A New and Comprehensive Taxonomy of DDoS Attacks and Defense Mechanism

ABBASS ASOSHEH, NAGHMEH RAMEZANI
Information Technology Department
Tarbiat Modares University
Jalal Ale Ahmad, PO BOX: 14115-111
Tehran-IRAN

Abstract: Distributed denial of services (DDoS) is the most important security problem for IT managers. These attacks are very simple organized for intruders and hence so disruptive. Moreover, its serious damage has been increased, the detection and defense of this attack has specific importance among network specialists. A new taxonomy of DDoS attack and defense mechanism has been proposed in this paper. It comprises all types of attacks and provides a comprehensive point of view for DDoS attacks. We introduce a useful tool that can be employed to a sophisticated selection defense method for DDoS attacks. The comprehensive defense classification will help to find the best strategy to overcome the DDoS attack.

Key-Words: DDoS attack, Defense mechanism, Taxonomy, Prediction, Detection and Defense

1 Introduction

DDoS is a relatively simple, very powerful technique to attack Internet resources and services. It is a coordinated attack on the availability of services of a given target system or network that is launched indirectly through many compromised computing systems. The services under attack called primary victim, while the compromised systems used to launch the attack are often called the secondary victims. The use of secondary victims in a DDoS attack provides the ability to wage a much larger and more disruptive attack while remaining anonymous. The secondary victims actually perform the attack and so make it more difficult to track down the real intruder for network forensics.

It is necessary to understand all aspects of DDoS attacks and deployed defense mechanisms to make an effective defense up. Some classifications have been proposed for DDoS attacks and defense mechanisms. In [1], it classified DDoS in two main branches based on vulnerability: bandwidth depletion and resource depletion attacks. A *bandwidth depletion attack* is designed to flood the victim network with unwanted traffic that prevents legitimate traffic from reaching the primary victim. A *resource depletion attack* is designed to tie up the victim resources to make the system unable to process legitimate service request. Various classification criteria are indicated in bold type: Degree of Automation, Exploited Vulnerability, Attack Rate Dynamics and Impact [2]. The Level of Computerization, attack networks, Oppressed vulnerability, Influence of DDoS attack, attack Intensity dynamics taxonomy have been presented in [3]. A realistic model of DDoS simulation and experimentation has been proposed a formalized and scalable taxonomy in [4]. Some taxonomy for defense mechanisms has been proposed, too. Three categories of DDoS countermeasures introduced in [1]: for the first, preventing the setup of the DDoS attack network, including preventing secondary victims and detecting and neutralizing handlers. Secondly, dealing with a DDoS attack while it is in progress, including detecting or preventing, mitigating or stopping, and deflecting the attack. The post-attack category which involve network forensic discussed for the third. Other defense classification is based on activity level and location [2] and on submissive defense mechanism, active defense mechanism, action and defense deployment position [3].

None of the mentioned DDoS taxonomies are comprehensive. Also the proposed classifica-

tions for defense mechanism are not effective to deploy for suitable defense mechanism selection. In this paper we will introduce a new comprehensive taxonomy for DDoS attack and defense mechanism.

The rest of this paper is organized as follows: the new proposed taxonomy of DDoS will discuss in section 2. In section 3, the taxonomy of defense mechanisms will propose. This paper will be concluded in section 4 and finally provide an overview of future work.

2 New taxonomy for DDoS attacks

Eight features will be deployed in new taxonomy for DDoS attacks. They are as : architecture, degree of automation, impact, vulnerability, attack rate dynamics, scanning strategy, propagation strategy and packet content which will be described in the following in details.

2.1 Architecture base:

Agent-Handler Model: This model consists of attacker, handler, agent and target network. The handlers are software packages located throughout the Internet that the attacker uses to communicate with the agents. The agent software exists in compromised systems that will eventually carry out the attack. The attacker communicates with any number of handlers to identify which agents are up and running, when to schedule attacks, or when to upgrade agents.

IRC-Based Model: This model is similar to the Agent-Handler model except that instead of using a handler program installed on a network server, an IRC (Internet Relay Chat) communication channel is used to connect the client to the agents. According to the communication mechanism has been deployed between agent and handler machines, there are two types of attacks [15].

2.2 Degree of automation base:

Manual: The attacker scanned remote machines for vulnerabilities, broke into them and installed the attack code, and then commanded the onset of the attack.

Semi-Automatic: The intruder deploys automated scripts to investigate and compromise the target machines for installation of the attack code. The handler machines will be employed to specify the attack type, the victim's address and then order the onset of the attack to agents who send packets to the victim. Attacks with direct and indirect communication are different. In direct one, the agent and handler machines need to know each other's identity in order to communicate. This is achieved by hard-coding the IP address of the handler machines in the attack code that is later installed on the agent.

