Computer Fraud and Security
ISSN (online): 1873-7056

The Role of Computer Deception in Network Security

Zhuqiang Ye[1]，Zexin Liu[2]*

[1] School of Law，Shanghai University of Political Science and Law, Shanghai 201710, China

Email: 17612107808@163.com

[2*] College of Policing Studies，Shanghai University of Political Science and Law, Shanghai 201710, China

Email：**liuzhexin@shupl.edu.cn**

Abstract: With the rapid development of Internet technology, computer has become an indispensable part of modern society. However, with the popularization of computer technology, the problem of network security is becoming increasingly prominent. In recent years, China's network security incidents occur frequently. As a means of attack, computer deception has seriously threatened national information security, social stability and people's life. Therefore, it is of great practical significance to study the role of computer deception in network security. Its purpose is to mislead and deceive users or systems by various means to achieve the purpose of illegally obtaining information, damaging the stability of the system or carrying out other illegal activities. Based on this, this paper aims to explore the role of computer deception in network security. Firstly, the concept, content and present situation of computer network security are expounded, and then the necessity of computer network security management and protection is analyzed. Secondly, the related technology of computer deception is introduced. Finally, the application of computer spoofing in network security is studied, and the effectiveness of computer spoofing in preventing and detecting network attacks is revealed. In addition, the ethical issues of computer deception and its potential in future cybersecurity strategies are discussed. Research shows that computer deception can not only enhance the defense mechanism, but also improve the organization's cognition and response ability to network threats, and become an indispensable security strategy. By evaluating current technologies and methods, this paper provides practical recommendations for researchers and practitioners to effectively use computer spoofing techniques to improve network security.

Keywords: network security; Computer deception; Necessity; Apply

1 Introduction

With the rapid development of information technology, the problem of network security becomes more and more prominent. The means of network attack are increasingly diversified, and the attackers invade the system through various complex technical means, which brings serious threats to the information security of individuals, enterprises and even countries. Under this background, computer deception technology, as an important means of network security protection, has gradually attracted the wide attention of researchers and industry. The core of computer deception technology is to induce attackers through false information or environment, so as to achieve effective defense against network intrusion. Compared with traditional network security protection measures, deception technology has stronger active defense ability. Not only is it able to detect potential threats before attackers gain access to the system, but it can also buy cybersecurity personnel valuable reaction time after an attack by providing false targets and information to slow or mislead attackers. Through in-depth analysis and application of computer deception technology, it can provide a new perspective and method for network security system and enhance the ability to cope with complex network attacks. In addition, with the constant change of the network environment, the traditional defense mechanism is facing more and more challenges, while the computer deception technology provides a new solution to deal with new threats.

In practical applications, computer spoofing technology has been widely used in intrusion detection system, honeypot technology and malware analysis. Through these applications, not only can effectively identify and prevent network attacks, but also can deeply analyze the behavior pattern of attackers, and improve the early warning ability and response ability of network security.

2 Overview of Computer network security

2.1 Concepts and contents of computer network security

Computer network security is through certain security management measures and technical means, so that the user's network can be safe and reliable, and through the storage and transmission of data information and download security prevention and control measures, to ensure that the integrity of user data and related content is not infringed. Computer network security can be divided into two aspects: physical security and information security. Physical security includes the security of network equipment and related hardware facilities, to ensure the normal work of related hardware, do not cause damage to the normal operation of the situation, and information security mainly refers to the storage and transmission of information, download and other processes of protection, to ensure the integrity and security of users.

Computer network security can be divided into four aspects: software security, equipment security, data security and system security. Software security mainly refers to different software that can run normally in the device and can run well within the scope of authorization; Network security refers to all kinds of network hardware equipment, can maintain normal, stable and effective work; Data security refers to ensuring the safety and effectiveness of data in the process of data transmission. System security means that the overall computer network will not be malicious attacks by hackers, resulting in overall network data leakage or paralysis.

