Proceedings of the 5th International Conference on Computing and Data Science
DOI: 10.54254/2755-2721/14/20230789

A research on attack and defense models of network security

Bowen Zhang

Pingyuanhu Campus, Henan Normal University, Hongqi District, Xinxiang City, Henan Province, 453000, China

1928524003@stu.htu.edu.cn

Abstract. This paper analyzes the attack and defense model in network security. For attack models, this paper focuses on Distributed Denial of Service (DDoS), Advanced Persistent Threat (APT), Man-in-the-Middle Attack (MITM), Trojan House, and Cross Site Script Attack (XSS). For each attack model, this article analyses the attack principle and attack effect and summarizes the advantages and disadvantages of various attack models. In the defense model, this paper studies policy, protection, detection, response (P2DR) and the zero-trust model. This paper introduces the basic principle and defense strategy of the P2DR model and analyzes the advantages and disadvantages of this model. At the same time, this paper also introduces the concept and basic principle of the zero-trust model and analyzes its advantages over the traditional security model. The comprehensive analysis shows that different defense strategies need to be adopted for different attack models. When choosing a defense model, it is necessary to choose the most suitable model according to the specific situation. The research of this paper has certain practical significance for improving the level of network security.

Keywords: Network security, Attack model, Defense model

1. Introduction

Cyber security is a set of methods that protect computer networks and other relative devices, systems, applications, and data from unauthorized access, damage, or theft. With the development of the internet and computer technology, cyber security has already become an important issue that companies and individuals must pay attention to and solve. In the field of network security, attack, and defense are two core concepts. The attack model [1] is that attacker uses specific techniques and methods to attack the target and the defense model [2] is that network security experts and organizations take measures and strategies to protect networks from attacks.

This paper will introduce some common attack and defense models. Attack model includes DDoS model [3], APT model [4], MITM model [5], Trojan House model [6] and XSS attack model [7]. The DDoS model is an attack model by sending many requests to the target server so that overloading the server. APT model is an advanced persistent attack model. Its purpose is to continuously access the target system or organization for sensitive information over a long period. MITM model is an attack model that intercepts and tampers with network communication to steal data or obtain top secrets. The Trojan House model uses software or applications trusted by the attacker to install malware. XSS attack model exploits the vulnerabilities of Web applications to inject malicious scripts into web pages to steal sensitive information from users. Defense model includes P2DR [8] and zero-trust model [9]. The P2DR

DOI: 10.54254/2755-2721/14/20230789

model is a comprehensive security framework based on the strategy of four defenses, namely, prevention, detection, response, and repair. Zero-trust model is a security policy that eliminates trust in network security, which assumes that all users and devices are untrusted and must be authenticated and authorized to access sensitive data in the network.

This paper also will introduce the advantage and disadvantages of attack and defense models. The advantages of the DDoS model are ease of implementation, high efficiency, anonymity, and various methods. The disadvantages of that are harming the innocent, network congestion, and large demand for resources. The advantages of APT models are latent, persistent, and targeting specific targets. The disadvantage of that is the high cost. The advantages of the MITM model are stealing and eavesdropping information, modifying communication content, and identity theft. The disadvantages of that are intermediate position and high ability requirement. For Trojan House, its advantages are concealment, effectiveness, destruction, and wide range. Its disadvantages are passivity, easing to intercept, non-transmission capacity, and traceability. For the XSS attack model, its advantages are a high attack effect, for any website, low attack difficulty, and simple operation. Its disadvantages are limitations of defense mechanisms, limitations of the same origin policy, high ability requirements, and traceability. The P2DR model's advantages are predictability, initiative, comprehension, and flexibility. Its disadvantages are complexity, high cost, possible error, and no update. The zero trust model’s advantages are minimizing trust, strategy, improving security, and cross-platform. Its disadvantages are dependence, high consumption, high ability requirement, and network performance.

In section 2, this paper will introduce various attack models in detail, including the principle of attack model, and working principle. In section 3, this paper will compare and analyze the advantages and disadvantages of the attack and defense models. Conclusion and future direction will be presented in Section 4.

2. Preliminary

Network attacks are launched by attackers who use certain attack models to attack the target network system. The attack model achieves certain attack effects so that realizing the intended attack intention of the attacker. The network defense model mainly aims at the maximum possible defense for some attacks and protects the information security of the attack target. The model summary is shown in Table 1.

