제20회 한국정보처리학회 추계학술발표대회 논문집 제10권 제2호 (2003. 11)

트래픽 제어 기법을 이용한 라우터에서의 서비스 거부 공격 방어 기법

이호균 O, 김정녀
한국전자통신연구원 보안운영체제연구팀
e-mail : {hglee O, jnkim, }@etri.re.kr

Methods of Defense DoS Attack by Traffic Metering and Controlling Technique in a Router

Ho Gyun Lee O, Jeong Nyeo Kim
ETRI Secure OS Research Team

Abstract

As the Distributed Denial of Service attack technique is getting smarter, defense method have been developed by various means. Existing defense method baseds on detection technique is not effective to DDoS attack. Because it depend on rule set that is used to detect attack and DDoS attack pattern has become very similar to real traffic pattern. So the rule set is not efficient method to find DDoS attack. To solve this problem, DDoS defense mechanism based on QoS technique has been suggested. In this paper, we summarize existing DDoS defense mechanism and focus on method based on QoS, and introduce a new DDoS defense framework.

1. Introduction

Jan.25th, 2003 and Nov.2nd 1988 are very meaningful days for the computer security managers, especially, network security managers. The former is the day which not only specialists, but also the general public came to recognize what DoS attack was, what destructive power DoS attack had. The latter is the day which Internet worm, the father of DoS attack, spread out in the network, and did real damage to the network in the USA[1]. With this as a momentum, the governmental agency and the academic world started to study Internet information warfare. DoS (Denial of Service) attack means that excessive service is demanded to several resources which are necessary for computer to handle normal operation, cash, memory, buffer which are essential for the network bandwidth and TCP/IP stack management. Service cannot be done by DoS attack.

Because the early DoS attack was not very precise, and sent ICMP messages such as Ping repeatedly, it was possible for the security system based on detection to confront against the DoS attack. However, as the DoS attack gets more precise, it is impossible to classify attack packets with common packets. To solve this problem, Traffic Sensing-based countermeasure gets more spotlight than detection-based countermeasure. Traffic Sensing-based countermeasure uses existing network technique that guarantees service quality contrary to the method that stores the existing attack patterns and then prepares these to all packets in the network. QoS (Quality of Service, also called diffserv) technique has two core techniques in connection with traffic measurement and traffic control[6][7]. Traffic Sensing-based countermeasure observes the traffic change to Layer 4 using the traffic measurement function. Therefore, it senses abnormal change of traffic, and uses traffic control function to confront this.

2. Existing countermeasures and traffic sensing-based countermeasures

There are three defense-methods to defend attacks in the DDoS mechanism, attack protection method that can be done before starting attack, attack detection and filtering method that can be done in the middle of attack, attacker position tracing method that can be done in the middle of attack and after attack[2]. These methods should be combined properly for perfect defense of DDoS.

2.1 Attack protection method

There are two protection methods. The passive method is to stop attack Master and Agent from installing in the host. The active method is to intercept the attack scenario process

between Master and Agent by developing cyber spy program. To use protection methods, a lot of knowledge about DDoS attack mechanism is required[8].

2.2 Attacker position tracing method

Position tracing method cannot protect the attack itself, but can be used in apply of tracing the criminals and collection of legal evidences about attack. There are two position-tracing methods. The first method is to write information about all packets that passed routers to trace later position in the router. The second method is for router to transmit other information packets such as ICMP to destination host of packets[9][10].

2.3 Attack detection and filtering method

Attack detection reports attack packets and flows that belong to the packets to network managers, and filtering function abolishes or controls attack packets according to the order of network managers or automatic policy. At this time FNR (False Negative Ratio) and FPR (False Positive Ratio) unit are used to measure the effectiveness of detection function, and NPSR (Normal Packet Survival Ratio) is used to measure effectiveness of filtering function[2]. NPSR is a drawback of DDoS mitigation method using traffic sensing method, so the improvement for this is one of the major projects.

