International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 31st Mar 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 03

10.48047/IJIEMR/V12/ISSUE 03/92

Title **A STUDY ON SECURITY ISSUES RELATED TO DISTRIBUTED DENIAL-OF-SERVICE (DDOS) ATTACKS ON COMPUTER SYSTEMS**

Volume 12, ISSUE 03, Pages: 634-639

Paper Authors
Nidamanuru Srihari Rao, Nidamanuru Sravya Varshini, Koriginja Bhasker, K. Surendra, Ummadisetty Narasimhulu

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

A Study on Security Issues Related to Distributed Denial-of-Service (DDoS) Attacks on Computer Systems

Nidamanuru Srihari Rao[1], Professor, Department of CSE, Bharat Institute of Engineering and Technology, Hyderabad
Nidamanuru Sravya Varshini[2], B.Tech. Student, CSE Branch, Andhra Loyola Institute of Engineering and Technology, Vijayawada
Koriginja Bhasker[3], Assistant Professor, Department of IT, Bharat Institute of Engineering and Technology Hyderabad
K. Surendra[4], Assistant Professor, Department of CSE, Bharat Institute of Engineering and Technology, Hyderabad
Ummadisetty Narasimhulu[5], Assistant Professor, Department of CSE, Bharat Institute of Engineering and Technology, Hyderabad

Abstract
Today, Internet is facing a lot of security attacks directly or indirectly. DDoS attacks are amongst the most important category of attacks, because these attacks involve no stealing of information, but result in high financial losses and loss of reputation to particular web services provided by commercial firms. In this context, we conducted a study on security issues against DDoS attacks for the computer systems.

Keywords: Security attacks, Security Services, DoS attacks, DDoS Attacks, Security issues, Computer Systems.

Introduction

With the development of advanced computers, the need for fully automated processes and tools for securing files and other data/information stored on the computers became evident. This is particularly the case for a system that is publicly shared, such as a time-sharing system, and the need is even more severe for systems that can be accessed over a public telephone network, data network, or the Internet. Computer security is the general name given for the assemblage of tools designed to secure data/information and to impede hackers. Security measures are needed to secure data/information during their transmission over the Internet. Internet security measures are needed to prevent, deter, detect, and correct security violations that involve the transmission of data/information [1]. From this point onwards we mention a single word "data" instead of the pair data/information as data can be generously used to mean both. While designing and developing a specific security algorithm or mechanism, one must carefully consider threats or possible attacks on features of security. Generally or in many cases, successful attacks are modelled or designed by considering the problem in a completely different perspective, therefore utilizing an unanticipated weakness in the mechanism.

Classification of Security Attacks

Passive attacks and active attacks are two helpful categories for categorising security attacks [1]. The resources of the system are not affected by a passive attack, which tries to gather or use information from it. An active attack makes effort to change system resources or impair their functionality.

Eavesdropping or transmission monitoring are the kind of attacks that are considered passive. The opponent's objective is to obtain the transmitted information. Traffic analysis and message content disclosure are two examples of passive attacks. Sensitive or confidential information may be included in phone conversations, emails, and files that are transmitted. We want to keep the contents of these transmissions from being discovered by an adversary. Traffic analysis is a subtler second category of passive attack. Imagine if there was a mechanism to conceal the information included in messages or other information flow, preventing adversaries from extracting the data from communications even if they intercepted them. Encryption is a widely used method of disguising contents. An adversary might still be able to determine the pattern of these messages even if we have encryption protection in place. The adversary could identify and pinpoint the hosts that were in communication, as well as track their frequency and message length. With this information, one might be able to infer the type of conversation that was occurring. Because there is no data modification involved, passive attacks are exceedingly challenging to identify. The success of these attacks can, however, be limited, usually through the use of encryption. As a result, prevention rather than detection is the key to dealing with passive attacks.

Masquerade, replay, message modification, and denial of service are the four subcategories of active attacks, which entail some alteration of the data stream or the generation of a false stream. When one thing impersonates another, it's called a masquerade. One of the other active attack types is typically included in a masquerade attack. For instance, authentication sequences can be recorded and replayed after a successful authentication sequence, allowing an authorised entity with limited privileges to impersonate an entity with those privileges to get additional privileges. Replay entails passively capturing a data unit and retransmitting it to have an unauthorised effect. A message is simply modified to achieve an unlawful effect if some of its original content is changed, a message is delayed, or a message is rearranged. The management or regular usage of communications infrastructure are prevented or impeded by the denial of service. An attack may be focused at a specific target; for instance, an entity may suppress all messages sent to a certain location (e.g., the security audit service). Another type of service denial is when an entire network is disrupted, either by turning it off or by sending it too many messages, which lowers its performance. Attacks that are active exhibit the opposite traits of those that are passive. Although passive attacks are challenging to identify, there are ways to stop them from succeeding. On the other hand, it is very challenging to completely thwart active attacks because doing so would need constant physical security of all communication facilities and pathways. Instead, the objective is to identify them and to recover from any delays or disruptions they may cause. The detection may also aid in prevention because it has a deterrent effect.