Table 1. Model summary

Attack and defense model	Principle
DDoS attack model	Consumes target system resources
APT attack model	Prolonged persistent attack
MITM attack model	Manipulate the intercepted data
Trojan horse model	Act as legitimate software
XSS attack model	Malicious code
P2DR model	Complete and dynamic security loop
Zero-trust model	Distrust any device

2.1. Network attack models

2.1.1. DDoS attack model. Distributed denial of service attack refers to using the client/server technology to unite multiple computers as attack platforms to launch DDoS attacks on one or more targets, thus increasing the power of DDoS attacks exponentially. Usually, the attack mode takes advantage of network service defects of the target system or directly consumes its system resources, so

DOI: 10.54254/2755-2721/14/20230789

that the target system cannot provide normal services. The DDoS attack diagram is shown in Figure 1. DDoS attack includes network layer attack and application attack.

In network layer attack, it contains three attack ways which are SYN(Synchronize) flood attack, UDP (User Datagram Protocol) flood attack, and ICMP (Internet Control Message Protocol) flood attack. SYN flood attack mainly uses the disadvantage of the three-way handshake process in TCP (Transmission Control Protocol). The process of a three-way handshake is that two parties who establish a connection send SYN, SYN+ACK (Acknowledge character), and ACK data to each other. But when the attacker constructs a source IP (Internet Protocol) address to send SYN packets randomly, the SYN+ACK returned by the server is not answered. Now, the server will try again to send it and at least have 30 second waiting time. In those 30 seconds, the resource saturation service is unavailable. In a UDP flood attack, an attacker can forge a large number of IP addresses to send a UDP package because UDP is a disconnection protocol. In normal, the two-way traffic of UDP packets is the same so attacker consumes their resources as they consume their opponents. ICMP flood attack is to send abnormal ICMP packages continuously. This can cause the target bandwidth to be occupied but its resources are also consumed. But this attack way is out of date because PING (Packet Internet Groper) is currently disabled on many servers.

An application attack has a CC (Challenge Collapsar) attack. CC attacks are designed to continuously send abnormal requests to resource-consuming pages to result in resource exhaustion. Before sending a CC attack, an attacker needs to find websites that load slowly and consume a lot of resources such as databases and read/write disk files. With CC attacks, web crawlers are used to make HTTP (Hyper Text Transfer Protocol) requests to some websites that consume a lot of resources to load.

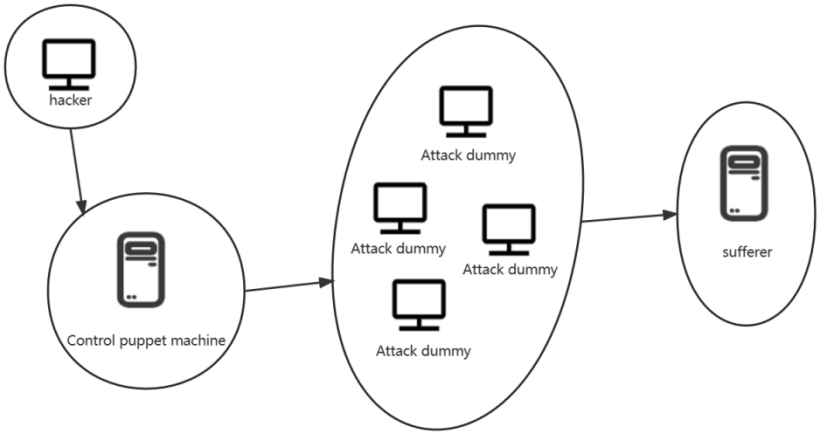

Figure 1. DDoS attack model process.

2.1.2. APT attack model. APT model is that organizations or small groups use current advanced attack techniques to attack a specific target with long-term persistence. The advanced aspects of APT attacks lie inaccurate information collection, a high degree of concealment, and using a variety of complex network infrastructure, and application vulnerabilities to the target of the precise attack. The attacker's attack form is more advanced and advanced, which is called the highest level of security confrontation in cyberspace. The APT attack is the attacker aims to steal core data and take the cyber-attack and invasion behavior to the client. APT attack contains two attack ways, which are harpoon attack and puddle attack.

