ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 3, Issue 2, pp: (67-71), Month: October 2016 – March 2017, Available at: www.paperpublications.org

Detecting Adversaries in IP Traceback Using Novel Acceleration Mechanism

E. B. Ebilin Dani[1], S. Jesintha Starvin[2]

[1]PG Student, Department of CSE, Ponjesly College of Engineering, Nagercoil
[2]Assistant Professor, Department of IT, Ponjesly College of Engineering, Nagercoil

Abstract: **One of the solutions for attributing cyber attack is the IP Traceback, which is used for accounting user traffic and network diagnosis. The existing approaches used for IP Traceback are Marking based approach, Logging based approach and Hybrid approach. While using probabilistic packet marking in IP Traceback, it is difficult to identify the origin of a single packet. To overcome the difficulties in the existing system, Opportunistic Piggyback marking technique has been proposed. Opportunistic Piggyback marking is one of the novel traceback acceleration mechanisms for IP Traceback. The main idea of this technique is to exploit free ride opportunities for expedited and robust delivery of traceback message fragments to end hosts. In this technique, the nodes have to be created and connected each other. Then the marking field allocation is used to browse the message which is to be sent from source to destination. Message fragment delivery selects the smaller bit messages for delivery because the higher bit messages take more time for delivery. The source and destination nodes need to be selected in traceback message triggering to transfer the message. This traceback message triggering can also be used to reconstruct the network path. While sending the message from source to destination, the traffic may occur in any of the path. The Opportunistic piggyback marking technique can be used to identify the traffic. The traffic is identified in the respective path and then the message is send back to the destination. When compared to the existing system, the proposed system reduced the traceback completion delay and router processing overhead, and also increases the message delivery ratio.**

Keywords: **IP Traceback, Opportunistic Piggyback Marking, Marking based traceback, Deterministic packet marking, Probabilistic packet marking, Traceback triggering.**

I. INTRODUCTION

Network Security is protection of the access to files and directories in a computer network against hacking, misuse and unauthorized changes to the system. An example of network security is an anti virus system. It guarantees the availability of resources. It is handled by a network administrator or system administrator.

Networks can be private, like a network within a company, or public. For securing the network, every user is given a unique user ID and password to access data pertaining to them. Without this authentication, no user is permitted to access the network. The network administrator oversees the operations of the network. Network Security applications includes:

- Authentication Application (Kerberos): Kerberos is a trusted third-party authentication protocol that enables clients and servers to establish authenticated communication.

- Web Security Standards (SSL/TLS): SSL provides security services between TCP and applications that use TCP. TLS is the Internet standard version. SSL/TLS provides confidentiality using symmetric encryption and message integrity using a MAC. SSL/TLS enables two TCP users to determine the security mechanisms and services they will use.

- Email Security: Email Security refers to the collective measures used to secure the access and content of an email account or service. It allows an individual or organization to protect the overall access to one or more email addresses or accounts.

- IP Security: IP Security is a protocol suite for secure Internet Protocol communications that works by authenticating and encrypting each IP packet of a communication session. IP security can be used in protecting data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

The network administrator oversees the operations of the network. The advantages of network security involves protect data, prevent cyber attack, levels of access, centrally controlled and centralized updates. Some of the threats in network security are as follows:

- Viruses: Computer programs written by programmers and designed to replicate themselves and infect computers when triggered by a specific event.

- Trojan horse programs: Delivery vehicles for destructive code, which appear to be harmless or useful software programs such as games.

- Vandals: Software applications or applets that cause destruction

- Attacks: Includes reconnaissance attacks, access attacks and denial-of-service attacks.

- Data interception: Involves eavesdropping on communications or altering data packets being transmitted.

- Social engineering: Obtaining confidential network security information through nontechnical means, such as posing as a technical support person and asking for people's passwords.