2.2 Analysis of the current situation of computer network security

With the continuous development of computer networks, there are also many new technologies based on this, such as cloud computing and big data. The development of new technologies has also brought a certain test to network security, which requires us to pay more attention to network hidden dangers. There are two kinds of security risks in the operation of computer network, one is virus infection, the other is system vulnerability. Virus infection is a way for hackers to attack computer networks. Through network transmission or E-mail communication, virus infection interferes with computer networks and causes a series of failures of computer networks, some of which are more serious and lead to the paralysis of the entire computer network, which will seriously affect people's life and work. It can also lead to the leakage of personal data and network data. System vulnerabilities refer to the security vulnerabilities caused by the hardware of the computer network, such as information leaks caused by telephone lines, information leaks caused by microwaves, etc., and some are caused by leaks caused by the computer's operating system or software problems. Leaking these system problems will bring certain hidden dangers to the computer network security. Serious ones can cause incalculable losses.

2.3 Necessity of computer network security management and protection

The development of computer network has brought great influence to the exchanges in various aspects such as economy and culture, which is far more influential than the computer network technology of several previous industrial revolutions, linking the major regional plates into a close whole, promoting economic exchanges and cultural progress. In this context, computer network security is particularly important. There are often some computer network attacks resulting in network paralysis news, which requires us to pay more attention to computer network security. The leakage of data information has brought great hidden dangers to personal privacy, resulting in people's distrust of computer network. With the rapid development of science and technology and the deepening of the application of computer network, we need to constantly update the means of network security management to protect network security.

3 Overview of computer spoofing techniques

3.1 Definition and classification of deception technology

Computer spoofing technology is a kind of security protection means to protect the real system and data by constructing false information or environment to induce the attacker to make wrong judgment or behavior. The main goal of this technology is to identify potential attackers, reduce the probability of success of the attack, and even mislead the attacker to spend time and resources in a false environment.

(1) Deception techniques can be classified according to different dimensions. First of all, according to the implementation of deception, it can be divided into active deception and passive deception. Active spoofing refers to the security system actively generating false information and illusions, such as fake websites, fake emails, etc., in order to induce the attacker to interact. Passive deception is to collect information about the attacker in a covert way, such as using honeypot technology to guide the attacker into a monitoring environment.

(2) According to the purpose of deception, deception techniques can be classified into information gathering, misleading and defensive. The purpose of information gathering deception technology is to obtain the behavior pattern and attack method of the attacker, for example, by recording the behavior of the attacker in the honeypot to analyze its technical level. Misleading spoofing techniques are designed to make attackers misjudge the security status of real systems, for example by posing as vulnerable targets to attract the attention of attackers. Defensive spoofing focuses on protecting critical assets and data in the event of an attack, preventing attackers from gaining access to sensitive information.

(3) In specific applications, deception technology can also be subdivided into network layer deception, application layer deception and data layer deception. Network layer spoofing is mainly realized through network protocol camouflage and traffic redirection. Application layer deception involves the simulation and manipulation of user behavior, such as forging user identity information; Data layer spoofing misleads attackers by manipulating the format and content of stored data. These classifications help researchers and security experts more accurately select the appropriate technology when designing and implementing computer deception strategies.

Cyber Deception: Security defense personnel deploy fraud in their own information and communication technology system to interfere with and mislead the attacker's cognition of their own information and communication technology system, so that the attacker can take actions (or no actions) in favor of the defense, so as to help detect, delay or block the activities of the attacker, and achieve the purpose of increasing the security of the information and communication technology system.

On the basis of the above definition, a formal definition of network deception is given:

Cyber-Deception=(Defender, Asset, Trick, Attacker, Profit)

(1) Defender: Security defender, initiator and perpetrator of deception, planning and executing deception to make the attacker take the action expected by the defender.

(1) Asset: assets in one's own information and communication technology system, the target to be protected by cyber fraud. Asset=(asset1, asset2,..., assetn), asseti refers to assets in information and communication technology systems, including equipment, systems, software, applications, data, etc.

(3) Trick: Constructed scam, deployed in ICT systems. There are two kinds of scams, one is to build fake assets, recorded as Simulation, and the other is to modify the characteristics of existing assets in the system, recorded as Modification, then Trick= (Simulation, Modification). Simulation={sasset1,sasset2,... , sassetp}, Mimulation={masset1, masset2,... , massetq}(p+q>0, q<=n). For each masseti, the assets in the corresponding Asset (i! =j), but to the attacker, it shows the characteristics of asseti, making the attacker think that what he sees is a resource asset; .

(4) Attacker: indicates the target of network deception. Attacker=(Tactics, Techniques, Procedures). Tactic, Technique, Procedure: indicates the tactic, technique and procedure used by the attacker respectively. In the process of network deception design, different schemes should be adopted according to the characteristics of the attacker.

