Implementation of IP Traceback Mechanism Using Authentication Framework For Cloud And Network Security

Sona John[1], Angel rose Antony[2], Dhanya Devassykutty[3], Navya Paulachan[4], Radhika Krishnan[5]
[1]Dept of Master of Computer Application(DDMCA)
[2]Assistant Professor
[1, 2] 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

The IP traceback methods are classified as reactive and proactive. Reactive identifies the traceback information after that the attack has been occurred. Proactive identifies the traceback information when packets are traversed through the network. The IP traceback can be determined using the technique packet marking. The main idea of this framework is token passing mechanism. The token is send along with the data is passed to the destination. Traceback server generates the token. After extracting the token only the data arrives at the destination. If an attack occurs the token can be used for identifying the sources and path of the packets[1].

Implementation is the process of converting a new or revised system design into operation. It is the key stage in achieving a successful new system because, usually it reveals a lot of up heal. It must therefore be carefully planned and controlled. Apart from planning the two major tasks of preparing for implementation are education and training of users and testing of the system.

Education of users should really take place much earlier in the project. Training has to be given to the web masters regarding the new system. Implementation is the stage of project where the theoretical design is turned into working system or it is the key stage in achieving a successful new system. Therefore it must be carefully planned and controlled. It can also be considered to be the most crucial stage in achieving a successful new system and in giving the user confidence that the new system and in giving the user confidence that the new system will work and be effective.

Implementation is the final and important phase. It is the phase where theoretical design is turned into working system, which works for the user in the most effective manner. It involves careful planning, investigation of the present system and the constraints involved, user training, system testing and successful running of developed proposed system. The implementation process begins with preparing a plan for the implementation of the system. through the shortest path to the destination. Token is generated by the traceback server.

II. DATA TRANSMISSION

According to this plan the activities are to be carried out, discussions made regarding the equipment and resources and the additional equipment has to be acquired to implement the new system. The user tests the developed system and changes are made according to their needs. The testing phase involves the testing of a system using various kinds of data. This method also offers the greatest security since the old system can take over if the errors are found or inability to handle certain type of transactions while using the new system.

In our project we are mainly using four modules[2] :

1. Network Formation(RIP)
2. Best Path and token generation
3. Data transmission
4. IP Traceback

1. Network Formation[Routing Information Protocol (RIP)]

The Routing Information Protocol (RIP) is one of a family of IP Routing protocols, and is an Interior Gateway Protocol (IGP) designed to distribute routing information within an Autonomous System (AS).RIP is a simple vector routing protocol with many existing implementations in the field. In a vector routing protocol, the routers exchange network reachability information with their nearest neighbors. In other words, the routers communicate to each other the sets of destinations ("address prefixes") that they can reach, and the next hop address to which data should be sent in order to reach those destinations. This contrasts with link-state IGPs; vectoring protocols exchange routes with one another, whereas link state routers exchange topology information, and calculate their own routes locally.

2. Best Path Selection and token generation

The routers involved in the route selection process are to select shortest path based on Dijkstras shortest path algorithm. The data is transferred through the shortest path to the destination. Token is generated by the traceback server.

3. Data transmission

The source node send data to destination, data is transferred through the shortest path. Data is transmitted in an encrypted format. So it provides high security. During data transmission the traceback server will initiate and it will trace the data transmission path and it is given to the cloud server. The node transmission details, traceback path and the message are stored in the traceback server.

4. IP Traceback

Here the source node send data to destination once the destination received the data it has know the data transmission path. So the destination send traceback request to the server with IP address and token. The server keeps all the records about nodes. Then the server checks the IP address and token. If the IP address and token are valid then server responds as data transmission path to destination.

Traceback Processing:

In our proposed cloud-based traceback, traceback procedure starts with an investigator sending queries to the traceback coordinator. Upon verification, retrieved result including the upstream traceback-deployed AS information will be returned from the corresponding traceback server that witnessed the flow of interest. In the next step, Suppose a user starts a traceback request consist and the estimated attack time.[3] The traceback coordinator will first contact the traceback server in the same domain of the victim, which is responsible for the authentication of this traceback request the traceback coordinator sends a query to the traceback server of the upstream AS. The traceback coordinator will terminate the recursive query process until a traceback server identifies itself as the first traceback-deployed AS on the attack path. Each traceback server generates an attack graph for its local domain. Apparently, this approach achieves efficient traceback processing by avoiding the traceback query flooding. Note that flexibility rests with the ISP—the granularity of an attack graph can be controlled by each individual traceback server to avoid leak of sensitive information. Attack graphs from each AS are assembled together to form a complete attack graph by the traceback coordinator.