A harpoon attack is an online fraud aimed at a particular organization. It is not intended to grant access to confidential data. The most common measure is to send a Trojan horse program as an attachment to an E-mail to a specific target and trick the target into opening the attachment. A puddle attack means that the hacker analyzes the target's network activity, finds the website's weakness that the

DOI: 10.54254/2755-2721/14/20230789

target often visits, attacks the website and inserts the attack code, and waits to attack the target visit the web site. The attack diagram of the two is shown in Figure 2.

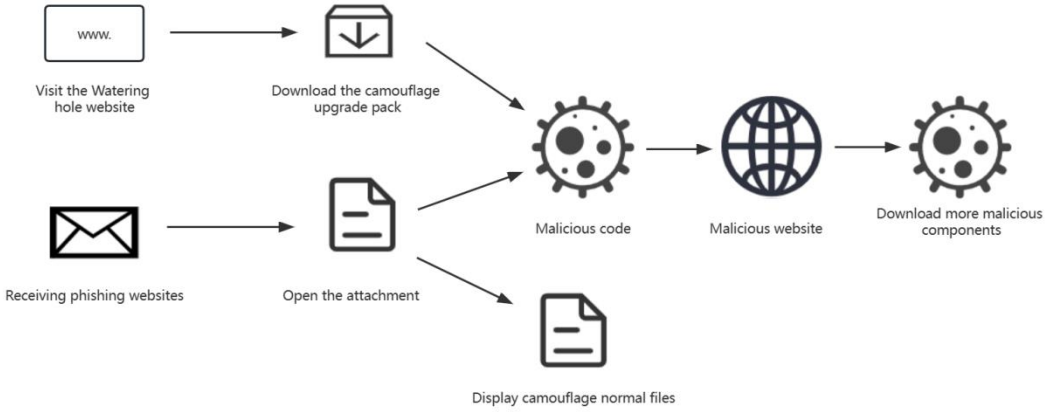

Figure 2. APT attack model process

2.1.3. MITM attack model. Man-in-the-middle attacks allow malicious agents to manipulate intercepted traffic in different ways either to monitor communications and obtain sensitive information such as access credentials, financial information, etc. or to assume the identity of either party. For a middleman attack to work successfully, an attacker must ensure that the attacker is the only point of communication between the two devices. This attack way includes an SSL (Secure Sockets Layer) hijacking attack and an SSL stripping attack. As shown in Figure 3.

In an SSL hijacking attack, the attacker needs to connect itself to the client and the target website to obtain plain text data transmitted over HTTPS (Hypertext Transfer Protocol Secure). The server's certificate in the process of transmission is forged, server's public key is substituted for the server's public key. In this way, the intermediaries can steal the client and server communication data.

In an SSL stripping attack, HTTPS sample text is returned to the browser instead of HTTP, but The HTTPS server remains between the middleman and the server. Because HTTP is transmitted in plain text, the middleman can capture both client and server transmission data.

Figure 3. MITM attack model process.

2.1.4. Trojan horse model. Trojan horses usually disguise themselves as legitimate software, tricking users by using typical naming conventions, the same file names, and a large number of other different variants. It can even hide in seemingly innocent e-mails or file downloads and can open an unexpected backdoor into user programs. Figure 4 shows the attacker using the back door that controls the target computer to invade the target computer.

DOI: 10.54254/2755-2721/14/20230789

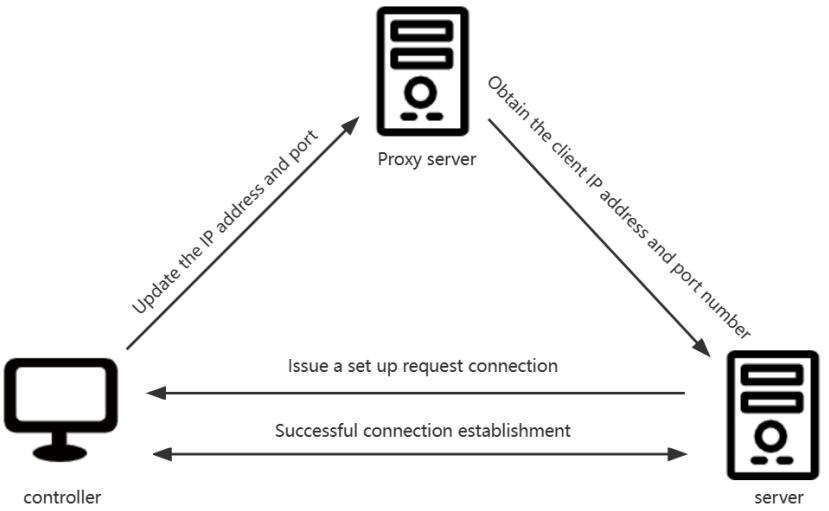

Figure 4. Trojan horse model process.

