should be displayed.

2.2.2 Functional requirements:

- When User clicks on Signup link; registration page with Name, Password, Confirm Password, Email, Mobile No, Address, Time, Security questions, Answer, register button should be displayed.
- When User clicks on register button with valid information, the registration successful message should be displayed for completing the registration.

2.3 User login

2.3.1 Description:

User login to this application appears with User Page after login is successful.

2.3.2 Functional requirements:

- When User login with the valid username, password ;
- Welcome page shows the service lists of the service user.

2.4 Admin can View Users Registered and Users Upload details

2.4.1 Description:

The registered Users and their uploaded data details should be present in view User details and view Upload details links respectively

2.4.2 Functional requirements:

- Admin logins with his credentials; his home page should be displayed.
- When admin clicks on view User details link; all registered User details should be displayed.
- When admin clicks on view Upload details link; all users uploaded data details should be displayed.

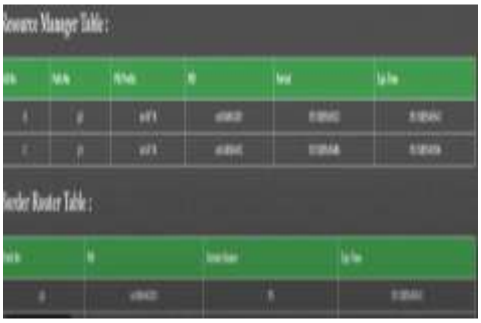
2.5 User can upload the Data.

2.5.1 Description:

To Upload the data User needs to login into his account by giving valid username and password.

2.5.2 Functional requirements:

- User in his home page clicks on to the Upload link.
- Then user can upload his data to the cloud in his access time.



esource Manager Table :

order Router Table :

Figure 2.2: Resource Manager

2.6 User can download the Uploaded data.

2.6.1 Description:

User can be able to download his data by answering security question given at the time of registration.

2.6.2 Functional requirements:

- User in his home page clicks on My-files link.
- Then User can be able to download his uploaded data by answering the security question given at the time of registration.

2.7 User can change password

2.7.1 Description:

User can change the password whenever his data misused by the attacker.

2.7.2 Functional requirements:

- User in his home page clicks on to change password link; the page to change password appears.
- Enters the old password, new, password and conform password; clicks on change password button.

III. System Architecture

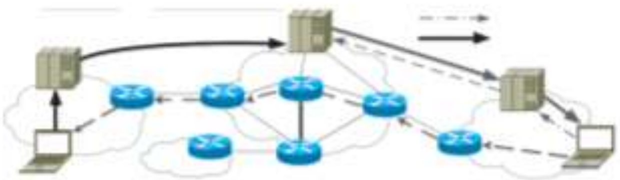


Figure 3.1: System Architecture for prevention of distributed Dos

3.1 Subscriber

Subscriber involves the users which they want to access to the cloud. Here user first needs to for the cloud by using the internet by giving his registration details. In fog computing first user should signup into the cloud by providing different registration details.

3.2 Network

In cloud computing network plays important role between the users and internet service provider. Whenever user wants to subscribe to the cloud he needs to access I through the network. Through network user can be able to get different services provided by the provider.

IV. MODULES

The modules implemented are the following -

4.1 Cloud Computing

4.2 User Behaviour Profiling

4.3 Decoy Documents

4.1 Cloud computing

Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service-provider interaction.

4.2 User Behaviour Profiling

This chapter monitor data access in the cloud and detect abnormal data access patterns User profiling is a well-known Technique that can be applied here to model how, when, and how much a user accesses their information in the Cloud. Such 'normal user' behaviour can be continuously checked to determine whether abnormal access to a user's information is occurring. This method of behaviour-based security is commonly used in fraud detection applications.

4.3 Decoy documents

This paper presents a different approach for securing data in the cloud using offensive decoy technology which monitor data access in the cloud and detect abnormal data access patterns. Here disinformation attack is launched by returning large amounts of decoy information to the attacker. This protects against the misuse of the user's real data. This technology to launch disinformation attacks against malicious insiders, preventing them from distinguishing the real sensitive customer data from fake worthless data the decoys, then, serve two purposes:

- Validating whether data access is authorized when abnormal information access is detected, and
- Confusing the attacker with bogus information.

