Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

IP TRACEBACK IN NETWORK BASED CLOUD USING ROUTING INFORMATION PROTOCOL

Laya Chacko[1], Bibin Varghese[2], Smita C Thomas[3]

[1]PG Scholar, Computer Science and Engineering, Mount Zion College of Engineering, Kadammanitta

[2]Assistant Professor, Computer Science and Engineering,Mount Zion College of Engineering,India

[3]Research Scholar, VelsUniversity, India,

--*************************----------------------------------

Abstract:Iptraceback is the effective solution for finding the source and paths of the packets. Network forensics, security auditing, network fault diagnosis, and performance testing are the wide range of applications of iptraceback. Several challenges related to existing traceback solutions mainly trouble to allow ISPs for providing the traceback services i.e., the risk of leaking sensitive information vulnerable to the network and inadequate in providing privacy. This paper mentions about the cloud based architecture for traceback. Cloud based traceback service offers more accessible. Regulating access to traceback service in a cloud-based architecture is an important issue. To this end, introduce a token based authentication structure for validating traceback queries. This token embeds with the data in encrypted format and the proposed system ensures actual recipient of the packets to be traced.

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

--*************************----------------------------------

I. INTRODUCTION

IP traceback is the efficacious key to determine the sources and the paths taken by the packets. IP traceback has numerous spectrum all as follows: Network forensics, security auditing, network fault diagnosis, performance testing, and path validation. The major challenges of traceback techniques mainly leaking of network topology information. ISPs (Internet Service Providers) provide external party to gain visibility to their internal structures, this leaks the sensitive information, since such risk leaks sensitive information to their opponents and also makes networks vulnerable. The current IP traceback mechanisms are inapt to bring the privacy and support for incremental deployment.

Here in this work presents a novel cloud-based traceback architecture, which deed moreaccessible cloud framework for logging traffic summary, in order to device forensic traceback. This type of cloud-based traceback shorten the traceback processing and accomplish thetraceback service more reachable. Hence which boost robustness against the attack and acquire privacy preserving properties. Still, controlling access to cloud-based traceback service becomes decisive issue.

II. EXISTING SYSTEM

IP traceback is the efficacious key to determine the sources and the paths taken by the packets. Generally, traceback needs because of network intruders or attackers along spoofed IP addresses. It also benefits in mitigating attack effects: DoS attacks. For example, if any of attack detected then traceback to the origins and definitely blocked at entry points.

IP traceback has numerous spectrum all as follows: Network forensics, security auditing, network fault diagnosis, performance testing, and path validation.Hencemany different IP trace-back approaches have been proposed, none of above has achieved universal approval or practical placement.

The major challenges of traceback techniques mainly leaking of network topology information. ISPs (Internet Service Providers) provide external party to gain visibility to their internal structures, this leaks the sensitive information, since such risk leaks sensitive information to their opponents and also makes networks vulnerable. The current IP traceback mechanisms are inapt to bring the privacy and support for incremental deployment. Incremental deployability is another important factor for a viable IP trace-back solution. Thus the existing IP traceback mechanisms are inadequate for providing guarantees on privacy and incremental deployment.

III. PROPOSED SYSTEM

In the proposed system, trace-back coordinator controls all the trace-back operations. Recently trace-back enabled autonomous system exhibit their trace-back services in the trace-back coordinator.

The proposed system exhibit three intra structure in the architecture. Intra AS structure in which the data transmission takes place and a traceback server generates the token. The token is a random bit number and holds the IP address of the router. So that if an attack occurs the receiver can easily identify the path. The source node also transmit the data along with the token and data send in an encrypted format. If an attack occurs then destination node sends the trace-back query to server for acquire the data transmission path. Thus the server checks the IP address and token is valid or not. If it valid then respond with the data transmission path. Communication between any two intra AS structure is inter AS structure. The trace-back server stores the transmission route details, transmission path message and the token.

CLOUD-BASED TRACEBACK DESIGN

Instead of authenticating with the user name and password, the user obtains a time limited token and uses this token for validation. This token based access control used to protect sensitive information in cloud structure. This access token associated with a validity period. A trace-back server contribute temporary access tokens to the host,thus the receipent of packets to be traced. This token issuance of on-demand security and helps to retrieve trace-back logs.

How to transmit a token to end-hosts in adequate and vigorous style after the token is issued by the trace-back server in an AS. One straightforward approach is to write the token in IP packet header, so that end-host can obtain the token when receiving the marked packets. However, the available marking space in IP header is rather limited.

The design objective is to adapt to the limited marking space in IP header for efficient token delivery. An ideal case is that, there is an entire bitwise match between certain pre-defined packet fields and the token, i.e., the bit values in specific packet fields and the token are entirely equivalent.

