International Journal of
Applied Mathematics,
Electronics and Computers

IJAMEC

ISSN: 2147-8228 www.atsciences.org/IJAMEC

Advanced Technology and Science

Original Research Paper

Internet Scale DoS Attacks

Berat Kurar [1], Radwan Tahboub [1]

Accepted 15th August 2014

Abstract: Internet scale DoS attack is a new evolution of conventional flooding DoS attack with the inspiration of shutting down the Internet due to its vulnerable infrastructure. Past DoS attacks directly attacked the victim, usually a single host. Consequently, defences were designed to identify the excessive traffic or filter illegitimate traffic. From the early two thousand, Internet scale DoS attacks started to appear. They aimed to disable highly connected routers or large links with a legitimate action in the form of low-rate traffic or high-rate wanted traffic with protocol messages that are unfiltered by congestion control. The latter can be more devastating due to its global impact therefore attracts the attention of researchers and some applications are now available. The goal of this paper is to introduce Internet scale DoS attack and to survey its theoretical underpinnings and experimental applications. Several attacking techniques will be presented, as well as their effects on the connectivity of the Internet. A comparison will be carried out among them to expose their pros and cons in order to study the possibility of their integration via usage of several botnets for destroying the Internet connectivity. Our discussion aims to clarify new directions that DoS, DoS defense and Internet design research can follow.

Keywords: *Internet topology, complex networks, communication system security, routing protocols, TCPIP*.

1. Introduction

Denial of service (DoS) attack prevents a network resource from being accessed by legitimate users [1]. DoS attacks are often launched to lead the victim to economic losses. For example, the DoS attack against Yahoo in 2000 caused its services to be offline for around 2 hours leading to significant loss of revenue through advertising [2]. In 2002, 9 Domain Name System (DNS) servers were down for around 1 hour because of a DoS attack [3]. In 2010, a group of activists calling themselves Anonymous orchestrated a DoS attack on the www.mastercard.com bringing its service to halt [4]. In 2013, a group called Izzaddin al-Qassam Cyber Fighters targeted major US banks with powerful DoS attacks [5].

Commonly attacker directs packet traffic to a victim and this illegitimate traffic consumes a resource and makes it unavailable to legitimate traffic. What makes DoS attacks possible is the current Internet architecture, because it was designed to provide an open and scalable network among research and educational communities, without any consideration of possible DoS attacks [6]. Followings are the Internet architecture vulnerabilities that can be exploited to conduct a DoS attack: Internet resources are limited: Each internet entity (node, network, service) has limited resources that can be consumed by too many users [7]. Internet security is highly interdependent: Whether an entity will be a victim or not depends on how secure the rest of Internet entities are [8]. Internet has an end-to-end design: Transmission Control Protocol (TCP) has an end-to-end design which pushes the complexity to end hosts to leave the intermediate network with best-effort packet forwarding. Therefore, if one of the end hosts exploits the other end, no one in the intermediate network will stop it, because it is designed to simply forward packets not to police them [7].

DoS attacks are carried out by three types of actions [9]: first, consumption of limited resources, second, destruction of configuration information, and third, physical destruction of network components.

In this paper, we are interested in the attacks with the first type of actions against the limited resources, e.g. network bandwidth, CPU, memory, or any combination of them. Furthermore, we are not concerned with the DoS attacks which need unauthorized access to resources in order to be carried out; rather we are concerned with the DoS attacks that don’t compromise confidentiality and integrity but only the availability. Availability is being accessible and usable upon demand by an authorized user [10]. Hereafter, we use the term DoS to refer to the type of DoS we are interested in.

This paper aims to present a survey of existing research on recent trends of DoS attacks, discuss their strong and weak points and conclude the directions that this research can take in the future.

The rest of the paper is organized as follows: Section 2 gives a classification of conventional DoS attacks, section 3 tackles the theoretical results related to Internet scale DoS attacks, section 4 surveys the implicational results related to Internet scale DoS attacks, section 5 defines Internet scale DoS and determine its place in classification, section 6 discusses the outcomes and finally section 7 concludes the paper with insights for some future work.

2. DoS Attack Classification

In order to clarify our path, we need to have a DoS attack classification as shown in Fig. 1, and determine the place of Internet Scale DoS attack inside it. Formerly proposed classifications by [1], [7], [11] and [12] are very detailed and unnecessary for the type of attacks that we are interested in. So we combined them in a way to combine the branches related to our work and to ignore the unrelated ones. Most importantly, our classification does not contain a branch based on the characteristics of the botnet that is used in the attack and a branch based on the

[1] *Electrical and Computer Engineering Department, Palestine Polytechnic University, Hebron/Palestine*
Corresponding Author: Email kurarberat@hotmail.com
Note: This paper has been presented at the International Conference on Advanced Technology&Sciences (ICAT'14) held in Antalya (Turkey), August 12-15, 2014.

