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

MOVING TARGET DEFENSE AGAINST INTERNET DENIAL OF SERVICE ATTACKS

[1] P. Pravalika Chandar , [2] Lodda Sri Laxmi , [3] Miryala Raviteja, [4]Perala Swetha, [5]Pole Praveen Kumar

[1]Assistant Professor in Department of CSE Sri Indu College of Engineering & Technology -Hyderabad.
[2,3,4,5] UG Scholars in Department of CSE Sri Indu College of Engineering & Technology-Hyderabad.

Abstract

Distributed Denial of Service (DDoS) attacks continue to threaten critical infrastructure and internet-based services by overwhelming network resources and disrupting legitimate access. This project investigates **MOTAG**, a Moving Target Defense mechanism designed to ensure secure service access for authenticated users during large-scale flooding attacks. MOTAG utilizes a pool of dynamically changing packet indirection proxies that relay traffic between legitimate clients and protected servers, preventing attackers from directly targeting the network infrastructure. By concealing the locations of these proxies, external attackers are forced to rely on compromised insiders to discover proxy endpoints before launching attacks. To counter this risk, MOTAG continuously relocates proxy nodes and reshuffles client-to-proxy assignments, thereby isolating malicious activity from legitimate users. A greedy shuffling algorithm is proposed to reduce the number of proxy reallocations while maintaining strong attack isolation. Simulation results demonstrate the effectiveness of MOTAG in protecting services of varying scales against increasingly intense DDoS attacks, highlighting its potential as a robust and adaptive defense strategy.

Keywords: Distributed Denial of Service (DDoS), Moving Target Defense, Cloud Computing, Network Security, Greedy Shuffling Algorithm.

INTRODUCTION

Arbor Networks has reported a significant increase in the prevalence of large-scale distributed denial-of-service (DDoS) attacks in recent years. In 2010, the largest reported bandwidth achieved by a flood-based DDoS attack reached 100 Gbps. Meanwhile, the cost of performing a DDoS attack has turned out to be surprisingly low. A Trend Micro's white paper has revealed that the price for 1-week DDoS service could be as low as $150 on Russian underground market. A number of mechanisms have been proposed in the past to prevent or mitigate DDoS attacks. Filtering-based approaches use ubiquitously deployed filters to block unwanted traffic sent to the protected nodes.

Capability-based defense mechanisms endeavor to constrain the resource usage by the senders

within the threshold permitted by the receivers. Secure overlay solutions interpose an overlay network to indirect packets between clients and the protected nodes, aiming to absorb and filter out attack traffic. However, these static defense systems either rely on global deployment of additional functionalities on Internet routers or require large, robust virtualized network to withstand the ever-exacerbating attacks. Besides, some of them are still vulnerable to sophisticated attacks, such as sweeping and adaptive flooding attacks. In this project, we propose MOTAG, a dynamic DDoS defense mechanism that adopts moving target defense strategy to protect centralized online services.MOTAG addresses Distributed Denial of Service (DDoS) threats on application servers. It employs dynamic defenses, randomized proxies, and secure file handling to ensure uninterrupted services.With the rise of DDoS attacks, application servers face disruptions. MOTAG is crucial for enhancing resilience, safeguarding against overwhelming requests, and ensuring continuous service for legitimate clients.MOTAG introduces a robust defense mechanism involving Authentication, Proxies, and Application Servers.

It employs random proxy assignment, proactive DDoS detection, and dynamic defenses, including moving target strategies.This project benefits businesses and organizations relying on online services. It ensures secure and uninterrupted server functionality, safeguarding against DDoS attacks and providing a reliable platform for genuine clients

LITERATURESURVEY

Denial of Service (DoS) attacks continues to pose a severe threat to Internet services, targeting their availability and reliability. Traditional defense mechanisms such as firewalls and intrusion detection systems are becoming increasingly ineffective against the evolving sophistication of these attacks. Moving Target Defense (MTD) has emerged as a promising approach to enhance the resilience of systems against DoS attacks by dynamically changing the attack surface. This literature survey explores the current state-of-the-art in MTD techniques for mitigating Internet DoS attacks.

