A SURVEY ON CLOUD-BASED IP TRACE BACK FRAMEWORK

Suraj Patil[1], Prof. Parth Sagar[2]

1 Suraj Patil, RMD Sinhgad School of Engineering, Pune, India
2 Prof. Parth Sagar, RMD Sinhgad School of Engineering, Pune, India

Abstract - *IP trace back plays an important role in internet cyber investigation processes, where the sources and paths of packets need to be identified the traversed path. It has a wide range of applications, including forensics network, auditing security, network fault diagnosis, and performance testing. Despite a plethora of research on IP trace back, the Internet is yet to see a large-scale practical deployment of trace back. While this makes the trace back service more available, regulating access to trace back service in a cloud- based architecture becomes an important issue. Consequently, we address the access control problem in cloud-based trace back. Our design objective is to check illegitimate users from requesting trace back information for malicious intentions such as ISPs topology discovery. To this end, we propose a temporal token- based authentication framework, called FACT, for authenticating trace back service queries. FACT embeds temporal access tokens in traffic flows, and then delivers them to end-hosts in an efficient manner. The proposed solution ensures that the entity requesting for trace back service is an actual recipient of the packets to be traced. Finally, we analyze and validate the proposed design using real-world Internet data sets.*

Key words: **IP trace back, marking based trace back, opportunistic piggyback marking, network forensics, Internet Service Provider (ISP), intrusion detection system**

1. Introduction

A great amount of effort in modern years has been directed to the network security issues. In this paper, we tackle the difficulty of identifying the source of attacks. The device that generates the attacks may be a reflector, zombie, or a final link in a stepping stone chain. While identifying the device from which the attack was initiated as well as the person, behind the attack is a final challenge, we limit the difficulty of identifying the packets whose addresses may be spoofed source of the offending. Numerous solutions have been proposed for this problem.

These solutions can be divided in two groups. The first group of the solutions depends on the routers in the network to send their identities to the destinations of definite packets, either encoding this information straightforwardly in seldom used bits of the IP header or by generating a new packet to the similar destination. The major limitation of this type of solutions is that they are paying attention only on flood-based (Distributed) Denial of Service {DoS) attacks and cannot handle attacks comprised of a small number of packets. The second group of solutions includes centralized management and logging of packet information on the network. Solutions of this type bring in a large overhead and are more complex and they are not scalable.

In this paper we have surveyed on various types of Cloud Based Frame work. Section 2 of this paper deals with literature survey, Section 3 presents the proposed system and Section 4 concludes the paper.

2. LITERATURE SURVEY

In the paper “Scalable packet digesting schemes for IP trace back” [1], the sources of an attack are identified in the Internet security area. An attack could consist of a large number of packet streams generated by many compromised slaves that consume resources associated with various network elements to deny normal services or a few offending packets to disable a system. Several techniques based on probabilistic samples of transit packets have been developed to determine the sources of large packet flows. It seems that logging of packet digests is necessary for trace back of an individual Packet.

In the paper “Lightweight source authentication and path validation” [2], for the purpose of feature extraction Single-Packet IP Trace back in order to save memory, hash-based IP trace back exploits hashing techniques to record the passage of individual packets through each auditing router. The passage of a set of packets is recorded by storing the corresponding packet digests to a digest table. A specific packet is determined, with a controlled false positive rate (FPR), to be a member of the set if its packet digest maps to an existing pattern stored in the digest table.

In the paper “Flexible deterministic packet marking: An IP traceback system to find the real source of attacks" [3], the proposed system assists in mitigating attack effects; DoS attacks, for instance, can be mitigated if they are first detected, then traced back to their origins, and finally blocked at entry points. In addition, IP trace back can be used for a a wide range of practical applications, including network forensics, security auditing, network fault diagnosis, performance testing, and path validation wide range of practical applications, including network forensics, security auditing, network fault diagnosis, performance testing, and path validation.

In the paper "Traceback of DDoS attacks using entropy variations" [4], a practical packet marking approach has been developed for IP trace back 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. For example, an adversary may misuse trace back services to reconstruct an ISP as network topology.