2.1.5. XSS attack model. XSS attack is to use the vulnerability left in the web page's development, through clever ways to inject instruction code into the web page, the user can load and execute the malicious web program created by the attacker. There are three attack types: reflection XSS, storage XSS, and DOM (Document Object Model) XSS.

In reflection XSS attack, an attacker can use a particular way to tempt the target to access a URL (Uniform Resource Locator) that contains malicious code. When the target clicks on the URL of the malicious link, the malicious code is executed directly in the browser on the target's host. The process is shown in Figure 5

In a storage XSS attack, the attacker uploads or stores malicious code to the server. The malicious code is executed the next time when target views the page containing the malicious code.

In a DOM XSS attack, client-side scripts can dynamically examine and modify page content without relying on server-side data.

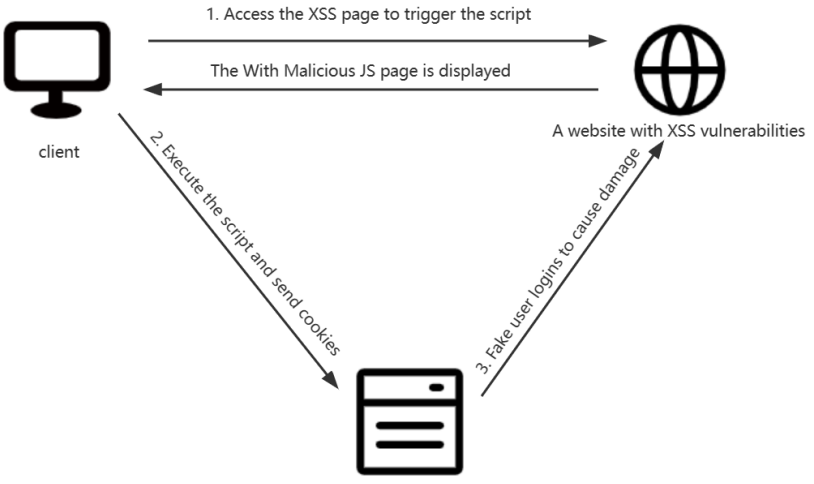

Figure 5. XSS attack model process.

DOI: 10.54254/2755-2721/14/20230789

2.2. Network defence models

2.2.1. P2DR model. Under the control and guidance of the overall security strategy, using protection tools and detection tools at the same time, through the appropriate response, understand and evaluate the security status of the system, and adjust the system to the safest and lowest risk state.Protection, detection and response forms a complete, dynamic security cycle, under the guidance of security policy to ensure the security of information system. The diagram shows in figure 6.

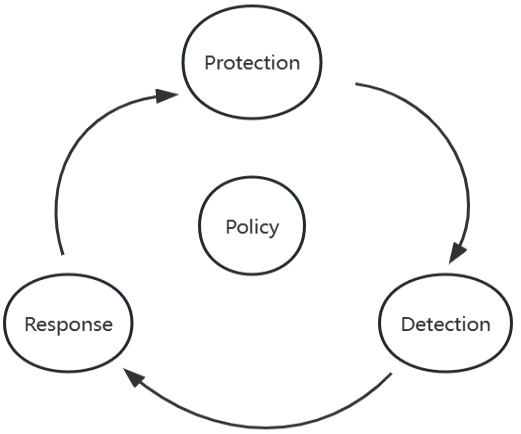

Figure 6. P2DR defense model process.

2.2.2. Zero-trust model. Zero trust models rely on each device and personal strong authentication and authorization. Whether devices and individuals are inside or outside the network boundaries, authentication is passed before any access or data transfer can take place on the private network. The process also combines analysis, screening, and logging to verify the correctness of the behavior and continuous monitoring of intrusion signals. If a user or device shows that the behavior of different signs, it is as suspicious threat for recording and monitoring. This fundamental shift in strategy has been effective against many common security threats. Attackers cannot exploit vulnerabilities in the boundaries and then misuse the sensitive data and applications by gaining access to the defense layer.

