A Review of Contemporary Network Attack Methods and Their Countermeasures

An Jian

China Software Evaluation Center (Software and Integrated Circuit Promotion Center of the Ministry of Industry and Information Technology) Beijing 102206

Abstract: ***This article comprehensively explores common attack methods in the current network environment, such as DDoS attacks, ransomware, zero day vulnerability exploitation, APT attacks, etc. These methods seriously threaten the network security of individuals, enterprises, and countries. At the same time, this article deeply analyzes prevention technologies such as firewalls, intrusion detection systems, encryption techniques, and multi factor identity authentication, and emphasizes the importance of building a comprehensive defense system. By comprehensively applying these prevention technologies, the network security protection capability can be effectively improved and the losses caused by network attacks can be reduced.***

Keywords: Network attack; Preventive technology; Trojan virus; Social engineering; Firewall; Intrusion detection and prevention system; Data encryption.

1. INTRODUCTION

With the wide application and popularization of Internet technology, informatization has become a major trend in the development of human society. However, with the continuous deepening of network applications, network security issues are becoming increasingly prominent. Network attacks, as a form of behavior that exploits security vulnerabilities in computer network systems and illegally obtains or destroys network resources and services, have posed a significant threat to network security. Network attacks may not only lead to personal information leakage and economic losses, but also damage national infrastructure and affect social stability. Therefore, researching and mastering the means of network attacks and their prevention techniques is of great significance for safeguarding the information security of individuals, enterprises, and countries. In autonomous systems, studies focus on foundational control mechanisms, such as PID-based speed control for vehicles [1], and advanced navigation systems that integrate local perception with global planning for beyond-visual-range driving [2]. Concurrently, significant efforts are directed towards enhancing the security and privacy of collaborative AI, with proposals for multi-layer defense strategies in federated learning against membership inference attacks [3] and the development of robust, privacy-conscious federated frameworks for specific applications like anti-money laundering [4]. The analysis of complex physical activities is advanced through spatiotemporal graph networks integrated with IoT for motion analysis [5]. In machine learning methodology, research addresses challenges in domain adaptation, such as regularization techniques for black-box scenarios [6]. Graph neural networks continue to be a focus, with architectures developed for recommendation systems via matrix factorization [7]. The application of AI in healthcare is particularly prolific, encompassing personalized medical plan generation using RAG-based systems [8], reviews of deep learning for ECG diagnosis [9], multimodal deep learning approaches tailored for low-resource healthcare settings [10], and the creation of benchmarks to assess and debias large language models in specialized medical fields [11]. Further medical imaging research explores efficient meta-driven visual prompting for segmentation [12], while other studies aim to optimize models for combating specific disease progression [13]. AI is also transforming industrial and operational processes, with multi-agent systems proposed for task recognition and optimization in manufacturing [14]. Privacy concerns in consumer applications are addressed through frameworks combining federated learning with differential privacy for advertising personalization [15]. Finally, research into dynamic resource management demonstrates the use of cohesive hierarchical clustering for optimizing the supply and demand of emergency materials [16].

2. COMMON METHODS OF NETWORK ATTACKS

2.1 Denial of Service Attacks (DoS/DDoS)

Denial of Service (DoS/DDoS) is an attack method aimed at exhausting the resources of the target system, making it unable to provide services to legitimate users. Attackers send a large number of invalid requests or packets to the

target server, causing the server's bandwidth, memory, or CPU resources to be exhausted and unable to respond to normal service requests.

2.2 Injection attacks (SQL injection, XSS, etc.)

Injection attack is a type of attack that exploits security vulnerabilities in an application by inserting malicious SQL code or scripts into its input to steal, tamper with, or destroy data.

2.3 Buffer overflow attack

Buffer overflow attack is a type of attack that involves writing data beyond the capacity of a program buffer, in order to overwrite and destroy data in adjacent memory spaces.

