Distributed Denial of Service Attacks and Defense Mechanisms

Dan Tang\textsuperscript{1,2, a}, Xiaohong Kuang\textsuperscript{1,2, b}

\textsuperscript{1}Hunan police academy, Changsha, China
\textsuperscript{2}Key Laboratory of Network Crime Investigation, Colleges of Hunan Province, Changsha, China
\textsuperscript{a}tacom@sohu.com, \textsuperscript{b}tacom@163.com

Abstract. Distributed denial-of-service (DDoS) attacks have become a common problem in networked environments. The large number of variations in both the types of DDoS attacks and their mitigating approaches are an apt indicator of the extent of the issue. This article will offer an analysis of the existing DDoS attacks and their corresponding countermeasures. The paper aims to highlight the strengths and weaknesses of the available defenses in order to demonstrate the degree of applicability and efficiency of the solution methodologies. To achieve these objectives, the paper assumes a systematic design whereby it evaluates the DDoS attacks according to similar attributes, which in turn informs the evaluation of defense tactics.

1. Introduction
The Internet is a common target for the propagation of distributed denial-of-service (DDoS) assaults. Likewise, the extent and high frequency of DDoS attacks have inspired Information Security (IS) practitioners to develop corresponding countermeasures. However, the field is prone to constantly shifting tactics based on the attackers’ efforts to adapt their DDoS strategies to defeat the existing IS mechanisms. Accordingly, the introduction and deployment of new attack and defense approaches has created a complex security ecosystem, whereby it becomes challenging to select the appropriate solution for a given DDoS attack incident. In turn, the magnitude of the problem deters the requisite consideration of DDoS typologies. Similarly, the defense mechanisms adopt the ad hoc nature of the attacks, which results in a field devoid of a systematic compartmentalization of the crucial factors such as cost, effectiveness and suitability of the defense systems. As a result, this paper will address the outlined issues through three major research concerns, namely:

- How do DDoS attacks perpetrate?
- How have defense systems historically mitigated DDoS attack problems?
- How can an IS practitioner choose between existing defense systems in case of attack from a non-documented DDoS?

2. A Synopsis of DDoS Attacks
The nature of DDoS attacks is such that Information Technology (IT) corporation, Cisco, admits that DDoS attacks commonly target “corporate assets” \cite{1}. By inundating network resources with fake
requests, DDoS attacks manage to divert the target’s IT facilities from their prescribed functions, which results in unprecedented downtimes and service outage.

2.1. Factors that motivate malicious attacks through DDoS

1) Malice: DDoS attacks are an effective means of denying their victims of their computing resources. Hence, they are an apt tool for individuals planning to inflict damage based on their malicious intent.

2) Financial gain: companies that experience the effects of a large-scale DDoS attacks are susceptible to pay the attackers monetarily in order to regain their operational capacities.

3) Activism: individuals who wish to make a political statement can exploit the power of DDoS to coerce their opponents or authorities towards a particular objective.

4) To gain ‘hacking’ credibility: ‘power’ computer users gain popularity in their circles when they can prove that they can initiate and sustain a DDoS attack on a prescribed target.

2.2. Factors that facilitate the perpetration of DDoS attacks

1) Ability to escape identification: the ability to spoof IP addresses affords attackers the capability of evading the unmasking of their identities [2]. The factor is both an aid to the actual attack and a protective utility for the attacker on conclusion of the DDoS attack.

2) Lack of a unified Internet security policy: the proliferation of diverse security approaches impacts the Internet with varying degrees of immunity from DDoS attacks [3]. The lack of a singular body to enforce best practices across the interconnected networks provides a loop hole for DDoS attackers to exploit the weaker defense systems.

3) Skewed allocation of network resources: the infrastructure that connects small networks to larger ones is usually of a higher bandwidth. The feature provides attackers with the capability to ‘flood’ the less endowed targets through the high capacity infrastructure [3].

Table 1. DDoS Attack Metrics

| Attack Metric                  | Features                           |
|-------------------------------|------------------------------------|
| Automation attribute          | Manual, semi-automatic, automatic  |
| Targeted weakness             | Brute force, semantic              |
| Validity of source address    | Spoofed, valid                     |
| Rate dynamics                 | Constant, variable                 |
| Characterization possibility  | Characterizable, non-characterizable|
| Agent set persistence         | Variable, constant                 |
| Choice of victim              | Infrastructure, resource, host, application, network |
| Intended effect on the victim | Degrading, disruptive              |

4) The limited nature of network resources: since target networks have a certain limit, which serves its requirements, DDoS attacks can force the network to reach that limit and deny the users of their deserved access to services [2].

3. Categorization of DDoS Attacks

DDoS attacks consist of three major facets, namely (1) the execution approach, (2) the nature of the attack, and (3) the intended impact of the attack [4].