3. Analyze attack and defense models

Both the network attack and defense models have different functions. Some models steal the information of target users, and some models invade the target system. But each of these models has its advantages and disadvantages. Some models have high technical requirements for attackers, some models consume large resources, and so on. The summary is shown in Table 2.

Table 2. Summary model's advantages and disadvantages.

Model	Representative works	Advantages	Disadvantages
DDoS	[1], [3], [10]	Easy to implement, high efficiency, anonymity, various methods	harm the innocent, network congestion, The large demand for resources
APT	[4], [11], [12]	Latent, Persistence, Targeting specific targets,	High cost,

DOI: 10.54254/2755-2721/14/20230789

Table 2. (Continued)

MITM	[5], [13], [14]	Steal and Eavesdrop on information, Modify communication content, Identity theft	Intermediate position, High ability requirement,
Trojan horse	[6], [15], [16]	Concealment, effective, destructive, wide range	Passivity, Easy to intercept, Non-transmission capacity, traceable
XSS attack	[2], [7], [17]	High attack effect, For any website, Low attack difficulty, Simple operation	Limitations of defense mechanisms, Limitations of the same origin policy, High ability requirement, traceable
P2DR	[8], [18]	Predictability, initiative, comprehensive, flexibility	Complexity, high cost, possible error, no update
Zero trust	[9], [19]	Minimize trust, Strategy, Improve security, cross-platform	dependence, High consumption, High ability requirement, Network performance

3.1. DDoS model

Al-Hadhrami et al. [1] shows that this paper reviews the attack about DDoS, and DDoS attack will cause serious damage to the system. DDoS model has the advantage of easing to implement and the disadvantage of harming the innocent. Easy to implement is that DDoS attack is relatively easy to carry out and attackers can quickly launch attacks with simple tools and techniques. Harming the innocent is that attack traffic cannot distinguish normal traffic.

Dayanandam et al. [2] shows that the DDoS model has the advantage of high efficiency and the disadvantage of network congestion. The advantage is that a DDoS attack can effectively disable the target network or system, making it unable to work properly. That can result in service shutting down or delays and cause serious financial and reputational damage to the target. The disadvantage is that DDoS attacks may cause network congestion, affect the normal use of other users, and make the network unstable.

Khader et al. [3] shows the advantage of anonymity and various methods and the disadvantage of the large demand for resources. Anonymity means that DDoS attacks can hide the identity and location of attackers by forging source IP addresses and using anonymous proxies. That can make them difficult to trace and punish.

3.2. APT model

Xing et al. [4] shows the use of machine learning to take a test of APT attack. The APT model has the advantage of latent and persistence. Latent is APT attack can be according to the characteristics of the target, around the target network defense system, theft or destruction of hidden data. Persistence means that attackers often lurk in the target network for months or even years when an attacker uses the APT attack model.

DOI: 10.54254/2755-2721/14/20230789

The advantage of targeting specific targets in the APT model is shown in Zhou et al. [5]. This paper writes about analyzing the characteristics of the APT attack model and using the APT attack model to attack SCADA. Targeting specific targets means that APT attacks focus only on pre-specified targets and targets only specific targets and specific systems.

Liu et al. [6] shows that dynamic IP address generation method based on SM4 and other methods to defend against APT attacks. APT model's disadvantage is high cost. The APT attack requires the attacker to spend a lot of manpower, material, and financial resources. The attacker needs to conduct sufficient intelligence collection and analysis to select the most effective attack mode and means. This process needs huge costs and resources.

3.3. MITM model

Conti et al. [7] reviews the preference for MITM, analysis and classify the range of MITM attack. MITM model has the advantage of stealing and eavesdrop information and the disadvantage of intermediate position. Steal and eavesdrop information is that MITM attacks can steal sensitive information, such as username and password, and eavesdrop on network communication. That can give access to their real-time communications. The disadvantage is that it needs an attacker in the middle position and the attacker needs to take control of a network device in the middle.

Canteaut et al. [8] uses the method of sieve-in-the-middle to improve MITM attacks. This paper shows that modifying communication content and high ability requirements. Modify communication is that MITM attacks can tamper with the communication content so that both parties to the communication receive the tampered information. A high ability requirement is that attacker needs to have a certain technical foundation because the attacker needs to trick both sides of the communication into thinking that the attacker is the other side.

