UDC 004.75: 004.49

E.I. KOLIBABCHUK, O.P. VOYTOVYCH, L.M. KUPERSHTEIN
Vinnytsia National Technical University, Ukraine

INVESTIGATION OF DENIAL-OF-SERVICE ATTACKS

Methods and ways to perform denial-of-service attack are analyzed and classified in this work. Famous Denial-of-Service attack classifications are reviewed and analyzed. New elements of modern DoS attack classification are proposed.
Keywords: denial-of-service attacks, attacks classification, computer network.

Е.І. КОЛІБАБЧУК, О.П. ВОЙТОВИЧ, Л.М. КУПЕРШТЕЙН
Вінницький національний технічний університет

ДОСЛІДЖЕННЯ АТАК НА ВІДМОВУ В ОБСЛУГОВУВАННІ

У статті проаналізовано та класифіковано засоби та способи проведення атак на відмову в обслуговуванні. Розглянуто та проаналізовано відомі класифікації атак на відмову в обслуговуванні. Запропоновано нові елементи сучасної класифікації атак на відмову в обслуговуванні.
Ключові слова: атаки на відмову у обслуговуванні, класифікація атак, комп'ютерна мережа.

Introduction

In today's world the using of computers and computer networks increases every day. Not only mobile devices like smartphones and tables but also smart household appliances – TV-sets, refrigerators, game consoles gained high popularity. One of the most wide-spread threats is Denial-of-Service attack. The Denial-of-Service attack makes impossible system operation and partially or completely disables an access to resources and services for users. It's important to not only detect the fact of attack but also to properly identify attack type to increase effectiveness of DoS-preventing technologies.

To simplify detecting and preventing Denial-of-Service attacks a clear good-structured classification of the DoS attacks is required. Currently there are a lot of different classifications of DoS attacks, the basic is Mirkovic's classification [1] but there is still no good classification adapted for today's features and trends with a possibility to use with real systems.

Proposed Classification

The main proposed classification criteria is listed below (Fig. 1). By the amount of source devices – DoS attacks can be divided into simple DoS attacks, group DDoS attacks (with up to 100 devices) and massive DDoS attack (more than 100 devices). According to this preventing ways should be different. For simple DoS or group DDoS it's enough to simply block packets from attacking sources using black list. For massive DDoS it's difficult to block every source of attack manually and not to block legitimate users from accessing the resource.

According to attack source computers belonging to malicious attacks can be divided into voluntary attacks from intruder's machines, attacks that use bot networks, attacks that use physical and virtual dedicated servers, tunnelled attacks and random users' attacks.

If the sources of attack are dedicated servers network traffic can be huge even when the amount of sources is tiny because dedicated servers usually have network speeds over 1Gb/s. When preventing the tunnelled attacks it's important to consider that tunnels can be used both by intruders and legitimate users simultaneously. Detecting the difference between legitimate tunnelled traffic and malicious one can be a challenge. Bot network attacks usually can be deterined by the same kind of traffice becayse all bots do the same things.

Attacks from bot networks can be divided into attacks that use infected servers, infected home computers and mobile devices. It's important to know that mobile devices' IP address is not constant and can be changed every time user connects to different wireless network. When bot network constists from infected servers the amount traffic can be very huge and the speed of attack can be much higher because servers often have gigabit channels.

By the list of source computers DoS attacks can be divided into static-listed (fixed list of computers), controlled dynamic-listed (list of attacking sources constantly changes but there is a list of possible attack sources somewhere, for example Tor nodes list or list of users of IRC channel) and dynamic unlisted (there is no way to constantly determine the list of attack sources). IRC is very popular between so called «Anonymous» group and it's a good idea to check popular hacking-related IRC servers like OnionIRC to determine if it is it.

By the triggering attacks can be divided into manual (when attacker manually crafts each required packed), controlled (when distributed attack is remotely controlled) and automatic (when the attack is triggered without manual actions).Controlled attacks can be divided by the way of controlling into direct-controlled attacks (attack is controlled from the single point and infected computers has open ports that allows to identifyfy them) and indirect-controlled (attack is controlled with reverse-connections or additional protocols like BitTorrent or IRC) [5].

Attacks can also be divided by the geographical position of sources into local (regional) and worldwide. It's useful for better recognizing legitimate traffic.

