D-WARD, DDoS and Three Network Administrative Domains

Hang Chau

1. Introduction

DoS/DDoS attacks are a virulent, relatively new type of Internet attacks, they have caused some biggest web sites on the world -- owned by the most famous E-Commerce companies such as Yahoo, eBay, Amazon -- became inaccessible to customers, partners, and users, the financial losses are very huge.

For defensing against the DDoS attacks, the network engineers have made many attempts to design the systems that help identify the machines of lunching DDoS attacks and stop the malicious attacks. The systems are deployed at three administrative network domains: victim network, intermediate network and source network. In this paper, I will take an overview for the three administrative domains; compare and analyze the potential abilities of the systems for detecting and defensing the DDoS attacks, when the systems are deployed on each kind of the administrative network domain.

It is easy to understand that the DDoS attacks should be stopped as close as possible the source of the attacks, that will save the network resources and reduce the traffic congestion, so I also discuss the D-WARD, or **D**DoS Net**w**ork **A**ttack **R**ecognition and **D**efense, it is an important DDoS defense system deployed at the source network.

2. Defense Systems on Three Network Administrative Domains

2.1 Victim Network

Historically, most of the systems detecting and defensing the DDoS attacks are deployed on the destination/victim network, because the victims have the greatest incentive to deploy the systems. The systems at the victim network facilitate easy detection for the DDoS attacks and possible characterizations of the DDoS attack signatures. However, compare to the systems deployed at the intermediate network and the source network, the systems deployed at the victim network are ineffective in stopping the attacks because they require the cooperation of upstream routers to push back the attacking flows.

At the victim network, traditionally, much of the works related to detect and defense the DDoS attacks have been carried on the Intrusion Detection System (**IDS**). The IDS detects the DDoS attacks either by using the database of known signatures (such as the Cisco Secure IDS Signatures watching for the DDoS attacks: 6501 TFN Client – 6508 mstream Control Traffic, see [4]), or by recognizing anomalies in system behavior. But, most of these systems do not take automated action to stop the attacks, they just raise an alert to the system administrator.

Currently, there are several kinds of the mechanisms detecting and defensing the DDoS attacks at the victim network:

1. In the on-off control approach, a router located at the victim of a DDoS attack detects the attack by monitoring the router's buffer queue size. Once the queue size grows over a specified threshold, the router reacts by switching to a different mode of operation and throttling the incoming traffic. Only the packets which identified as a certain problematic type of traffic are dropped. When the queue size is reduced, the throttling is stopped. Under the reasonable volume of attack packets, this approach efficiently protects the victim from overflowing its buffers by early detection of DDoS attacks, and does not completely cut off the traffic from the source network.

2. The analysis of TCP/IP packet streams through the network, which could be beneficial to fighting the intrusion attacks. This idea is implemented in **EMERALD** (**E**vent **M**onitoring **E**nabling **R**esponses to **A**nomalous **L**ive **D**isturbances, see [1] and [2]). EMERALD "represents a state-of-the art in research and development of systems and components for anomaly and misuse detection in computer system and networks", and developed at **SRI** (**S**tanford **R**esearch **I**nstitute). EMERALD combines a signature-based approach to the Intrusion Detection System (IDS) with the statistical analysis for anomaly detection.

3. Cisco routers have the built-in features (such as debug logging and IP accounting), which can be used for characterizing and tracing the common DDoS attacks. An access list can be configured to log [5] many network events. The feature only gathers statistical data and offers no automated analysis or response.

All the mechanisms above increase a victim's ability to recognize early the destination of a DDoS attack, thus gain more time to respond. This ability would be useful for defensing the DDoS attacks that aim to degrade only the victim's services rather than denying the services completely. However, most of the DDoS attacks aim at crippling the victim completely by exhausting its resources, the attack's effect is so excessive and differs so greatly from normal behavior that the detection on the victim network becomes trivial. Therefore, at the victim network, most of the proposed mechanisms for defending the DDoS attacks attempt to characterize the attack traffic and install the filtering rules in the upstream routers. In some cases, the mechanisms/systems can successfully relieve the attack's effect. However, the mechanisms/systems will fail in following situations:

1. The offending traffic has the same characteristics with the legitimate traffic.

2. The amount of the offending traffic is so great that the filtering mechanism in the upstream router cannot handle the traffic.