Chen et al. [9] shows the advantage of identity theft. Identity theft is a MITM attack that can steal the identity information of both parties, such as IP address and MAC address so that more attacks can be carried out.

3.4. Trojan horse model

Sajeed et al. [10] writes about the advantages of concealment and automaticity and the disadvantages of passivity and easing to intercept. Concealment means that attackers can hide malicious code in legitimate applications and make it difficult to detect. Effective is that Trojan Horse attacks can steal sensitive information and damage systems. Passivity is that the user needs to actively download and execute the malicious code, and the attacker does not have initiative. Easy to intercept means that a Trojan horse is easily detected by defense software such as antivirus software and firewalls.

Spalka et al. [11] propose a secure electronic paper to defend against Trojan horse attacks on electronic signatures. It shows the advantages of destructive and the disadvantages of non-transmission capacity. Destructive figures that Trojan Horse attacks can cause serious damage to the system, such as deleting files and modifying data. Non-transmission capacity is that Trojan horses are not self-propagating. Attackers need other methods to spread the virus.

Zhenfang et al. [12] shows that this model is a wide range and traceable. A wide range is this model can attack various operating systems d applications. Traceable means attackers are easy to track and identify.

3.5. XSS model

Cui et al. [13] mainly aims at cross-site attacks and introduces injection, detection, and defense of cross-site attacks. This paper shows that the XSS attack model has a high attack effect, attacking any website, limitations of defense mechanisms, and limitations of the same origin policy. Attacking any website is that the XSS attack model can attack any website if the website has an XSS loophole. Attackers can use that loophole to attack. The limitation of defense mechanisms is that modern browsers and Web applications typically employ a variety of defenses to prevent XSS attacks. The limitation of the same-

DOI: 10.54254/2755-2721/14/20230789

origin policy is that XSS attacks are restricted by the same-origin policy, and attackers need to obtain the cookies of victims by other means such as inducing the target to visit a malicious website.

Dora et al. [14] solves a problem about often occurs in the field of Network security called the exploitation of websites by XSS attacks. This shows that the XSS attack model has the advantage of low attack difficulty and the disadvantage of high ability requirement. An attacker can attack using off-the-shelf tools and scripts, but attackers need to have certain technical knowledge and attack experience.

Stacy et al. [15] figures that are simple operation and traceable. XSS attacks do not require the user's username and password to be obtained. The attacker only needs to steal the user's Cookie to achieve login and obtain user information.

3.6. P2DR model

Yu [16] proposes a framework for artificial intelligence with security boundaries as the core. This paper shows the P2DR model's advantages and disadvantages which are predictability, initiative, complexity, and high cost. The P2DR model can predict possible security threats in the future so that appropriate preventive measures can be taken in advance and security risks can be effectively reduced. The P2DR model can proactively detect and respond to security threats without relying on passive defensive measures. This initiative can detect and defend against attacks before they occur reducing security vulnerabilities and losses. But the P2DR model needs to adopt a variety of techniques and methods to implement, which makes the model complicated. The P2DR model also requires a large amount of equipment and resources to implement, including network equipment, security software, etc., which makes it costly.

Xin et al. [17] shows that the P2DR model is comprehensive, and flexible, with possible errors, and no update. The P2DR model adopts a variety of technologies and methods to defend against security threats, including machine learning and can cope with a variety of different types of attacks. It can also adjust and optimize defense policies based on actual conditions to adapt to different security threats and attacks. However, the prediction and detection of the P2DR model depend on data and algorithms, and there is a certain possibility of false positives and missing positives. The defense strategy of this model is based on the data and behavior analysis of previous attacks, so it may not be able to detect and deal with new attacks in time.

3.7. Zero-trust model

Ahmed et al. [18] shows that minimizes trust, strategy, dependence, and high consumption. This model is a policy-based access control principle. The zero-trust network model does not trust internal and external users or devices and requires each user or device to authenticate and authorize before accessing the application or data to ensure that only authorized users or devices can access the application or data. But this model relies on authentication, and if the authentication system is compromised or attacked, the security of the entire system will be affected. The zero-trust model authenticates and authorizes all users or devices, which requires a lot of human and material resources.

Wylde et al. [19] shows that improve security, cross-platform, network performance, and high-ability requirement. The zero-trust model reduces internal and external security vulnerabilities and ensures that only authorized users can access data or programs. This model can be implemented on different devices or platforms and can be applied to cloud computing, mobile devices, etc. But the zero-trust model increases network latency and degrades network performance because all network traffic has to be authenticated and authorized. Network administrators must also have comprehensive network knowledge to understand and manage different network traffic.

