Scintilla of Pollution Attacks by using Entropy Variations

K.Anusha#1, Ramesh Jonnalagadda #2

#1 Student, QIS College Of Engineering Technology, Ongole, Prakasam(dt)

#2 Assoc. professor, QIS College Of Engineering Technology, Ongole, Prakasam(dt)

#1 anusha1264@gmail.com, #2 rameshmtech512@gmail.com,

Abstract: Denial-of-service (DoS) attacks pose an increasing threat to today's Internet. It is important to protect the resource and trace from the Distributed Denial of Service (DDoS) attack, but it is difficult to distinguish normal traffic and DDoS attack traffic because the DDoS generally hide their identities/origins. Especially the attackers often use incorrect or spoofed source IP address, so tracing the source of the denial of service is hardest in internet. In this paper, we implement a hop-by-hop IP traceback method that can reliably trace a source of an attack. The main features of our proposed method are the packet feature, which is composed of specific packet information contained in a packet for identification of an unauthorized packet. Most of the existing techniques deal with flood type DoSattacks, there are more attacks using only one or a few IP packets such as attacks exploiting IP fragment or UDP. It is important to be able to trace unauthorized access using single packet. we have implementing a hop-by-hop traceback method Our system performs real-time tracing and exactly identifies the source of the specific packet along the attack path.

I INTRODUCTION

Attack against network resources are common in today's internet dependent world. Attacks are launched for a variety of reasons, including monetary gain, maliciousness, fraud, warfare and to gain an economic advantage. While the Internet as a business infrastructure increases its importance, the number of unauthorized access incidents on the Internet is growing, and such activity tends to cause a great problem.

In a distributed DoS (DDoS) attack, the attacker uses a number of compromised slaves to increase the transmission power and orchestrate a coordinated flooding attack. Highly automated attack tools have been developed where a common ingredient is the use of spoofed source addresses. Particularly, DDoS attacks with hundreds or thousands of compromised hosts, often residing on different networks, may lead to the target system overload and crash. In the DDoS attacks, there might still be a single packets, but the effect of the attacks is multiple by use of attack servers. The attack not only disables that server but denies access to legitimate user.

The access control technologies including firewalls are commonly used to prevent unauthorized access, but some specific way of access cannot be stopped by the access control technologies. As the measure of unauthorized access, it is necessary to pinpoint the source in order to prevent the unauthorized activity. The ability required to perform traceback is "to identify the true IP address of the terminal originating attack packets." If we can identify the true IP address of the attacker's terminal, we can also get information about the organization involved in the attack or the attacking terminal.

Several methods that identify a source of a packet with forged source IP address have been proposed. Although most of the existing techniques deal with flood type DoSattacks, there are more attacks using only one or a few IP packets such as attacks exploiting IP fragment or UDP.

In this paper, we are implementing a hop-by-hop traceback method. In our approach, we keep forwarded packets and MAC address corresponding to their datalink-level identifier in each forwarding unit and identify the adjacent unit by searching for the forwarded packet that corresponds to an attack packet. Beginning with the forwarding unit closest to the sensor that has detected unauthorized access, we identify each adjacent forwarding unit along the attack path, and ultimately reach the source of the attack packet even if a forged source IP address is used.

II REALTED WORK

Controlled Flooding: Burch and Cheswick have developed a link-testing traceback technique that does not require any support from network operators. We call, this technique controlled flooding because it tests links by flooding them with large bursts of traffic and observing how this perturbs traffic from the attacker. Using a pregenerated "map" of internet topology, the victim coerces selected hosts along the upstream route into iteratively flooding each incoming link on the router closest to the victim. Since router buffers are shared, packets traveling across the loaded link including any sent by the attacker have an increased probability of being dropped.

Logging: An approach to log packets at key routers and then use data mining techniques to determine the path that the packets traversed. This scheme has the useful property that it can trace an attack long after the attack has completed. However, it also has obvious drawbacks, including potentially enormous resource requirements (possibly addressed by sampling) and a large scale interprovider database integration problem. We are unaware of any commercial organizations using a fully operational traceback approach based on logging.

Advanced Marking and Authenticated Marking: In this scheme present two new IP marking techniques to solve the IP traceback problem: The Advanced Marking Scheme and the Authenticated Marking Scheme. This approach has the same low network and router overhead as FMS proposed by Savage et al., yet this approach is much more efficient and accurate for the attacker path reconstruction under DDoS. In particular, this approach can reconstruct the attacker path within seconds and has a low false positive rate. Furthermore, this Authenticated Marking Scheme supports efficient authentication of routers' markings.