(5) Profit: the profit of network fraud, which is also the purpose of the defense party to implement fraud, is denoted as Proftt= {TTP, Trace, Protection, Delay). TTP represents the Tactics, Techniques, and Procedures information of the attacker obtained through network deception. Trace indicates the tracing of the attacker. Protection represents the protection of real assets. Delay Indicates the delay of an attacker's attack.

The process of network deception is the process in which the defender achieves the purpose of defense by laying a scam, which is recorded as:

$$\text{Asset} \times \text{Trick} \rightarrow \text{Profit} \tag{1}$$

This paper draws on the basic attribute of information security to extract the basic attribute of network deception system and scheme. The basic security attributes concerned in the design and implementation of network spoofing are summarized into Availability, Confidentiality, Controllability and Authentication, as shown in Figure 1.

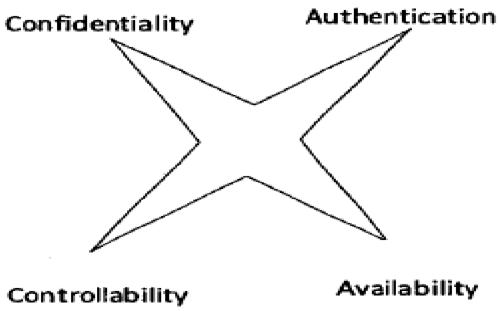

Figure 1 Network deception attribute is able

According to the implementation environment and means, as shown in Table 1, network deception techniques can be divided into the following categories.

Table 1 Technology and scheme practice of network deception technology at different levels

level	Typical deception technique	Existing scheme
Equipment floor	Low interaction honeypot	DTK etc.
Network layer	Network address randomization	Honeyd，MUTE etc.
Data layer	Honeymarking technique	PII，Honeydwords etc.
Application layer	Web application honeypot	Glastopf etc.

3.2 Development history of deception technology

The history of computer deception can be traced back to the early days of computer science. The original spoofing techniques were developed primarily to study the vulnerabilities and security of computer systems. In the 1970s, with the rise of the web, researchers began to explore how false information could be used to confuse attackers, thereby protecting real data and systems.

In the 1980s, with the increase of hacking activities, the application of computer deception technology gradually expanded. Researchers are beginning to design various deception mechanisms, such as camouflage systems and disinformation generation, to cope with the evolving means of attack. During this period, the appearance of honeypot technology marked an important milestone in deception technology. Honeypot, as an active defense mechanism, can attract the attention of attackers and collect attack data, which provides valuable information for subsequent security analysis. In the 1990s, with the rapid development of the Internet, computer deception technology has been more widely used. Researchers continue to improve honeypot technology, developing new structures such as honeynets, so that multiple honeypots can work together to form a more complex defense system. At the same time, the increase in cybercrime has driven a deeper study of deception techniques, and many companies are starting to include them as part of their security offerings. In the 21st century, computer deception technology has experienced significant progress. Techniques based on machine learning and artificial intelligence are introduced into the deception mechanism, enhancing its intelligence and adaptability. For example, some modern honeypots are able to analyze an attacker's behavior in real time and automatically adjust their own deception strategies based on their patterns. In addition, the popularity of cloud computing provides greater flexibility and scalability for the deployment of deception technology, allowing enterprises to implement complex deception defenses at a lower cost. In recent years, with the continuous evolution of network attack methods, computer deception technology is still developing rapidly. The countermeasures against advanced persistent threats (APT) and zero-day attacks have become a research hotspot. The emerging deception technology not only focuses on the innovation at the technical level, but also begins to pay attention to the combination of law and ethics, such as how to effectively implement the deception strategy without violating the user's privacy.

Overall, the development of computer deception technology reflects the continuous evolution of the field of network security, and as technology advances and attack methods become more complex, deception technology will continue to play an important role.