4. Conclusion

Network security is an important and complex problem. The attack and defense model are two core concepts in the field of network security. In terms of attack models, DDoS, APT, MITM, Trojan House, and XSS attack models are the most common attack models in the current network security field. In terms of defense models, the P2DR model and zero-trust model are the most commonly used network

DOI: 10.54254/2755-2721/14/20230789

security defense models. The in-depth study of the attack and defense model and comparative analysis can provide effective guidance and recommendations for network security defense.

In the future, with the continuous development of technology and increasing threats to network security, network security will face greater challenges and pressure. To better cope with network security threats, network security experts and researchers need to continuously improve and perfect the existing attack and defense models, while constantly researching and developing new security strategies and technologies.

References

[1] Dayanandam G, Rao T V, Bujji Babu D, et al. 2019 Innovations in Computer Science and Engineering: Proceedings of the Fifth ICICSE DDoS attacks—analysis and prevention Springer Singapore pp 1-10.

[2] Cui Y, Cui J, Hu J. 2020 Proceedings of the 2020 12th International Conference on Machine Learning and Computing A survey on XSS attack detection and prevention in web applications pp 443-449.

[3] Al-Hadhrami Y, Hussain F K. 2021 World Wide Web DDoS attacks in IoT networks: a comprehensive systematic literature review pp 971-1001.

[4] Zhou X, Xu Z, Wang L, et al. 2018 MATEC Web of Conferences APT attack analysis in SCADA systems p 173.

[5] Canteaut A, Naya-Plasencia M, Vayssiere B. 2013 Advances in Cryptology–CRYPTO 2013: 33rd Annual Cryptology Conference Sieve-in-the-middle: improved MITM attacks Springer Berlin Heidelberg pp 222-240.

[6] Sajeed S, Minshull C, Jain N, et al. 2017 Scientific reports Invisible Trojan-horse attack p 8403.

[7] Dora J R, Nemoga K. 2021 Journal of Cybersecurity and Privacy Ontology for Cross-Site-Scripting (XSS) attack in cybersecurity pp 319-339.

[8] Yu R. 2021 Journal of Physics: Conference Series Security Framework of Artificial Intelligence System IOP Publishing p 012011.

[9] Ahmed I, Nahar T, Urmi S S, et al. 2020 Proceedings of the International Conference on Computing Advancements Protection of sensitive data in zero trust model pp 1-5.

[10] Khader R, Eleyan D. Sustainable Engineering and Innovation Survey of dos/DDoS attacks in iot pp 23-28.

[11] Xing K, Li A, Jiang R, et al. 2020 2020 IEEE Fifth International Conference on Data Science in Cyberspace (DSC) A review of apt attack detection methods and defense strategies IEEE pp 67-70.

[12] Liu X, Li L, Ma Z, et al. 2019 IEEE 5th International Conference on Computer and Communications (ICCC) Design of APT attack defense system based on dynamic deception IEEE pp 1655-1659.

[13] Conti M, Dragoni N, Lesyk V. 2016 IEEE communications surveys & tutorials A survey of man in the middle attack's pp 2027-2051.

[14] Chen Q A, Osterweil E, Thomas M, et al. 2016 2016 IEEE Symposium on Security and Privacy (SP) MitM attack by name collision: Cause analysis and vulnerability assessment in the new gTLD era IEEE pp 675-690.

[15] Spalka A, Cremers A B, Langweg H. 2002 INFORMATICA-LJUBLJANA- Trojan horse attacks on software for electronic signatures pp 191-204.

[16] Zhenfang Z H U. 2015 International Journal of Engineering and Applied Sciences Study on computer trojan horse virus and its prevention p 257840.

[17] Stency V S, Mohanasundaram N. 2021 Journal of Physics: Conference Series A study on XSS attacks: intelligent detection methods IOP Publishing p 012047.

[18] Xin H, Yu S D, Wan R Z. 2013 Advanced Materials Research Study on Application of Honeypot in Campus Net Security Trans Tech Publications Ltd pp 1560-1563.

[19] Wylde A. 2021 2021 international conference on cyber situational awareness, data analytics and assessment (cybersa). Zero trust: Never trust, always verify IEEE pp 1-4.