Spoofing Attack Detection based on Passive IP Backtrace

Ranjitha J, Divyashree J
PG Scholar, Dept. of CSE
Assistant Professor, Dept. of CSE
SJB Institute of Engineering and Technology,
Bangalore, India

***Abstract*— This paper gives the information about PIB that bypasses the deployment difficulties of IP backtrace techniques and this PIB takes the help of routing protocol that investigates ICMP (Internet Control Message Protocol error messages) that is named path backscatter triggered by spoofing traffic, and tracks the spoofers based on public available information. This causes collection and the statistical results on path backscatter, and it demonstrates the processes and effectiveness of passive IP backtrace and shows the captured locations of spoofers through applying PIB on the routing Protocol of ICMP data set. Passive IP backtrace cannot work in all the spoofing attacks, it may be the most useful mechanism to trace spoofers before an internet level backtrace system has been deployed in real.**

Index Terms*— *CN Management, CN Security, DoS, IP traceback.

I. INTRODUCTION

IP spoofing is nothing but attackers launching attacks with some IP address and has been recognized as a security problem on the Internet for a long time. Using the addresses that are assigned to or not assigned to someone, attackers cannot avoid exposing of their real locations or enhance the effect of attacking or reflection based attacks. Many of notorious attacks rely on internet protocol spoofing including SYN flooding, SMURF, DNS amplification. The domain name space amplifications attacks which are degraded the service of a Top Level Domain (TLD) name server is reported. Even though there has been a popular conventional wisdom that denial of service attacks are launched from botnets and spoofing is no more critical the report of ARBOR on the meeting of NANOG shows significance of spoofing is observed denial of service attacks. Infact, it is captured backtrace messages based on UCSD Network Telescopes, spoofing activities are observed very frequently.

Great importance is off to capture the origins of IP spoofing traffic. The real as long as the locations of spoofers are not disclosed, they can't be further deterred from launching further attacks. Even by approaching the spoofers for example- determining the ASSes or networks that reside in attackers can be located in a smaller area. Filters should be placed closer to the attackers before attacking traffic. It is going to identifying the origins of traffic spoofing this is going to build a reputation system for ASSes, which would be helpful to push the corresponding internet service provider to verify address of internet protocol source.

In normal network flow it says that one user requesting the web page in the web server and that user would request from its internet protocol configuration and this web server would see the request from client and the web server is going to replies the message with its internet protocol config.

In network spoofer traffic says that if one user is not sending any request to the web server with its own internet protocol address but the spoofer performs like the other client is going to request the server for the webpage and this is done as that original user is requesting the webpage but actually spoofer using its own protocol requesting to the webserver for the webpage. And this server replies back to the user. This is about how the normal network and spoofing attack can be done.

II. PREVIOUS WORK

The existing internet protocol backtrace approaches can be classified into five main categories: The packet marking, ICMP backtrace, log in to router, testing the link, overlay and tracing the hybrid. The Packet marking require method to the routers to do the modifying to the header of the packet to contain the information of the router and decision forwarding. The different packet marking methods internet control message protocol backtrace and generates the addition of named path backtrace messages to a collector or the destination.

When the router makes a record on the forwarded packet the attacking path is re-constructed by logging into the router. Testing the link is an approach which uses to determine the upstream of attacker traffic hop-by-hop while the attack is in progress.

Offloading is proposed by Centertrack the suspecting a traffic from edge routers to special tracking routers through an overlay network.

Disadvantages of existing system:

1. Based on the captured backscatter internet control messages from UCSD Network Telescopes, spoofing activities are still frequently observed.
2. To build an IP traceback system on the Internet faces at least two critical challenges. The first one is the cost effective for adopting a traceback mechanism in the routing system. Existing traceback mechanisms are not widely supported by the current commodity routers, or will introduce considerable overhead to the routers (Internet Control Message Protocol (ICMP) packet generation logging, especially in high-performance networks. The second one is the difficult to make Internet service provider (ISP) to collaborate.
3. Since the spoofer could spread over every corner of the world a one internet service provider (ISP) to

deploy its own backtrace system is almost meaningless.