Algebraic Approach to IP Traceback: This is similar to the technique used by Savage, et al, with the major difference being that this scheme is based on algebraic techniques. This paper reframes the traceback problem as a polynomial reconstruction problem and uses techniques from algebraic coding theory to provide robust methods of transmission and

reconstruction. This has the advantage of providing a scheme that offers more flexibility in design and more powerful techniques that can be used to filter out attacker generated noise and separate multiple paths.

Hash Based IP Traceback: Hash based approach is called as Source Path Isolation Engine (SPIE). In these methods the forwarding path of a single packet can be reconstructed by querying such routers soon after the packet is observed. More recent work (private communication) moves the processing from the router to a specialized machine observing traffic on a link. This method can be viewed as a special case of Remote Monitors. Attacks on SPIE: Attackers can attack the query/response communication, either the traffic or the endpoints. For that reason access to traceback data will normally be restricted to the administrative domain owning the routers and possibly a few other trusted places.

Packet Marking Algorithm: In Packet Marking Algorithm schemes, each router in addition to forwarding a packet also inserts a mark in the packet. This mark is a unique identifier corresponding to this particular router. As a result the victim can determine all the intermediate hops for each packet by observing the inserted marks. There are two variants to this marking scheme. First is the Deterministic Packet Marking (DPM) scheme in

which each router marks all the packets passing through it with its unique identifier. This scheme is thus similar to the IP record-route option. This makes the reconstruction of the attack path at the victim trivial. But the downside to this scheme is that routers are slowed down as they have to perform additional functionality. Attacks on DPM: An attacker who controls a trusted router can forge any path up to that router unless some further authentication scheme is used. A router that trusts data from an attacker effectively allows that attacker to act like a compromised router. Authentication methods could be used, but these add significant cost in the form of processing time and space in the marked packets.

III PACKET FEATURES

Our traceback method uses a packet feature as a parameter for Trace Request and Trace Order. In order to uniquely identify the individual packet, we extract several fields of the IP packet that are not altered by tracers and create a packet feature. The extracted fields are as follows:

- Version
- Header Length
- Identification
- Protocol
- Source and Destination IP addresses
- A part of IP data

If we create a packet feature consisting of only IP header fields, identical packets may exist. Therefore, in order to improve the precision of packet identification, we decide to include a part of IP data field (maximum 20 bytes).

IV TRACEBACK MODEL

Our traceback model consists of sensor, manager, tracer.

(1)Sensor

This component has two functions. One is to detect unauthorized access from the network (the same function as existing IDSs have) and another is to request a manager to start tracing.

(2)Tracer

This component implements a function to maintain information about forwarded IP packets as well as a function to trace the source of the forwarded packet along the attack path on forwarding unit.

(3)Manager

In response to a request from a sensor, this component controls traceback tasks. We cannot trace a packet beyond our own network perimeter if neighboring networks impose different policy. Therefore, we consolidate managers in a specific policy controlled network perimeter and install an overall manager (”monitoring manager”) for each perimeter. Using the monitoring manager, we can give orders for tracing to the different policy-controlled networks and receive the results from them. We select the single manager model that enables us to control and monitor tracing tasks between network perimeters that impose different policy.

The basic functions of the traceback model define the following tasks:

(1) A trace request from a sensor and a notice of the

tracing result to the sensor

(2) A trace order from a monitoring manager to a tracer and a notice of the processing result to the monitoring manager

(3) A trace request and a notice of the tracing result exchanged between monitoring managers

If a sensor detects unauthorized access, the sensor notifies the monitoring manager of detection.

At this time, unauthorized access's information (packet feature) is notified to the manager as follows:

Step 1: The pursuit of unauthorized access's source starts by this notification (Trace Request).

Step 2: The monitoring manager sends the unauthorized access's information to a tracer with which the sensor is connected, and inquires to the tracer from which tracer the unauthorized access came (Trace Order).

Step 3: The tracer analyzes this information, specifies the tracer by which the unauthorized access came, and returns information on the tracer by which the unauthorized access came (Notification of Processing Result).

Step 4: The monitoring manager decides the next tracer from information returned from the tracer, and puts out the inquiry to the next tracer. This procedure is continued to the tracer with which unauthorized access's source is connected.

Step 5: The tracer with which unauthorized access's source are connected returns source's information to the monitoring manager, when unauthorized access information from the monitoring manager and source's information is corresponding.

