Survey on IP Traceback Mechanism To Ensure Cloud And Network Security

Sona John[1], Angel Rose Antony[2], Dhanya Devassykutty[3], Navya Paulachan[4], Radhika Krishnan[5]
[1, 2, 3, 4] Dept of Dual Degree Master of Computer Application
[5]Assistant Professor, Dept of Computer Science
[1, 2, 3, 4, 5] Depaul Institute Of Science And Technology(DIST)., Angamaly, Kerala, India.

Abstract- *IP traceback is used to find network traffic attack. Origin of IP packet is not authenticated. So source of IP address is not trusted. A time limited token based authentication framework for authenticating traceback service queries is implemented. The design objective of the framework is preventing the illegal users for accessing traceback information.Thus to prevent network traffic attack.And ensures that the entity requesting for traceback service is an actual recipient of the packets to be traced.*

Keywords- IP Traceback, Access Control, Authentication, Cloud based Traceback.

I. INTRODUCTION

Internet contains huge collection of data. If your data does not provide appropriate control and security measures, it may be subjected to an attack. The most common type of network attack is denial of service attack. In this an attacker is trying to access illegal use of the service. The opponents are attacking networks by flooding and the computers with lots of traffic from one or more computers in the control of the attackers.It practical applications, including network forensics, security auditing, network fault diagnosis, performance testing, and path validation. While many different IP traceback approaches have been proposed, none of them has achieved universal acceptance or practical deployment. The risk of leaking network topology information ranks as the major challenge in hindering the acceptance of traceback techniques.

IP tracebackis amethod that finds source and path of packets. The attackers are spoofed with hidden IP address. These traceback schemes are used in intra and inter autonomous system. Cloud based IP traceback simplify the traceback procedure. The main aim of the proposed system reducing the unauthorized users for accessing traceback data.. ISPs (Internet Service Providers) are normally reluctant to allow any external party to gain visibility into their internal structure, since such exposure not only leaks sensitive information to their competitors but also makes their networks vulnerable to attacks.

II. LITERATURE SURVEY

There are number of IP traceback approaches. These approaches are using different methods. IP spoofing attacks are critical issues to the internet. All of them have advantages and disadvantages. IP traceback is to find attack source when the source address is false. The existing traceback techniques do not provide satisfactory properties for traceback deployment.

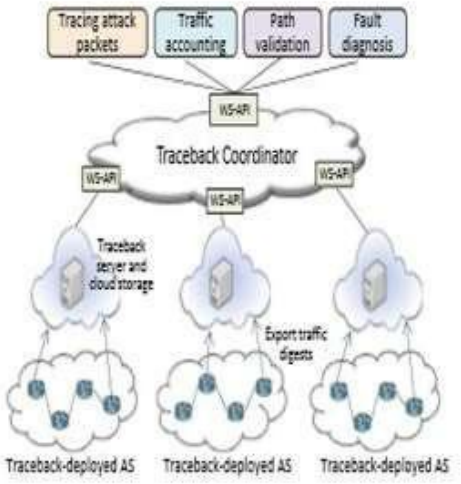

Figure 1: Architecture overview of cloud-based traceback.

Existing IP traceback techniques having number of limitations. The major problem of IP traceback is leaking network topology information. This will leads to economic inefficiency and technical shortcomings. Existing systems insufficient for providing security and practical alignment. In order to avoid the limitations of existing system cloud based authentication framework is proposed.

The new technique consists of traceback architecture. It contains of three layers, the central traceback coordinator layer, autonomous system level server layer and router layer. The main part of the system is central traceback coordinator. In the cloud based authentication framework, user gets a token that have a specific time for accessing traceback service. The proposed system ensures the user requesting traceback

information is valid or not. The advantage of cloud based traceback is, it is incrementally deployable and reducing traffic flow attack [1].

Light weight source authentication and path validation, in this concept introducing two secure protocols. This protocol is used for dynamically recreatable key set up, source authentication and path validation. The dynamically recreatable keys are recreatable and efficient. Source authentication and path validation is provided by origin and path trace protocol. It is scalable, lightweight secure protocol. The retroactive key set up process, the router cannot know advance paths and it is for preventing coward attacks [2].

Dynamic probabilistic packet marking scheme is a new marking scheme. In probabilistic packet marking scheme uses certain probability. But in the case of dynamic probabilistic packet marking scheme it replaces the probability of marked packets. As a result it addresses the problem of leftover packets. In this scheme the victim can identify the true source of the attacker and also it contains no unmarked packets. Less number of attack packets required for IP and efficient for distributed denial of attacks is the advantages of this scheme. The difficulty of this scheme is marking generated by dynamic probabilistic packet marking is more than probabilistic packet marking and also high overhead of routers closest to source [3].

A novel hybrid traceback scheme integrates packet logging and marking. The router has an interface number. Packet is marked by interface number. Path reconstruction, false positive and negative rates in this scheme is more efficient. This scheme provide fixed storage requirement. Using this hybrid scheme, filter malicious traffic is identified. Marking field is marked in the hash table and table index is stored on the packet. The difficulty of the scheme is, if router is subverted then it gives false result [4].