2.4 Malicious software attacks

Malicious software attack refers to the illegal access, destruction, or theft of computer systems, networks, or personal data through various forms of malware, including but not limited to viruses, trojans, etc. A Trojan Horse is a malicious program disguised as legitimate software, typically hidden in seemingly harmless files and installed on a computer without the user's knowledge. Once activated, the Trojan can perform various malicious operations, such as stealing user data, damaging system files, or remotely controlling the computer. A virus is a type of malicious code that can self replicate and infect other programs. It spreads itself by modifying other programs and triggers malicious attacks and ransomware under specific conditions.

2.5 Social Engineering Attacks

Social engineering attacks are a broader form of attack that deceive users into leaking sensitive information by disguising themselves as trusted sources. Attackers typically send fake emails or messages that appear to come from banks, social media, or email service providers, enticing users to click on malicious links or download attachments. Once a user is caught, their personal information, account passwords, or financial data may be stolen. The success of social engineering attacks often depends on the attacker's skills and the victim's alertness.

2.6 Advanced Persistent Threat (APT)

Advanced Persistent Threat (APT) is a network security threat that involves long-term, covert, and sustained attacks against specific targets. APT attacks are typically initiated by skilled and resource rich attackers who utilize advanced tools and techniques to bypass traditional security measures. The targets of APT attacks are usually important organizations such as government agencies, large enterprises, or critical infrastructure. Attackers will collect target information, infiltrate target networks, steal sensitive data, or disrupt systems through various means. The harm of APT attacks is enormous, as they are not only difficult to detect and prevent, but once successful, they can also have serious economic and political impacts on the target.

2.7 Supply Chain Attacks

Supply chain attacks are an emerging threat aimed at software developers and suppliers. By exploiting vulnerabilities in the supply chain, attackers can attack a certain link in the supply chain through means such as destruction, tampering, and implantation of malicious code, thereby affecting the security of the entire supply chain.

3. PRINCIPLES AND TECHNICAL ANALYSIS OF NETWORK ATTACKS

3.1 Target selection and identification for attacks

The first step in a cyber attack is to carefully select and accurately identify the target of the attack. Attackers typically develop attack plans based on the value, vulnerability, and accessibility of the target. They may collect target information through public channels such as social media, company websites, domain registration information, etc. to understand the target's business scope, technical architecture, and personnel composition. In addition, attackers may also use vulnerability scanning tools and techniques to detect security vulnerabilities and

weaknesses in the target system. Once a potential attack target is identified, the attacker will further analyze the target's network architecture, security policies, and protective measures to find the best attack entry point and path.

3.2 Introduction to Attack Tools and Platforms

In order to carry out network attacks, attackers usually use various professional attack tools and platforms. These tools include but are not limited to vulnerability exploitation tools, password cracking tools, network scanners, malware generators, etc. Vulnerability exploitation tools can exploit known or unknown vulnerabilities to execute malicious code, gain system privileges, or steal sensitive data. Password cracking tools are used to crack user passwords or encrypt data. Network scanners help attackers discover open ports, services, and potential security vulnerabilities in the target network. In addition, there are some automated attack platforms, such as Metasploit, which integrate various attack tools and scripts, making it easier for attackers to carry out complex network attacks.

3.3 Analysis of Attack Process and Strategy

The process of a cyber attack typically includes stages such as intelligence gathering, vulnerability detection, attack implementation, data theft/destruction, and trace removal. In the intelligence gathering stage, attackers will collect as much target information as possible to develop effective attack strategies. The vulnerability detection stage is the use of scanning tools and techniques to discover security vulnerabilities in the target system. Once a vulnerability is found, the attacker will enter the stage of attack implementation, using the vulnerability to execute malicious code or launch other forms of attacks. During the data theft/destruction phase, attackers may attempt to obtain sensitive data, disrupt systems, or crash services. Finally, during the trace clearance phase, attackers will take measures to conceal their attack behavior in order to avoid detection and tracking. In order to successfully carry out an attack, attackers often employ various strategies and techniques, such as disguising the source of the attack, using social engineering principles to deceive users, and bypassing security measures.

