

Research on Human-Computer Interaction Security Risk Analysis and Defense Strategy Based on Software Engineering Perspective

Qian Lin ^a

International college, Guangzhou College of Commerce, Guangzhou, Guangdong, China

Keywords: Software Engineering, Human-Computer Interaction, Security Risks, Defense Strategies.

Abstract: This article mainly analyzes the impact of human-computer interaction on users and software from the perspective of software engineering. This article first explains the concept and periodicity of software engineering, then explores the risk factors in human-computer interaction, and finally analyzes them with practical cases. Subsequently, this article implemented strategic strategies through Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). Finally, this article aims to provide comprehensive security protection for software systems through these strategies. The analysis in this article comprehensively covers multiple key aspects such as technology, management, and personnel. By integrating IDS and IPS technologies, real-time and comprehensive monitoring of network traffic is achieved. Once any abnormal or potential intrusion signs are detected, the system will immediately trigger a response mechanism, thereby promoting the deep application and continuous innovation of human-computer interaction security technology in the field of software engineering. In addition, a systematic analysis of human-machine interaction security risks from a software engineering perspective can not only effectively enrich and improve the existing software security theoretical system, but also open up new perspectives and paths for subsequent related research.


1 INTRODUCTION

In the Internet era, applications such as software systems have fully penetrated into social life. From health care, and mobile payment to intelligent transportation, human-computer interaction as the core link between software systems and users, its importance is self-evident. However, in this rapidly developing era, with the increasing power of software functions and the growing number of users, the security risks exposed during human-computer interaction have become increasingly severe. They exploit vulnerabilities in human-computer interaction systems for attacks, which can have a significant impact on users' user experience, hinder their normal use, and even threaten their personal information security. It has caused direct economic losses and privacy violations to users, and has also had a serious impact on the stable operation of software systems and the reputation of enterprises. Meanwhile, the continuous upgrading of cyber attack methods poses unprecedented challenges to the security of human-

computer interaction. Therefore, an in-depth analysis of security risks in human-computer interaction processes and an exploration of effective defense strategies are currently the key to solving the problem (Sun & Liang, 2018; Ge & Chen, 2019).

This article mainly analyzes the impact of human-computer interaction on users and software from the perspective of software engineering. This article first concludes the concept and periodicity of software engineering, then explores the risk factors in human-computer interaction, and finally analyzes them with practical cases. Subsequently, this article implemented strategic strategies through IDS and IPS. Finally, this article aims to provide comprehensive security protection for software systems through these strategies.

The analysis in this article comprehensively covers multiple key aspects such as technology, management, and personnel. By integrating intrusion detection system (IDS) and intrusion defense system (IPS) technologies, real-time and comprehensive monitoring of network traffic is achieved. Once any

^a <https://orcid.org/0009-0001-2127-0574>

abnormal or potential intrusion signs are detected, the system will immediately trigger a response mechanism, thereby promoting the deep application and continuous innovation of human-computer interaction security technology in the field of software engineering. In addition, a systematic analysis of human-machine interaction security risks from a software engineering perspective can not only effectively enrich and improve the existing software security theoretical system, but also open up new perspectives and paths for subsequent related research.

2 SOFTWARE ENGINEERING

As a discipline, software engineering is mainly committed to the efficient development of high-quality software, and plays a very important role in today's era of rapid digital development (Sui, 2025). Its core goal is to produce high-quality, low-cost software products that meet the needs of users. In the field of human-computer interaction, the concept of software engineering runs throughout, from the initiation of the software project to the final delivery, each stage has an important impact on the safety of human-computer interaction.

The software engineering life cycle consists of five closely related phases: requirements analysis, design, coding, testing, and maintenance. In the requirements analysis stage, the development team should clarify the software functions, performance, and security requirements, estimate security risks such as identity fraud and information leakage in human-computer interaction scenarios, and point out the direction for subsequent development. In the design stage, developers plan the system architecture, module interface and security mechanism according to the requirements, and use encryption and identity authentication technologies to build a multi-level protection system. During the coding phase, developers need to strictly follow the secure coding specifications to avoid introducing security vulnerabilities such as SQL injection. In the testing phase, functional, performance, and security tests are carried out to simulate attack scenarios to test protection capabilities. During the maintenance phase, the development team continuously monitors system security, fixes vulnerabilities in a timely manner, and updates the protection mechanism. As cyber threats are constantly changing, vigilance and timely response are the only ways to keep your software safe from emerging attacks.