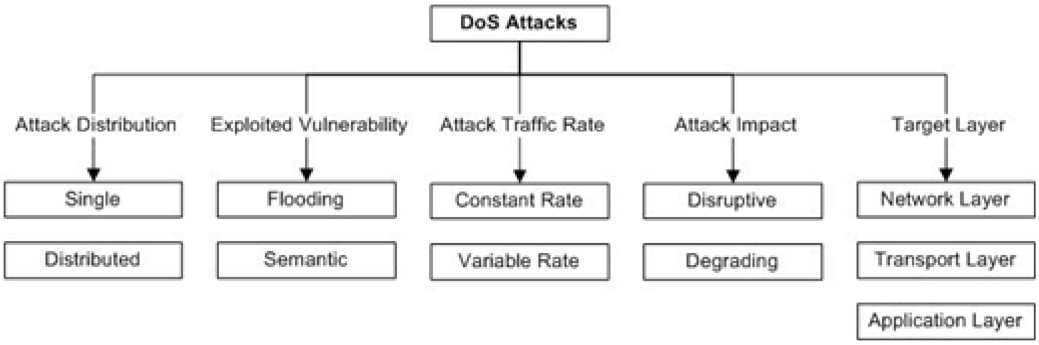

Fig. 1 DoS attack classification

enhancement of botnet traffic. Although botnets are closely related to DoS attacks, they require a separate study.

2.1. Attack Distribution

Single DoS attack generates traffic packets from a single host. The earliest DoS attack claimed by Dave Dennis [13] in the University of Illinois was a single DoS attack.

Distributed DoS (DDoS) attack generates traffic packets from multiple hosts. DDoS attack uses two components: the agent, who runs on compromised hosts and generates attack traffic packets; and the handler, which is a program installed on a server that controls the agents, telling them when to attack, what to attack, and how to attack [14]. Agents are also called bots. A set of bots that are controlled by a single attacker is called a botnet. Most of DoS attacks are distributed such as UDP flood, ICMP flood, VoIP flood, and Trinoo and Tribe Flood Network based attacks [15] [8].

2.2. Exploited Vulnerability

Flooding attack directs a vast amount of traffic to the victim in order to exhaust its resources. For example, in a User Datagram Protocol (UDP) flood attack, an attacker sends excessively a high number of UDP segments to random ports on a target host to saturate its bandwidth, rendering the target unreachable by other hosts [16]. Smurf attack uses ICMP echo packets and Fraggle attack uses UDP packets to exhaust the victim's resources [17].

Semantic attack directs traffic to victim in order to exploit a specific feature of a protocol installed at victim. For example, Transmission Control Protocol (TCP) SYN flooding attack sends a flood of TCP SYN packets to the victim without completing the TCP handshake and exhausts the victims connection state memory [18], [19].

2.3. Attack Traffic Rate

Constant rate attack directs traffic to victim in a constant rate, while **variable rate attack** directs traffic to victim in a changing rate to avoid detection [7].

2.4. Attack Impact

Disruptive attack aims to completely deny the victim's services to its clients. However, degrading attack aims to partially deny the victim's services to its clients. Degrading attacks are hard to be detected due to their low-rate behavior, but they can cause serious damage to the victims business. As a result some customers, dissatisfied with slow services, would change their service provider. Mirkovic et al. [7] expressed their seriousness as: Almost all existing proposals to counter distributed DoS attacks would fail to address degrading attacks.

2.5. Attack Targets

Internet is structured into multiple TCP/IP stack protocols. DoS attacks can mainly be directed to the network layer, transport layer and application layer [20] [21].

Network layer attack like ICMP ping flooding attack directs attack traffic via network layer by sending ICMP echo requests at a very fast rate to the targeted host or router [22].

Transport layer provides end-to-end connectivity. An end system is a host that implements all five layers of TCP/IP stack. The two primary protocols in this layer are Transmission Control Protocol (TCP) [23] and User Data- gram Protocol (UDP) [24]. **Transport layer attack** like UDP flood attack and TCP SYN flood attack directs attack traffic via transport layer [16] [18].