By spread in time attacks can be divided into real-time attacks which action «just now» and scheduled attacks that can change during the time of attack or be planned to change during a period of time.

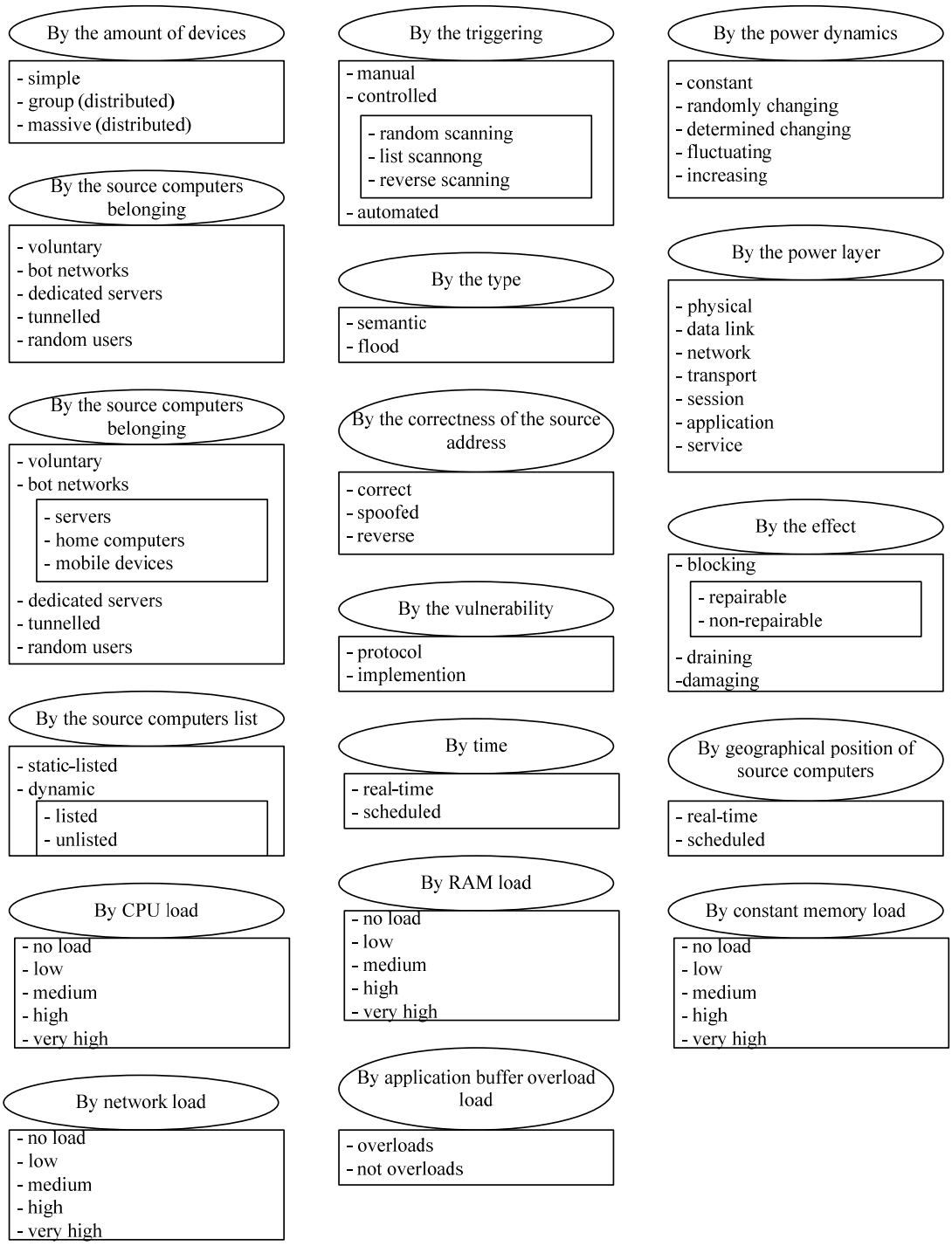

Fig. 1. Classification of DoS-attacks

Direct-controlled attacks can be divided by the way that infected computers are added into network into: random scanning (attacker randomly scans IP-addresses looking for infected computers), list scanning (attacker uses the list of infected machines) and reverse-scanning (infected machines notify the attacker themselves).