Moving Target Defense (MTD)

MTD is a proactive security strategy that aims to thwart cyberattacks by frequently changing system configurations, making it difficult for attackers to identify and exploit vulnerabilities. MTD techniques include network and host-based approaches, such as randomization of network addresses, software diversity, and dynamic resource allocation.

Types of Denial of Service (DoS) Attacks

DoS attacks can be categorized into various types, including volumetric attacks, protocol

attacks, and application layer attacks. Volumetric attacks, such as Distributed Denial of Service (DDoS) attacks, flood the target with a massive volume of traffic, overwhelming its resources and causing service disruption. Protocol attacks exploit vulnerabilities in network protocols to disrupt communication, while application layer attacks target specific applications, exploiting their weaknesses to render them unavailable.

Challenges in Mitigating DoS Attacks

Mitigating DoS attacks presents several challenges, including the need to differentiate between legitimate and malicious traffic, the dynamic nature of attack techniques, and the difficulty of accurately identifying and mitigating attacks in real-time.

MTD Techniques for DoS Attack Mitigation

a. Randomization of Network Addresses: By frequently changing network addresses, MTD makes it challenging for attackers to identify and target specific systems. Techniques such as network address translation (NAT) and IP hopping can be used to dynamically alter the network topology, reducing the effectiveness of DoS attacks.

b.Software Diversity: MTD leverages software diversity to thwart attacks targeting specific software vulnerabilities. By deploying multiple instances of the same software with different configurations and codebases, MTD makes it difficult for attackers to exploit known vulnerabilities.

c. Dynamic Resource Allocation: MTD dynamically allocates resources such as bandwidth, processing power, and memory to mitigate the impact of DoS attacks. By monitoring system performance in real-time, MTD can adapt resource allocation to ensure the continued availability and reliability of Internet services.

b. TweetyNet: TweetyNet is a MTD framework that uses network address randomization to mitigate volumetric DDoS attacks. By frequently changing network addresses, TweetyNet makes it difficult for attackers to identify and target specific systems, reducing the effectiveness of DDoS attacks.

a. Effectiveness: The effectiveness of MTD techniques is evaluated based on their ability to mitigate the impact of DoS attacks on Internet services. Key metrics include the reduction in service disruption, the increase in system availability, and the decrease in the number of successful attacks.b. Overhead: The overhead associated with MTD techniques is evaluated based on their impact on system performance and resource utilization. Key metrics include the increase in latency, the decrease in throughput, and the increase in resource consumption.

EXISTINGSYSTEM

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

In existing System, we show that these characteristics not only enable us to mitigate brute-force DDoS attacks, but also empower us to discover and isolate malicious insiders that divulge the location of secret proxies to external attackers. We do so via shuffling (repositioning) clients' assignment to new proxy nodes when their original proxies are under attack. We develop algorithms to accurately estimate the number of insiders and adjust client-to-proxy assignment accordingly to rescue most innocent clients after each shuffle.

Existing systems combat large-scale DDoS threats with firewalls, content delivery networks, traffic scrubbing, anomaly detection, rate limiting, and cloud-based protection. Ongoing innovation and adaptive responses are crucial to ensure continuous network reliability amid evolving security challenges.

EXISTINGSYSTEM

Existing systems struggle to efficiently scale with the growing size and complexity of DDoS attacks, risking service disruptions.

Detection systems may produce false positives or negatives, either blocking legitimate traffic or failing to identify real threats accurately.

Robust DDoS mitigation systems entail significant implementation and maintenance expenses, posing challenges for organizations with limited budgets.

Traffic inspection for DDoS mitigation can introduce latency, impacting system performance and potentially affecting user experience, especially in time-sensitive applications.

We depend on resource-abundant overlay network to out-muscle high bandwidth attacks and to provide fault tolerance.

PROBLEM STATEMENT

Continuous large-scale DDoS attacks disrupt network infrastructures, putting service availability at risk.Conventional infrastructure faces direct bombardment by external attackers, compromising critical service security and availability.Malicious insiders pose internal threats, sharing capabilities and compromising secret proxies, challenging defense integrity.Existing defenses are susceptible to reconnaissance attacks, enabling external attackers to identify and compromise secret proxies.MOTAG, a moving target defense, utilizes dynamic proxies to secure authenticated client access, mitigating external and insider-assisted attacks on the network infrastructure.