In indirect one, an attacker controls the agents using IRC communications channels. Thus, discovery of a single agent may lead no further than the identification of one or more IRC servers and channel names that used by the DDoS network.

Automatic: Automatic DDoS attacks additionally automate the attack phase to avoid any communication needs between attacker and agent machines. The time of the onset of the attack, attack type, duration and victim's address is preprogrammed in the attack code.

2.3 Impact base:

Disruptive: In this class the entire of the bandwidth will be cutoff and so it is known as disorderly attack.

Degrading: If DDoS attack causes the partial bandwidth consumption, it is said to be degrading attack. It is hard to detect because of slowly cutoff legitimate bandwidth.

2.4 Vulnerability base:

Bandwidth depletion: In this class, attacker sends unwanted traffic to target network. Flood and amplification methods are the well known method in this line. A flood attack involves zombies sending large volumes of traffic to a victim system, to congest the victim system's network bandwidth with IP traffic. The victim system slows down, crashes, or suffers from saturated network bandwidth and preventing access by legitimate users. Flood attacks have been launched using both UDP and ICMP packets. An amplification attack involves the attacker or the zombies sending messages to a broadcast IP address, by that all systems in the subnet receive from the broadcast address and so send a reply to the victim system. Smurf and Fraggle are examples of these attacks.

Resource depletion: In this attack the attacker sends packets which misuse network protocol communications or are malformed. Network resources are tied up so that none are left for legitimate users. In protocol exploit attacks a specific feature or implementation bug of some protocol will be employed at the victim in order to consume excess amounts of its resources. The TCP SYN and PUSH+ACK are examples of these attacks. However, in Malformed Packet

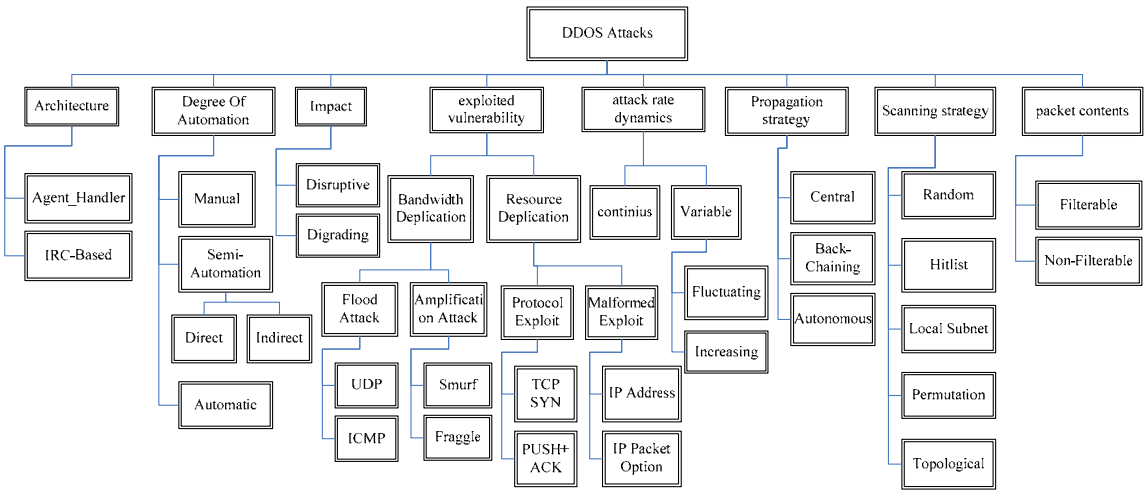

Fig.1: DDoS attacks Classification

Attacks, attacker instructs the zombies to send incorrectly formed packets to the victim system in order to crash it. Examples include malformed IP address and OPTION field in IP packet.

2.5 Attack rate dynamic base:

Continuous: The agent machines after getting the onset order will generate the attack packets with full force. Detection is so simple in this attack.

Variable: Variable rate attacks are more cautious in their engagement. The attack rate will be changed to avoid detection and response. According to the rate change mechanism, there are two types of attacks, increasing and fluctuation. In increasing, attacks have a gradually increasing rate lead to a slow exhaustion of victim's resources. A state change of the victim could be so gradual that its services degrade slowly over a long period time and so delaying detection of the attack. In Fluctuating, attacks have a fluctuating rate adjust the attack rate based on the victim's behavior, occasionally relieving its effect to avoid detection.