4. MAIN PREVENTION TECHNOLOGY RESEARCH

4.1 Firewall Technology

4.1.1 Basic concepts and types of firewalls

As the first line of defense for network security, firewall is a security system located between internal and external networks, used to monitor and filter data packets entering and leaving the network to prevent unauthorized access and data leakage. According to different implementation technologies and deployment methods, firewalls can be divided into various types such as software firewalls, hardware firewalls, and hybrid firewalls. Software firewalls are typically integrated into operating systems, while hardware firewalls are independent physical devices. A hybrid firewall combines the advantages of software and hardware to provide more flexible and powerful security protection.

4.1.2 Working principle and deployment strategy of firewall

The working principle of a firewall is based on predefined security rules, which determine which packets can be allowed to pass through and which packets should be blocked. When a packet passes through a firewall, the firewall checks its source address, destination address, port number, and other information to match it with security rules. If the packet complies with the allowed rules, it will be forwarded to the target network; If the blocking rule is not met or triggered, it will be discarded or rejected. When deploying a firewall, it is necessary to develop appropriate strategies based on the network environment and security requirements, such as state detection, packet filtering, proxy services, etc., to ensure the security and availability of the network.

4.2 Intrusion Detection and Prevention System (IDS/IPS)

4.2.1 Basic concepts and functions of IDS/IPS

Intrusion Detection and Prevention System (IDS/IPS) is one of the important technologies in the field of network security, used to detect and prevent malicious activities targeting computer systems and networks. IDS mainly

focuses on detection functions, which can monitor network traffic and system logs in real time, identify potential attack behaviors or abnormal activities, and issue alerts. IPS, on the other hand, adds prevention functions on the basis of detection, which can automatically block or respond to detected attack behaviors to prevent actual damage caused by attacks.

4.2.2 Detection Techniques and Methods for IDS/IPS

The detection technology of IDS/IPS mainly includes three methods: signature detection, anomaly detection, and hybrid detection. Signature detection identifies attack behavior by matching feature signatures with known attack patterns; Anomaly detection identifies abnormal activities that deviate from normal patterns by analyzing the normal patterns of network traffic or system behavior; Hybrid detection combines the advantages of signature detection and anomaly detection to improve the accuracy and efficiency of detection. In addition, IDS/IPS also adopts advanced technologies such as deep packet inspection and protocol analysis to cope with increasingly complex network attacks.

4.3 Data Encryption Technology

4.3.1 The role of Multi party Computation (SMPC) in defense systems

Multi party computing technology can be applied to build cross institutional data sharing and analysis platforms, achieving data privacy protection and collaborative computing. For example, in the financial sector, different banks can share customer credit data for risk assessment while protecting customer privacy; In the medical field, medical institutions can jointly analyze patient data for disease prediction and medical research, while protecting patient privacy.

4.3.2 The role of homomorphic encryption (HE) in defense systems

Homomorphic encryption technology can be applied to build secure cloud computing and big data processing platforms, achieving data privacy protection and efficient computing. For example, in a cloud computing environment, users can store sensitive data in the cloud and use homomorphic encryption technology to compute and analyze encrypted data without worrying about the risk of data leakage. Meanwhile, homomorphic encryption can also be combined with multi-party computing techniques to further enhance the security and collaborative computing capabilities of data processing.

4.4 Security authentication and authorization mechanism

4.4.1 Identity authentication and access control

Zero Trust Network Architecture (ZTNA) is an advanced network security model with the core concept of "never trust, always verify". This architecture overturns the traditional trust model, no longer granting trust based on network location or user identity, but strictly authenticating and authorizing each user, device, and process to ensure data and application access security. Identity authentication is the foundation of network security, used to confirm the authenticity of user identity. By using various methods such as passwords, biometric authentication, and digital certificates to authenticate users, it can ensure that only legitimate users can access network resources. Access control is based on identity authentication, controlling the user's access scope and operational permissions to network resources according to their permissions and roles. By developing fine-grained access control policies, unauthorized access and data leakage can be prevented.