Application layer is the top layer of TCP/IP stack and provides services to applications. Common protocols in this layer are File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), Internet Relay Chat (IRC), and Domain Name System (DNS). Routing related application layer protocol, Border Gateway Protocol (BGP) [25], is implemented only in the routers. **Application layer attack** directs attack traffic via application layer [26]. For example, an attacker sends HTTP requests to download a large file from a victim to exhaust its memory, CPU and bandwidth.

3. Survey of Theoretical Results Related to Internet Scale Dos Attacks

There are theoretical works that study the Internet topology robustness to attacks and the consequences of such targeted attacks. Internet topology is an example of a complex network. Steen [27] defines complex networks informally as a graph of huge number of interlinked nodes with an unpredictable over- all behavior. In case of Internet, nodes are routers and links are the physical connections between them.

3.1. Internet is a Scale-Free Network

Barabasi et al. [28] claimed that for more than 40 years science treated all complex networks as being random. According to [28], random network nodes have approximately the same number of links. In other words, it is a fixed number of nodes connected by random links. The nodes follow a Poisson distribution with a bell shape as shown in Fig. 2 and it is rare that a node has significantly more or less links than the average. The probability that a node is connected to other nodes decreases exponentially for large k. On the other hand, this paper introduced the scale-free network as the complex network with some nodes having a relatively large number of connections to other nodes; whereas the rest of nodes have relatively a small number of connections. The popular nodes are called hubs. Such a network has no scale due to the hubs that have seemingly unlimited number of links. The nodes follow a power law distribution. The probability that a node is connected to

k other nodes is proportional to $1/k^n$, typical range of n is $2 < n < 3$. Power law distribution is described by a continuously decreasing function as in Fig. 2, in contrast to the democratic distribution of links in random networks.

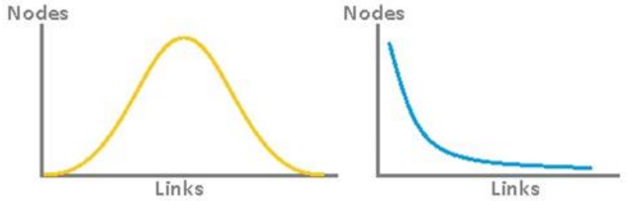

Fig. 2 Bell curve and power law distribution of node linkages

Faloutsos brothers [29] analysed the physical structure of Internet. They found out that the Internet topology, composed of routers and physical connections between them, is too a scale-free network. Therefore Internet topology robustness is tightly related to the robustness of scale-free network.

Scale free networks are resistant to random node failures but extremely vulnerable to coordinated attack against their hubs [30], [31]. Consequently, Internet, a scale-free network, is robust against random node failures but highly vulnerable to coordinated attacks against its popular nodes. The ability of a small group of well-informed attackers to crash the entire Internet via a coordinated attack should be considered [28].

The following section investigates such kind of attack and its consequences via Internet map experiments.

3.2. Internet Robustness

In order to study Internet robustness, Internet topology needs to be studied as well. Internet topology is represented by an Internet map which is a scheme displaying Internet entities relative position; but unlike real maps the entities are not aligned on a surface. Internet map is a bi-dimensional presentation of links between entities on the Internet [32]. Magoni [33] worked at router level of the Internet, instead of Autonomous System (AS) level, to obtain more accurate results. Therefore the Internet entities in the Internet map are routers linked via IP layer connectivity.

Magoni [33] presents 5 types of attacks on three Internet maps; however for simplicity we will discuss only static attack technique. In the static attack each node is assigned once and for all an importance value based on its degree, number of links it has to other nodes. The higher the degree, the higher the importance of the node is. The nodes are then removed from the network one by one in decreasing order of importance. Experimental results concerning the static attack shows that the network can be torn down by removing around 5% of its nodes. That means the relative size of the largest connected component to the initial total number of nodes in the network, converges to zero.

Despite this worrying result, values are dependent on the size of the network which means that tearing down Internet would require simultaneous attacks on hundreds of thousands of routers. Internet had 200 million hosts in June 2002 according to [34]. Assuming that 1% are routers then there were 2 million routers. Last of all Magoni [33] concludes that; undertaking a massive attack on the Internet connectivity may not be feasible.

3.3. Shrew Attack Against TCP

Common DoS attacks are done by a high-rate transmission of packets towards the victim. The high-rate nature can easily be detected by network monitors. Kuzmanovic and Knightly [35] studied the low-rate DoS attack against TCP flows (Shrew attack). They showed that TCP's deterministic retransmission timeout mechanism is vulnerable to periodical low-rate DoS traffic.