2.4 Traffic Sensing-based countermeasures

DDoS attack mitigation method detecting change of the traffic belongs to the protection method and detection method at the same time of the three defense methods. The reason is that Traffic Sensing-based countermeasure observes the information of traffic change using the traffic measurement function of QoS method, detects the outbreak of attack and at the same time, prevents the host from stopping service previously using traffic control function. However, it is hard to say that Traffic Sensing-based countermeasure has high quality if considering FNR, FPR as estimation standard because this method is to analogize by change of the entire traffic, not to check by pattern information of the traffic. Likewise, NPSR is not high because traffic isn't controlled by accurate judgment that a packet is an attack packet or not. Nevertheless, this method is an excellent countermeasure comparing of detection-based countermeasure because it has a merit of performance and it can give a service without stopping. In addition, detection-based countermeasure is in a defenseless state against new attack that is not known before, but Traffic Sensing-based countermeasure can confront regardless of attack pattern because it analogizes with traffic measurement information. Therefore, the most important project is to decide the sense result to increase FNR, FPR, NPSR, and to set a new standard for traffic classification to discriminate attack packets.

The method that Aman Garg from Texas A&M University suggested is similar to existing IDS system in view of development method of system. The core of Dos attack defense is the system located in the ingress router, called a fortress host[5]. The difference from IDS is that IDS let the manager know the traffic inflow same as known attack pattern using packet check and waits confronting order, on the other hand, fortress host observes if the resource consumption of inflowing traffic exceeds critical mass or not managing all hosts of subnet network, the resource critical mass information of network bandwidth as a table. To do this, fortress host is applying to traffic meter function, the core factor of Diffserv, traffic control function and window-based control method to control resources in the host. The merit of this method is that any modification to hosts inside the subnet that should be protected is not necessary. The policy for control, management, and measurement of traffic happens in the fortress host only; the terminal server may not know the fact that a new policy is applied. However, fortress host should know exactly the resource capacity of terminal system and consumed resource quantity by the packets, flow, and traffic class that each has a different level to perform well. To solve this, Aman Garg focuses the fact about resources only, and doesn't consider discrimination of flow. So he classifies traffic class, presumes and confronts that each traffic class consumes what kind of resources. Figure 1 shows application of this idea.

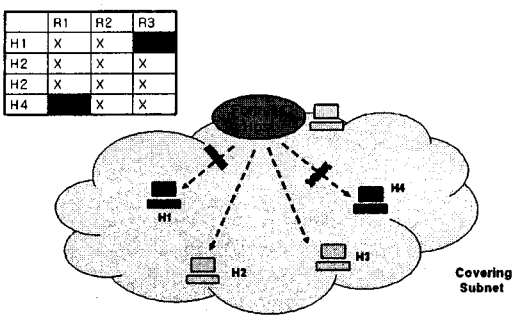

Fig 1. Fortress Host technique that suggeested by Aman Garg

3. NGSS and SRS

NGSS (Network Generation Security System) is an abbreviation of Network Integrated Infringement System. NGSS is the system to provide next generation network security service to customer site. This is located in the access network such as public network or ISP network and protects for the traffic passing the access network. NGSS consists of SMS that does security management function, SGS and SRS that do security node function, and Interface providing reciprocal action among them. SMS system provides security service of network in charge of NGSS system and supports all functions for efficient security management. SGS (Security Gateway System) is the security node for detecting an intrusion and confronting in the large network environment. SRS is the router added security functions. Security functions include packet filtering, intrusion-detection, trusted-channel, user-certification, access-control, and audit trace, traffic-metering and security management. This paper brings to a focus on security functions of SRS in the NGSS system, especially, DDoS attack defense by traffic metering. Figure 2 shows network structure between SMS and SRS in the NGSS network.

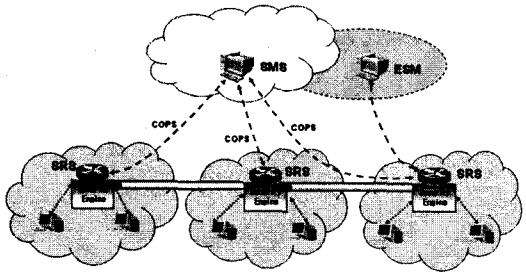

Fig 2. The Relationship of SMS and SRS in the NGSS system

SRS is based on common use routers, builds up security function on those, and is classified with three engines. The bottom part is a network-engine, which needs management of unit of packets, and it may use exclusive hardware for improvement of performance. There are traffic meter function, packet sensor/filter function, and trusted-channel function in this part. The part that is on the network-engine is security-engine, which belongs to network interface or functions that are not dependent on specific hardware. There are user-certification, access-control, policy-application, intrusion-detection and audit/log function in this part. The part that is on the security-engine is service engine, which includes instructions library, certification-interface, alert-management, confrontation-management, policy-management, node-management and key-management interface function.