By the vulnerability type attacks can be divided into semantic (use the features of network protocol or applications) and flood (floods and overloads with a large amount or size of packets). By the correctness of the source address attacks can be divided into: attacks with correct source addresses (it's possible to determine the source of the attacking machine), spoofed attacks (the source address in packets is malformed) and reverse-attacks (use servers' replies for attacking, for example DNS. It seems that the legal service attacks when really just it's just responding to incorrectly formed queries).

By the power dynamics attacks can be divided into the attacks with constant power, attacks with randomly changing power, attacks with determined changing power, attacks with fluctuating power and attacks with increasing power.

By the layer attacks can be divided into attacks on physical layer (physical intrusion into a computer system, a cable break, radiation), attacks on the data link layer [4] (overloading on the frame layer), attacks on the network level (attacks on the IP protocol layer), attacks on the transport layer (attacks on the layer of datagrams and

segments), attacks on the session layers (attacks inside of logical connections), application level attacks [3] (attacks on the application protocols like HTTP or FTP) and attacks on services (attacks on the application that runs on top of the application layer, for. example cloud service or web framework) [6].

It's important to note that then higher the layer of the attack is than less services are damaged. Physical ot data link layer attack can disable all the network but the application layer attack can only slow down or make inaccessible for users the web server with all websites. The application layer attack is the less dangerous and can only disable an end-user application for example a web application or service.

By the effect attacks can be divided into blocking attacks (as a result it's impossible to connect to service for users), draining attacks (attacks drain a lot of network or CPU resources but the service remains available) and damaging attacks (they damage an attacking component for example a cache or file system and as a result the data can be lost).

Blocking attacks can be divided into repairable and non-repairable. Attack is repairable when the service becomes available again after the attack stops without any manual actions. By the type of the vulnerability attacks can be divided into protocol attacks and current implementation attacks. Direct-controlled attacks can be divided by the way that infected computers are added into network into: random scanning (attacker randomly scans IP-addresses looking for infected computers), list scanning (attacker uses the list of infected machines) and reverse-scanning (infected machines notify the attacker themselves). By the vulnerability type attacks can be divided into semantic (use the features of network protocol or applications) and flood (floods and overloads with a large amount or size of packets). Semantic attacks can sometimes be prevented just with software update or proper reconfiguration but the uncontrolled professional massive flood attacks can be prevented only by increasing the hardware power and network channel or using load-balancing or professional specialized anti-DDoS services.

By the correctness of the source address attacks can be divided into: attacks with correct source addresses (it's possible to determine the source of the attacking machine), spoofed attacks (the source address in packets is malformed) and reverse-attacks (use servers' replies for attacking, for example DNS. It seems that the legal service attacks when really it's just responding to incorrectly formed queries).

Attacks with spoofed source address are very dangerous because it's quite difficult to identify the true source address of the attacker and it's important not to block legitimate users. Reverse attacks became very popular few years ago and are even more difficult to prevent because if the attacker use BitTorrent-tracker or DNS server the attack even from the single attacking computer can be very powerful because DNS servers are designed to deal with very large amount of queries and torrent tracker can has thousands or even millions of users connected at the same time and they can send a lot of traffic to victim machine [7].

By the power dynamics attacks can be divided into the attacks with constant power, attacks with randomly changing power, attacks with determined changing power, attacks with fluctuating power and attacks with increasing power.

By the layer attacks can be divided into attacks on physical layer (physical intrusion into a computer system, a cable break, radiation), attacks on the data link layer [8] (overloading on the frame layer), attacks on the network level (attacks on the IP protocol layer), attacks on the transport layer (attacks on the layer of datagram and segment), attacks on the session layers (attacks inside of logical connections), application level attacks [9] (attacks on the application protocols like HTTP or FTP) and attacks on services (attacks on the application that runs on top of the application layer, e.g. cloud service or web framework) [10].

It's important to note that than higher the layer of the attack is than less services are damaged. Physical of data link layer attack can disable the entire network but the application layer attack can only slow down or make inaccessible for users the web server with all websites. The application layer attack can only disable an end-user application e.g. a web application or service as well as protection mechanism.