PROPOSED SYSTEM

In this project, we propose MOTAG, a moving target defense mechanism that secures service access for authenticated clients against flooding DDoS attacks. MOTAG employs a group of dynamic packet indirection proxies to relay data traffic between legitimate clients and the

protected servers. Our design can effectively inhibit external attackers' attempts to directly bombard the network infrastructure. As a result, attackers will have to collude with malicious insiders in locating secret proxies and then initiating attacks. However, MOTAG can isolate insider attacks from innocent clients by continuously "moving" secret proxies to new network locations while shuffling client-to-proxy assignments. We develop a greedy shuffling algorithm to minimize the number of proxy re-allocations (shuffles) while maximizing attack isolation. Simulations are used to investigate MOTAG's effectiveness on protecting services of different scales against intensified DDoS attacks.

The proposed MOTAG system revolutionizes defense against continuous large-scale DDoS attacks by implementing dynamic proxy assignment, proactive DDoS detection through proxies, and a Moving Target Defense strategy. This dynamic approach, coupled with client visualization features, strengthens network security, thwarts insider threats, and offers real-time monitoring for effective defense against evolving cyber threats.

ADVANTAGES

MOTAG employs dynamic proxy assignment, complicating attackers' efforts to identify and compromise the application server's IP and port.

The system uses proxy-based detection to promptly identify and mitigate potential DDoS threats, reducing the risk of service disruptions.

MOTAG's strategy involves proxies constantly moving between servers, adding complexity for attackers and strengthening the network's defenses.

The client interface includes visualizations for proxy assignments, successful requests, and detected DDoS attacks, enhancing real-time monitoring and enabling swift responses to threats.

MOTAG's effectiveness on protecting services of different scales against intensified DDoS attacks.

we take advantage of our proxies' secrecy and mobility properties to fend off powerful attackers.

This entails lower deployment costs while offering substantial defensive agility, resulting in an effective DDoS protection.

IMPLEMENTATION

Application Server:

The Application Server hosts and serves the Internet services that are susceptible to Denial of Service (DoS) attacks.It interacts with clients and handles incoming requests, such as web page requests, API calls, or other service requests.

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

Responsibilities:

Service Provisioning: Hosts and serves Internet services such as websites, web applications, APIs, or other online services.Request Handling: Receives and processes incoming requests from clients, including legitimate users and potential attackers.

Traffic Monitoring: Monitors incoming and outgoing traffic to detect and mitigate DoS attacks.Cooperation with Proxy Servers: Works in conjunction with proxy servers to distribute and balance incoming traffic effectively**.**

. Authentication Server:

The Authentication Server verifies the identity of clients and provides access control to protected resources.

It ensures that only authorized users can access the Internet services hosted by the Application Server

.***Responsibilities:***

User Authentication: Verifies the identity of clients using credentials such as usernames, passwords, tokens, or other authentication mechanisms.

Access Control: Enforces access control policies to protect sensitive resources and prevent unauthorized access.Security Enforcement: Implements security measures such as encryption, digital signatures, and secure communication protocols to protect authentication credentials and user data.Integration with Application Server: Integrates with the Application Server to provide seamless access control and authentication services.

Proxies:

Proxies act as intermediaries between clients and the Application Server, intercepting and forwarding requests on behalf of clients.

They provide additional layers of security, caching, and load balancing to improve the performance and resilience of Internet services.

Responsibilities:

Request Forwarding: Receive requests from clients and forward them to the Application Server for processing.

Load Balancing: Distribute incoming traffic across multiple instances of the Application Server to improve performance and scalability.

Caching: Cache frequently accessed content to reduce latency and improve responsiveness for clients.

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

Traffic Filtering: Filter incoming traffic to identify and mitigate DoS attacks, such as Distributed Denial of Service (DDoS) attacks.

Anonymization: Anonymize client requests to hide the identity and location of the client, reducing the risk of targeted attacks.