2.6 Scanning strategy base:

Random: During random scanning each compromised host probes random addresses in the IP address space. This potentially creates a high traffic volume since many machines probe the same addresses. Code Red (CRv2) used this method [16].

Hitlist: A machine that perform hitlist scanning, probes all addresses from an externally supplied list. When it detects the vulnerable machine, it sends one half of the initial hitlist to the recipient and keeps the other half. This technique allows a great propagation speed and no collisions during the scanning phase.

Topological: Topological scanning uses the information on the compromised host to select new targets. All email worms use this method.

Permutation: During permutation scanning, all compromised machines share a common pseudo-random permutation of the IP address space; each IP address is mapped to an index in this permutation. A machine begins scanning by using the index computed from its IP address as a starting point. Whenever it sees an already infected machine, it chooses a new random start point.

Local Subnet: Local subnet scanning can be added to any of the previously described techniques to preferentially scan for targets that reside on the same subnet as the compromised host that used local subnet scanning.

2.7 Propagation strategy base:

Central: In this method the attack code resides on a central server or set of servers. After compromising the agent machine, the code is downloaded from the central source through a file transfer mechanism. Li0n worm used this central propagation [17].

Back-chaining: In this method the attack code is downloaded from the machine that was used to exploit the system. The infected machine then becomes the source for the next propagation step. Ramen worm used this method [18].

Autonomous: This method avoids the file retrieval step by injecting attack instructions directly into the target host during the exploitation phase. Warhol worm used autonomous method [19].

2.8 Packet content base:

Filterable: Filterable attacks use bogus packets or packets for non-critical services of the victim's operation, and thus it can be filtered by a firewall. Examples of such attacks are a UDP flood attack or an ICMP request flood attack on a Web server.

Non-filterable: Non-filterable attacks use packets that request legitimate services from the victim. Thus, filtering all packets that match the attack signature would lead to an immediate denial of the specified service to both attackers and the legitimate clients. Examples are a HTTP request flood targeting a Web server or a DNS request flood targeting a name server.

3 New taxonomy for DDoS defense mechanism

The proposed taxonomy of defense mechanism is based on human thinking logic to defense. Fig. 2 shows this classification. All defense mechanism has been divided to two categories: prevention and detection. Moreover it must determine where the defense has to be deployed. In the following the new taxonomy for DDoS defense will be described in details.

3.1 Prevention mechanism:

The best option to defend against DDoS attacks is prevention. In this approach researchers try to stop attack in start. Several preventing mechanisms have been proposed [20,21,22]. The prevention can be done in target network or intermediate network.

Target network is one that the attack organized for denial of that. Security mechanisms increase the overall security of the system, guarding against illegitimate accesses to the machine, removing application bugs and updating protocol installations to prevent intrusions and misuse of the system.

The protocol security mechanisms address the problem of bad protocol design. Many protocols contain operations that are cheap for the client but expensive for the server. Classic misuse example is the TCP SYN attack that can increase bandwidth on critical connections to prevent them to go down in an attack.

Load balancing can improve both normal performances as well as mitigate a DDoS attack. Additionally, providers can replicate servers and provide additional failsafe protection if some go down during a DDoS attack. Flow control is another technique proposed to prevent servers from going down. The Max-min Fair server-centric router throttle method sets up routers that access a server with logic to adjust incoming traffic to levels that will be safe for the server to process. Resource multiplication mechanisms provide an abundance of resources to counter DDoS threats. The straightforward example is a system that deploys a pool of servers with a load balancer and installs high bandwidth links between itself and upstream routers. Resource accounting mechanisms restrict the access of each user to resources based on the privileges of the user and his behavior. Such mechanisms guarantee fair service to legitimate well-behaving users [6,7].

Filtering refers to the scanning of IP packet headers leaving a network and checking to see if they meet certain criteria. If the packets pass the criteria, they are routed outside of the sub-network from which they originated. Otherwise, the packets will not be sent. Firewall is important tool in this area. Deflect method serve to pervert attacks from hitting the systems. It protects as well as serves as a means for gaining information about attackers by storing a record of their activity and learning what types of attacks and software tools has been using. Honeypots intentionally set up with limited security to be an enticement approach for an intruder's attack.

One of the best methods to prevent DDoS attacks is to prevent themselves from participating in the attack for the secondary victim systems (intermediate network). This requires a heightened awareness of security issues and prevention techniques from all Internet users. Secondary victims would be prevented from becoming infected with the DDoS agent software; these systems must continually monitor their own security. They should check the system status to make sure that no agent programs have been installed on their systems and also they are not indirectly sending agent traffic into the network. Because of the de-centralized Internet, and different hardware and software platforms variety, it is quite difficult for users to implement the right

protective measures such as anti-Trojan software.