4. However, ISPs, which are commercial entity with the competitive relations, are generally lack of explicit economic incentive to support the clients of the others to trace attacker in their managed ASes.
5. Since the deployed backtrace mechanisms is not cleared with the gains but apparently high overhead to the best knowledge of authors and there has been no deployed Internet-scale IP backtrace system till this time.
6. Inspite there are a lot of IP backtrace mechanisms proposed and a large number of spoofing activities observed and the real locations of spoofers still remain a mystery.

III. PROPOSED FRAMEWORK

To bypass the challenges in deployment named Passive IP Trace back proposal of a novel solution can be done. Routers could fail to forward an IP spoofing packet due to various reasons, example- TTL exceeding. In such cases, the routers it may generate an ICMP error message named path backscatter and send the message to the spoofed IP address. Because the routers could be close to the spoofers of the IP address, the named ICMP path backscatter messages could disclose the spoofers location.

By path backscatter messages ICMP, PIT could exploits to find the location of the spoofers. After locations of the spoofers known, the victim can seek help from the internet service provider to filter out the attacking packets or take any counterattacks.

PIT is mainly useful for the victims in the reflection based spoofing attacks, example, domain name space amplifications attacks. The spoofers location can find directly from the attacking traffic

Advantages of proposed system:

1. In the proposed system this is the first article tells which deeply investigates named path backscatter messages ICMP. These ICMP messages are valuable to help understand spoofing activities. Even though Moore has been exploited the named path backscatter messages which is generated by the targets of spoofing messages to study denial of services, ICMP named path backscatter message which is sent by intermediate devices rather than the targets, have not been used in backtrace.
2. The practical and effective internet protocol traceback solution based on internet control message protocol and it is named as path a backscatter message that means passive IP traceback is proposed. This passive IP traceback that by passes the deployment difficulties of existing IP traceback mechanism and actually is already in force. Even specifying the limitation that path backscatter messages are not generated with stable possibility passive IP traceback can't work in all the attacks but it does work in a number of spoofing activities. At least it could be the most useful traceback mechanism before an asses level traceback system has been deployed in real.
3. Through which applying the passive IP traceback on the ICMP it is named as path backscatter dataset a number of locations of spoofers are captured and presented. Even though this is not a complete list it is the first known list disclosing the locations of spoofers.

Through applying PIT on the path backscatter dataset, a number of locations of spoofers are captured and presented. Though this is not a complete list, it is the first known list disclosing the locations of spoofers.

The fig 1 shows how the 1 sink, 2 router, 1 destination of Passive IP back trace work.

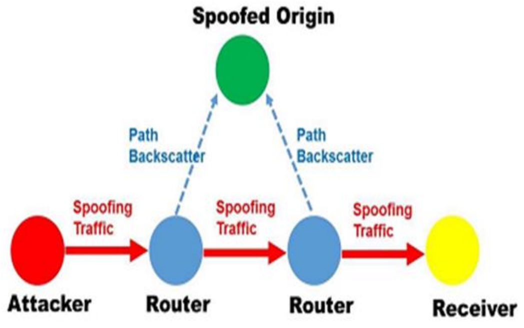

Fig. 1. The scenario of path backscatter generation and collection.

A. Learning and Analysis Phase

This phase includes:

1. The collection of knowledge about the existing communicating techniques.
2. Understanding of the project phase design review from the client.
3. Technologies & programming Language & Learning tools for coding purpose.

B. Design and Implementation

This phase includes:

1. The overall functional view designs that means the system architecture of the project.
2. Explaining the language, platform used in the project applications.
3. Implementing the design modules and the Identification.
4. The different types of services can be controlled and accessed by these applications.

C. Testing Phase

This phase includes:

1. Writing the test cases to test the modules implemented.
2. To do the test cases manually and comparing and evaluating the actual with expected result.

VI. ANALYSIS

Analysis is process of finding the best solution to the problem related. System analysis is which can be learned about the existing problems and it will defines object and system requirement and can evaluate the best solution available. It is one of the ways of thinking about the related organization and problem related a pack of technologies which will helps to solve those problems related. A feasibilities study plays a main role in analysis of a system that shows the target and which helps in design and development.