Default retransmission timeout (RTO) value is equal to 1 second by protocol recommendation. At each packet loss, RTO doubles [36]. This timeout mechanism is developed for congestion control. However its deterministic RTO values can be exploited by sending high-rate but short duration bursts having Round Trip Time (RTT) burst length to ensure packet loss and repeating periodically at RTO timescales. The short durations of the attacker's loss inducing bursts are referred as outages. Considered a single TCP flow, an attacker creates an initial outage at `time0`; the TCP sender will wait for RTO duration, and then double its RTO to 2 seconds. If the attacker creates a second outage at `time1`, TCP sender will wait another 2 seconds. So the attacker denies service of link to TCP flow by creating outages at times $3,7,15,\ldots$ with averagely low-rate traffic.

Thus, a shrew attack is designed as shown in Fig. 4. It has a rate large enough to induce loss (aggregated with existing traffic must exceed the link capacity), duration of scale RTT (long enough to induce timeout to all the flows), and period of scale RTO (chosen such that when flows attempt to exit timeout, they are faced with another loss, best selection is minimum RTO).

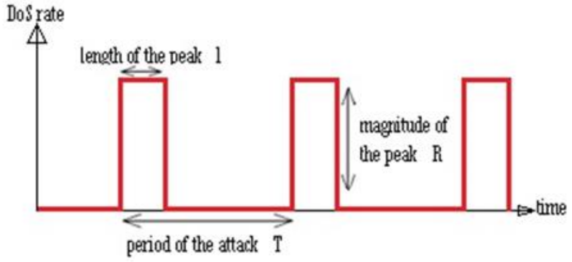

Fig. 3 Square wave DoS stream

3.4. BGP Overview

The Internet is organized as autonomous systems (AS). An AS is a network under the control of a single administrative authority [37]. For example, the network of a single Internet Service Provider might be an AS. ASes divide routing problem of Internet into two parts: Routing within a single AS and routing between ASes. An AS is also called a routing domain thus the two parts of Internet routing problem are named as intradomain routing and interdomain routing. Each AS can run the intradomain routing protocol it likes such as Routing Information Protocol (RIP) [38] or Open Shortest Path First (OSPF) [39]. However the interdomain routing protocol between the ASes is not for their choice and is the de facto standard Border Gateway Protocol (BGP) [25].

BGP connects ASes in a non-tree structure via BGP routers at the edges of ASes. Thus, Internet consists of interconnection of multiple backbone service providers who provide service to some large corporations and Internet Service Providers (ISP). ISPs provide service to individual PCs at homes and some small corporations (Fig. 3). Hence an Internet backbone router must be able to forward any packet in the Internet.

BGP routers maintain a table of AS paths to every destination. They are also referred as border routers, since they are located at the connection points of their home AS and another AS. Peering border routers establish session to exchange reachability information among ASes. When a link failure happens border router re-computes its routing table, removes the failed link and informs neighboring ASes about the change via a BGP update message [40].

BGP runs on the services provided by reliable transport protocol TCP. This means that any information sent from one speaker to another is guaranteed to be delivered. BGP speakers send periodic

KeepAlive messages to ensure the connection health. If a BGP router crashes, it will stop sending KeepAlive messages, and the other BGP routers that have routes from it will know that those routes are no longer valid. Each BGP router maintains a HoldTimer to limit the maximum amount of time between successive KeepAlive messages from its peer in the BGP session. If the HoldTimer expires, BGP connection is closed and all routes previously learned from the session are withdrawn, causing instability to propagate to other networks [25].

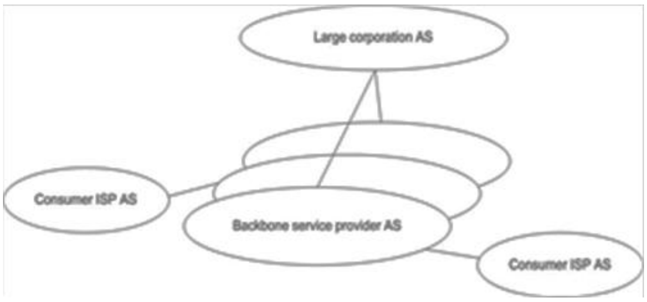

Fig. 4 Internet ASes

Data and Control Plane Stability: Local changes in a border router such as link cuts or hardware failures causes some routes to be withdrawn and leads routing table re-computation and re-advertisements to other routers. Then same series of events happen in other border routers as well. As a result, update propagates globally, meaning that in BGP local changes might be seen globally [41]. Instability in control plane can reduce the performance of the data plane [42] and [43].