3. PROPOSED SYSTEM

We propose a cloud-based trace back architecture, as depicted in Fig. 1. It exhibits a hierarchical structure which is organized in three layers, the central trace back coordinator layer, AS-level trace back. The layers are as follows:

3.1 Intra-AS Structure:

A trace back server is deployed in each trace back-deployed AS. Traffic flow information collected at trace back-enabled routers will be exported to internal cloud storage which is managed by the trace back server in each AS for long-term storage and analysis. Routers may independently sample the traffic or collect the traffic flow in a coordinated fashion.

3.2 Trace back as a Service:

Trace back-enabled ASes expose their trace back services in the trace back coordinator.

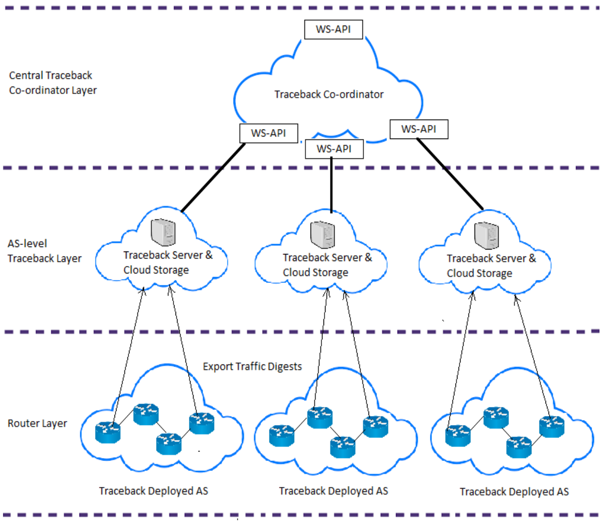

Fig-1: Cloud Based IP Traceback System Architecture

3.3 Inter-AS Logical Links:

To maintain inter-AS logical relations, and achieve efficient trace back processing and high incremental deploy ability.

4. CONCLUSION

In this work, we first presented the cloud-based IP trace back architecture, which possesses several favorable properties that previous trace back schemes failed to satisfy simultaneously. We then focused on the access control problem in the context of cloud-based trace back, where the objective is to prevent illegitimate users from requesting trace back information for ill intentions. To this end, we proposed the FACT, an enhanced user authentication framework which ensures that the entity requesting for the trace back 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 trace back tested.

ACKNOWLEDGEMENT

It is my privilege to acknowledge with deep sense of gratitude to my guide Prof. Parth Sagar for his kind cooperation, valuable suggestions and capable guidance and timely help given to me in completion of my paper. I express my gratitude to Prof. Vina M. Lomte, Head of Department, RMDSSOE (Computer Dept.) for her constant encouragement, suggestions, help and cooperation.

REFERENCES

[1] Aloysius Wooi Kiak Ang, Wee Yong Lim, and Vrizlynn L. 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] 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.

[4] S. Yu, W. Zhou, R. Doss, and W. Jia, "Traceback of DDoS attacks using entropy variations," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 3, pp. 412-425, Mar. 2011.

[5] L. Cheng, D. M. Divakaran, W. Y. Lim, and V. L. L. Thing, "Opportunistic piggy-back marking for IP traceback," IEEE

Trans. Inf. Forensics Security, vol. 11, no. 2, pp. 273-288, Feb. 2016.

[6] H. Tian and J. Bi, “An incrementally deployable flow-based scheme for IP trace-back,” IEEE Commun. Lett., vol. 16, no. 7, pp. 1140-1143, Jul. 2012.

[7] G. Yao, J. Bi, and A. V. Vasilakos, “Passive IP trace back: Disclosing the locations of IP spoofers from path back scatter,” IEEE Trans. Inf. Forensics Security, vol. 10, no. 3, pp. 471-484, Mar. 2015.

[8] H. Zhang, J. Reich, and J. Rexford, “Packet traceback for software defined networks,” Princeton Univ., Princeton, NJ, USA, Tech. Rep. TR-978-15, 2015.