Denial-of-Service attacks investigation

Voytovych O.P.[1], Kolibabchuk E.I.[2]

[1] Ph.D., associate professor of Information Security Department, Vinnytsia National Technical University
Khmelnytske shosse str., 95, Vinnytsia, Ukraine, voytovych.op@gmail.com
[2] Student, Information Security Department, Vinnytsia National Technical University
Khmelnytske shosse str., 95, Vinnytsia, Ukraine, alexyuvkovetskyi@gmail.com

Abstract – **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, classification, computer networks*.**

Дослідження атак на відмову у обслуговуванні

Войтович О. П.[1], Колібабчук Е. І.[2]

[1]К.т.н., доцент кафедри захисту інформації, Вінницький національний технічний університет
вул. Хмельницьке шосе 95, м. Вінниця, Україна, voytovych.op@gmail.com
[2]студент кафедри захисту інформації, Вінницький національний технічний університет вул. Хмельницьке шосе 95, м. Вінниця, Україна, alexyuvkovetskyi@gmail.com

***Анотація* — 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, комп’ютерні мережі.

INTRODUCTION

In today's world the using of computers and computer networks increases day on 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 [1]. The Denial-of-Service attack makes impossible system operation and partially or completely disables an access to resources and services for users.

In our time Denial-of-Service attack is one of the most dangerous and popular attacks and it's particularly dangerous when government information resources or critical for national security and people's health services are under such attack [2]. It's also very expensive for large and medium business especially web-based organizations or financial institutions like banks or exchanges.

Denial-of-Service attacks can be divided into 2 groups - actually Denial-of-Service-attacks and Distributed Denial-of-Service attacks. The last group is for attacks that are initiated using more than one network device, usually large amount of attacking devices. Detecting and preventing the Distributed Denial-of-Service attack usually is much more difficult.

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 [3] but there is still no good classification adapted for today's features and trends with a possibility to use with real systems protection.

DOS-ATTACKS CLASSIFICATION CRITERIA

The main proposed classification criteria are 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 attacks (more than 100 devices).

According to this preventing methods should be different. For simple DoS or group DDoS it's enough to simply block packets from attacking sources using e.g. black list. For massive DDoS [4] it's difficult to block every source of attack manually and in the same time 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 machines, attacks that use botnet, 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 much over 1Gb/s [5]. 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.

Attacks from botnets 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.

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).

If the list of source computers is static it's a good idea to simply get this list and put into firewall's blacklist. For dynamic unlisted attacks it's very difficult to determine which IP address would take a part in the attack.

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).