In this paper, an efficient token delivery scheme to spread a token across a wide spectrum of packets. This design makes the token difficult to be captured and thus reduce the risk that attackers launch packet dropping attacks, while minimizing the bit space per packet required for marking. The basic idea is that, partition a token into a sequence of non-overlapping fragments. Given an IP packet at the last-hop router, check whether certain field of this packet matches any fragment of the token that is to be delivered to an end-host. If there is a match, mark the packet to notify the end-host that it carries partial information of the token. When the end-host receives a marked packet, it will extract the partial token information embedded in the received packet. Given a collection of marked packet, the end-host can reconstruct the complete access token.

Let NM denote the selected match attribute for token fragment match. First define the token fragment match, and then describe the marking procedure. Token Fragment Match: Given a token segment (TS) and the selected attribute (NM) of an IP packet, if NM contains a non-empty subset of set bits (i.e., bits that are set to 1) in TS, and MA retains all the clear bits (i.e., bits that are set to 0) in TS, then call this a token fragment match between NM and TS.

If the last-hop router simply marks all the packets that match any token fragment, then call such simple marking scheme as the blind marking. One drawback of the blind marking is that, since the last-hop router does not keep track of the portions of the token that has been relayed to an end-host, it has to be executed throughout a specified time period without knowing whether an access token has been fully matched or not. Moreover, when a partial token has already been formed at the end-host, the blind marking may result in marked packets carrying redundant information to the endhost. To minimize the marking overhead, introduce the idea of concise marking.

Algorithm1: Algorithm for token delivery using concise marking

```
Input: Token fragments $TS_i$, $i \in [0,n-1]$
Output: Marked packets
$remainingBits_i \leftarrow TS_i$; $i \in [0,n-1]$
while ConciseMarking(Packet P) do
    MA = getMatchAttribute (P);
    mark ← 0;
    for i=0 to n−1 do
        if ConciseMatch (NM, $TS_i$, &$remainingBits_i$) then
            mark |= (1 << (8-i)); //8-bit marking space
        end
    end
    if mark ≠0 then
        MarkPacket (P, mark);
    end
    if ∀i, $remainingBits_i$= = 0 then
        break;
    end
end
```

IV. CONCLUSION

In this work, first present the cloud-based IP traceback architecture, which possesses several favorable properties that previous traceback schemes failed to satisfy simultaneously. Here 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. 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 IP traceback Routing information protocol. As for the future work, investigate the optimal marking scheme in token delivery, and implement framework on cloud-based IP tracebacktestbed.

The future work will focus on the following two areas:

- Blocking of attacked IP
- Optimizing node relationships in a super-router network.

REFERENCES

[1] H. Aljifri, "IP trace-back: a new denial-of-service deterrent?" IEEE Security and Privacy, vol - 1, no.3, pp: 24–31, 2003.

[2] M.Sung and J.Xu, "IP trace-back-based intelligent packet filtering: a novel technique for defending against Internet DDoS attacks", IEEE Trans. on Parallel and Distributed Systems, vol-14, no. 9, pp: 861–872, 2003.

[3] L. Lu, M.C. Chan, and E.C. Chang, "A general model of probabilistic packet marking for IP trace-back", in ASIACCS '08, pp: 179–188, 2008.

[4] T. H.-J. Kim, C. Basescu, L. Jia, S. B. Lee, Y.-C. Hu, and A. Perrig, "Lightweight Source Authentication and Path Validation", in SIGCOMM '14, pp: 271–282, 2014.

[5] B. Liu, J. Bi, and V. Vasilakos, "Toward incentivizing anti-spoofing deployment," IEEE Transactions on Information Forensics and Security, vol-9, no.3, pp: 436–450, 2014.

[6] C. Gong and K. Sarac, "Toward a Practical Packet Marking Approach for IP Traceback," International Journal of Network Security, vol. 8, no. 3, pp: 71–84, 2009.

[7] A. Yaar, A. P., and D. Song, "FIT: fast internet traceback," in INFOCOM '05, 2005, pp: 1395–1406.

[8] H. Lee, M. Kwon, G. Hasker, and A. Perrig, "BASE: An incrementally deployable mechanism for viable ip spoofing prevention," in ASIACCS '07, 2007, pp: 20–31.

[9] A. Belenky and N. Ansari, “On Deterministic Packet Marking,” Computer Networks, vol. 51, no. 10, pp: 2677–2700, 2007.

[10] Y. Xiang, W. Zhou, and M. Guo, “Flexible Deterministic Packet Marking: An IP Traceback System to Find the Real Source of Attacks,” IEEE Trans. on Parallel and Distributed Systems, vol. 20, no. 4, pp: 567–580, 2009.

[11] D. X. Song and A. Perrig, “Advanced and authenticated marking schemes for IP traceback,” in INFOCOM ’01, 2001, pp: 878–886.

[12] T. Peng, C. Leckie, and K. Ramamohanarao, “Adjusted probabilistic packet marking for IP traceback,” in NETWORKING 2002, 2002, pp: 697–708.

.