Security Services

A system's security service is a processing or communication service that it offers to provide a particular level of protection for system resources. Security mechanisms and security services put security policies into practice. These services are separated into fourteen distinct services and five categories by X.800. Assuring the authenticity of a transmission is what the authentication service does. The purpose of the authentication service in the event of a single communication, such as a warning or alarm signal, is to reassure the recipient that the message is from the source that it purports to be from. There are two factors at play when there is an ongoing interaction, such as when a host and a terminal are connected. Initially, the service confirms that the two entities are legitimate, i.e., that each is the entity that it represents, at the moment of

connection initiation. Second, the service must guarantee that the connection is not disrupted in such a way that a third party can pose as one of the two legitimate parties in order to transmit or receive data that is not authorised. Peer entity authentication and data origin authentication are the two distinct authentication services that are defined in the standard. Access control refers to the capacity to restrict and regulate the access to host systems and applications via communications channels in the context of network security. To accomplish this, each entity attempting to get access must first be identified, or authenticated, in order for access rights to be personalised for the user.

Data transmissions are shielded from passive threats by confidentiality. Many tiers of protection can be distinguished with regard to a data transmission's content. The most comprehensive service safeguards all user information sent back and forth between two users over time. This service can also be defined in more specialised ways, for as by protecting just one message or perhaps just a few message fields. Security against traffic flow analysis is the other part of confidentiality. This necessitates that an attacker be unable to see the origin and destination, frequency, duration, or other aspects of the traffic on a communications facility. Like confidentiality, integrity may be applicable to a single message, a stream of messages, or particular fields within a message. Again, complete stream protection is the most practical and simple strategy. Both the sender and the recipient are unable to retract a communicated communication thanks to nonrepudiation. As a result, when a communication is sent, the recipient can demonstrate that the purported sender actually did send the message. Similar to how a message is sent, the sender can demonstrate that the message was indeed received by the claimed recipient.

If a system responds to user requests for services in accordance with the system design, it is said to be available. The loss of or reduction in availability may be caused by a number of attacks. While some of these attacks can be stopped or recovered from using automated defences like authentication and encryption, others necessitate taking physical action to restore availability of dispersed system components. The availability of different security services is treated as a property in the X.800 standard. A service that guarantees system availability is known as an availability service. The security issues brought up by denial-of-service attacks are addressed by this service [2]. It is dependent on proper system resource management and control, which in turn depends on access control services and other security services. The methods can be further broken down into those that are implemented in a particular protocol layer and those that are not protocol layer- or security service-specific at all. Reversible and irreversible encipherment mechanisms are distinguished by the X.800 standard. An encryption procedure that enables data to be encrypted and then later decrypted is known as a reversible encipherment mechanism. Hash algorithms and message authentication codes are examples of irreversible encipherment techniques that are utilised in digital signature and message authentication applications.

Denial-of-Service (DoS) Attacks

An attempt to stop authorised users of a service from utilising it is known as a denial of service (DoS) attack. Early DoS attacks were competitive underground hacker games. By bringing down well-known websites, attackers could gain notoriety in the underground community. Normal computer users can also become DoS attackers because simple DoS programmes like Trinoo are readily available online for download. They

occasionally launched coordinated DoS assaults against organizations whose policies they disapproved of in order to voice their opinions. DoS attacks also showed up in unlawful activities. DoS attacks may be used by businesses to eliminate their rivals in the market. DoS attacks used for extortion have increased recently. Online businesses were threatened with DoS attacks, and attackers demanded payment for security.

Distributed Denial-of-Service (DDoS) Attacks

Known DoS attacks on the Internet often defeat the target by depleting its resources, which can include link bandwidth, TCP connection buffers, application/service buffers, CPU cycles, etc. linked to network computing and service performance. Individual attackers may also use vulnerabilities to access target servers, disrupt services, and then leave. Many recent denial-of-service (DoS) attacks were launched via a huge number of distributed assaulting sites in the Internet since it is challenging for attackers to overload the target's resource from a single computer. DDoS (distributed denial of service) attacks are what these are. In a DDoS attack, the victim may be forced to severely reduce the performance of its services or possibly cease providing any services because the aggregation of the attacking traffic might be very large in comparison to the victim's resources. DDoS attacks are more complicated and difficult to stop than traditional DoS attacks, which may be stopped by tightening service system security or forbidding unauthorised local or remote access. It is difficult to identify the assaulting hosts and take an action against them since a large number of unintentional hosts are involved in DDoS attacks. Due to the rapid increase in computer vulnerabilities that let attackers to access many machines and install different assaulting tools, DDoS attacks have become more frequent, sophisticated, and severe in recent years. Because mobile nodes (like laptops, cell phones, etc.) share the same physical media for transmitting and receiving signals and because mobile computing resources (like bandwidth, CPU, and power) are typically more limited than those available to wired nodes, wireless networks are also susceptible to DoS attacks. Forging, altering, or injecting packets into a wireless network makes it simple for a single attacker to break off connections between legal mobile nodes and produce DoS effects.