3.3 Main technologies and key characteristics of deception technology

3.3.1 Protocol spoofing technology

Protocol spoofing is mainly used to deceive network intruders by covering up real network information and injecting forged information. At present, there are mainly several kinds of protocol spoofing techniques in our country: (1) multi-address protocol spoofing. This spoofing technology enables network data information to arrive at the destination in a timely and effective manner through the conversion between physical addresses and IP addresses. The computer maps the latest address through the cache and makes it arrive at the sender after dynamic binding. (2) Domain name server network spoofing technology. The domain name server implements the mapping between the host domain name and IP address, and the client program implements the effective authentication of the domain name server by setting the serial number. Therefore, the serial number is vulnerable to attack when the client performs DNS matching queries. (3) IP address spoofing. IP address attack is more complex than the previous two spoofing techniques. Network intruders send packets by stealing other people's IP addresses. The source IP address of an IP packet can be forged without the IP protocol authentication. Therefore, once an IP packet is sent, the source IP address is not used. If the attacker uses other trusted hosts to send IP packets, the purpose of information attack can be achieved.

(2) Honeypot and honeynet technology

Honey Pot is the earliest cyber deception tool, which places some attractive targets in some easy to find places, so that attackers can find and induce intruders to be fooled. The primary goal of the honeypot is to disrupt the attacker's access to valuable information resources and steer them toward systems that are not truly valuable. Honeynet technology is based on honeypot technology, the network deception is distributed in the network system resources, using more idle service ports to deceive the attacker, so as to increase the possibility of the attacker being deceived. Of course, this honeypot honeynet network deception technology also has certain limitations, honeypot technology is easy to be detected, and honeynet technology requires more resources, affecting the efficiency of the use of network resources, and it is only more effective for remote scanning attackers, when the attacker has entered the system, it loses its network deception role.

(3) Cheating space technology

Spoofing space technology increases the attacker's network search space infinitely, enlarges the attacker's attack scope and tasks, and finally makes him give up the attack, so as to achieve the purpose of successful protection of network information security. This kind of network spoofing technology has low cost and is easy to realize. Through the application of computer multi-host system function, a computer can have multiple IP addresses and realize the infinite expansion of spoofing space. So many IP addresses increase the workload of network attackers and increase the intrusion time, which can maximize the consumption of the attacker's intrusion resources and reduce the possibility of valuable network resources being attacked. Even when the attacker's scanner is aware of being spoofed by the network, through the redirection of network traffic, the attacker can continue to be spoofed in the next attack. Of course, this kind of network deception technology also has relative limitations, when the network traffic and service redirection, it must be strictly confidential, if once detected, there is the risk of attack.

3.3.2 Key features of spoofing technology

Spoofing technology has several key characteristics in the field of network security, which make it play an important role in countering network attacks.

(1) Deception technology is flexible and can be adjusted according to different attack scenarios and defense needs. The behavior patterns and attack methods of attackers are constantly evolving, and the flexibility of deception technology enables it to adapt to these changes and achieve dynamic defense.

(2) Deception technology is highly customizable. Network security experts can design specific spoofing mechanisms and decoys according to specific network environments and security policies. For example, for specific attack patterns, security teams can deploy specially designed honeypots that attract attackers and collect data on their behavior. This customized strategy can effectively improve the effectiveness of deception techniques.

(3) The concealment of deception techniques is also crucial. Effective spoofing mechanisms can hide in the network environment, allowing the attacker to enter the false environment without being aware. Through clever design, spoofing systems can simulate real network services and data, thus fooling attackers into thinking their attacks are successful. This invisibility increases the cost for attackers, as they need to devote additional time and resources to identifying the real target.

(4) Deception technology is also considered to have a high degree of countermeasures. By directing attackers into a false environment, security teams can collect data on the attackers' behavior and analyze their tactics and tactics. This counter-capability not only helps the security team understand the attacker's behavior, but also provides important intelligence support for subsequent cybersecurity measures.

(5) Spoofing technology also performs well in terms of real-time responsiveness. The modern network environment is complex and changeable, and spoofing technology can quickly deploy and monitor abnormal activity in the network in real time. Once the intrusion behavior is detected, the system can quickly take measures to guide the attacker into the spoofing environment, so as to obtain attack information while protecting real assets and improve the overall security protection capability.

3.4 The role of network deception in network security

3.4.1 Network spoofing can improve network security analysis

Traditional network security technologies mainly include anti-virus network, IDS, firewall, etc. Network deception can be organically combined with these technologies, and they are not completely opposed to each other. Network deception can improve network security to a large extent. Many technologies in network deception have a strong and high network prevention effect, such as slow response, decoy, address space technology and the creation of decoy information, etc. Network deception technology has a strong detection function, it can create a deceptive address space, this deceptive address space is different from the real address space, it is unknown to the outside world. Network attacks are almost always started by network scanning. In this way, network spoofing does not need to restore the original content of packets, avoiding missing and false positives.