Step 6: The monitoring manager ends the pursuit, and notifies source's information to the sensor (Notification of Tracing Result).

VIMPLEMENTATION

In our traceback method, Sensor detects unauthorized activity, then asks for tracing the source and receives the result. Tracer actually traces packets from the victim site to the source of the packets along the attack path. In order to utilize existing forwarding unit, we append the tracing functions to forwarding unit. Monitoring manager orders tracers to start tracing in response to requests from sensor. Additionally, it orders upstream tracer to start tracing. When the source of a packet is identified, monitoring manager returns the result to the sensor. It also monitors the status of tracing tasks based on the status information sent from tracers.

While tracing two major functions are implemented. They are: Packet Conversion and Store process and Trace and Search process.

Packet Conversion and Store process: After routing process, Packet Conversion and Store process gets a packet to forward and creates a record containing the address of the upstream unit (MAC address) and a packet feature extracted from the packet. This record is stored into Packet Information Area in the tracer. Every incoming packet is processed through this procedure.

Trace and Search process: Trace and Search process perform: Packet Searching and Upstream Network Interface Decision. Packet Search accepts Trace Order and searches for the specified packet feature from Packet Information Area. If a record matching with the trace packet is found, Upstream Network Interface Decision decides the upstream network interface and notices this trace result to the monitoring manager using Notification of Processing Result.

VI CONCLUSION

In this paper, we proposed an effective and efficient IP traceback scheme against DDoS attacks. Our traceback system can pursue the source even if an IP address is forged, and have demonstrated the effectiveness of the traceback processing. The main features of our proposed method are the packet feature, which is composed of specific packet information contained in a packet for identification of an unauthorized packet. Proposed method is to identify matching packets and identify the sources under DDOS attack where identical packets are sent from different sources. In our approach, we keep forwarded packets and MAC address corresponding to their datalink-level identifier in each forwarding unit and identify the adjacent unit by searching for the forwarded packet that corresponds to an attack packet.

VII REFERENCES

[1] S.Taketsume, S.Matsuda, H.Watanabe, M.Yanagida, and K.Kokubo. "A Study of Architecture for Unauthorized Access Tracing System," in Proceedings of the 60th National Convention of IPSJ(Japanese only), vol. 3:287–288,
March 2000.

[2] D.X.Song and A.Perrig. "Advanced and Authenticated Marking Schemes for IP Traceback," Technical Report, University of California at Berkeley, (UCB/CSD-00-1107), June 2000.

[3] R.Stone. "CenterTrack: An IP Overlay Network
for Tracking DoSFloods," in Proceedings of the 9th USENIX Security Symposium, pages 199–212, August 2000.

[4] M.Ikeda, S.Tanaka, A.Hayakawa, and S.Matsuda.
"A Study of architecture for unauthorized access tracing system," in Proceedings of the 62nd National Convention of IPSJ(Japanese only), vol.3:285–286, March 2001.

[5] K.Park and H.Lee. "On the Effectiveness of Probabilistic Packet Marking for IP Traceback under
Denial of Service Attack," Technical Report, Purdue University, (CSD-TR 00-013), June 2000.

[6] K.Ohta, G.Mansfield, Y.Takei, and Y.Nemoto. "Detection, defense, and tracking of Internet wide illegal access in distributed manner," in Proceedings of INET 2000, July 2000. http://www.isoc.org/ inet2000/cdproceedings/1f/1f .htm.

[7] H.Y.Chang, R.Narayan, B.Vetter S.F.Wu, M.Brown, X.Wang, J.Yuill, C.Sargor, F.Gong, and F.Jou. "DecIdUouS: Decentralized Source Identification for Network-Based Intrusions," in Proceedings of the 6th IFIP/IEEE International Symposium on Integrated Network Management, pages 701–714, May 1999.

[8] H.Watanabe, T.Baba, S.Taketsume, and S.Matsuda. "A Study of packet identifier for unauthorized access tracing system," in Proceedings of the 60th National Convention of IPSJ(Japanese only), vol.3:289–290, March 2000.

[9] S.Savege, D.Wetherall, A.Karlin, and T.Anderson. "Practical Network Support for IP Traceback," in Proceedings of the 2000 ACM SIGCOMM Conference, 30(4):295–306, August 2000.

[10] K.Kokubo, H.Watanabe, S.Matsuda, et al. "A
study of unauthorized access tracing system," in Proceedings of the 60th National Convention of IPSJ(Japanese only), vol. 3:283–284, March 2000.