2.2 Intermediate Network

Defensing against the DDoS attacks at the intermediate network is obviously more effective than at the victim network, because large volumes of the DDoS attacks can be handled easily on the intermediate network, and the attacks can be cooperatively traced back to the sources of the DDoS attacks. But, there are several problems that prevent from deploying the defense systems at the intermediate network:

1. Performance: usually, the intermediate network handles large traffic volumes. Defensing against the DDoS attacks on the intermediate network requires additional resource for traffic profiling and rate limiting, it will degrade the network's performance, and might in turn degrade the Internet service as a whole.

2. Detection: for an intermediate network, it usually does not feel any effect of the DDoS attacks, so it is hard to detect the DDoS attacks and identify the victim. Thus, most proposed mechanisms/systems at the intermediate network rely on the signals from the victim to trigger the response. The victim must be authenticated to assure that the attackers cannot misuse the proposed systems at the intermediate network, which adds the cost. Also, it is often the victim is damaged so severely by the DDoS attacks that the victim cannot send back the signals to the intermediate network.

3. Lack of the inter-domain cooperation: on most of current network architecture, there are very little cooperation between the different administrative domains such as the victim network and the intermediate network. Adding the cooperation service(s) will require a large restructuring of inter-domain relations.

4. Deployment: all proposed systems defensing against the DDoS attacks rely on the cooperation among participants. If there are non-participating domains, or the participants are not adjacent, then the performance of entire the network will degrade rapidly.

There are several mechanisms to defense against the DDoS attacks at the intermediate network:

1. Algorithm WATCHERS [3], it detects the misbehaving routers which lunch the DDoS attacks by absorbing, discarding or misrouting packets. WATCHERS uses the conservation of flow principle to examine flows between the neighbors and endpoints. WATCHERS cannot detect packets with forged source addresses. Even worse, such packets could be used by the attackers to misidentify a target as a bad router. WATCHERS can only detect the compromised routers, it is helpless against misbehaving hosts and is not a feasible solution for large networks.

2. Trace-back mechanisms: they can locate the attacking nodes, and provide the information about the identity of the attacking machines, but they do not stop the DDoS attacks. The tracking technology becomes ineffective when the volume of attack traffic is small or the attacks are distributed, and is also susceptible to the attempts lunching by the attackers to deceive the tracking.

3. Filtering mechanisms: they can prevent spoofing of the source address in IP packets. Eliminating IP spoofing would facilitate easy distinction of normal flows from attack flows, and would help greatly to identify the attacking machines. Although the IP spoofing is not necessary for the DDoS attacks, yet the IP spoofing helps the attackers to hide the identity of attacking machines so the attackers can reuse them for future attacks. However, with highly distributed attack sources, the information about the identity of the attack machines still does not prevent an efficient attack.

4. To augment routers with the ability to detect and control the flows that create congestion, the flows are frequently the signs of the DDoS attacks. This approach offers a powerful tool, the tool not only combats DDoS attacks, but also locates and removes the network congestion caused by any other reason. However, it requires significant augmentation of the routers on the whole path from the victim to the sources. If there is a single legacy router on the path from the victim to the sources, then the legacy router will complicate the scheme and imposes the need for secure communication of non-adjacent routers, which makes the system vulnerable to the DDoS attacks. The approach also requires the cooperation of different administrative domains.

2.3 Source Network

It is easy to understand that the DDoS attacks should be stopped as close as possible the source of attacks. If we deploy the systems defending the DDoS attacks at the source network side, it will greatly save the network resources and reduce the congestion.

The attacks appear different at the source network from at the victim network. At the victim network, all DDoS flows converge and affect the victim greatly so that the detection is inevitable; at the source network, the flows are still dispersed and appear as a set of perfectly valid transactions. It is usually the sheer amount of the transactions that saturates the victim network.

Deploying the systems defending DDoS attacks at the source network side of the attacks has many advantages over deploying the systems further downstream to the intermediate network or the victim network:

1. The attack flows can be stopped before they transfer to the Internet core part and before they aggregate with other attack flows, the two flows achieve together the power to create network congestion and exhaust resources.

2. Being close to the sources can facilitate easier trace back and investigation of the DDoS attacks.

3. Due to the low degree of flow aggregation, more complicate detection strategies can be deployed to achieve higher accuracy.

But, as with an intermediate network, the source network is hard to detect the occurrence of the DDoS attacks, because it does not experience any difficulties for passing the attack flows on it. For detecting the attacks becomes better, a source network can sacrifice some of its resources and performance (the source network doesn't need to sacrifice too much, because it does not handle such large volumes of traffic as does on an intermediate network or victim network).