3.4.2 Network deception can carry out accurate effect evaluation

There are three main indicators to detect the effect of network deception, the first one is the probability of detected attacks, and the first measure is to improve the overall operation ability of the system. In the security measures taken by the system, the redundancy and backup of hardware resources, the reasonable distribution of system software and application software and the use of high-reliability cluster software are generally adopted. In the course of its specific use, the AIX operating system and HACMP software are generally installed on rootvg. This is because in the process of the entire system operation, once the rootvg is damaged, the entire system will be paralyzed, or even unable to carry out any operational activities, and in serious cases will have a serious impact on the computer hardware; Even in the case of a full backup, it can cause a long downtime of the system. This shows that it is extremely important to co-install the AIX operating system with the HACMP software on rootvg when conditions permit. In the process of its installation, the specific approach includes the following aspects: first, rootvg as a separate mirror, and through this way to improve the security of the entire system, to avoid a single hard disk damage to the entire system caused serious impact; In this case, even if the hard disk is damaged, the normal operation of the entire system is not affected. Secondly, in the process of establishing rootvg images, the staff should try to connect them to different SCSI hard disks so that the load can be uniform during operation. Thirdly, in the process of improving the fault tolerance of the system, the hard disk memory mirroring configuration or RAID5 redundancy configuration can be configured on the disk array, and its configuration is set to datavg, and the database and application are installed on it. Finally, in the process of improving the reliability of system nodes, designers can build an HACMP cluster environment if conditions permit, so that it can fully achieve dual-system hot backup during operation, and configure corresponding HACMP parameters on the two hosts that are mutually backup, so that it can meet the hot backup requirements during the system operation.

4 Application of computer deception in network security

4.1 Intrusion detection and prevention

The application of computer deception technology in intrusion detection and prevention has gradually become an important research direction in the field of network security. Intrusion detection systems (IDS) are designed to identify malicious activity in a network and detect potential attacks by analyzing traffic and log data. The combination of deception technology and intrusion detection can significantly improve the defense capability of the system.

By introducing spoofing mechanisms, intrusion detection systems are able to create false environments and induce attackers to enter these environments, thereby exposing their true intentions. Honeypot technology is a typical example of this application. A honeypot is a fake system designed to be vulnerable in order to attract attackers and monitor their behavior. In the honeypot, the attacker's operations are recorded in real time, and security experts can analyze this data to understand the attacker's strategies and tools. This analysis not only helps to update security measures in time, but also provides an important basis for future attack prediction. On the defense side, spoofing techniques can interfere with an attacker's decision-making process. By generating fake network traffic or pretending to be a real system, security teams can make it difficult for attackers to identify the real target. Such interference can not only slow down the attacker's action, but also lead to the waste of its resources, and eventually prompt it to abandon the attack.

4.2 Honeypot and honeynet technology

Honeypot and honeynet technology is an important application of computer deception in the field of network security, aiming to trap attackers by simulating real environment, so as to protect the real system from threats. A honeypot is a decoy to an external attacker, usually a virtual or physical computer system designed to attract the attacker's attention and record its behavior. Honeynet is a network environment made up of multiple honeypots, enabling more comprehensive monitoring and analysis of attack patterns.

The working principle of honeypots is based on "trapping and observation", which can be divided into low interaction honeypots and high interaction honeypots. Low-interaction honeypots simulate the characteristics of services and applications, but have limited interaction with the real environment and are suitable for catching common automated attacks. The highly interactive honeypot provides a complete operating system environment capable of simulating real applications and services, suitable for in-depth analysis of attacker behavior and techniques. For example, modern honeypots can run real databases and file systems, allowing attackers to fully interact to gather more detailed attack information.

Honeynet technology integrates multiple honeypots to form a complex network environment, which enhances the confusion and misleading effect of attackers. Honeynet design takes into account the attacker's behavior pattern, through the changing honeypot configuration and service, can effectively extend the attacker's residence time, accumulate more attack data. This data will not only help security experts analyze attack tactics, but can also be used to improve existing defense mechanisms.