3 IMPACT OF HUMAN-COMPUTER INTERACTION SECURITY RISKS

3.1 Multi-Dimensional Impacts on Users

3.1.1 Financial Losses

In human-computer interaction scenarios, user identity impersonation is a common cause of financial losses. If there are cybersecurity issues, it may lead to the leakage of users' personal information, endangering their privacy rights and property rights (Hu, 2023). For instance, phishing attackers create fake websites or emails that appear legitimate to trick users into entering sensitive information such as bank account numbers and passwords. Once attackers obtain this information, they can transfer funds from the users' accounts without their knowledge, causing direct financial losses. Additionally, some malicious software may tamper with transaction information during online payments, redirecting funds to accounts designated by the attackers, further exacerbating users' financial losses.

3.1.2 Privacy Infringement

The leakage of sensitive information is the primary means of infringing upon users' privacy. In many software systems, users input a large amount of personal information during human-computer interaction, including names, ID numbers, contact details, and home addresses. If the software system's security measures are inadequate, this information may be leaked. For example, certain non-compliant shopping platforms may have security vulnerabilities, leading to the leakage of users' shopping records, delivery addresses, etc. Once this information falls into the hands of criminals, it may be used for illegal activities such as spamming and fraud, seriously infringing upon users' privacy.

3.1.3 Trust Crisis

Frequent human-computer interaction security incidents can lead to a trust crisis among users regarding software systems. When users encounter issues such as information leakage or identity impersonation while using a particular software system, they will question the system's security. As a result, they may reduce their usage of the software,

and even spread negative information about it, affecting the software system's user reputation and market image. This trust crisis can significantly impact users' experience, hindering their normal use and even threatening their personal information security.

Such a trust crisis not only affects the number of existing users of the software system but also impedes the acquisition of new users, adversely impacting the software system's long-term development.

3.2 Comprehensive Impact on Software Systems

3.2.1 Reputation Damage

The reputation of a software system is a critical intangible asset, and human-computer interaction security incidents can severely damage it. Once security incidents such as user information leaks or identity impersonation occur, the media often widely reports on them, rapidly spreading negative perceptions of the software system and eroding user trust and goodwill. For example, when users encounter constant intelligent push notifications from digital ads during daily browsing, they not only feel annoyed and fatigued but also develop deep concerns about privacy violations. Users often attribute the collection of private data to digital advertising, fueling fears of privacy infringement and damaging the social reputation of digital ads (Pan & Zhou, 2018). Therefore, incidents involving user data leaks frequently attract significant attention, leading many users to question the platform's security. This results in decreased user engagement and a tarnished brand image.

3.2.2 Legal Risks

With the rapid advancement of artificial intelligence technology, we are witnessing technological innovation and unprecedented convenience, stepping into a new era of large-scale AI models. However, this progress also poses multifaceted challenges to existing legal frameworks (Li, 2025). If a software system fails to effectively protect user information security, it may face lawsuits and regulatory penalties. As laws and regulations increasingly emphasize personal information protection, many countries and regions have enacted relevant legal requirements mandating that software systems implement necessary security measures when collecting, using, and storing user data to ensure its safety. Violations of these laws and regulations may

lead to lawsuits from users seeking compensation, as well as penalties from regulatory authorities, such as fines or revocation of business licenses.

4 RISK CLASSIFICATION FROM A SOFTWARE PERSPECTIVE AND CASE STUDIES

4.1 Identity Impersonation Risk - Facebook Phishing Attack Incident

In 2021, Facebook suffered a large-scale phishing attack. The attackers impersonated official Facebook emails and sent fake account security notification emails to users. The emails claimed that the users' accounts were at security risk and required them to click a link for identity verification. The link led to a meticulously forged phishing website whose interface was almost identical to the official Facebook login page. Many users, without carefully scrutinizing it, entered their Facebook account credentials on the phishing site. After obtaining this information, the attackers successfully impersonated the users, posting false information, defrauding their friends, etc., which brought significant negative impacts to both the users and the platform.