V. REFERENCES

[1] Hongbin Luo, Member, IEEE, Zhe Chen, Jiawei Li, and Athanasios V. Vasilakos, Senior Member, IEEE, "Preventing Distributed Denial-of-Service Flooding Attacks with Dynamic Path Identifiers", **IEEE TRANSACTIONS ON INFORMATION AND FORENSICS SECURITY, 2017.**

[2] J. Francois, I. Aib, and R. Boutaba, "Firecol: a Collaborative Protection Network for the Detection of Flooding ddos Attacks," IEEE/ACM Trans. on Netw., vol. 20, no. 6, Dec. 2012, pp. 1828-1841.

[3] OVH hosting suffers 1Tbps DDoS attack: largest Internet has ever seen. [Online] Available: https: //www.hackread.com/ovh-hostingsuffers- 1tbps-ddos-attack/.

[4] 602 Gbps! This May Have Been the Largest DDoS Attack in History. http://thehackernews.com/2016/01/biggest-ddos-attack.html.

[5] S. T. Zargar, J. Joshi, D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," IEEE Commun. Surv. & Tut., vol. 15, no. 4, pp. 2046 - 2069, Nov. 2013.

[6] P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks that Employ IP Source Address Spoofing," IETF, Internet RFC 2827, May 2000.

[7] K. Park and H. Lee, "On the Effectiveness of Route-Based Packet Filtering for Distributed DoS Attack Prevention in Power-Law Internets," In Proc. SIGCOMM'01, Aug. 2001, San Diego, CA, USA.

[8] A. Yaar, A. Perrig, D. Song, "StackPi: New Packet Marking and Filtering Mechanisms for DDoS and IP Spoofing Defense," IEEE J. on Sel. Areas in Commun., vol. 24, no. 10, pp. 1853 - 1863, Oct. 2006.

[9] H. Wang, C. Jin, K. G. Shin, "Defense Against Spoofed IP Traffic Using Hop-Count Filtering," IEEE/ACM Trans. on Netw., vol. 15, no. 1, pp. 40 - 53, Feb. 2007.

[10] Z. Duan, X. Yuan, J. Chandrashekar, "Controlling IP Spoofing through Interdomain Packet Filters," IEEE Trans. on Depend. and Secure Computing, vol. 5, no. 1, pp. 22 - 36, Feb. 2008.

[11] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical Network Support for IP Traceback," In Proc. SIGCOMM'00, Aug. 2000, Stockholm, Sweden.

[12] A. C. Snoeren, C. Partridge, L. Sanchez, C. E. Jones, F. Tchakountio, S. T. Kent, and W. T. Strayer, "Hash-Based IP Traceback," In Proc. SIGCOMM'01, Aug. 2001, San Diego, CA, USA.

[13] M. Sung, J. Xu, "IP traceback-based intelligent packet filtering: a novel technique for defending against Internet DDoS attacks," IEEE Trans. On Parall. and Distr. Sys., vol. 14, no. 9, pp. 861 - 872, Sep. 2003.

[14] M. Sung, J. Xu, J. Li, L. Li, "Large-Scale IP Traceback in High-Speed Internet: Practical Techniques and Information-Theoretic Foundation," IEEE/ACM Trans. on Netw., vol. 16, no. 6, pp. 1253 - 1266, Dec. 2008.

[15] Y. Xiang, K. Li, W. Zhou, "Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics," IEEE Trans. on Inf. Foren. and Sec., vol. 6, no. 2, pp. 426 - 437, May 2011.

[16] H. Ballani, Y. Chawathe, S. Ratnasamy, T. Roscoe, S. Shenker, "Off by default!," In Proc. HotNets-IV, Nov. 2005, College Park, MD, USA.

[17] A. Yaar, A. Perrig, and D. Song, "SIFF: a stateless internet flow filter to mitigate DDoS flooding attacks," In Proc. IEEE Symposium on Security and Privacy, May 2004, Oakland, CA, USA.

[18] B. Parno, D. Wendlandt, E. Shi, A. Perrig, B. Maggs, and Y. Hu, "Portcullis: Protecting connection setup from denial-of-capability attacks," In Proc. SIGCOMM'07, Aug.2007, Kyoto, Japan.

[19] X. Yang, D. Wetherall, and T. Anderson, "TVA: A DoS-Limiting Network Architecture," IEEE/ACM Trans. on Netw., vol. 16, no. 3, pp. 1267 - 1280, Jun. 2008