In practical applications, honeypot and honeynet technologies have been adopted by many organizations and enterprises to enhance their network security protection capabilities. A financial institution successfully captured an APT attack on its network using honeypot technology, and the analysis revealed that the attackers used advanced social engineering techniques to penetrate. Through in-depth analysis of honeypot data, organizations can repair vulnerabilities in time and enhance their defense capabilities.

Honeypot and honeynet technology not only play an important role in attack detection and analysis, but also promote the development of network security research. By observing the behavior of attackers, researchers can better understand the motivation and strategy of attacks, so as to provide a more scientific basis for network security protection. In addition, these research results also provide an important reference for the future design of network security products and services.

4.3 Malware analysis and anti-forensics

Malware analysis and anti-forensics is one of the important applications of computer deception technology in the field of network security. The rapid development and diversification of malware make traditional detection and defense methods face great challenges. By creating a false environment, computer spoofing technology can effectively trick malware into analysis, thus providing important insights for network security protection.

In malware analysis, spoofing techniques attract malware by setting up a virtual operating system or application environment. This virtual environment can simulate the real operating environment, so that the malware running in it does not pose a direct threat to the real system. For example, researchers can use honeypot technology to create a seemingly vulnerable system that attracts malware attacks. After the malware enters the honeypot, analysts are able to document its behavior and characteristics in detail for further analysis of how it spreads, targets and potential harm.

Counter-forensics is another important area, which involves how to preserve and collect evidence in the course of a malware attack to aid in investigation and forensics. In this process, computer deception technology provides a reliable solution. By deploying spoofing technology, after a malware infection, data related to the attack can be collected, which is often difficult to obtain in a real environment. For example, by using fake files or fake network traffic, malware can be directed to send information to the wrong target, thereby protecting the security of real systems and obtaining important forensic information in the process.

In addition, reverse engineering analysis of malware also benefits from the application of computer spoofing techniques. By building a dynamic analysis environment, researchers are able to observe the behavior of malware in a secure environment. This dynamic analysis can not only reveal the function and structure of the malware, but also help researchers understand its transmission mechanism and attack mode, and then formulate corresponding preventive measures.

In future research, computer spoofing techniques for malware analysis and anti-forensics will continue to evolve. With the advancement of machine learning and artificial intelligence, the intelligence level of deception technology will be further improved, making the creation of false environments and the trapping of malware more efficient and precise. At the same time, researchers need to pay attention to how to balance security and privacy protection to avoid the disclosure of potentially sensitive information when conducting malware analysis.

5 Challenges and future development direction of computer deception technology

5.1 Current Challenges

Computer deception technology is widely used in the field of network security, but its development also faces many challenges.

(1) The rapid iteration of technology makes attackers constantly update their methods, especially the ability to identify and avoid deception mechanisms is increasingly enhanced. Through advanced techniques such as deep learning and machine learning, attackers can effectively analyze the behavior patterns of honeypot systems to identify potential spoofing environments. This increase in capability puts the effectiveness of traditional deception techniques at risk, forcing security researchers to constantly update and optimize defense strategies.

(2) The implementation of computer deception technology requires a significant investment of resources, including time, money and technical support. In the case of limited resources, how to efficiently allocate and use these resources becomes a difficult problem. For some smes, spoofing based defenses can be difficult to implement due to high maintenance costs, leaving them powerless in the face of sophisticated cyber attacks.

(3) Lack of information sharing and cooperation mechanism. Network security is a holistic issue, and the protection measures of a single organization are often difficult to cope with cross-organizational attacks. The lack of effective information sharing platform makes it difficult for various institutions to form joint forces in the face of common threats, resulting in the application of deception technology is greatly reduced. Effective collaboration can improve overall defense capabilities, but in practice, interests and information barriers between units hinder such collaboration.

(4) Ethical and legal issues also restrict the application of computer deception technology. The essence of deception technology is to create false information and environment, which may give rise to legal liability and ethical disputes. How to comply with laws, regulations and ethical standards while ensuring network security has become an important issue that researchers and practitioners must face. Failure to properly deal with these problems may lead to the legitimacy of the technology application being questioned, thus affecting its promotion and application.

5.2 Future development trend

The future development trend of computer deception technology in the field of network security will be affected by technological progress, the evolution of attack methods, and the change of market demand.