There are two ways to initiate a DDoS attack. The first method involves delivering malicious packets to a target in order to take advantage of software flaws and crash the system [3]. The second method involves flooding the target machine's computational or communication resources with a large number of legitimate-looking but garbled packets in order to prevent it from serving its legitimate users. Network bandwidth, disk space, CPU time, data structures, network connections, and other resources are all consumed by attacks. While the first form of attack can be protected by patching known vulnerabilities, the second form of assault is more difficult to stop. The targets are vulnerable to assault just by virtue of their public Internet connection.

Security Issues Against Distributed Denial-Of-Service (DDoS) Attacks

Design of an effective DDoS defense system faces many challenges. The large number of attacking machines and use of source-address spoofing prevent identification of malicious streams and their originators. Thus, filtering and traceback of the attack traffic is extremely difficult. Additionally, the availability of vast numbers of insecure machines connected to the Internet provides fertile ground on which to acquire new attack zombies using automated infection tools. Since securing every machine on the Internet is

impossible, we need effective defense mechanisms that can detect attacks and withstand or respond to them. Similarities between attack and legitimate traffic hinders early attack detection (before denial-of-service is achieved) and classification of malicious flows [4,5]. Many defense systems thus take indiscriminate actions, blocking or limiting all traffic, legitimate and attack alike, to the victim. While this stops the attack and relieves the victim, it inflicts collateral damage and denies service to some legitimate clients., we must still keep in mind The original goal to be kept in our minds while designing DDoS defenses to prevent these disturbances is to guarantee continued communication between well-behaved participants in the presence of attacks.

To identify DDoS floods in the network, detection technologies that operate at the network level already exist. Several detection techniques aim to detect intrusions on the host and network levels. A system that uses CAPTCHAs—an acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart"—has already been developed to defend a web cluster against DDoS attacks [6]. Sadly, forcing customers to solve graph puzzles runs the risk of irritating users and adding further service delays for legitimate users. This also prevents web crawlers from accessing the site, which may prevent search engines from indexing the content. As a defence mechanism against DDoS attacks, rate-limiting unwanted or hostile traffic is frequently utilized. Several plans for routers to work together to stop malicious traffic have already been put out at the infrastructure level. Another approach is one in which clients would ask routers for capabilities before being permitted to send traffic. Many of the above strategies are oriented towards fighting high bandwidth flows. In contrast, we can stop assaults on network bandwidth as well as those directed at other sorts of system resources, like CPU or storage, by rate limiting the work a server cluster does.

Conclusion

DDoS attacks cause severe degradation to the service availability of Web Servers. Though the context for the security concern against the DDoS attacks is insignificant in India at present, it is definitely going to be a technology topic for consideration in near future. In this context, we explored this topic deeply and succeeded to come up with a review of the same. Our future work is going to be the study of DDoS attack impacts on various types of Computer Network establishments.

Acknowledgment
We thank the BIET, Hyderabad Management and ALIET, Vijayawada Management for giving necessary support and encouragement in moulding our research work and producing this paper wonderfully.

References

[1] Cryptography and Network Security by William Stallings, Fourth Edition, Pearson Education 2007.
[2] Krishan Kumar, R.C. Joshi, and Kuldip Singh, “An Integrated Approach for Defending Against Distributed Denial-of-Service (DDoS) Attacks”, IRISS 2006, IIT Madras.
[3] B.B. Gupta, R.C. Joshi, and Manoj Misra, “Distributed Denial of Service Prevention Techniques”, International Journal of Computer and Electrical Engineering, Vol. 2, No. 2, April, 2010, pp.268-276.
[4] J. Jung, B. Krishnamurthy, and M. Rabinovich, “Flash crowds and denial of service attacks: Characterization and implications for CDNs and web sites,” presented at theWorldWideWeb Conf., Honolulu, HI, May 2002.
[5] S. Ranjan, R. Swaminathan, M. Uysal, and E. Knightly, “DDoS-resilient scheduling to counter application layer attacks under imperfect detection,” presented at the IEEE INFOCOM, Barcelona, Spain, Apr. 2006.

[6] Supranamaya Ranjan, Ram Swaminathan, Mustafa Uysal, Antonio Nucci, and Edward Knightly, "DDoS-Shield: DDoS-Resilient Scheduling to Counter Application Layer Attacks," IEEE/ACM Transactions on Networking, Vol.17, No.1, Febraury, pp.26-39, (2009).