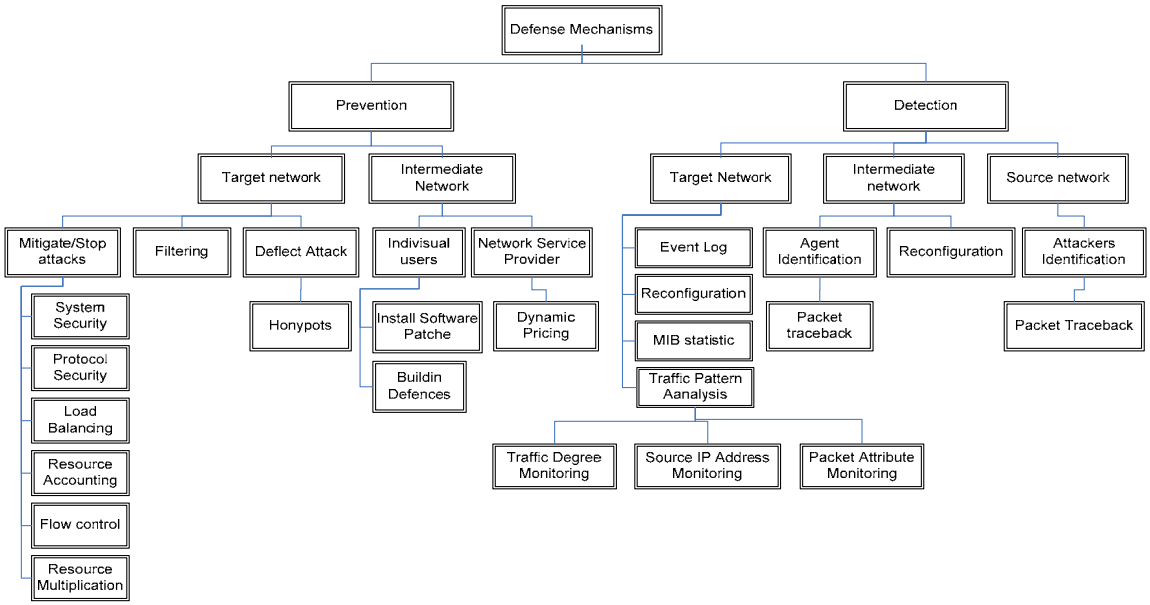

Fig.2: DDoS defense Classification

Network users should have enough resources to afford protective measures and the knowledge of the right protections method selection. End user can provide defense against malicious code insertion through buffer overflow violations by installing software patches and built in mechanisms in the core hardware and software of computing systems. Another strategy is for network service providers and network administrators to add dynamic pricing to network resource usage. If providers choose to charge differently for the use of different resources, they would be better able to identify legitimate users

3.2 Detection and defense:

This approach uses attacks signatures or learning normal behavior of network to detect attacks. Many intrusion detection systems are written based on this approach and used data mining and artificial intelligence techniques. It can be employed to detect attacks in target network or intermediate network.

Target network: the goal is to detect attack in network that attack organized for. With monitoring the traffic degree any traffic pattern changed could be detected and by monitoring the IP address and other field the usage pattern of resources can be detected. Also we are able to defend by using filtering, load balancing and access control. Some attacks scenarios are known. Therefore we can detect attacks by analysis existent log files in systems and severs and comparison the result by known scenarios or normal pattern (event analysis).

MIB information analysis is another method to identify when a DDoS attack is occurring. MIB data includes parameters that indicate different packet and routing statistics. Identifying statistical patterns in different parameters during a DDoS attack looks promising for possibly mapping ICMP, UDP, and TCP packet statistical abnormalities to a specific attack. This approach could provide methods to identify when a DDoS attack is happened and how to adjust network parameters to compensate for the unwanted traffic [5]. Reconfiguration mechanisms change the topology of the target network to either add more resources to the target network.

In intermediate network, the goal is to detect intermediate systems to prevent from participating in the attack.

Agent identification mechanisms provide the victim with information about the identity of the machines that are performing the attack. Agent identification uses trace back techniques [9, 10, 11, 12] that enabling the usage of the source address field for agent identification. Reconfiguration mechanisms change the topology of the intermediate network to isolate the attack machines.

Source network mechanism has been used to detect and defend against attackers [13, 23]. Attacker's identification uses trace back

techniques to find attacker by source address of IP packet.

