IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023

DOI: 10.17148/IJARCCE.2023.12622

Distributed Denial of Service Attacks and Défense Mechanisms

POOJA RAVINDRA KANADE[1], DR. MRS. RAMA BANSODE[2]

P.G. Student, Department of Computer Application, P.E.S. Modern College of Engineering, Pune, Maharashtra, India[1]

Professor, P.E.S. Modern College of Engineering, Pune, Maharashtra, India[2]

Abstract: In networked systems, distributed denial-of-service (DDoS) assaults have proliferated. The extent of the problem is best indicated by the enormous number of variations in both the types of DDoS assaults and their mitigating techniques. This article will analyse current DDoS assaults and the accompanying mitigation strategies. To show the degree of application and effectiveness of the solution techniques, the study tries to highlight the strengths and shortcomings of the existing defences. To accomplish these goals, the study makes the assumption that DDoS attacks may be compared based on similar qualities, which in turn helps to compare defence strategies.

There is a developing issue with distributed denial-of-service (DDoS). It's astonishing how many and how different the defense strategies are from the attackers. Researchers will have a better knowledge of the issue and the available solution space thanks to the paper's presentation of two taxonomies for categorizing attacks and defenses.

The selection of the attack classification criteria was made to draw attention to commonalities and significant characteristics of attack techniques that define problems and guide the development of defenses. The defense taxonomy organizes the corpus of existing DDoS defenses into categories according to design choices, and it then illustrates how these choices determine the benefits and drawbacks of suggested solutions.

I. INTRODUCTION

There are numerous defense techniques that have been proposed to address the issue of distributed denial-of-service (DDoS) assaults, which are a danger to the Internet. To get around these security measures, attackers are constantly changing their tools, while researchers are changing their methods to deal with evolving threats. It is become increasingly difficult to distinguish between the forest and the trees in the rapidly evolving field of DDoS.

This makes it more difficult to explain the DDoS phenomenon, on the one hand. The range of known assaults gives the impression that the problem area is large and difficult to investigate and address. On the other hand, current defense systems use a variety of tactics to combat the issue, making it challenging to comprehend their parallels and divergences, and evaluating the standard chunk of Lorem Ipsum used since the 1500s is reproduced below for those interested. Sections 1.10.32 and 1.10.33 from "de Fin bus Bono rum et Malo rum" by Cicero are also reproduced in their exact original form, accompanied by English versions from the 1914 translation by H. Rackham.

The suggested taxonomies are full in the sense that: The attack taxonomy includes both known attacks and undiscovered but plausible threats that could affect existing defense mechanisms; the defense system taxonomy includes both published strategies and some commercial strategies that are well-documented enough to be analyzed. In addition to classification, we offer illustrative examples of current mechanisms.

Our objective was to identify a few key characteristics of attack and defense mechanisms that may be used as classification criteria to guide researchers in developing creative solutions. Additionally, it was crucial to avoid confusing the reader with an overly intricate and thorough classification. We hope that future researchers will build on our findings in more detail.

Our objective was to identify a few key characteristics of attack and defense systems that may be used as classification criteria for new solutions developed by researchers. Additionally, it was crucial to avoid confusing the reader with a too complex and thorough classification. We are hoping that additional researchers will build on our findings.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023
DOI: 10.17148/IJARCCE.2023.12622

II. METHODOLOGY

DDOS ATTACK OVERVIEW

An explicit attempt to stop the proper usage of a service is what distinguishes a denial-of-service attack [14]. To do this, a distributed denial-of-service attack sends out several attacking entities. This paper focuses primarily on DDoS assaults, which are committed by making the victim receive malicious traffic and then sustain damage as a result.