3.5. Shrew Attack Against BGP Routing (ZMW Attack)

Shrew attack [35] can also be launched against interdomain routing protocol BGP which runs over TCP layer services. Zhang et al. [44] shows that remotely launched low-rate TCP targeted DOS attack against BGP routers (ZMW attack) can cause session resets as a result of sufficiently large number of consecutive packet drops and consequently impacts network reachability [45], [46]. Because control plane packets, that are destined to routers or sourced from routers, has no priority over the data plane packets, that are sourced from end hosts and destined to end hosts. Thus congestion caused by data traffic adversely effects BGP control packets [47].

To reset a BGP session, attack traffic needs to induce congestion sufficiently long to cause the BGP `HoldTimer` to expire. BGP session reset then can lead to severe churn on the Internet's control plane. Each of both routers involved in the BGP session withdraws all the routes previously advertised by its neighbor. For example number of routes in a backbone service provider router is around 500.000 [48]. So withdrawing large number of routes can cause many destination networks to become unreachable and a large amount of traffic to be rerouted which leads to congestion as well [49].

4. Survey of Theoretical Results Related to Internet Scale Dos Attacks

4.1. Coremelt Attack

Studer and Perrig [50] presented Coremelt as a new attack mechanism where attackers send wanted traffic between each other, not towards a victim host, to congest bandwidth of a backbone link within an AS in the core of the Internet. $O(n^2)$ connections between n attackers makes Coremelt powerful so it can induce a significant amount of congestion to the core links (that's why named Coremelt) of Internet by eluding prior defense mechanisms with its legitimate traffic. Impact of Coremelt is examined by simulation of Internet topology, routing data and distributions of real botnets.

Coremelt attack needs knowledge of network topology and a way to generate a traffic that intermediate nodes will forward. It solves network topology problem by tracerouting the paths between every pair of bots and handling knowledge $n(n-1)/2$ of paths. Then simply it decides which paths traverse the target link and send the traffic only across those paths. Coremelt does not use TCP packets to create its traffic since TCPs congestion control slows down the traffic once its path is under stress. But it may use greedy traffic that is labeled as TCP [51] or UDP traffic with the assumption that ISPs do not throttle it.

While botnet distribution is simulated according to CodeRed and GT-DDoS datasets, CAIDA AS relationships dataset [52] is used. Their simulator is lack of native legitimate traffic, all the traffic is between the bots. Additional traffic can cause congestion on downstream links and prevent attack traffic from reaching the target link, and reduce the impact of Coremelt. However, most of the legitimate traffic will likely use congestion avoidance so as to allow greedy attack traffic to reach to target link. The addition of legitimate traffic on the target link will increase the impact of Coremelt.

Coremelt's goal is to achieve a high destructiveness while limiting the number of ASes that experience collateral damage so as to maintain secrecy.

Destructiveness is a measure of Coremelt's ability to overload different target ASes. Since it aims to attack the core of the Internet, the destructiveness is defined as the fraction of the targeted top ten ASes which can be congested with a given botnet size and traffic generation capabilities.

Secrecy indicates the number of non-target ASes that are impacted by a Coremelt attack. Since it aims to shut down the target ASes, it needs to minimize the impact on the rest of the Internet. Additional congested ASes increase the chance of ASes reacting to congesting flows by dropping packets before they reach to target.

Studer and Perrig's work [50] experimentally indicated that an attacker with a realistically distributed botnet under realistic traffic and network settings can launch a Coremelt attack and fail core links of target ASes without congesting much collateral ASes and raising suspicion.

4.2. Losing Control of the Internet

Schuchard et al. [41] introduced the Coordinated Cross Plane Session Termination (CXPST) attack against the control plane of the Internet. Control plane of the Internet is responsible of determining the path to any given destination. Data plane of the Internet is responsible of forwarding packets to their destination. Control plane and data plane packets use the same physical medium. As we mentioned ZMW attack [44] exploits this fact to terminate a BGP session. CXPST chooses multiple BGP sessions with high centrality measures, and terminates them using ZMW attack to create a wave of BGP updates causing control plane instability which ripples globally. This leads to overwhelming the processing capacity of core Internet routers, crippling the Internets control plane and so the data plane. They showed that a 250.000 node botnet can increase the processing delays from orders of microseconds to orders of hours.

Conceptually CXPST uses ZMW attack. ZMW uses data traffic to terminate the session between two border routers. This leads to route withdrawals, re-computations and re-advertisements. Since the targeted link is no longer congested with attack traffic, targeted routers reestablish their BGP session after a small amount of time. So the routes that were just withdrawn are re-advertised and this results in additional BGP updates. When the previous routes become available again, the attack traffic again is directed to the target link. Therefore the attack resumes without any intervention from the attacker and terminates the BGP session again. The cycle repeats itself and leads targeted links to oscillate between up and down states. In short, CXPST causes targeted route flapping and so overwhelms large set of routers in the Internet.