4.4.2 Permission Management and Audit Mechanism

Permission management refers to the process of assigning and managing user permissions, including granting, changing, and revoking permissions. Permission management can ensure that users can only access resources within the minimum permission range they need, reducing security risks. The audit mechanism is an important means of recording and monitoring user behavior and network activities. Audit logs can track user behavior, analyze security incidents, and identify potential security threats. Meanwhile, the audit mechanism can also provide a basis for post accountability and compliance checks.

5. CONSTRUCTION OF AI BASED DEFENSE SYSTEM

5.1 The Core Role of AI in Defense Systems

Intelligent recognition and monitoring: AI technology can monitor network traffic and abnormal behavior in real time, quickly identify potential attack patterns through machine learning algorithms, and improve the accuracy and efficiency of security detection.

Automated response: Once a security threat is detected, AI systems can automatically trigger corresponding defense mechanisms, such as blocking attack sources, isolating infected devices, implementing security policies, etc., to quickly respond to security incidents.

Threat Intelligence Analysis: AI technology can process and analyze massive threat intelligence data, uncover hidden attack patterns and trends behind the data, and provide strong support for security decision-making.

5.2 Key Technologies and Applications

Deep learning: Deep learning algorithms have achieved significant results in fields such as image recognition and speech recognition, and are also applicable to the field of network security. By training deep learning models, precise identification of malicious software, phishing websites, etc. can be achieved.

Natural Language Processing (NLP): NLP technology can understand and analyze human language, which is of great significance for processing and analyzing text data such as threat intelligence reports and security logs. Through NLP technology, key information can be automatically extracted to improve the efficiency and accuracy of intelligence analysis.

Reinforcement learning: Reinforcement learning is a machine learning algorithm that learns through trial and error, which enables AI systems to continuously optimize their defense strategies in complex and changing network environments, improving the system's adaptability and robustness.

5.3 Defense System Construction Plan

Building an intelligent monitoring platform: Utilizing AI technology to build an intelligent monitoring platform that enables comprehensive monitoring and real-time analysis of network traffic, user behavior, system logs, and more. Quickly identify abnormal behavior through intelligent algorithms and promptly discover potential security threats.

Establish an automated response mechanism: Based on the monitoring platform, establish an automated response mechanism. Once a security threat is detected, the system can automatically trigger corresponding defense measures, such as blocking the attack source, isolating infected devices, etc., to reduce the damage caused by the attack.

Strengthen threat intelligence analysis: Establish a threat intelligence analysis system and utilize AI technology to process and analyze massive threat intelligence data. By mining the attack patterns and trends behind the data, powerful support is provided for security decisions. At the same time, strengthen cooperation and communication with other security organizations, and share threat intelligence resources.

Enhancing the security and reliability of AI models: When building AI based defense systems, special attention should be paid to the security and reliability of AI models. By strengthening the review and validation of model training data and introducing adversarial training methods, the resistance of the model to malicious attacks can be improved. At the same time, establish a model update mechanism to promptly fix vulnerabilities and defects in the model.

6. CONCLUSION

In summary, the threat of network security is becoming increasingly severe, and building a multi-level and coordinated comprehensive defense system is the only way to ensure network security. By continuously

optimizing and adjusting defense strategies, strengthening collaboration and linkage between various levels, we can effectively enhance the overall level of network security protection. At the same time, strengthening user security education and training, increasing the awareness and importance of network security in the whole society, is also an indispensable part of building a secure network environment. In the future, with the continuous advancement of technology and the continuous evolution of threats, we will continue to explore and practice more efficient and intelligent network security defense systems to safeguard the healthy development of the digital economy.