One frequently exercised manner to perform a DDoS attack is for the attacker to send a stream of packets to a victim; this stream consumes some key resource, thus rendering it unavailable to the victim's legitimate clients. Another common approach is for the attacker to send a few malformed packets that confuse an application or a protocol on the victim machine and force it to freeze or reboot. In September 2002 there was an onset of attacks that overloaded the Internet infrastructure rather than targeting specific victims [55]. Yet another possible way to deny service is to subvert machines in a victim network and consume some key resource so that legitimate clients from the same network cannot obtain some inside or outside service. This list is far from exhaustive. It is certain that there are many other ways to deny service on the Internet, some of which we cannot predict, and these will only be discovered after they have been exploited in a large attack.

DA: Degree of Automation

The processes of Manual, Semi-Automatic, automatic, and use can all be carried either manually or automatically. We distinguish between manual, semiautomatic, and automatic DDoS attacks based on the level of automation.

Manual

The attacker manually searches for vulnerabilities on distant machines, enters them, installs attack code, and then commands the attack to begin. The only DDoS attacks that fit under the manual category were the early ones. The recruitment processes were soon fully automated.

Semi-Automatic

The DDoS network used in semi-automatic attacks is made up of handler (master) and agent (slave, daemon, or zombie) machines. Phases of recruitment, exploitation, and infection are automated.

In the use phase, the attacker instructs agents to transmit packets to the victim and defines the attack type, timing, and victim via the handler.

Automatic

In addition to automating the recruit, exploit, and infect phases, automatic DDoS attacks also include the usage phase. As a result, no contact between the attacker and agent machines is necessary. The attack code has preprogramed parameters for the assault's start time, kind, duration, and victim. Since the attacker is only involved in giving one command—at the beginning of the recruitment process—the deployment procedures of this attack class offer the attacker limited exposure. A single-purpose use of the DDoS network or the rigid design of the system are suggested by the hardcoded attack specification.

A backdoor to the compromised machine is typically left open by the propagation mechanisms, allowing for simple access in the future and the modification of the attack code. In addition, if agents speak to one another via IRC channels.

III. DDOS DEFENSE CHALLENG

Numerous defence techniques have been proposed because of the importance of the DDoS issue and the escalating frequency, sophistication, and power of attacks. However, even though numerous remedies have been created, the issue is barely ever addressed, let alone resolved. What causes this? The development of DDoS defence research is being hampered by several significant problems.

DOI: 10.17148/IJARCCE.2023.12622

Demand for a distributed response at numerous Internet locations. There are numerous potential DDoS attacks, but only a small number of them can be addressed solely by the victim, as was discussed in more detail in the earlier sections. A dispersed, possibly coordinated response mechanism is frequently required. The response must also be spread out across a large portion of the Internet to accommodate a variety of agents and victims. Distributed management of the Internet makes it impossible to enforce or ensure the widespread deployment of any defence system or even network collaboration. Many academics are deterred from even creating distributed solutions because of this.

IV. TAXONOMY OF DDOS DEFENSES

Activation Level

We distinguish between preventive and reactive techniques based on the level of activity of DDoS defiance mechanisms.

Protective

The goal of preventive methods is to either eliminate the possibility of DDoS attacks or to give potential victims the ability to withstand them without interfering with the services provided to legitimate customers.

Prevention

We further categories preventive measures into attack prevention and denial-of-service prevention measures in accordance with the preventative goal.

V.USING THE TAXONOMIES

When creating the taxonomies, we focused on attack and defense mechanism characteristics that, in our opinion, provide crucial information about the gravity and nature of threats as well as the efficiency and cost of defenses. How might one employ these taxonomies?

A diagram of the DDoS research area. These taxonomies provide a thorough overview for new researchers to have a rapid introduction to the DDoS topic. These taxonomies can be extended and used by seasoned researchers to structure and organize their subject-specific information. This ought to result in the discovery of fresh avenues for DDoS research and enhance comprehension of the danger.