- *Feasibility Study*

  From results of the investigation of the survey initial done is now can be expand to a many more feasibility studies in detailed. 'Feasibility Study' is a test in proposal of a system and as per its workability, impacts from the organizational and capability to achieve the needs and resource process effective uses.

  Following steps are followed in the feasibility analysis:

1. Appointing a leader and form a team of project
2. Enumerating potentialities of a system proposed.
3. Knowing the characteristics system proposed by defining and identifying it.
4. Calculating and evaluating performances of a system and working out the cost effectiveness of each system proposed.
5. Evaluating the performance of a system and its cost data.
6. Selecting the appropriate system proposed.
7. Preparing the report of final project as per the direction of management.

Following are the keys considered in the feasibility analysis:

1) Economical
2) Technical
3) Social

1) *ECONOMICAL FEASIBILITY*

This is carried out to check the economical work out that the system will impact on the organization. The total cost of fund that the company can invest into research and development team of the system is constraint. The total spending must also be justified. Hence the system which is developed as also within the limited budget and this was accomplished because many of the technologies are available for free of cost. Only need to purchase the customized products.

2) *TECHNICAL FEASIBILITY*

The feasibilities studies is done to check the technical impact, which is, the technical requirements and needs of the system. The developed system must not have a demand on the technical resources available. It will lead to the demand on the technical resources available. This will definitely lead to demand that is been placed on the users. The system which is developed must have a normal requirement because minimum or no changes are needed for implementing the system.

3) *SOCIAL FEASIBILITY*

The matter of study is to check the acceptances level of the system by the customer. This also including the training process that the user to efficiently use the system. The user must not feel any difficulties in the use of the system, instead should accept it as a easy necessity. The degree of acceptance from the users mainly depends on the methods which are involved to educate the consumer about system and to make them familiar to it. their degree of confidence must be increased to that they are also able to make any constructive criticism, which are welcomed, as they are the final user.

V. CONCLUSION

In our work trying to tell how the spoofers works based on investigating the path backscatter messages. The proposed passive internet protocol traceback which is going to track the spoofer based on named path backscatter message. This illustrates causes, collection, and statistical results on path backscatter. In this case specified how to apply PIT when the topology and routing are known or if the routing is unknown or neither of it known. There is an effective routing protocol for applying the PIT in large networks and results are proven with their correctness. The result is demonstrated the effectiveness of PIT based on deduction and simulation and showed how the spoofers may perform and the receiver get to know that he or she is getting the spoofed attack in there window alert message applying PIT on the named path backscatter dataset. These results are helpful in further reveal IP spoofing.

REFERENCES

[1] S. M. Bellovin, "Security problems in the TCP/IP protocol suite," ACM SIGCOMM Comput. Commun. Rev., vol. 19, no. 2, pp. 32–48, Apr. 1989.

[2] ICANN Security and Stability Advisory Committee, "Distributed denial of service (DDOS) attacks," SSAC, Tech. Rep. SSAC Advisory SAC008, Mar. 2006.

[3] C. Labovitz, "Bots, DDoS and ground truth," presented at the 50th NANOG, Oct. 2010.

[4] The UCSD Network Telescope. [Online]. Available: http://www.caida.org/projects/network_telescope/

[5] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical network support for IP traceback," in Proc. Conf. Appl., Technol., Archit., Protocols Comput. Commun. (SIGCOMM), 2000, pp. 295–306.

[6] S. Bellovin. ICMP Traceback Messages. [Online]. Available: http://tools.ietf.org/html/draft-ietf-itrace-04, accessed Feb. 2003.

[7] A.C.Snoeren et al., "Hash-based IP traceback," SIGCOMM Comput. Commun. Rev., vol. 31, no. 4, pp. 3–14, Aug. 2001.

[8] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, "Inferring internet denial-of-service activity," ACM Trans. Comput. Syst., vol. 24, no. 2, pp. 115–139, May 2006. [Online]. Available: http://doi.acm.org/10.1145/1132026.1132027

[9] M. T. Goodrich, "Efficient packet marking for large-scale IP traceback," inProc. 9th ACM Conf. Comput. Commun. Secur. (CCS), 2002, pp. 117–126.