4. Traffic sensing-based countermeasure mechanism of SRS

I will describe DDoS attack defense function by traffic sensing of the various functions of NGSS in this section. As mentioned in previous section, NGSS consists of three nodes according to charge range and major functions. The following is the classification of the roles of each node about traffic sensing function of the various functions provided by NGSS.

• SMS : determine confrontation policy by receiving and analyzing traffic statistical information from SRS and SGS. Traffic analyzing functions are divide to real-time and no real-time. Real-time function is the function that maintains normal traffic profiles, compares these to current traffic and distributes immediate confrontation policy in case of inflow of abnormal traffic and forecasting service-incapable state among each node. No real-time function is the function that sets up long-term analysis and confrontation by analyzing traffic change history data and confrontation policy history. All data analysis range of SMS is the whole network that lower nodes are arranged. So the trace of attack traffic movement is possible as long as the lower nodes are arranged.

• SGS : is a exclusive gateway for security function not carrying out network function like routers. This is located before and after the network equipment, and checks out security of all traffic inflowing to the network. This collects statistical information by traffic flow unit, reports it to SMS, and sets up self-confrontation policy on the basis of reporting statistical information. Contrary to SMS, it is impossible for SGS to analyze overall the network, but it is possible for SGS to analyze traffic change of its own link. So self-confrontation against abnormal traffic outbreak situation happening on link is possible. Because this is exclusive security equipment not providing network service like routers, wider range service (or high-speed service) is possible comparing to SRS, and this provides security analysis better than SRS (, worse than SMS).

• SRS : is router adding security function to access network level router. Because this carries out security function and routing function of Giga-bps level, simultaneously. This cannot provide high-quality security analysis function to reduce the load of routing function. Therefore, DDoS attack defense function using traffic sensing focuses on traffic statistic information reporting function and confrontation function using policy generated by SMS. The same as SGS, this can trace traffic change only happening in its own link, not the whole network. It is impossible for SRS to analyze high-quality traffic like relevance analysis, but immediate automatic confrontation against obvious abnormal situation is possible by tracing traffic volume change classified by application.

4.1 Traffic Sensing functions of SRS

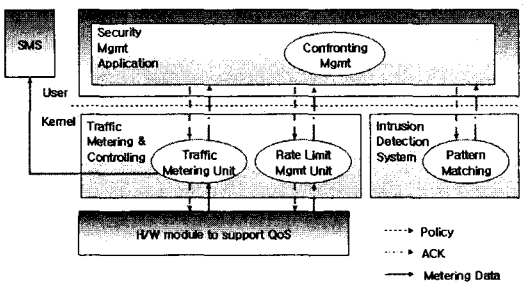

Fig 3. Confront Mechanism based on Traffic Sensing of SRS

Traffic Sensing functions are classified three things.

1. Traffic statistic information reporting function

SRS transmits traffic statistic information periodically for Upper class SMS to analyze to traffic flow unit. Transmitting protocol follows Netflow format for compatibility with existing network equipment. Timing control function is provided to control conflict requirements properly to improve accuracy of information collection for SMS and to reduce the load at existing network function service of SRS.

2. Traffic control function (confrontation function)

This uses traffic control function of Diffserv as the function to remove or control flows that SMS judges it is an attack. Existing Diffserv-traffic control functions classify traffic using TOS field value of IPv4 protocol, and control traffic using various queuing theories. SRS modifies existing mechanism to classify traffic with 5-tuple criterions, not TOS field. 5-tuple are Source IP, Destination IP, Source port,

Destination port, and protocol type.