Seeking up fresh offensive tactics. In addition to well-known dangers, the attack taxonomy looked at a few tactics used Variable agent set, variable rate attacks, as well as a few cutting-edge attack strategies like growing rate attacks—are attack types that are sporadically used in the field. These novel attacks will become more common as defense mechanisms get more adept at stopping the regular suspects. It will be easier for researchers to stay one step ahead of the attacker if they are aware of these risks, develop them in a test bed setting, and use them to test defense systems.

Generation of DoS benchmarks. The development of assault benchmarks for assessing DDoS defenses is now underway. The assault taxonomy will contribute to the production of complete benchmarks. The defense taxonomy will assist in exposing and identifying common weaknesses of a class of DDoS solutions and in the design of experiments specifically aimed at testing these problems.

A common vocabulary. Researchers frequently use descriptive explanations of complex attack processes or vulnerabilities of a particular solution, except for assaults that are generally recognized (e.g., UDP flood, ICMP flood, etc.). For these conversations, the taxonomies provide a shared language.

designing solutions appropriate to each attack class. The goal of DDoS defenses is typically to be a one-stop solution to all potential attacks. It's not realistic.

improving unstudied scientific topics. The effectiveness of various defense classes against various attack types should reveal untapped areas for further study. (Bug or overload) Vulnerability. This category focuses more While we are interested in examining the entire attack mechanism to emphasize the attack phase itself, characteristics unique to distributed attacks. Flooding is categorized by Hussain as brute-force. DDoS assaults are classified based on the number of agent machines involved and whether the attack was reflected.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023
DOI: 10.17148/IJARCCE.2023.12622

Howard suggests a taxonomy of computer and network assaults in [35] and [36]. This taxonomy emphasizes computer attacks in general rather than the distinctive characteristics of DDoS attacks.

VI. CONCLUSION

A comprehensive understanding of the DDoS issue is hampered by the abundance of attack and defense techniques seen in the DDoS arena. This essay is an initial effort to break through the The knowledge in this topic is structured and obscure. The proposed taxonomies are meant to assist the community in considering the dangers wear comprehensive understanding of the DDoS issue is hampered by the abundance of attack and defense techniques seen in the DDoS arena. This essay is an initial attempt to clarify the confusion and organize the body of knowledge in this area. The proposed taxonomies are meant to stimulate discussion among the community members about the risks we face and potential defenses.

We anticipate that these taxonomies will facilitate simpler research collaboration as one advantage. Attackers work together to organize their agents into coordinated networks with enormous strength and resilience by sharing attack code and knowledge about vulnerable targets. To combat the DDoS threat, the Internet community must work equally well with one another. Communication will be facilitated and a common language for discussing solutions will be provided by effective taxonomies. They will also highlight how various processes are likely to cooperate and point out any areas of weakness that still need improvement.

The need for the research community to create standard measurements and benchmarks for DDoS defense assessment is urgent. These tasks will benefit from the taxonomies' guidance as well.

The suggested taxonomies are far from exhaustive and comprehensive. There will be new attacks, some of which we cannot now foresee. They will emphasize novel aspects for categorization. DDoS defense strategies that are novel will be developed. They will also provide fresh design elements, each with advantages and disadvantages. We anticipate that these taxonomies will serve as a foundation for categorizing threats and countermeasures in the DDoS space. The taxonomies will advance and expand as the field does.

REFERENCES

[1]D. G. Andersen. Mayday: Distributed filtering for internet services. In In Proceedings of 4th Use nix Symposium on Internet Technologies and Systems, March 2003.
[2] D. G. Andersen, H. Balakrishnan, M. F. Kai-shek, and R. Morris. Resilient Overlay Networks. In Proceedings of 18th ACM SOSP, October 2001.
[3] T. Anderson, T. Roscoe, and D. Wetherell. Preventing internet denial-of-service with capabilities. In In Proceedings of Hot Nets II, November 2003.
[4] Arbor Networks.
[5] T. Aura, P. Sikander, and J. Lewi. DOS-Resistant Authentication with Client Puzzles. Lecture Notes in Computer Science, 2133, 2001