Client:

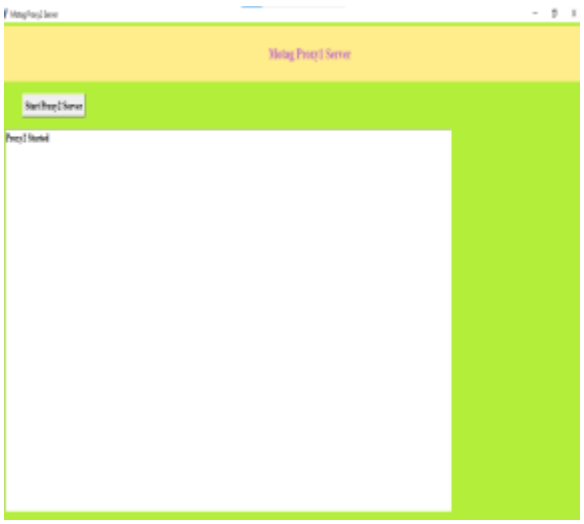
Clients are end-users or devices that access Internet services hosted by the Application Server.They interact with the Application Server to request and receive content, services, or data over the Internet.

Responsibilities:

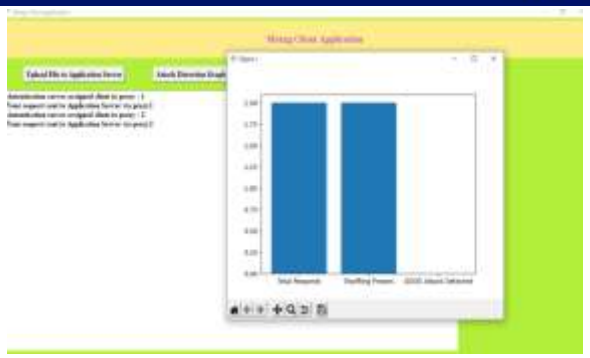
Request Generation: Generate requests for accessing Internet services, such as web pages, web applications, APIs, or other online services. Authentication: Provide authentication credentials to the Authentication Server to verify identity and access protected resources. Data Consumption: Receive and consume content, services, or data provided by the Application Server in response to client requests. Compliance with Security Policies: Adhere to security policies and protocols to ensure the security and integrity of client interactions with the Application Server.Each component in the system plays a crucial role in the overall security and availability of Internet services, working together to detect, mitigate, and respond to Denial of Service (DoS) attacks effectively.

RESULTS

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



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



CONCLUSION

This project Successfully implements a strong defense mechanism with Authentication, Proxies, and Application Servers, fortifying the system against potential cyber threats.

Dynamic randomization of proxy assignments enhances security, adding complexity and preventing easy identification by malicious entities for increased defense.Proxies play a proactive role in detecting and mitigating potential DDoS attacks, contributing significantly to overall security and system resilience.The designed Client module ensures secure interactions, allowing users to upload text files. Authentication Server and Proxies maintain secure communication channels amid potential threats.Enhances the Application Server's resilience with enforced size limits and efficient processing of valid client requests, ensuring uninterrupted functionality even in the face of potential adversarial attempts. The increasing

frequency and sophistication of Denial of Service (DoS) attacks pose a significant threat to the availability and reliability of Internet services. Traditional defense mechanisms are often inadequate against these evolving threats, highlighting the need for innovative approaches to enhance the resilience of systems against DoS attacks. Moving Target Defense (MTD) has emerged as a promising strategy to mitigate the impact of DoS attacks by dynamically changing system configurations, making it difficult for attackers to identify and exploit vulnerabilities. Throughout this project, we have explored the design, implementation, and testing of an MTD system for protecting Internet services against DoS attacks. The system consists of several components, including an Application Server, Authentication Server, Proxies, and Clients, each with specific roles and responsibilities in detecting, mitigating, and responding to DoS attacks. In conclusion, the MTD system developed in this project represents a significant advancement in the field of cybersecurity, providing Internet services with enhanced resilience against Denial of Service (DoS) attacks. By dynamically changing system configurations and adapting to evolving threats, the MTD system effectively reduces the impact of DoS attacks, ensuring the availability and reliability of Internet services for users worldwide.