[10] D. X. Song and A. Perrig, "Advanced and authenticated marking schemes for IP traceback," inProc. IEEE 20th Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM), vol. 2. Apr. 2001, pp. 878–886.

[11] A. Yaar, A. Perrig, and D. Song, "FIT: Fast internet traceback," in Proc. IEEE 24th Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM), vol. 2. Mar. 2005, pp. 1395–1406.

[12] J. Liu, Z.-J. Lee, and Y.-C. Chung, “Dynamic probabilistic packet marking for efficient IP traceback,”Comput. Netw., vol. 51, no. 3, pp. 866–882, 2007.

[13] K. Park and H. Lee, “On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack,” inProc. IEEE 20th Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM), vol. 1. Apr. 2001, pp. 338–347.

[14] M. Adler, “Trade-offs in probabilistic packet marking for IP traceback,” J. ACM, vol. 52, no. 2, pp. 217–244, Mar. 2005.

[15] A. Belenky and N. Ansari, “IP traceback with deterministic packet marking,”IEEE Commun. Lett., vol. 7, no. 4, pp. 162–164, Apr. 2003.

[16] 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.

[17] R. P. Laufer et al., “Towards stateless single-packet IP traceback,” in Proc. 32nd IEEE Conf. Local Comput. Netw. (LCN), Oct. 2007, pp. 548–555. [Online]. Available: http://dx.doi.org/10.1109/ LCN.2007.160

[18] M. D. D. Moreira, R. P. Laufer, N. C. Fernandes, andO. C. M. B. Duarte, “A stateless traceback technique for identifying the origin of attacks from a single packet,” in Proc. IEEE Int. Conf. Commun. (ICC), Jun. 2011, pp. 1–6.

[19] A. Mankin, D. Massey, C.-L. Wu, S. F. Wu, and L. Zhang, “On design and evaluation of ‘intention-driven’ ICMP traceback,” inProc. 10th Int. Conf. Comput. Commun. Netw., Oct. 2001, pp. 159–165.

[20] H. C. J. Lee, V. L. L. Thing, Y. Xu, and M. Ma, “ICMP traceback with cumulative path, an efficient solution for IP traceback,” inInformation and Communications Security. Berlin, Germany: Springer-Verlag, 2003, pp. 124–135.

[21] H. Burch and B. Cheswick, “Tracing anonymous packets to their approximate source,” inProc. LISA, 2000, pp. 319–327.

[22] R. Stone, “CenterTrack: An IP overlay network for tracking DoS floods,” in Proc. 9th USENIX Secur. Symp., vol. 9. 2000, pp. 199–212.

[23] A. Castelucio, A. Ziviani, and R. M. Salles, “An AS-level overlay network for IP traceback,”IEEE Netw., vol. 23, no. 1, pp. 36–41, Jan. 2009.[Online]. Available: http://dx.doi.org/10.1109/MNET.2009.4804322

[24] A. Castelucio, A. T. A. Gomes, A. Ziviani, and R. M. Salles, “Intradomain IP traceback using OSPF,”Comput. Commun., vol. 35, no. 5, pp. 554–564, 2012. [Online]. Available: http://www.sciencedirect.com/ science/article/pii/S0140366410003804

[25] J. Li, M. Sung, J. Xu, and L. Li, “Large-scale IP traceback in high-speed internet: Practical techniques and theoretical foundation,” inProc. IEEE Symp. Secur. Privacy, May 2004, pp. 115–129.

[26] 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, May 2006.

[27] M.-H. Yang and M.-C. Yang, “Riht: A novel hybrid IP traceback scheme,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 789–797, Apr. 2012.

[28] 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, Oct. 2008.

[29] R. Beverly, A. Berger, Y. Hyun, and K. Claffy, “Understanding the efficacy of deployed internet source address validation filtering,” in Proc. 9th ACM SIGCOMM Conf. Internet Meas. Conf. (IMC), 2009, pp. 356–369.

[30] G. Yao, J. Bi, and Z. Zhou, “Passive IP traceback: Capturing the origin of anonymous traffic through network telescopes,” inProc. ACM SIGCOMM Conf. (SIGCOMM), 2010, pp. 413–414. [Online]. Available: http://doi.acm.org/10.1145/1851182.1851237