3. D-WARD

3.1 Introduction

D-WARD, or **D**DoS Net**w**ork **A**ttack **R**ecognition and **D**efense, is a very important DDoS defense system deployed at the source router network (either LAN or border router).

Due to the similarity of the DDoS attacks and the legitimate traffics, it is unwise to take any defensive action based on per-packet observations. D-WARD takes most of its decisions based on flow and connection monitoring over time (a connection is defined as the aggregate traffic, a flow is consisted of one or more connections), rather than establishing the legitimacy of individual packets. D-WARD observes the traffic flows outgoing from and incoming to the source network, and gathers lightweight statistics on the flows, classified by destination. These statistics, along with built-in traffic models, define the legitimate traffic patterns. Any discrepancy between the observed traffic and the legitimate traffic pattern for a given destination/victim is considered to be the signal of the potential DDoS attacks. After the source router obtains the signal, it decides to throttle all the traffic to the suspected destination/victim of the attacks; at the same time it attempts to separate the attacking flows from the legitimate flows and identify the attacking machines. This approach has the benefit of preventing malicious flows from entering the network and consuming resources.
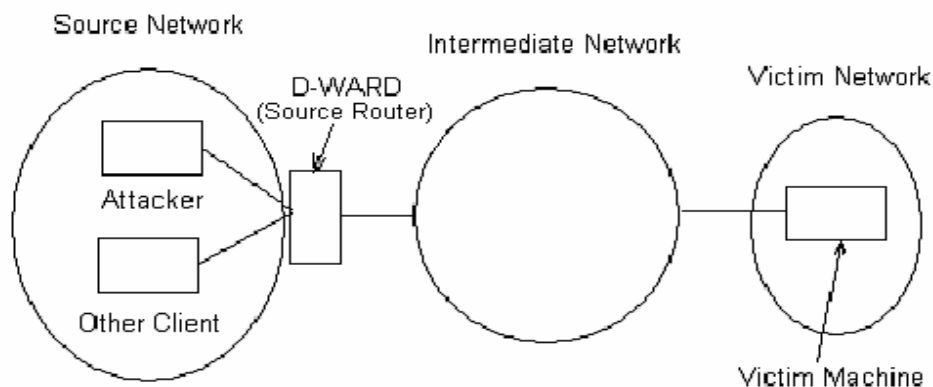

Figure 1

See the Figure 1, the D-WARD system is installed at the source router, the source router serves as a gateway between the source network and the rest part of the Internet. There are four kinds of the deployments for the D-WARD system:

1. In the basic deployment, the source router is considered as the only connection point between the source network and the rest part of the Internet. Thus, the D-WARD can observe every packet transferred between the source network and rest part of the Internet.
2. In another scenario, there are many gateway routers on the source network border, but each gateway is a default exit and entry for a set of the foreign addresses. A D-WARD system can be deployed at each gateway and observe every packet exchanged between the source network and the set of the foreign addresses signed to that D-WARD system.
3. Some gateway routers host the D-WARD systems, and partially police the source network's outgoing traffic only to certain destinations/victims.
4. Multiple gateway routers exist and there is **asymmetric** routing of incoming and outgoing packets (an outgoing packet to the destination X may traverse a different gateway than an incoming packet from the source Y) is unfavorable for D-WARD system since it cannot form complete traffic observations.

D-WARD is configured with a set of local addresses, or D-WARD's police address set. The set of addresses identifies all machines in the stub network or all customers of an Internet Service Provider (ISP). D-WARD observes total traffic between its police address set and the rest of the Internet. A flow is defined as the aggregate traffic between the police address set and one foreign host (such as one foreign IP address; the "foreign" means the outside the source network).

3.2 Architecture of D-WARD

D-WARD is a self-regulating reverse-feedback system, it is consisted of by three components, see the Figure 2:

1. Observation Component: it can be part of a self-contained unit that interacts with the source router to obtain the traffic statistics.

2. Rate-Limiting Component: it can be part of a self-contained unit that interacts with the source router to install the Rate-Limiting Rules.