Application layer attacks quickly gains popularity as the result of high popularity of mobile applications that are often built on top of the Web and use HTTP-based queries such as JSON. By the effect attacks can be divided into blocking attacks (as a result it's impossible to connect to service for users), draining attacks (attacks drain a lot of networks or CPU resources but the service remains available) and damaging attacks (they damage an attacking component for example a cache, file system or protection mechanisms and as a result the data can be lost). Blocking attacks can be divided into repairable and non-repairable. Attack is repairable when the service becomes available again after the attack stops without any manual actions. By the type of the vulnerability attacks can be divided into protocol attacks and current implementation attacks.

Examples of using the proposed classification

The application of this proposed classification is an identification of the DoS-attack using proposed methods. For example, here is the identification and comparison of some types of DoS attacks (Table 1).

At first, Slowloris attack. By the amount of devices it's usually a single device attack or group attack because usually it's enough to use the single device to block access to webserver. By the source computer it's usually voluntary. Because of using a single computer it's a static-listed manually triggered attack. It's a semantic type of attack because it doesn't use any types of flood but just exceeds the limit of opened connections. The source address it's correct because web server should respond to request. The vulnerability there is in the implemention, not in HTTP protocol. Only some web servers are affected, for example Apache. By power dynamics it's a constant attack. It doesn't overload anything like CPU or RAM. It's an application-level attack (on HTTP server) [7]. By the effect the attack is repairable blocking because after the end of attack the web server will automatically resume its normal

functioning.

DoS attacks, usually flood and lower-layer attacks can also be divided by the the resouces they drain. In the most cases massive overusing of the single type of resource can trigger draining of other resource types. For example, overusing RAM will trigger using of swap files or partition which will heavily uses system's hard drive which can trigger web server cache overloading on poorly configured systems. The main types of drained resources are CPU, RAM, HDD, network and local application buffer (for example an amount of queries or opened connections that application can handle at the single moment of time). So it's important to determine the usage of each type of resource and determint if local application buffer is overloaded.

Here is another example: the attack that is used by so called «Anonymous» group. By the amount of devices it's a group or massive attack depending on the quantity of «operation» members. The computers belong to voluntaries. Their attacks are usually tunneled because Anonymous moderators recommend to use paid VPN services. Source computers are usually listed on the IRC server [8]. It's a controlled attack. By type its flood attack usually using ICMP or TCP protocol. Source addresses are corrected or spoofed but not reversed. The vulnerable is implemention because attacked websites are not designed to handle such a big amount of traffic. By the power dynamics attack is usually increasing until the end of the «operation». The layer of the attack can be different but usually network, session or application. By the effect it's non-repairable blocking.

Table 1

Comparisons of DoS-attacks

	Slowloris	Flood	Google Spreadsheet bug	DC++ bug
By amount of devices	Single or group	Massive or group	Group	Massive
By the source computer belonging	Voluntary	Voluntary	Dedicated servers	Home computers botnet
By the source computers list	Static-listed	Dynamic-listed	Static	Dynamic-listed
By time	Real-time	Real-time	Real-time	Real-time
By the triggering	Manually triggered	Direct-controlled	Manually triggered	Direct-controlled
By the correctness of the source address	Correct	Tunneled	Correct	Correct
By the vulnerability	Implemention	Implemention	Implementation	Protocol
By the type	Semantic	Flood	Flood	Flood
By power dynamics	Constant	Increasing	Constant	Fluctuating
By the power layer	Application	Network, session, application	Application	Application
By the effect	Repairable blocking	Non-repairable blocking	Non-repairable blocking	Repairable-blocking or draining
By time	Scheduled	Real-time	Scgeduled	Real-time
By the geographical position	The single point	Worldwide or regional	The single point	Wordlwide or regional (depending on DC++ hub users)
By CPU load	No load	Medium load	High load	Low load
By RAM load	No load	Low load	High load	Low load
By constant memory load	No load	No load	Low load	No load
By network load	No load	Very high load	Low load	Very high load
By local application buffer overload	Overloaded	Not overloaded	Not overloaded	Not overloaded