CXPST needs to handle two challenges. First, it needs to select the correct BGP sessions to maximize the control plane instability. Second, it needs to direct attack traffic to the targeted links without causing link failures on the way to the target.

Selecting targets: CXPST uses centrality measures to maximize the number of BGP update messages and in turn to maximize the control plane instability. The links with high BGP betweenness are selected prior to attack. As much as an edge appears in the traceroutes between the bots, as much as it has higher BGP betweenness.

Attack Traffic Management: CXPST selects which bots will attack a given link keeping in mind that CXPST changes the network topology. It ensures that the path does not contain other links that are targeted also. So when those links fail, attack traffic will not be rerouted. Attack traffic can be rerouted because of unintended failure of a non-targeted link. Therefore CXPST sends more attack traffic than needed to congest a targeted link. This extra traffic is named Safety Net, and it prevents relaxing the pressure on targeted link because some amount of attack traffic is diverted. CXPST also minimizes the amount of congestion prior to reaching the targeted link by dispersing the attack traffic until it reaches the target, then aggregating on the target link, and then dispersing not to congest downstream links. Lastly the attack traffic is created between selected source and destination bots as described in Coremelt [50]. In this way, it creates a wanted traffic and not reported by end host.

Simulation Results: Defined links as: 1) Targeted links: any link selected for disruption. 2) Last mile links: untargeted links that connect fringe ASes to the rest of the network. 3) Transit link: any link out of previous categories. Authors simulated CXPST on their own event driven simulator [53] with botnets of 64, 125, 250, and 500 thousands of nodes. With a 30% extra safety net traffic, CXPST disrupts around 90% of targeted links, 19% of last mile links and 4% of transit links. This demonstrates that CXPST maximizes target link failures while minimizing the failures in other categories.

5. What and Where is the Internet Scale Dos Attack

Based on the above survey, Internet scale DoS attack can be expressed as a DoS attack against highly connected links or highly connected nodes of the Internet topology. It has the potential to be the most destructive DoS because of its target importance. Among the above classification it takes place as a distributed DoS attack according to attack distribution, a flooding or semantic attack according to exploited vulnerability, a constant rate or variable rate attack according to attack traffic rate, disruptive attack according to attack impact and a network layer or application layer attack according to target layer. We can conclude that Internet scale DoS attack does not differ from conventional DoS, except for its target victim.

Table 1. Comparison of DoS attacks

Design Goals	Conventional DoS	Coremelt	CXPST
Control Plane Instability	Not a goal	Yes	Yes
Data Plane Congestion	Yes	Yes	Yes
Network Topology Change	Not a goal	Yes	Yes
Reverse Feed to Itself	Not a goal	No	No
Secrecy	Some of them	Yes	Yes
Control Plane Attack	No	No	Yes
Data Plane Attack	Yes	Yes	No
Against AS Routers	No	No	Yes
Against AS Links	Not a goal	Yes	No
Maximize Destructiveness	Yes	Yes	Yes
Low Rate Traffic	Some of them	No	Yes
High Rate Traffic	Some of them	Yes	No

6. Discussion

The theoretical underpinnings of Internet scale DoS attacks start with the work of Barabasi et al. [28]. They defined the scale-free network as the complex network with some nodes having a relatively large number of connections to other nodes; whereas the remaining nodes have relatively small number of connections. Later on, Faloutsos brothers [29] discovered that the Internet topology is too a scale-free network. This means Internet topology robustness is tightly related to the robustness of scale-free network. And scale free networks are resistant to random node failures but extremely vulnerable to coordinated attack against their hubs [30]. Against this conclusion of Barabasi, Magoni [33] concludes that robustness is dependent on the size of the network which means tearing down the Internet would require simultaneous attacks on hundreds of thousands of routers and that undertaking a massive attack on the Internet connectivity may not be feasible. Despite this unfavorable outcome, works in this field did not stop and continue with the implicational studies.