REFERENCES

[1] Y. Zhang, Z. Tian and H. Hua, "Design of an Autonomous Vehicle Speed Control System Based on a PID Controller," 2025 International Conference on Advances in Electrical Engineering and Computer Applications (AEECA), Dalian, China, 2025, pp. 491-495, doi: 10.1109/AEECA65693.2025.00092.

[2] Deng, X., & Yang, J. (2025, August). Multi-Layer Defense Strategies and Privacy Preserving Enhancements for Membership Reasoning Attacks in a Federated Learning Framework. In 2025 5th International Conference on Computer Science and Blockchain (CCSB) (pp. 278-282). IEEE.

[3] Sultan, N., Patwar, N., Wei, X., Chew, J., Liu, J., & Du, R. (2026). FedGuard: A Robust Federated AI Framework for Privacy-Conscious Collaborative AML, Inspired by DARPA GARD Principles. International Academic Journal of Social Science, 2, 1–16. https://doi.org/10.5281/zenodo.18253151

[4] Zhu, Y., Yu, W., & Li, R. (2025). SAGCN: A spatiotemporal attention-weighted graph convolutional network with IoT integration for adolescent tennis motion analysis. Alexandria Engineering Journal, 128, 652-662.

[5] Peng, Qucheng, Chen Bai, Guoxiang Zhang, Bo Xu, Xiaotong Liu, Xiaoyin Zheng, Chen Chen, and Cheng Lu. "NavigScene: Bridging Local Perception and Global Navigation for Beyond-Visual-Range Autonomous Driving." arXiv preprint arXiv:2507.05227 (2025).

[6] Peng, Qucheng, et al. "RAIN: regularization on input and network for black-box domain adaptation." Proceedings of the Thirty-Second International Joint Conference on Artificial Intelligence. 2023.

[7] Yang, J., Wang, Z., & Chen, C. (2024). GCN-MF: A graph convolutional network based on matrix factorization for recommendation. Innovation & Technology Advances, 2(1), 14–26. https://doi.org/10.61187/ita.v2i1.30

[8] Hsu, Hsin-Ling, et al. "MEDPLAN: A Two-Stage RAG-Based System for Personalized Medical Plan Generation." arXiv preprint arXiv:2503.17900 (2025).

[9] Ding, Cheng, et al. "Deep learning for personalized electrocardiogram diagnosis: A review." arXiv preprint arXiv:2409.07975 (2024).

[10] D. Restrepo, C. Wu, S.A. Cajas, L.F. Nakayama, L.A. Celi, D.M. López. Multimodal deep learning for low-resource settings: A vector embedding alignment approach for healthcare applications. (2024), 10.1101/2024.06.03.24308401

[11] Restrepo, David, et al. "Multi-OphthaLingua: A Multilingual Benchmark for Assessing and Debiasing LLM Ophthalmological QA in LMICs." Proceedings of the AAAI Conference on Artificial Intelligence. Vol. 39. No. 27. 2025.

[12] Wu, Chenwei, et al. "Efficient In-Context Medical Segmentation with Meta-driven Visual Prompt Selection." International Conference on Medical Image Computing and Computer-Assisted Intervention. Cham: Springer Nature Switzerland, 2024.

[13] Xie, Minhui, and Shujian Chen. "Maestro: Multi-Agent Enhanced System for Task Recognition and Optimization in Manufacturing Lines." Authorea Preprints (2025).

[14] Qin, Haoshen, et al. "Optimizing deep learning models to combat amyotrophic lateral sclerosis (ALS) disease progression." Digital health 11 (2025): 20552076251349719.

[15] Li, X., Lin, Y., & Zhang, Y. (2025). A Privacy-Preserving Framework for Advertising Personalization Incorporating Federated Learning and Differential Privacy. arXiv preprint arXiv:2507.12098.

[16] Zhang, X. (2024). Research on Dynamic Adaptation of Supply and Demand of Power Emergency Materials based on Cohesive Hierarchical Clustering. Innovation & Technology Advances, 2(2), 59–75. https://doi.org/10.61187/ita.v2i2.135