(1) With the rapid development of artificial intelligence and machine learning, computer deception technology will incorporate more intelligent elements. By analyzing massive amounts of data, the system is able to identify potential threats in real time and automatically generate deception strategies. For example, the spoofing mechanism based on user behavior analysis can dynamically adjust the honeypot Settings to adapt to different attacker behavior patterns and improve the defense effect.

(2) The popularity of cloud and edge computing will drive the distributed application of deception technology. While traditional centralized honeypot deployments have the risk of a single point of failure, distributed honeypots allow data capture and analysis on multiple nodes, increasing security and flexibility. This architecture can effectively deal with large-scale cyber attacks and achieve broader defense coverage.

(3) The development of the Internet of Things (IoT) will provide new application scenarios for computer deception technology. With the popularity of smart devices, the targets for attackers are also expanding. Spoofing technology for iot devices will be able to effectively protect these devices from intrusion. For example, by creating false device information, attackers are induced to make false attack attempts, thus providing protection for real devices.

(4) At the technical level, the introduction of blockchain technology may also change the direction of the development of computer deception technology. The decentralized nature and immutable nature of blockchain can be used to build a transparent spoofing policy management system to prevent attackers from identifying and countering spoofing mechanisms. This combination of emerging technologies will increase the credibility and effectiveness of deception techniques.

Conclusion

Computer deception plays an important role in computer information security system and is widely used in all aspects of social life. Through the elaboration and application of computer deception, this paper enables the users of computer network to enhance the quality of computer deception and improve the defense level of their own information system. There are reasons to believe that in the context of the rapid development of computer networks, computer deception will have a broader application prospect. Only by constantly improving the technical level of the quality of computer deception can we guarantee the security performance of computer information technology and prevent the information resources of computer network from being stolen. Therefore, the study of computer deception is urgent.

Reference

[1]Liu Z .Intelligent classification of computer vulnerabilities and network security management system: Combining memristor neural network and improved TCNN model.[J].PloS one,2025,20(1):e0318075.

[2]Liu H ,Wang C ,Wu Z .A probabilistic automata-based network attack-defense game model for data security by using security service chain[J].World Wide Web,2024,28(1):11-11.

[3]Xu Y ,Zhou Z ,Zhang K .Role and Innovative Strategies in the Development of Computer Network Technology[J].The Frontiers of Society, Science and Technology,2024,6(12):

[4]Kachen Z .Computer Network and Database Security Technology Optimization[J].Journal of Electronic Research and Application,2024,8(6):188-193.

[5]Bo W ,Huanying C ,Zhaoji H , et al.Design of network security processing system in 5G/6gNG-DSS of intelligent model computer[J].Intelligent Decision Technologies,2024,18(4):2759-2774.

[6]Xuxia Z ,Weijie C ,Jian W , et al.Application of machine learning algorithm and data evaluation in computer network security situation awareness technology[J].Intelligent Decision Technologies,2024,18(4):2827-2839.

[7]Tajudeen M M ,Perumal R ,Thakur K G , et al.Mittag-Leffler function based security control for fractional-order complex network system subject to deception attacks via Observer-based AETS and its applications[J].Physica Scripta,2024,99(8):085269-085269.

[8]Zhou C ,Chunhua W ,Wei Y .Quasi-synchronization of stochastic memristive neural networks subject to deception attacks[J].Nonlinear Dynamics,2022,111(3):2443-2462.

[9]Shuo W ,Qingqi P ,Jianhua W , et al.An Intelligent Deployment Policy for Deception Resources Based on Reinforcement Learning[J].IEEE Access,2020,835792-35804.

[10]Ying G H ,Feng L .Network Security System Design Integrating Intrusion Deception and Dynamic Forensic Technology[J].Applied Mechanics and Materials,2013,443(443-443):451-455.

[11]Lin F S ,Li P X .Design of Network Security Monitoring System with Mechanical Properties Suitable for LAN Based on ARP Deception[J].Advanced Materials Research,2013,2250(648-648):319-322.

[12]Carroll E T ,Grosu D .A game theoretic investigation of deception in network security[J].Security and Communication Networks,2011,4(10):1162-1172.

[13]Du J ,Zhang X ,Zhou Y , et al.Active Defense Security Model in the Application of Network Deception System Design[C]//[出版者不详],2013.