Network security is a real boon to the users to ensure the security of their data. While it has many advantages, it has lesser disadvantages. Some of the disadvantages are costly setup, time consuming, requires skilled staff and careless admin. IP Traceback is a solution to identify the source of attack packets and the path followed by these attack packets. The IP traceback technique has been motivated by adversarial applications and also they can be used for non-adversarial applications, such as traffic accounting, fault diagnosis, network problem identification and path validation.

Marking based traceback (MBT) approach has been used. The idea behind this MBT is that the routers convey their traceback message to the end-hosts by marking on passing packets. Then an end-host construct a graph of network paths traversed by these marked packets inspite of source IP address spoofing. There are two key issues in MBT. The first issue is to traceback decision making at individual routers, which means, a router receives a packet and it makes a decision whether to send a traceback message to the end-host or not. The second issue is the message content encoding, that determines the information a router marks in the IP header.

II. RELATED WORK

IP Traceback in the existing system has been classified into three categories such as Marking-based approach, Logging-based approach and hybrid approach.

A. Marking-based Approach:

In marking-based approach, routers embed identity information in the IP headers of passing packets to convey network path information to an end-host. Marking-based traceback methods can be divided into Deterministic Packet Marking (DPM) [10] and Probabilistic Packet Marking (PPM) [8]. DPM embeds the first access border router’s identity information on packets in a deterministic manner, while PPM probabilistically augments packets with partial path information as they traverse in the network. The goal of DPM is to locate the attack source, and the main purpose of PPM is to identify the attack path. Deterministic marking incurs less computational overhead to trace back to the attack source at the end-host side, it lacks incremental deployment property since it assumes that ingress routers are always traceback enabled. It may overload the ingress routers by marking each passing packet compared with the probability based measure. More recently, Marking On Demand (MOD) scheme is proposed based on the DPM mechanism to dynamically distribute router IDs in both temporal and space dimensions. Belenky et al. [3] proposed to store the source address in the marking fields of passing packets. To reduce the number of marked packets, [1] presented a flow-level deterministic marking method for traceback. PPM based approaches are able to reconstruct the attack path only after receiving sufficient marked packets at the end-host.

B. Logging-based Approach;

Logging-based approach [9] involves the storing of packet digests at intermediate routers on the path toward end-hosts, achieving single packet traceback. A topology-aware single packet IP traceback system was presented for logging-based approach. The main disadvantage of logging-based traceback is that large storage space is required for packet logs. To reduce the storage requirements for logging, Lee et al. [7] proposed flow digesting on routers instead of logging individual packets.

C. Hybrid Approach:

Hybrid approach [2] takes advantages of both packet marking and logging to reduce the number of marked packets when conducting the traceback process and improve the high storage overhead at routers. The hybrid approach proposed two hybrid traceback schemes, Distributed Link-List Traceback (DLLT) and Probabilistic Pipelined Packet Marking (PPPM), to reduce the number of packets needed for constructing attack paths in PPM through utilizing packet logging. In DLLT, if a router decides to mark a packet, it first stores the marking information which was written by the previous marking router, and then marks the packet by overwriting the marking field with its IP address. A link list is therefore established to guide the marking information collection from the end-host. PPPM is a logging-assisted marking scheme, which loads traceback messages into packets going to the same destination of these traceback messages.Gong et al. [5] presented a hybrid solution called HIT, which reduces the storage overhead at routers to one half and could track a single IP packet. The basic idea is to recursively mark the accumulated information of multiple routers on packets, and log these accumulated path information at some of the routers on the path.

III. PROPOSED SYSTEM

To overcome the drawbacks in the existing system, the Opportunistic Piggyback Marking has been proposed. The OPM is one of the novel traceback acceleration mechanisms for IP traceback. The main idea of OPM is to exploit free ride opportunities for expedited and robust delivery of traceback message fragments to end hosts. Here first the nodes are created and connected each other. Then for sending the packet, the source and the destination are selected and the packet which is to be sent from source to destination is also been selected. While sending the packet the attack node is found and the 16-bit marking value is generated. Using the marking value, the original message is identified. When the router receives the reconstruction request, it tries to find the attack packet’s upstream router. Then it checks whether the packet came from an upstream router. The requested router then restores the marking field. The path is reconstructed and the packet is sent back to the destination.