The implicational survey starts with the fact that Internet is designed to use the physical medium fairly between its data plane and control plane. This fact is firstly exploited by ZMW attack [44] to disrupt BGP session via data plane traffic. ZMW uses UDP traffic in order to maintain the attack traffic rate easily. ZMW attack is only a theoretical study of an attack against control plane. Their work was extended by CXPST attack [41] to a real like environment with multiple BGP sessions with high centrality measures to maximize the number of BGP update messages and in turn to maximize the control plane instability and in turn to maximize the data plane packet losses. CXPST exploits the fact that ASes use BGP in their speaking routers. Therefore CXPST is an attack against control plane which directly targets the speaking routers of ASes to disrupt their BGP sessions and cause a churn in their table. CXPST maintains its secrecy via usage of low-rate traffic flooding and by creating traffic between selected source and destination bots as described in Coremelt [50]. In contrast to CXPST, Coremelt is an attack against data plane and congests the links of backbone ASes. Its key idea is to create only wanted traffic and to surpass all the defense mechanisms, in the time it creates high-rate TCP traffic. Coremelt maximizes its destructiveness by limiting the number of ASes that experience collateral damage thus maintaining its secrecy.

7. Conclusion and Future Work

In this paper, we surveyed Internet scale DoS attacks from theoretical underpinnings to implicational results. In contrast to Magoni's conclusion, a well designed attack with sufficient traffic volume can tear down the Internet. Since modern world heavily depends on the Internet, tearing it down would surely cause significant damages. DoS attacks do exist and continuously improve their destructiveness to the target and their robustness against defense mechanisms. Therefore, defense and connectivity design mechanisms have to be improved continuously to protect against even imaginary scenarios. This paper presents a distinct and imaginary look into DoS attacks to stimulate researchers to take it into consideration.

Future work may be conducted to create a new imaginary scenario by combining Coremelt and CXPST attacks via the usage of two botnets. Coremelt aims to congest the links of ASes while CXPST aims to churn the routers of ASes. The data plane traffic caused by Coremelt strengthens CXPST [41]. The control plane churn caused by CXPST does not affect Coremelt adversely since it happens in the backbone ASes not in collateral ASes [50].

References

[1] M. Handley and E. Rescorla, "Internet Denial-of-Service Considerations," RFC 4732, 2006.

[2] (2000) Yahoo on Trail of Site Hackers. [Online]. Available: http://www.wired.com/techbiz/media/news/2000/02/34221

[3] (2002) Powerful attack cripples majority of key Internet computers. [Online]. Available: http://www.securityfocus.com/news/1400

[4] (2010) Operation Payback cripples MasterCard site in revenge for WikiLeaks ban. [Online]. Available: http://www.theguardian.com/media/2010/dec/08/operation-payback-mastercard-website-wikileaks

[5] (2013) DDoS: Lessons from Phase 2 Attacks. [Online]. Available: http://www.bankinfosecurity.com/ddos-attacks-lessons-from-phase-2-a-5420/op-1

[6] H. F. Lipson, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy," CERT Coordination Center, 2002.

[7] J. Mirkovic and P. Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," in Proc. ACM SIGCOMM, 2004.

[8] N. Long and R. Thomas, "Trends in Denial of Service Attack Technology," CERT Coordination Center, 2001.

[9] (1997) CERT/CC Denial of Service. [Online]. Available: http://www.cert.org/tech_tips/denial_of_service.html

[10] W. Stallings and L. Brown, Computer Security: Principles and Practice, Pearson, 2008.

[11] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art," Computer Networks, 2004.

[12] M. Abliz, "Internet Denial of Service Attacks and Defense Mechanisms," University of Pittsburgh, Department of Computer Science, Technical Report, 2011.

[13] (2010) Perhaps the First DoS Attack. [Online]. Available: http://www.platohistory.org/blog/2010/02/perhaps-the-first-denial-of-service-attack.html

[14] K. Scarfone and K. Masone, "Computer Security Incident Handling Guide Recommendations of the National Institute of Standards and Technology," National Institute of Standards and Technology, 2008.

[15] (2013) RioRey Taxonomy of DDoS Attacks. [Online]. Available: https://riorey.com/x-resources/2013/RioRey_Taxonomy_DDoS_Attacks_2.4_2013.pdf

[16] (1996) CERT Advisory CA-1996-01 UDP Port Denial-of-Service Attack. [Online]. Available: http://www.cert.org/advisories/CA-1996-01.html

[17] B. K. Lokesh, "Denial of Service Attacks - DDOS, SMURF, FRAGGLE, TRINOO," 2001.

[18] (1996) CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks. [Online]. Available: http://www.cert.org/advisories/CA-1996-21.html

[19] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of Network Based Defense Mechanisms Countering the DoS and DDoS Problems," in Proc. ACM-CSUR, 2007.

[20] G. Malkin, "Internet Users' Glossary," RFC 1983, 1996.