One of the very interesting attacks was an attack using Google Spreadsheet service. Because of the bug in this application Google bot tried to download image from website 1000 times and it was a quite powerful HTTP-GET DoS attack [9]. By the amount of devices it was a group devices attack (a group of Google servers). The source computers were a kind of dedicated servers. The source list was static and it was a list of Google FeedFetcher bot servers. The attack was triggered manually. By the type it was flood attack, the source of attack was correct (Google servers). There was vulnerability in implementation. By the power dynamics the attack was constant. By the level it was application-layer attack. The effect was non-repairable blocking of the website, high CPU and RAM load [10]. Another interesting example is DoS attack based on a bug in old peering file-sharing network DC++ protocol version that can make a lot of connected peers attack victim's IP address. This attack is massive and it is a kind of bot network. The list of attacking machines is dynamic and it is available on vulnerable DC++ hub. It's controlled attack, the source addresses are correct on protocol with fluctuating (as users join and leave hub fluctually)

dynamics. The attack layer is application-layer. By the effect it can be draining or even repairable blocking, by type – flood [11]. This type of attack makes very heavy network load and medium CPU load.

The proposed classification allows determining the single attack or a group of similar attacks just by analyzing the attack by proposed criteria. For example, if the attack if performed by single voluntary static-listed computer, it's manually triggered, the source address is connect, it's semantic and exploits application (implemention), it's constant, repairable blocking scheduling with constant dynamic, performed from the single , overloads local application buffer and doesn't use heavily computers' resources it's a Slowloris attack or similar attack.

It's also possible sometimes to select DoS-preventing methods depending on the proposed criteria. For example flood attack attack with determined geographical position can be prevented by using local restrictions, service-layer attacks can be prevented by fixing the vulnerability in the application and so on.

Summary

There were reviewed and analysed known Denial-of-Service attack classifications in this paper. New modern classification of different types of Denial-of-Service attack depending on different aspects was proposed for future development. Four different DoS-attacks were analyzed using proposed classification for example. Future plans are to complete investigation of different Denial-of-Service attacks and to improve proposed classification. This investigation can be used for future development and research.

References

1. J. Mirkovic "A taxonomy of DDoS attack and DDoS defense mechanisms" (05/20/16). URL: https://www.researchgate.net/profile/Peter_Reiher/publication/2879658_A_taxonomy_of_DDoS_attack_and_DDoS_defense_mechanisms/links/02e7e51d1ce0432910000000.pdf.

2. J. Sah "Impact of DDOS attacks on cloud environment" (05/20/16). URL: http://ijrcct.org/index.php ojs/article/download/276/pdf.

3. J. Yu. "A detection and offense mechanism to defend against application layer DDoS attacks" (05/20/16). URL: https://www.researchgate.net/profile/Xiaoming_Chen17/publication/4314603_A_Detection_and_Offense_Mechanism_to_Defend_Against_Application_Layer_DDoS_Attacks/links/546ee4da0cf29806ec2ebfeb.pdf.

4. V. Gupta. "Denial of service attacks at the MAC layer in wireless ad hoc networks" (05/20/16). URL: https://www.cs.wmich.edu/wise/doc/spins/dos/denial-of-service-attacks.pdf.

5. Z. Chi. "Detecting and blocking malicious traffic caused by IRC protocol based botnets" (05/20/16). URL: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4351531.

6. M. Srivatsa. "Mitigating application-level denial of service attacks on Web servers: A client-transparent approach" (05/20/16). URL: http://researcher.ibm.com/files/us-aruni/TWEBDos.pdf.

7. E. Cambiaso. "Slow DoS attacks: definition and categorization" (05/20/16). URL: http://www.inderscienceonline. com/doi/abs/10.1504/IJTMCC.2013.056440.

8. S. Mansfield-Devine. "Anonymous: serious threat or mere annoyance?" (05/20/16). URL: http://www.sciencedirect.com/science/article/pii/S1353485811700046.

9. D. Hobbs. "Using Spreadsheets as a DDoS weapon" (05/20/16). URL: https://blog.radware.com/security/2012/05/spreadsheets-as-ddos-weapon/.

10. P. Ipeirotis. "The Google attack: How I attacked myself using Google Spreadsheets and I ramped up a $1000 bandwidth bill" (05/20/16). URL: http://www.behind-the-enemy-lines.com/2012/04/google-attack-how-i-self-attacked.html.

11. B Ion. "Dc++ and ddos attacks" (05/20/16). URL: http://www.iiis.org/cds2009/cd2009sci/SCI2009/PapersPdf/ S167TT.pdf.

Рецензія/Peer review : 20.5.2016 р. Надрукована/Printed : 7.6.2016 р.
Рецензент: д.т.н., проф. Мартинюк Т.Б.