3. Automatic confrontation decision function

SRS carries out traffic control function according to confrontation policy of SMS and blocks inflow of relevant traffic automatically in case of inflow of obvious abnormal traffic that can make service incapable state of SRS itself or the subnet network under SRS. This is similar to the idea of Aman Garg that was introduced in the chapter 2, but this classifies each traffic, and traces volume change of each classified traffic not tracing resources consumption change of all subnet host like idea of Aman Garg. This is to minimize the load at existing service of router adding traffic sensing function. Traffic classification methods standardize 3-tuple only, not 5-tuple that has Netflow format reporting to SMS. 3-tuple includes protocol type, Source port, and Destination port. SRS maintains traffic classification table, which manages dynamically 3-tuple items in a hash table. Besides, each 3-tuple item is updated according to the time set by timer-control, which doesn't exceed 5 minutes. This time should be within the time that SRS and relevant subnet can be service incapable state.

4.2 Problems of confrontation according to volume change of classified traffic

Attack confrontation policies on the basis of traffic sensing have some drawbacks.

1. In case of SRS, if confrontation policies are applied by classified traffic, the attacker who knows the mechanism can use SRS as equipment that interrupts service. For example, if the cracker who knows that A bank uses 8484 port as an exclusive service port let attack packets inflow to 8484 port on purpose, SRS that detects increasing of abnormal packet inflow to 8484 port prevents using of 8484 port, automatically. This may stop the overall internet service incapable state, but this causes 8484 port incapable state, which was the cracker's purpose.

- There are two solutions for these. The two solutions need pattern matching function of IDS.

• Service acceptance method about normal packets : service is accepted to the packets for bank service use only by pattern matching check of the packets that were flowed into 8484 port. To do this, it should be guaranteed that crackers couldn't forge packets for bank service use. The difficulty of this method is that supporting services that are not officially registered in the authorized group like IETF is difficult because knowing all the protocol that uses 8484 port is difficult.

• Service denial method about abnormal packets : if the attack packets flowing into the 8484 port have uniform pattern, only the attack packets can be eliminated using existing detection countermeasure. This has a merit that the design of this method is easier than service acceptance method, but this has a drawback that the discrimination between normal packets and attack packets is hard if the attack packets generated by crackers are smarter.

To solve this problem, SRS adds IDS engine on the basis of snort using the network processor. By adding detection function of IDS, faster and more precise security engine can be made because precise attack packets classification by only the traffic sensing method is difficult.

2. When SRS is cracked, Cracker controls traffic freely. SRS carries out traffic control function according to policy of SMS to confront against DoS attack. If someone cracks policy grammar of SMS and the transporting protocol, SRS can be the system that makes network service incapable state, not the system that prevents attacks. Therefore, security of SRS itself and security of communication lines of SRS are essential. To solve this problem, SRS include access control function inside the system. And trusted-channel is used to transmit policies in order to guarantee security of communication lines of SRS.

5. Conclusion

I summarized DDoS attack mechanism and tendency, described countermeasures that had been studied so far in this paper and introduced DDoS attack mitigation function by traffic sensing of the NGSS, SRS system and SRS system functions. NGSS is being developed by setting a goal of construction of network integrated infringement confrontation system including attack protection, tracing, detection and countermeasures that are three defense methods against DDoS attack.

Reference

[1] Lars Klander, " Hacker Proof : The Ultimate Guide to Network Security", Delmar Learning, Jan. 1997

[2] Rocky K.C. Chang, "Defending against Flooding-based Distributed Denial-of-Service Attack : A Tutorial", IEEE Communication Magazine, Oct. 2002

[3] Dai Kashiwa, "Active Shaping : A Countermeasure against DDoS Attck", ECUMN 2002 Conference Proceedings, Calmar, France

[4] Haining Wang "Layer-4 Service Differentiation and Resource Isolation", Proceedings of IEEE RTAS'2002, Sep. 2002

[5] Aman Garg, "Mitigating Denial of Service Attack Using QoS Reguration", Nov. 2001

[6] Y. Bernet et al., "A Framework for Differentiated Services", IETF Internet Draft, Feb. 1999.

[7] S. Blake et al., "An Architecture for Differentiated Services", RFC 2475, Dec. 1998.

[8] S.Gilson, "The Strange Tale of the Denial of Service Attack Against GRC.COM," http://grc.com/dos/grcdos.htm, Mar. 2002

[9] A. Snoeren et al., "Hash-Based IP Traceback," Proc. ACM SIGCOMM, Aug. 2001, pp. 3–14.

[10] S. Savage et al., "Practical Network Support for IP Traceback," Proc. ACM SIGCOMM, Aug. 2000, pp. 295–308.