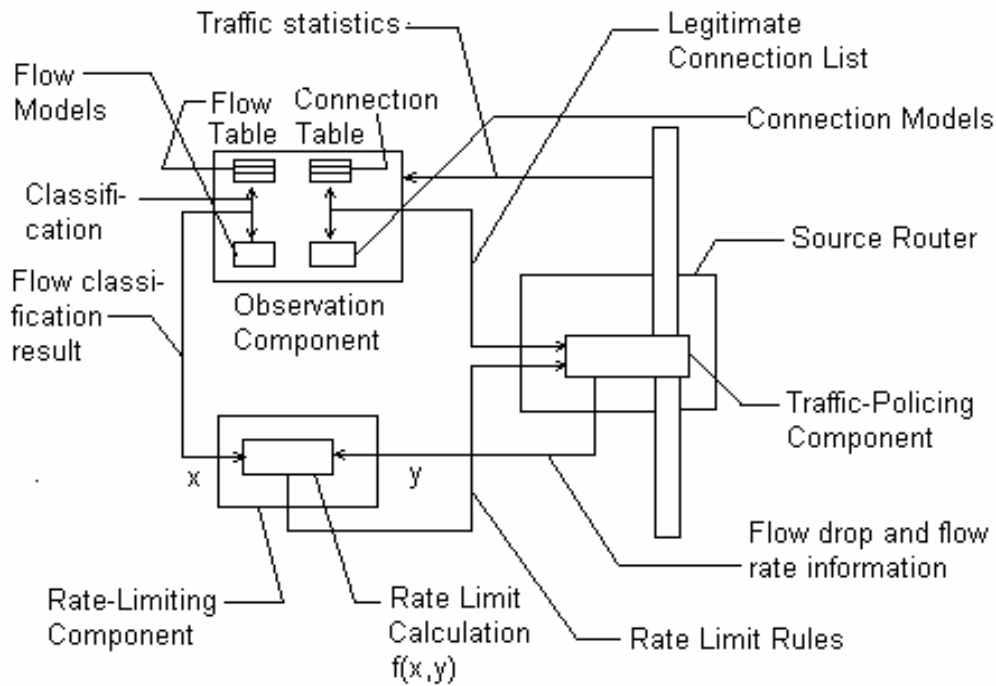3. Traffic-Policing Component: it must be part of the source router.

Figure 2

3.2.1 Observation Component

The Observation Component monitors all packets passing through the source router and gathers statistics on the two-way communications between the police address set and the rest of the Internet, and records the flow and connection granularity. This monitoring can be performed by sniffing the traffic at the interface of the source router. Periodically, the statistics are compared to the Flow Models and the Connection Models of the legitimate traffic (see the Figure 2), and the flows and connections are classified. The classification results are passed to the Rate-Limiting Component, which adjusts the Rate Limit Rules. Both the Legitimate Connection List (which comes out the Observation Component) and the Rate Limit Rules (which comes out the Rate-Limiting Component) are communicated to the Traffic-Policing Component (a part of the source router), which then enforces the rate limits and ensures forwarding of legitimate packets. The imposed rate limits modify the associated traffic flows and thus affect future observations, and close the feedback loop.

In the Observation Component, the flow statistics are stored in the Flow Table, and the connection statistics are stored in the Connection Tables, see the Figure 2. The spoofed attacks may generate a large number of records in two kinds of the tables, the sizes of the tables are limited to avoid excessive memory consumption. The Observation Component cleans the tables by two methods:

1. Periodically expels all records that are stale;

2. When the tables overflow, expels those records that are deemed less useful than others.

The Observation Component also periodically classifies the flows and connections. The flow classification is used to detect the occurrences of the **DDoS attacks**; the connection classification is used to identify the legitimate connections that should receive good service, in case the associated flow becomes rate-limited. The advantage of this approach is that the Connection Table is already populated when the DDoS attacks occur. D-WARD uses the approach to provide continued good service to connections, and the systems suffer no damage by the DDoS attacks.

The connection above is performed continuously. But, if D-WARD uses the on-demand (un-continued) approach, a delay would exist between the detection signals of the DDoS attacks and the populating of the Connection Table, the legitimate connection traffic would be damaged by the DDoS attacks.

3.2.2 Rate-Limiting Component

The Rate-Limiting Component adjusts rate limit values on every Flow Observation Interval, it receives classification results from the Observation Component and flow behavior history from the Traffic-Policing Component, and devises a rate-limit value for each active flow.

The flow behavior history is expressed by two metrics:

1. B-sent, the byte amount of the flow traffic forwarded to the victim;
2. B-dropped, the byte amount of the flow traffic dropped due to rate limiting.