From a software engineering perspective, although Facebook had an account password verification mechanism, the single-factor verification method allowed attackers to easily impersonate users once they acquired the account credentials. This reflects that during the software design phase, there was a lack of consideration for multi-factor authentication methods (such as Short Message Service (SMS) verification codes, biometric recognition, etc.), making it unable to effectively resist such attacks. It indicates that if various possible attack methods and security requirements are not fully considered in the early stages of software engineering, it will pose hidden dangers to human-computer interaction security.

4.2 Sensitive Information Leakage Risk - Marriott International Hotel Group User Information Leakage Incident

In 2018, Marriott International Hotel Group announced that the guest reservation database of its subsidiary, Starwood Hotels, had been hacked, and the information of approximately 500 million guests might have been leaked. This information included

names, mailing addresses, phone numbers, email addresses, passport numbers, account information, dates of birth, genders, and other sensitive details. The attackers had been lurking in the hotel's network for a long time and exploited security vulnerabilities in the database to obtain this information. After the information was leaked, some guests received fraudulent phone calls and emails, bringing serious security risks to them.

Marriott International Hotel Group's database had security vulnerabilities that the attackers could exploit to infiltrate it. The database's security protection measures were inadequate, such as loose access control and imperfect encryption measures, enabling the attackers to easily obtain a large amount of sensitive information.

In terms of data management, the access permission management for data was not detailed enough, and there was a risk of information leakage due to potential violations by internal personnel. In terms of data storage, sensitive information was not sufficiently encrypted. Even if the data was illegally obtained, the attackers could directly read it.

This reflects negligence in database security management and insufficient encryption of sensitive data during the software development and maintenance stages.

5 DEFENSE STRATEGY BASED ON SOFTWARE ENGINEERING

Intrusion detection systems and intrusion defense systems are key technologies for detecting and preventing attacks by monitoring and analyzing network traffic, and are the cornerstone of network security (Wang, 2025). There are significant differences between the two in terms of functional positioning, working methods, deployment locations, and applicable scenarios, which need to be selected or combined according to actual needs. IDS detects abnormal behavior and features through deep analysis of network traffic, audit data, and system logs, identifies potential malicious activities and security threats, matches known attack patterns with algorithm models and feature databases, and uses dynamic learning and adaptive machine learning techniques to deal with unknown threats, cyclically improving detection strategies. Once abnormal or intrusion signs are detected, IDS will immediately sound an alarm and report relevant information to the security information and event management system for

processing by IPS. IPS will immediately execute response actions, reset network connections, reject packet transmission, and automatically deploy new security rules (Xia, 2024).

5.1 Security Design Phase Strategy

Conduct comprehensive security testing and evaluate the functionality and performance of IDS/IPS during the testing and validation phase of the software system. Security testing includes multiple aspects such as functional testing, performance testing, and security vulnerability scanning. In functional testing, verify whether IDS/IPS can accurately detect and defend against various network attacks. In performance testing, test the processing capability and response speed of IDS/IPS under high load conditions. Considering that software systems may face a large number of concurrent requests during actual operation, it is necessary to ensure that IDS/IPS does not affect the normal operation of the entire system due to performance bottlenecks. Security vulnerability scanning uses professional vulnerability scanning tools to scan IDS/IPS itself, and with the continuous application of new technologies such as cloud computing and big data in software engineering, IDS/IPS also needs to adapt to new security challenges and discover potential security vulnerabilities. In the design phase, it is necessary to fully consider the compatibility and security of different verification factors. For example, SMS verification code services should choose reliable telecom operators to ensure the timely and accurate sending of verification codes. Biometric recognition technology requires the use of advanced algorithms and equipment to ensure the accuracy and stability of recognition. At the same time, it is necessary to design a reasonable verification process to avoid the verification process being too cumbersome and affecting the user experience. The integration of artificial intelligence technology in these systems enables them to more accurately identify and defend against various network attacks (He, 2019; Jiang, 2024; Bai, 2025).