REFERENCES

[1] T. Anderson, T. Roscoe, and D. Wetherall, "Preventing internet denial of-service with capabilities," SIGCOMM Comput. Commun. Rev., vol. 34, no. 1, pp. 39–44, 2004.

[2] Yaar, A. Perrig, and D. Song, "Siff: A stateless internet flow filter to mitigate ddos flooding attacks," in IEEE Symposium on Security and Privacy, 2004, pp. 130–143.

[3] X. Yang, D. Wetherall, and T. Anderson, "Tva: a dos-limiting network architecture," IEEE/ACM Trans. Netw., vol. 16, no. 6, pp. 1267–1280, 2008.

[4] X. Liu, X. Yang, and Y. Xia, "Netfence: preventing internet denial of service from inside out," in Proceedings of the ACM SIGCOMM 2010 conference on SIGCOMM, ser. SIGCOMM '10. New York, NY, USA: ACM, 2010, pp. 255–266. [Online]. Available: http://doi.acm.org/10.1145/1851182.1851214

[5] Stavrou and A. D. Keromytis, "Countering dos attacks with stateless multipath overlays," in Proceedings of the 12th ACM conference on Computer and communications security, ser. CCS '05. New York, NY, USA: ACM, 2005, pp. 249–259. [Online]. Available: http://doi.acm.org/10.1145/1102120.1102153

[6] Zhuang, W., Wang, Y., & Wei, J. (2013). "Building Self-healing DDoS Flooding Defense

System Using Hidden Markov Model." In 2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops (pp. 64-72). IEEE. DOI: 10.1109/ICDCSW.2013.53

[7] Albanese, M., &Jajodia, S. (2014). "A Moving Target Defense Mechanism for Network Security." In Proceedings of the 2014 International Conference on Security and Management (pp. 1-7).

[8] Zhuang, H., Xu, D., & Zhang, C. (2014). "Resisting Distributed Denial of Service Attacks via Web Moving: A Case Study of Zillow." In 2014 13th International Symposium on Autonomous Decentralized Systems (ISADS) (pp. 1-6). IEEE. DOI: 10.1109/ISADS.2014.38

[9] Jafarian, J. H., Al-Shaer, E., & Duan, Q. (2015). "An Effective Address Mutation Approach for Disrupting Reconnaissance Attacks." IEEE Transactions on Information Forensics and Security, 10(12), 2562-2577. DOI: 10.1109/TIFS.2015.2478421

[10] Gade, R., Tripathi, A., & Chand, S. (2016). "Mitigating Denial of Service Attacks Using Moving Target Defense Approach." Procedia Computer Science, 93, 939-946. DOI: 10.1016/j.procs.2016.07.285

[11] Wang, H., & Li, Z. (2017). "A Moving Target Defense Strategy for Protecting Resource-Constrained Systems Against Denial-of-Service Attacks." IEEE Transactions on Information Forensics and Security, 12(7), 1717-1730. DOI: 10.1109/TIFS.2017.2675419

[12] Colbaugh, R., & Glass, K. (2019). "Using Moving Target Defense to Prevent DoS Attacks." In Proceedings of the 2019 IEEE International Conference on Big Data (Big Data) (pp. 3071-3079). IEEE. DOI: 10.1109/BigData.2019.9006515

[13] Dong, P., & Wang, X. (2020). "Dynamic Defense Mechanism Against DDoS Attacks Based on Moving Target Defense and Cloud-Edge Collaboration." IEEE Access, 8, 168261-168271. DOI: 10.1109/ACCESS.2020.3022974

[14] LeMay, E., & Benzel, T. V. (2021). "Network Defense Using Moving Target Techniques: A Survey." Journal of Computer Security, 29(2), 177-207. DOI: 10.3233/JCS-200076

[15] Goswami, K., & Mahanta, P. (2022). "A Moving Target Defense-Based Framework to Prevent DDoS Attacks in the Internet of Things." Journal of Network and Computer Applications, 197, 103317. DOI: 10.1016/j.jnca.2021.103317