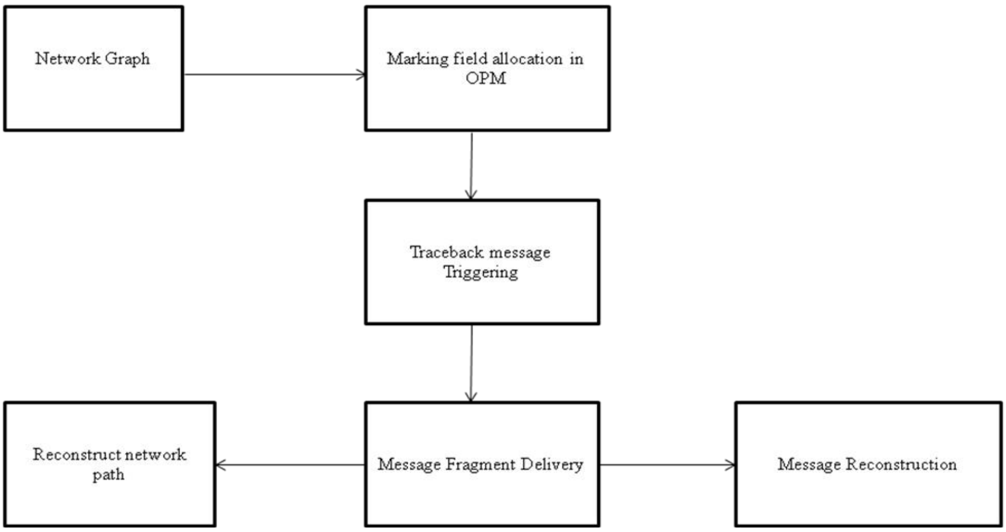
Network Graph
Marking field allocation in OPM
Traceback message Triggering
Reconstruct network path
Message Fragment Delivery
Message Reconstruction

Fig.1 Architecture of OPM

A. *Marking Field Allocation in OPM:*

In marking field allocation the nodes are created and connected each other. The IP header provides K bits for the purpose of traceback marking. To ensure correct reassembling of message fragments and identification of a network path at end-hosts, the control information is necessary in all MBT methods with message fragmentation. In other words, OPM does not introduce extra control information overhead. The source and destination nodes are selected. The packet which is to be send from source to destination are selected and sent. The file size and file name is shown. The file size should be below 117 bytes. While sending the packet, the attack node appears. Assume that a traceback-enabled router R captures a packet P and decides to send its message M_r to the destination of P. Router R first generates a random number as the associative identifier of M_r, then breaks the M_r message into N message fragments and stores them in its local buffer. These message fragments will be delivered to the destination of P through packet marking. This process is repeated until all message fragments have been transmitted to the destination. The attack node is found using the hash value of the IP address.

B. *Traceback Message Triggering:*

The traceback objective is to let the end-host reconstruct the network path. All traceback-enabled routers along the path will be involved in the trace-back procedure. It verifies the path in which packet has been send. Then the spoofer node is identified and the destination node has been shown. After the traceback message triggering process, traceback messages are generated at routers on the routing path. The packet's marking field is used to censor attack traffic on its upstream routers. Extra packets are needed to trace the origin of attack packets. Packet marking approaches are introduced to mark the router or path information on the triggering packets. Then it randomly chooses a segment and the digest to mark on its passing packets. When the destination host receives enough packets, it can use the digest to assemble the different segments. As the packet reaches its destination, the destination source send acknowledgement to the sender that the packet has reached to it and it may send the next packet and if packet somehow lost before reaching to the destination source. It send request for path reconstruction. The marking value for each node in the respective path will be generated. Using the marking value, the original message will be identified.