5.2 Maintenance and Update Strategy

Vulnerability patching and patch management are essential components of network security, involving updates to operating systems, applications, and device firmware. During the maintenance and update phase of the software system, regular security checks and updates are conducted on the system, while upgrading IDS/IPS. Security checks include checking

the security configuration, software version, security vulnerabilities, and other aspects of the system. Regularly update software components and libraries of the software system, and promptly fix known security vulnerabilities. For IDS/IPS, timely attention should be paid to its updated information and upgrading to the latest version to obtain better detection and defense capabilities. Timely patching of discovered vulnerabilities can effectively prevent attackers from exploiting these vulnerabilities to invade the system. For example, when IDS/IPS vendors release new attack feature libraries or defense strategies, they should update them in a timely manner to identify and defend against the latest network attacks. Establish a regular safety inspection and update mechanism, clarify the inspection and update cycle and responsible persons. Use professional security inspection tools to conduct a comprehensive security check on the system. Promptly address any issues discovered during the inspection and update process, and record relevant information. Timely follow the updated information of IDS/IPS suppliers and upgrade according to official documents.

6 CONCLUSIONS

With the continuous innovation and development of computer network technology, information technology network systems are becoming increasingly robust. However, looking at the current state of computer network technology, there are still many problems and shortcomings. These issues lead to vulnerabilities in computer network information technology, posing significant security risks to computer networks. This study focuses on the security risks of human-computer interaction, which has important practical and theoretical significance. From a multidimensional perspective, these risks can not only lead to user information leakage, privacy violations, and operational errors, affecting trust and user experience, but also cause software system failures, data loss, and service interruptions, damaging their stability and availability. Through risk classification and case analysis, the characteristics and hazards of these risks have been clarified, providing a basis for defense strategies.

The impact of security risks can have many negative effects on both individuals and enterprises, resulting in substantial losses. In terms of defense strategies, during the security design phase, security concepts should be integrated into every aspect, with enhanced code review, as well as intrusion detection

system and intrusion prevention system testing. During the maintenance and update phase, continuous monitoring and response to security incidents are necessary. However, challenges such as rapid updates in security technology, lack of unified standards, and differences in user security awareness still exist. In the future, it is necessary to strengthen research on the security of emerging technologies, promote the unification of security standards, and conduct user security education. This study provides a reference for human-computer interaction security in the field of software engineering. With in-depth research and technological development, human-computer interaction security will be better safeguarded.

REFERENCES

- Bai, Z. (2025). Vulnerability Detection and Countermeasure Analysis of Computer Network Security. *Electronics Technology*, 54(01), 286–287.
- Ge, K., & Chen, T. (2019). A Survey of Offensive and Defensive Security in Human-Computer Interaction. *Telecommunication Science*, 35(10), 100–116.
- He, J. (2019). Analysis and Defensive Strategies of Computer Software Security Issues. *Computer Knowledge and Technology*, 15(11), 44–45.
- Hu, J. (2023). Risk Control of Computer Network Security in the Context of Artificial Intelligence. *Digital Communication World*, (04), 186–188.
- Jiang, H. (2024). Research on Risk Assessment and Prevention Strategies of Internet Information Security Based on Artificial Intelligence. *China New Communications*, 26(20), 32–34+172.
- Li, J. (2025). Challenges, Opportunities, and Innovative Strategies Facing Fundamental Jurisprudence in the Era of Large AI Models. *Jinyang Journal*, (03), 63–71.
- Pan, H., & Zhou, Y. (2018). The “Guilt by Association” Effect of Reputation Damage among Corporate Group Members: Empirical Evidence from Bank Loan Costs. *Journal of Xiamen University (Philosophy and Social Sciences)*, (05), 53–64.
- Sui, Q. (2025). Research on Software Engineering Technology Based on Explainable Artificial Intelligence in Higher Education. In *Proceedings of the 2025 Forum on Higher Education Development (Volume II)* (pp. 195–196). Henan Private Education Association. Harbin Guangxia College.
- Sun, J., & Liang, L. (2018). Analysis of Computer Software Security Issues and Protection Strategies. *Computer Knowledge and Technology*, 14(26), 22–23.
- Wang, Y. (2025). Research on Computer Network Information Security Protection under the Background of “Internet Plus.” *Home Appliance Repair*, (05), 77–79.
- Xia, S. (2024). Application of Cybersecurity Technologies in Network Security Operation and Maintenance. *Cybersecurity and Informatization*, (02), 135.