4 Conclusions

Exact recognition of DDoS attacks and choose the proper strategy in defense against these attacks is so important. Therefore, in this paper in a comprehensive research on the DDoS attacks and ways to deal with them, is given a general classification of DDoS attacks and the ways to deal with them. The introduced taxonomy of DDoS attack is a comprehensive one which involved the whole features of a DDoS attack. The classification which is given in this paper for the defense mechanism is so useful in the selection of a proper strategy in defense against DDoS attacks.

5 Future work:

One of the important tasks which can be done in the following is to give a way for clustering DDoS attacks. For this purpose it's necessary to identify the features of DDoS attacks and perform the clustering on the basis of it. Then label to each cluster, the way to deal with them, till the appearance of a new DDoS attack, recognize its level in order to select a proper way to deal with it.

References:

[1] Specht, S. M. and R. B. Lee., *Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures*. Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems 2004 International Workshop on Security in Parallel and Distributed Systems: 543-550, 2004.

[2] Mirkovic, J., J. Martin, et al., *A Taxonomy of DDoS Attacks and DDoS Defence Mechanisms*. Los Angeles, Computer Science Department, University of California, 2002.

[3] Tariq, U., M. Hang, et al., *A Comprehensive Categorization of DDoS Attack and DDoS Defense Techniques.,* ADMA2006 LNAI 4093: pp. 1025-1036, 2006.

[4] Kang, j., Y. Zhang, et al., *A Formalized Taxonomy of DDoS Attacks based on Similarity*., ISI 2006 3975: pp. 717-719, 2006.

[5] Joao B. D. Cabrera, Lundy Lewis, Xinzhou Qin, Wenke Lee, Ravi K. Prasanth, B. Ravichandran, and Ramon K. Mehra,*Proactive Detection of Distributed Denial of Service Attacks Using MIB Traffic Variables – A Feasibility Study*, Integrated Network Management Proceedings, pp. 609-622, 2001.

[6] A. Juels and J. Brainard, *Client puzzles: A cryptographic countermeasure against connection depletion attacks*, In Proceedings of the 1999 Networks and distributed system security symposium (NDSS'99), Mar 1999.

[7] F. Lau, S. H. Rubin, M. H. Smith, and Lj. Trajkovic, *Distributed denial of service attacks*, In Proceedings of 2000 IEEE International Conference on Systems, Man, and Cybernetics, October 2000.

[8] A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, S. T. Kent, W. T. Strayer, *Hash-Based IP Traceback*, In Proceedings of ACM SIGCOMM 2001 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, August 2001.

[9] D. X. Song and A. Perrig, *Advanced and authenticated marking schemes for IP Traceback*, IEEE Infocom, 2001.

[10] D. Dean, M. Franklin and A. Stubblefield, *An algebraic approach to IP Traceback*, In Proceedings of the 2001 Network and Distributed System Security Symposium, February 2001.

[11] S. M. Bellovin, *ICMP traceback messages, Internet draft*, http://search.ietf.org/internet-rafts/draft-ietf-itrace-01.txt, Oct. 2001.

[12] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, *Practical network support for IP Traceback*, In Proceedings of 2000 ACM SIGCOMM Conference, Aug. 2000.

[13] T. M. Gil and M. Poleto, *MULTOPS: a data-structure for bandwidth attack detection*, In Proceedings of 10th Usenix Security Symposium, August 2001.

[14] D. G. Andersen, H. Balakrishnan, M. F. Kaashoek, R. Morris, *Resilient Overlay Networks*,In Proceedings of 18th ACM SOSP, October 2001.

[15] Distributed Denial of Service attacks and their defenses:http://www.lancs.ac.uk/postgrad/pissias/net sec /ddos/

[16] D. Moore, *The spread of the code red worm (crv2),*http://www.caida.org/analysis/security/codered/coderedv2_analysis.xml.

[17] CERT Coordination Center, *erkms and li0n worms,* http://www.cert.org/incident_notes/IN-2001-03.html

[18] CERT Coordination Center*, Ramen worm*, http://www.cert.org/incident_notes/IN-2001-01.html

[19] N. Weaver, *Warhol Worm*; http://www.cs.berkeley.edu/~nweaver/ warhol.html

[20] Tripwire, *Tripwire for servers*, http://www.tripwire.com/products/servers/

[21] McAfee, *Personal Firewall*, http://www.mcafee.com/myapps/firewall/ov_firewall.asp

[22] Cisco, *Strategies to protect against distributed denial of service attacks*, http://www.cisco.com/warp/public/707/newsflash.html

[23] Mananet, *Reverse Firewall*, http://www.cs3-inc.com/ps_rfw.html

[24] Information Sciences Institute, *Dynabone*, http://www.isi.edu/dynabone/.