C. *Path Reconstruction:*

After the traceback message triggering process, traceback messages are generated at routers on the routing path that P traverses. When a traceback-enabled router receives an unmarked packet, it checks whether this packet can carry any message fragment in the buffer to its intended destination by comparing their respective destinations. If yes, the router marks P with the first matched message fragment. When the end-host receives a marked packet, it will extract the message fragment from the received packet before sending it to upper layers for further processing. Given a collection of message fragments associated with a specific TTS received at the end-host, the message reconstruction is based on a combinatorial process. The end-host first classifies all received traceback message fragments according to their capture identifiers. Then, it groups the message fragments with the same message identifiers in the right order based on the fragment offset. Finally, the end-host recovers all the traceback messages, where the topological order of routers can be derived based on the relative hop distance value.The path reconstruction receives the request from traceback message triggering. As soon as the request has been received, it tries to find the attack packet's upstream router. Then it checks whether the packet came from an upstream router. The requested router then restores the marking field. The destination node collects the message fragments from each node. Finally, the path reconstruction method detects the attacker and reconstructs the path.

IV. CONCLUSION

The Opportunistic Piggyback Marking has been proposed in this project. This OPM is a novel traceback acceleration mechanism for IP traceback. The main idea of OPM is to utilize free ride opportunities and robust delivery of traceback message fragment to end-host. When designing a trigger-based IP traceback approach, it supports the traceback of individual packets. The advantages of the OPM are it reduces the traceback completion delay and it increases the message delivery ratio. A theoretical analysis of marking-based traceback is provided, and it showed the potential of opportunistic piggyback marking. Also a flexible marking-based traceback framework is presented, which meets several favourable objectives that previous individual traceback schemes failed to satisfy simultaneously. Comprehensive performance comparisons demonstrated the effectiveness and efficiency of the design for IP traceback.The existing System does not uses marking field so the performance is low, but the OPM uses 16-bit marking field so the performance is high. Finally, for future work, 32 bit marking field should be used, which provides higher performance than OPM.

REFERENCES

[1] V. Aghaei-Foroushani and A. Zincir-Heywood, "IP traceback through (authenticated) deterministic flow marking: an empirical evaluation," EURASIP Journal on Information Security, 2013.

[2] B. Al-Duwairi and M. Govindarasu, "Novel hybrid schemes employing packet marking and logging for IP traceback," IEEE Trans. Parallel Distrib. Syst., vol. 17, no. 5, pp. 403–418, 2006.

[3] A. Belenky and N. Ansari, "On deterministic packet marking," Computer Networks, vol. 51, no. 10, pp. 2677–2700, 2007.

[4] Q. Dong, S. Banerjee, M. Adler, and K. Hirata, "Efficient probabilistic packet marking," in ICNP '05, 2005.

[5] C. Gong and K. Sarac, "A more practical approach for single-packet IP traceback using packet logging and marking," IEEE Trans. Parallel Distrib. Syst., vol. 19, no. 10, pp. 1310–1324, 2008.

[6] Long Cheng, Dinil Mon Divakaran, Wee Yong Lim, Vrizlynn L. L. Thing, "Opportunistic Piggyback Marking for IP Traceback", IEEE Transactions on information forensics and security, February 2016.

[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] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical network support for IP traceback," in SIGCOMM '00, 2000, pp. 295–306.

[9] A. 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.

[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. Parallel Distrib. Syst., vol. 20, no. 4, pp. 567–580, 2009.

[11] S. Yu, W. Zhou, S. Guo, and M. Guo, "A dynamical deterministic packet marking scheme for DDoS traceback," in GLOBECOM '13, 2013.

[12] L. Zhang and Y. Guan, "Topo: A topology-aware single packet attack traceback scheme," in Securecomm and Workshops, 2006, pp. 1–10.