Both values are measured with the Flow Observation Interval.

A measure of how well a flow complies to the imposed rate limit – Flow Compliance Factor (FCF) – is calculated as:

$$FCF = \text{B-send} / (\text{B-send} + \text{B-dropped})$$

FCF values range from 0 (if B-send=0) to 1 (if B-dropped=0 and B-send is not equal to zero). The higher FCF values means the better compliance with the imposed rate limit.

3.2.3 Traffic-Policing Component

See the Figure 2, the Traffic-Policing Component periodically receives:

1. The rate-limited flow information (the Rate Limit Rules) from the Rate-Limiting Component (every Flow Observation Interval);

2. The connection classification information (the Legitimate Connection List) from the Observation Component (every Connection Observation Interval).

The Traffic-Policing Component uses the information to make the decision whether to forward or drop every outgoing packet in the following list of manners:

1. If the packet belongs to a <u>non-limited</u> flow, forward it, else

2. If the packet belongs to a <u>good</u> connection, forward it, else

3. If the packet is the <u>TCP</u>, and its sequence number matches the predicated value and the Early Packet Rate Limit for the flow is <u>not exhausted</u>, forward it, else

4. If the flow rate limit <u>not exhausted</u>, forward it, else

5. Otherwise, <u>drop</u> the packet.

Notes

[1] http://www.sdl.sri.com/projects/emerald/
System Design Laboratory, Projects: Intrusion Detection

[2] http://www-106.ibm.com/developerworks/webservices/library/co-emrld.html
IBM: EMERALD's component-based approach to network security

[3] See: http://research.microsoft.com/users/tuomaura/Publications/hughes-aura-bishop-ssp00.pdf
WATCHERS is a distributed network monitoring protocol designed to detect and isolate these malicious routers which discards or misroutes packets that pass through the routers.
See: http://citeseer.ist.psu.edu/bradley97detecting.html
WATCHERS is based on the principle of conservation of #ow in a network: all data bytes sent into a node, and not destined for that node, are expected to exit the node.

[4] Cisco Secure IDS Signatures watching for the DDoS attacks are:
      6501 TFN Client
      6502 TFN Server Reply
      6503 Stacheldraht Client Request
      6504 Stacheldraht Server Reply
      6505 Trinoo Client Request
      6506 Trinoo Server Reply
      6507 TFN2K Control Traffic
      6508 mstream Control Traffic

[5] log: the process of recording everything pertinent to a machine run; or a collection of messages.

Reference

http://www.lasr.cs.ucla.edu/ddos/
D-WARD: DDoS Network Attack Recognition and Defense

http://staff.washington.edu/dittrich/misc/ddos/
Book on DDoS

http://staff.washington.edu/dittrich/security.html
General Computer Security

http://www.sciencedaily.com/print.php?url=/releases/2002/09/020924072621.htm
Proposed Computer Defense System Could Protect Networks From Becoming Launch pads
For Crippling Internet Attacks

http://www.lasr.cs.ucla.edu/ddos/dward-thesis.pdf
D-WARD: Source-End Defense Against Distributed Denial-of-Service Attacks, Jelena
Mirkovic, University of California, Los Angeles, 2003.

http://www.lasr.cs.ucla.edu/ddos/prospectus.pdf
D-WARD: DDoS Network Attack Recognition and Defense, Ph.D. Dissertation Prospectus,
2002.

Network Security Principles and Practices, author: Saadat Malik, Cisco Press, 2003, ISBN:
1-58705-025-0.

Cisco Secure Intrusion Detection System, Author: Earl Carter; Issued: October
2001; Publisher: Cisco Press, 1st edition; ISBN: 158705034X.

Hang Chau
Senior Network/System Administrator, Ming Plaza Development
hcdanny@yahoo.com
28925 Clear Spring Lane, Highland, CA 92346, U.S.A.
M.S. on Computer Science, California State University.
CCIE, CCNP, CCNA (Cisco/CCIE: passed the Qualification Exam);
SCSA, SCNA (Sun/Solaris: Certified System and Network Administrators);
SCJP, SCWCD (Sun/Java: Certified Programmer and Web Component Developer);
MCSE, MCSA.
Also research on Network Attacks and Network Security:
Cisco IDS/Secure PIX (Intrusion Detection Systems and Firewall);
D-WARD, DoS/DDoS (Denial of Service/Distributed Denial of Service);
Mydoom/Doomjuice Worms and DoS/DDoS attacks.