Based on entropy variations, a novel traceback method is proposed. The entropy variation is in between normal and distributed denial of attack traffic. At given interval of time entropy variation determines the disordered flows. It works as independent software component. When the victim identifies an attack then the pushback tracing procedure. The advantage of this approach is, it is fast in large scale network attack. And also it is easy to implement [5].

Flexible deterministic packet marking is an IP traceback system used for find the true source of attacks. According to the requirement, the marking field length is changed in flexible deterministic packet marking. The marking field length is adjusted because it is flexible and there by the rate of marking is varied according to traffic in the router. Large number of true sources with less false positive in packets and low resource requirement on routers. When compared with probabilistic packet marking flexible deterministic packet marking requires lesser configuration [6].

Scalable packet digesting schemes for IP traceback approach investigated two ways of aggregating the packets. The packet aggregation is to extend time of traceback query length. Packet aggregation consists of two parts, namely flow and source-destination set. These two parts provide lower memory requirements. Aggregated IP traceback schemes generate attack graphs. But the attack graph does not contain individual packet traceback information. An individual packet traceback approach contains logging of packet digests is necessary [7].

On deterministic packet marking, it addresses the drawback of packet marking algorithm. At ingress filtering marking is done all packets. The marking field has two fields such as ID field and Reserve flag field. When the victim gets the information of these two fields the victim can reconstruct the IP address. Whenever the packet enters the network, marking procedure is takes place. Deterministic packet marking is scalable and simple to implement. This scheme is false positive and also whenever the source address is spoofed it fails [8].

Firstly analyze the probabilistic packet marking algorithm. The proposed approach is to solve the problem of IP traceback. In this concept is to mark packets in the router with certain probability. It contains two fields such as markbit field, data field. These fields constitute the 16-bit identification field. This identification field is used for packet marking. Victim uses the marked packet for further investigation. The advantage of this approach is less overhead. High probability over leftover packets is the drawback of probabilistic packet marking algorithm [9].

Advanced and authentication packet marking techniques is for IP traceback. Path reconstruction is efficient and more accurate in advanced marking scheme. Authentication packet marking scheme provides authentication of marking. These schemes allow the victim to find the origin of spoofed IP packets. The main advantage of this scheme is, it is efficient against spurious markings. The limitations is, it have to perform additional functionality so the router is slow down. Also router requires private key for victim and router [10].

Hash based IP traceback system generates audit trails within the network. Each router stores the hash of the

invariants. It is a 32-bit digest. Bloom filter is a space efficient data structure that store hash digests. To enable IP traceback, source path isolation engine is developed. It consists of three components such as Data Generation Agents, Source Path Isolation Engine Collection and Reducing Agent and Source Path Isolation Engine Traceback Manager. This traceback system can handle fragmentation and perform single packet traceback. The drawback of the system is, it requires high internet service provider's involvement [11].

III. CONCLUSION

One of the most popular techniques in identifying the attack source is the cloud based IP traceback mechanism. The cloud based IP traceback is an enhanced user authentication framework which make sure that the entity requesting for the traceback procedure is a real recipient of packets to be traced. The aim of the framework is to check illegal users from requesting trace back information. Such cloud based traceback simplifies the traceback processing and makes traceback service more accessible.

REFERENCES

[1] Aloysius WooiKiakAng, Wee Yong Lim, and VrizlynnL.L.Thing "FACT: A Framework for Authentication in Cloud-Based IP Traceback,"IEEE Transactions on Information Forensics And Security, Vol. 12, No. 3, March 2017.

[2] T. H.-J. Kim, C. Basescu, L. Jia, S. B. Lee, Y.-C.Hu, and A. Perrig, "Lightweight source authentication and path validation," in Proc.SIGCOMM, 2014, pp. 271-282.

[3] K.P. Chaudhari, A.V. Turukmane, in:, V.V. Das, Y. Chaba (Eds.), Mobile Communication and Power Engineering, Springer Berlin Heidelberg(2013) 381.

[4] M.-H. Yang and M.-C. Yang, "RIHT: A novel hybrid IP traceback scheme," IEEE Trans. On Info. Forensics and Security,vol.7,no. 2,pp., 2012.

[5] S. Yu, W. Zhou, R. Doss, and W.Jia,"Traceback of ddos attacks using entropy variations," IEEE Trans. on Parallel and Distributed Systems,vol. 22, no. 3, pp. 412– 425, March 2011.

[6] Y. Xiang, W. Zhou, and M. Guo, "Flexible deterministic packet marking: An IP traceback system to find the real source of attacks," IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 4, pp. 567-580, Apr. 2009.

[7] T.-H. Lee, W.-K. Wu, and T.-Y. Huang,"Scalable packet digesting schemes for IP traceback," in ICC '04, 2004, pp. 1008–1013.

[8] A .Belenky ,N.Ansari, IEEE Communications Letters 7 (2003) 162.

[9] K. Park, H. Lee, in:, IEEE INFOCOM 2001.Twentieth Annual Join Conference of the IEEE Computer and Communications Societies. Proceedings (2001) 338.

[10] DD. X. Song and A. Perrig, "Advanced and authenticated marking schemes forIPtraceback," in INFOCOM '01, 2001,pp. 878–886.

[11] AA. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, S. T. Kent, and W. T.Strayer, "Hash-based IP Traceback," in SIGCOMM01, 2001, pp. 3–14.