3.1. Execution approach

The execution phase of the DDoS attack requires the concerned attacker to (1) select, (2) compromise, and (3) infect the target resource [4]. However, the three commitments need substantial effort, which informs the attacker to either deploy a malicious agent beforehand such as a Trojan horse or virus in the
targeted network. In that case, therefore, the contemporary attacker prefers the automatic mode to the manual or semi-automatic mode of execution (see 0).

3.2. Nature of Attack
The DDoS attack assumes its nature based on either the vulnerability of the target, for instance through semantic attacks; or through flooding of the target resource with bogus requests, for instance through brute-force [5]. On the other hand, the DDoS attack could assume its character through the validity of the source address. By using spoofed IP addresses, the attacker could hide his or her identity, thus making the potential defense reaction more complex to implement.

3.3. Intended Impact
A DDoS could either deny the legitimate users access to their deserved resources or cause a degradation of the target’s reputation by reducing its ability to serve its intended users. The phenomenon, as a result, provides the taxonomy classes of a (1) disruptive or (2) degrading DDoS attack [6].

4. Defense Approaches
Defense mechanisms assume varying approaches (see 0). The DDoS countermeasures could protect the potential victim in such a manner that even in case of an attack; the users do not experience a loss of service, for instance, through the use of the preventive tactic. On the other hand, the defense mechanism could aim to respond to the DDoS attack in such a manner that the impact of the service outage is minimal; for instance, through the use of the reactive method [7].

The IS response to a DDoS attack could involve the use of a standalone mechanism (that is, an autonomous entity), such as a firewall; or involve cooperative and interdependent mechanisms. On the other hand, the defense mechanism could function at the victim’s network, the intermediate network or at the source network. However, the installation of a DDoS defense application at the source network, for instance in all the customer’s devices that access a corporation’s network, poses a substantial financial commitment, which reduces its economic practicability for a large network [7].

5. Evaluation and Choice of Countermeasures
According to this paper’s categorization of DDoS attacks and defense mechanisms, practitioners have the opportunity to familiarize themselves with the types of DDoS approaches more easily. In addition, the grouping of DDoS threats could facilitate the development of more appropriate countermeasures in contrast to generic ones. Moreover, the taxonomy of defense mechanisms highlights the limitations of certain tactics, which would inform the IS practitioner of the suitability of a particular defense choice.

6. Conclusion
This paper has offered a mapping of the common DDoS attack types and the corresponding defense mechanisms. The categorization has illustrated the need for IS practitioners to develop DDoS benchmarks, which would simplify the creation of countermeasures against novel DDoS threats. On the other hand, the paper has also highlighted the factors, which facilitate the perpetration of DDoS attacks. The examination would
Figure 1. Categorization of DDoS defense methods

Inform researchers who aim to generate defense mechanism in spite of the existing Internet security deficiencies.

Acknowledgments
Supported by National Natural Science Fund of China (No.61471169) Supported by Hunan province science and technology plan (No.2012GK3047).

References
[1] Cisco, ‘DDoS attack prevention’, Cisco, 2015. [Online]. Available: http://www.cisco.com/c/en/us/solutions/enterprise-networks/ddos-attack-prevention/index.html. [Accessed: 14- Sep - 2015].
[2] J. Mirković, G. Prier and P. Reiher, ‘Attacking DDoS at the source’, in Network Protocols, 2002. Proceedings. 10th IEEE International Conference, 2002, pp. 312-321.
[3] F. Freiling, T. Holz and G. Wicherski, ‘Botnet tracking: Exploring a root-cause methodology to prevent distributed denial-of-service attacks’, in Proceedings of the 10th European Symposium on Research in Computer Security, Milan, Italy, 2005, pp. 319–335.
[4] C. Douligeris and A. Mitrokotsa, ‘DDoS attacks and defense mechanisms: classification and state-of-the-art’, Computer Networks, vol. 44, no. 5, pp. 643-666, 2004.
[5] R. Chang, ‘Defending against flooding-based distributed denial-of-service attacks: A tutorial’, IEEE Commun. Mag., vol. 40, no. 10, pp. 42-51, 2002.
[6] S. Specht and R. Lee, ‘Distributed denial of service: Taxonomies of attacks, tools, and countermeasures’, in Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems, 2004 International Workshop on Security in Parallel and Distributed Systems, 2004, pp. 543-550.
[7] A. Srivastava, B. Gupta, A. Tyagi, A. Sharma and A. Mishra, ‘A recent survey on DDos attacks and defense mechanisms’, in Advances in Parallel, Distributed Computing, 1st ed., D. Nagamalai, E. Renault and M. Dhanuskodi, Ed. Springer, 2011, pp. 570-579.