Benefits of the Cloud-based Traceback:

Given the promise of cloud computing with reduced in- frastructure costs, ease of management, high flexibility and scalability deploying traceback service in cloud not only meets several favorable properties identified by prior arts but also presents new appealing opportunities.[4]We argue that such a centralized system simplifies the traceback processing and well addresses the technical and economic challenges for the practical deployment of an IP traceback system. We list the main advantages of cloud-based traceback as follows.

1. The cloud architecture makes a traceback system incrementally deployable without much extra effort, thus pro- viding a progressive traceback solution.
2. It has the potential to offer stronger privacy-preserving guarantees. With each ISP handling their individual traceback servers independently, their privacy and autonomy can be securely and adequately maintained.
3. Cloud-based traceback shows increased ro- bustness against attacks. As the cloud storage is for private use, the AS can hide the storage server from the Internet, by placing it within its private network. Besides multi-layer restrictions (using IP addresses, ports, protocol, user access control, etc.) can be put in place. The information can also be stored in encrypted form. A private cloud storage is robust against the tampering by the attackers, without resorting to cryptographic techniques. For example, it is possible the cen- tral server checks for any routing inconsistencies and figures out compromised routers or corrupted information. This is in contrast to marking-based approach, where compromised routers pass spoofed or erase marking information to misdirect the traceback procedure. Likewise, in traditional logging- based approach, the hop- by-hop traceback process is also vulnerable to compromised routers.

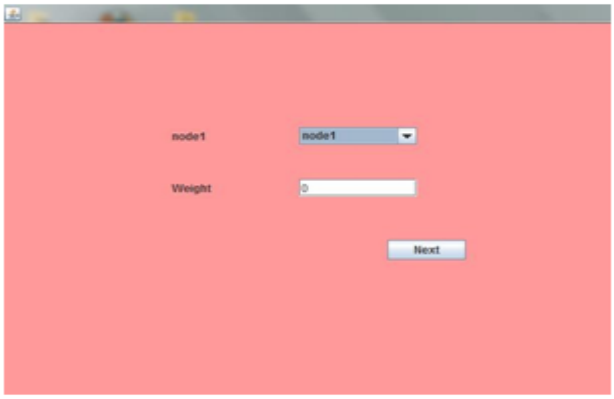
4. Cloud-based traceback architecture enables forensic investigations in the aftermath of attacks, as logs can be maintained for longer period than in traditional logging-based traceback (where router storage capacity is limited)
5. The pay-by-use nature of cloud service encourages ISPs' involvement to deploy the traceback service, where the traceback coordinator can distribute monetary re- wards to tracebackdeployers. It is worth mentioning that the proposed cloud-based trace- back architecture resonates highly with the software-defined networking (SDN), which is an emerging paradigm that de- couples networks control plane and data plane physically. SDN offers a centralized view of the network in each AS, and shows similarities with our cloud-based traceback architecture. Since SDN architecture provides more customized and flexible traffic flow measurement, and routers regularly send collected flow statistics to the controller, our cloud-based traceback can well integrate into SDN[5].

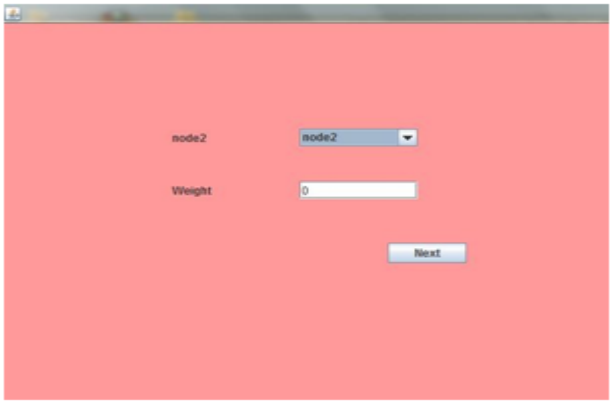
The Need For a New Traceback Authentication:

In the context of cloud based traceback, suppose a malicious entity has assess to the cloud based service and can retreaive recordings from the corresponding traceback server.On one hand,there exist a risk that a misbehaving user derives the ISP 's network topology after collecting sufficient traceback results.On the other hand, malicious users may Launch denial of service(DoS) attacks against the traceback service[6].In addition we except to protect legal internet users privacy since they normally donot want to be trace.There for any entity wishing to perform a traceback should be appropriately authenticated. Username and password are widely used as the main authentication mechanism.However password-based authentication is not scalable and suffers from password cracking vulnerability.
This paper proposes and enhanced user authentication scheme which is customized for regulating access to traceback service in a cloud- based traceback system.

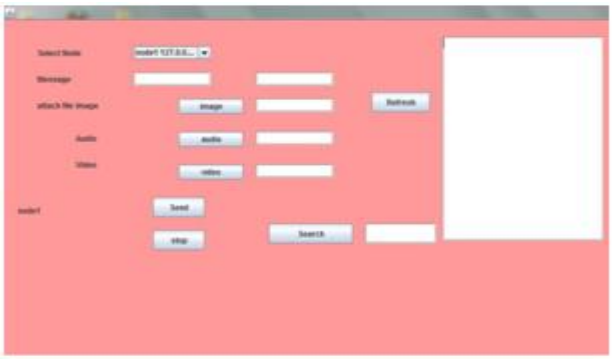
Result Analysis:

Node Generation-

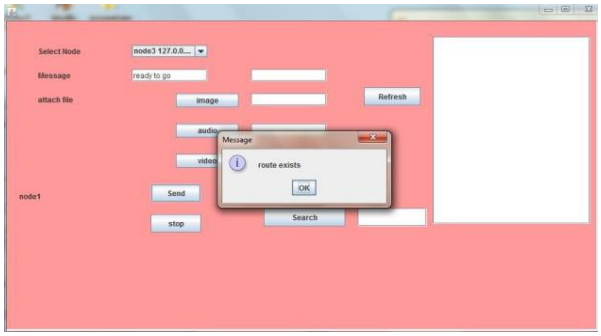




Message sending node 1 to node 3



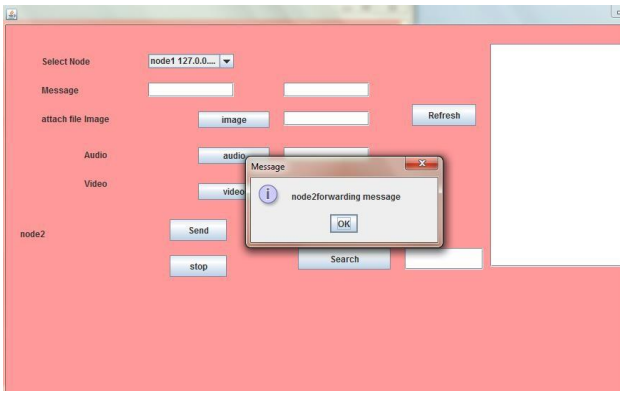
Route exsisting



Token generation

Forwading to node 2

Message reached at node 3



III. CONCLUSION

In this work, we first presented the cloud-based IP traceback architecture, which possesses several favorable properties that previous traceback schemes failed to satisfy simultaneously. We then focused on the access control problem in the context of cloud-based traceback, where the objective is to prevent illegitimate users from requesting traceback information for ill intentions. To this end, we proposed the FACT, an enhanced user authentication framework which ensures that the entity requesting for the traceback procedure is an actual recipient of the flow packets to be traced. Evaluation studies based on real-world Internet traffic datasets demonstrated the feasibility and effectiveness of the proposed FACT. As for our future work, we will investigate the optimal marking scheme in token delivery, and implement FACT framework on our cloud-based IP traceback testbed.

REFERENCES

[1] Aloysius Wooi Kiak Ang, Wee Yong Lim, and Vrizlynn L.L.Thing “FACT: A Framework for Authentication in CloudBased 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] C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio,S. T. Kent, and W. T. Strayer, “Hash-based IP Traceback,” in *SIGCOMM ’01*, 2001, pp. 3–14