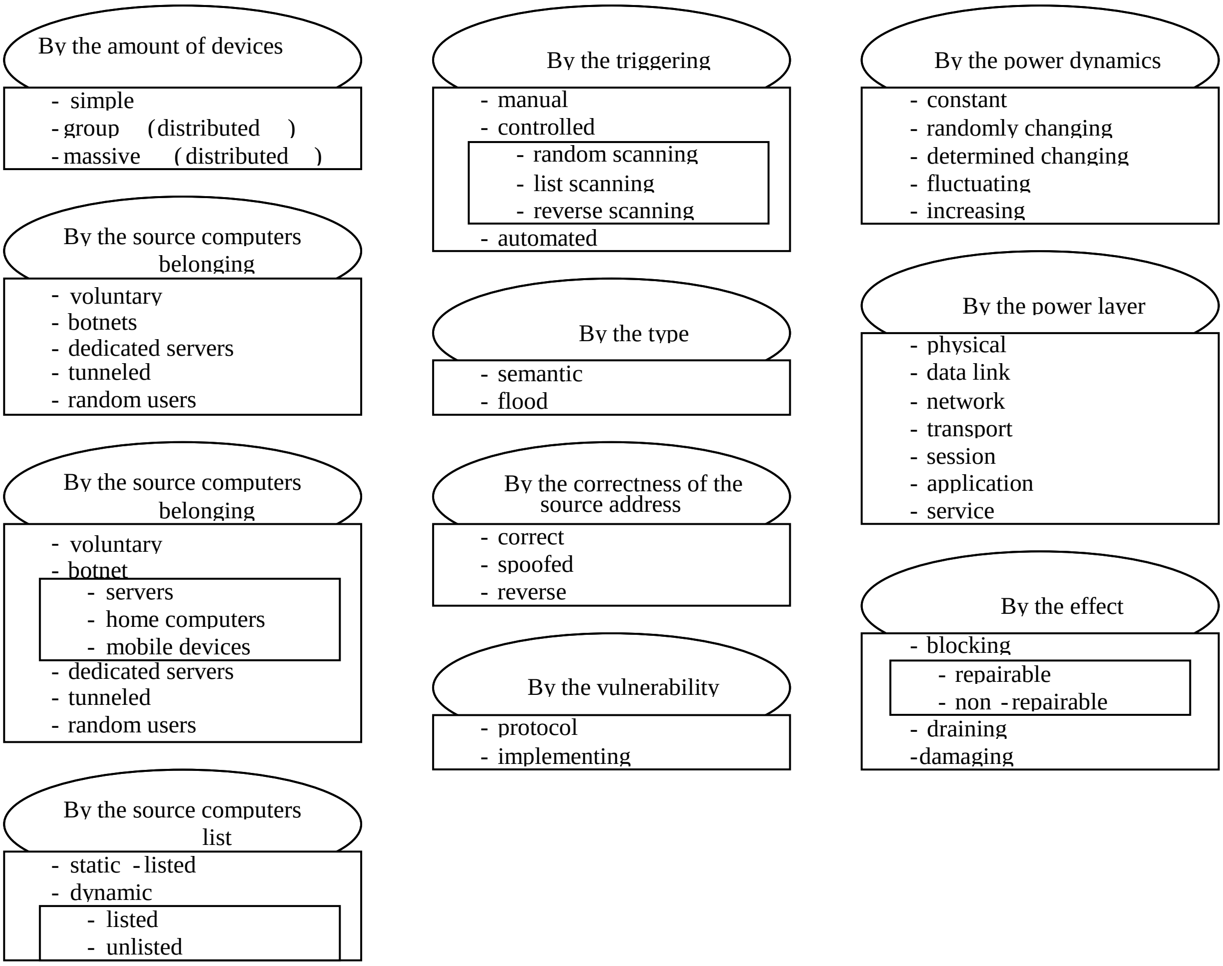

Figure 1 – Classification of DoS-attacks

Controlled attacks can be divided by the way of controlling into direct-controlled attacks (attack is controlled from the single point and infected computers have open ports that allow to identify them) and indirect-controlled (attack is controlled with reverse-connections or additional protocols like BitTorrent or IRC) [6].

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. Revers 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 then 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.

Summary

There were reviewed and analyzed 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.

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] The Future of DDoS Attacks on the Phone Network // Режим доступу до ресурсу: https://www.fraudtechwire.com/the-future-of-ddos-attacks-on-the-phone-network/

[2] Security 101: Distributed Denial of Service (DDoS) Attacks - Security News - Trend Micro USA // Режим доступу до ресурсу: http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/security-101-distributed-denial-of-service-ddos-attacks

[3] Mirkovic J. A taxonomy of DDoS attack and DDoS defence mechanisms / J J Mirkovic, P Reiher // ACM SIGCOMM Computer Communication. – 2004. – Режим доступу до ресурсу : https://www.researchgate.net/profile/Peter_Reiher/publication/2879658_A_taxonomy_of_DDoS_attack_and_DDoS_defense_mechanisms/links/02e7e51d1ce0432910000000.pdf.

[4] Kaspersky Lab. Statistics on botnet-assisted DDoS attacks in Q1 2015 // Режим доступу до ресурсу: https://www.slideshare.net/KasperskyLabGlobal/statistics-on-botnet-assisted-ddos-attacks-in-q1-2015.

[5] Sah JJ. Impact of DDOS attacks on cloud environment / JJ Sah, DLJ Malik // IJRCCT. – 2013. – Режим доступу до ресурсу: http://ijrcct.org/index.php/ojs/article/download/276/pdf.

[6] Z. Chi. Detecting and blocking malicious traffic caused by IRC protocol based botnets / Z. Chi, Z. Zhao // Parallel Computing Workshops. – 2007. – Режим доступу до ресурсу: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4351531.

[7] P. Ferguson. Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing / P. Ferguson. - 2000 – Режим доступу до ресурсу: http://tools.ietf.org/html/rfc2827.html.

[8] V. Gupta. Denial of service attacks at the MAC layer in wireless ad hoc networks / V. Gupta, S. Krishnamurthy // MILCOM. – 2002. – Режим доступу: https://www.cs.wmich.edu/wise/doc/spins/dos/denial-of-service-attacks.pdf.

[9] J. Yu. A detection and offense mechanism to defend against application layer DDoS attacks / J. Yu, Z. Li, H. Chen, X. Chen // Networking and Services. – 2007. – Режим доступу до ресурсу: https://www.researchgate.net/profile/Xiaoming_Chen17/publication/4314603_A_Detection_and_Offense_Mechanism_to_Defend_Against_Application_Layer_DDoS_Attacks/links/546ee4da0cf29806ec2ebfeb.pdf.

[10] M. Srivatsa / Mitigating application-level denial of service attacks on Web servers: A client-transparent approach / M. Srivatsa, A. Iyengar, J. Yin, L. Liu // ACM Transactions on the Web. – 2008. – Режим доступу до ресурсу: http://researcher.ibm.com/files/us-aruni/TWEBDos.pd