[21] J. Postel, "Internet Control Message Protocol," RFC 792, 1981.

[22] H. Burch, "Tracing Anonymous Packets to Their Approximate source," in Proc. 14th Systems Administration Conference, 2000.

[23] J. Postel, "Transmission Control Protocol," RFC 793, 1981.

[24] J. Postel, "User Datagram Protocol," RFC 768, 1980.

[25] Y. Rehkter, T. Li, S. Hares, "A Border Gateway Protocol 4," RFC 4271, 2006.

[26] J. Nazario, "Black Energy DDoS Bot Analysis," Arbor Networks, 2007.

[27] M. V. Steen, Graph Theory and Complex Networks, 2010.

[28] A. L. Barabasi and E. Bonabeau, "Scale-Free Networks," Scientific American, 2003.

[29] M. Faloutsos, P. Faloutsos, and C. Faloutsos, "On power-law relationships of the Internet Topology," National Science Foundation, 1999.

[30] R. Albert, H. Jeong, and A.-L. Barabasi, "Error and Attack Tolerance of Complex Networks," Nature, 2003.

[31] S. Tauro, C. Palmer, G. Siganos, and M. Faloutsos, "A Simple Conceptual Model for the Internet Topology," National Science Foundation, 2001.

[32] (2013) The Internet Map. [Online]. Available: http://internet-map.net/

[33] D. Magoni, "Tearing Down the Internet," IEEE Journal on Selected Areas in Communications, 2003.

[34] (2013) NetSizer: Internet growth forecasting tool. [Online]. Available: http://www.netsizer.com/

[35] A. Kuzmanovic and E. Knightly, "Low Rate TCP Targeted Denial of Service Attacks," in Proc. SIGCOMM, 2003.

[36] V. Paxson, M. Allman, J. Chu, and M. Sargent, "Computing TCP's Retransmission Timer," RFC 6298, 2011.

[37] J. Hawkinson and T. Bates, "Guidelines for creation, selection, and registration of an Autonomous System," RFC 1930, 1996.

[38] G. Malkin, "RIP Version 2," RFC 2453, 1998.

[39] J. Moy, "OSPF Version 2," RFC 2328, 1998.

[40] L. L. Peterson, B. S. Davie, Computer Networks, Morgan Kaufmann Publishers, 2010.

[41] M. Schuchard, Y. Vasserman, A. Mohaisen, D. F. Kune, N. Hopper, and Y. Kim, "Losing Control of the Internet: Using the Data Plane to attack to Control Plane," in Proc. NDSS,

ACM, 2010.

[42] K. Sriram, D. Montgomery, O. Borchert, O. Kim, and D. R Kuhn, “Study of BGP Peering Session Attacks and Their Impacts on Routing Performance,” IEEE Journal on Selected Areas in Communications: Special issue on High-Speed Network Security, 2006.

[43] F. Wang, Z. M. Mao, J. Wang, L. Gao, and R. Bush, “A Measurement Study on the Impact of Routing Events on End to End Internet Path Performance,” in Proc. SIGCOMM, 2006.

[44] Y. Zhang, Z. M. Mao, and J. Wang, “Low Rate TCP Targeted DoS Attack Disrupts Internet Routing,” in Proc. 14th Annual Network and Distributed System Security Symposium, 2007.

[45] C. Labovitz, A. Ahuja and F. Jahanian, “Experimental Study of Internet Stability and Wide-Area Network Failures,” National Science Foundation, 1999.

[46] C. Labovitz, R. Malan, and F. Jahanian, “Internet Routing Instability,” IEEE/ACM Transactions on Networking, 1998.

[47] A. Shaikh, L. Kalampoukas, R. Dube, and A. Varma, “Routing Stability in Congested Networks: Experimentation and Analysis,” in Proc. ACM SIGCOMM, 2000.

[48] (2013) BGP Routing Table Analysis. [Online]. Available: http://bgp.potaroo.net/

[49] (2013) BGP Instability Report. [Online]. Available: http://bgpupdates.potaroo.net/instability/bgpupd.html

[50] A. Studer and A. Perrig, “The Coremelt Attack,” in Proc. ESORICS, 2010.

[51] S. Savage, N. Cardwell, D. Wetherall, and T. Anderson, “TCP Congestion Control with a Misbehaving Receiver,” National Science Foundation, USENIX, 1999.

[52] (2013) CAIDA: As relationships dataset. [Online]. Available: http://www.caida.org/data/as-relationships/

[53] M. Schuchard, “Stormcaller Simulator,” 2010.