Theory and Practice of Science and Technology
2024, VOL. 5, NO. 6, 18-23
DOI: 10.47297/taposatWSP2633-456903.20240506

Research on the integration of software engineering security challenges and information security technology

Yuanhaocheng Li

Sanya Yinggong Education and Training Co., Ltd 572099

ABSTRACT

under the background of the era of information technology, the security of software engineering is given the unprecedented importance, but it also faces multidimensional challenges, such as security vulnerabilities and design flaws, the complexity of input validation and identity authentication, sensitive data closely protection requirements and the potential threat of malicious code, etc. Information security technology system, covering encryption algorithm, authentication and authorization mechanism, security audit and real-time monitoring and other aspects, provides a strong technical support for solving the above challenges. In order to effectively deal with the security dilemma in the field of software engineering, a series of strategic suggestions are put forward in this study: first, build and improve the comprehensive security supervision framework of computer software; second, strengthen the privacy protection measures of users' personal information; secondly, rationally deploy cryptographic technology and strengthen the training of professional and technical personnel; finally, strengthen the security review and supervision of the full cycle of software engineering projects. The results show that the deep integration of information security technology and software engineering has profound significance for solving the current security problems. In the future, relevant research and application should be further strengthened to improve the security of software engineering and promote the healthy development of computer technology.

KEYWORDS

software engineering security; information security technology; security challenges response; technology integration

1 Introduction

In the rapid development of information technology, software engineering is playing a vital role in the field of information technology. However, with the extensive application and deep penetration of software system, the security threat is also increasingly severe. From data leakage, malicious software attacks to system paralysis, the security problem of software engineering has become an important bottleneck restricting the healthy development of information technology. (Chen Xingyu, 2024) [1]. In this context, it is particularly necessary and urgent to study the integration of software engineering security challenges and information security technology. By integrating information security technology, it can effectively deal with security threats in software engineering, protect the confidentiality, integrity and availability of user data, and maintain the stability and reliability of the system. At the same time, this research also helps to promote the healthy development of software engineering technology, improve the quality and safety of software products, and provide a solid security guarantee for the wide application of information technology.

Reviewing the research status in related fields, predecessors have made a series of important achievements in software engineering security and information security technology. These studies cover many aspects of security code specification, security design mode, security audit and monitoring, and provide strong technical support for the security design and development of software engineering. However, the existing research still has some shortcomings, such as insufficient research on the emerging security challenges, and insufficient integration and application of security protection technologies. Therefore, it is necessary to further strengthen the research on the integration of software engineering security challenges and information security technologies to cope with the increasingly complex and changeable security threats.

This paper aims to study the integration mechanism of software engineering security challenge and information security technology, clarify its necessity and urgency, and discuss how to effectively handle the security threat in software engineering by integrating information security technology. The main research contents include the analysis of software engineering security challenges, the integration strategy of information security technology, the design and implementation of security protection technology, etc. Through the research of this paper, it is expected to provide new ideas and methods for the safety design and development of software engineering, promote the innovation and development of software engineering safety technology, and make positive contributions to the protection of user data, maintain the stability of the system and promote the healthy development of technology.

2 A summary of the related theories

2.1 Overview of software engineering safety

Under the background of the rapid development of information technology, software engineering security is facing unprecedented challenges. As the core field of information technology, software engineering needs to ensure that the software system is protected from malicious attacks, data leakage, function tampering and other threats in the whole life cycle of development, deployment, operation and maintenance. The core goal of software engineering security is to maintain the integrity, confidentiality and availability of the software system, that is, the software shall not be modified or destroyed without authorization, the data and information processed by the software shall not be illegally accessed or leaked, and the software can operate normally and provide services when needed. However, with the increasing complexity and interconnection of software systems, as well as the wide application of emerging technologies such as cloud computing, big data and the Internet of Things, software engineering security faces more severe challenges. Design defects, coding vulnerabilities, DDoS attacks, SQL injection, cross-site scripting attacks and other security risks are becoming increasingly prominent. In order to meet these challenges, the software engineering field needs to strengthen the integration with information security technology, using encryption technology, firewall technology, intrusion detection technology and identity authentication technology, to provide security guarantee. At the same time, the software engineering security also need to pay attention to the whole life cycle of safety management, from demand analysis, design, coding, testing to the deployment, operation and maintenance of each stage should be considered security issues, by establishing safety specification, strengthen safety training, establish safety audit mechanism, to ensure that the software system in the whole life cycle to maintain high security. To sum up, software engineering security is the key to ensure the stable operation of the software system in the complex network environment. In the face of severe challenges, it is necessary to strengthen the integration of information security technology and the whole life cycle security management to build a safe and

reliable software system.

2.2 Overview of information security technology

With the increasingly complex challenges of software engineering, information security technology has become the key to guarantee software system and data security. This field covers the technical means to prevent, detect and respond to potential security risks, with encryption technologies, hash functions, authentication and authorization mechanisms, and security audit and monitoring technologies all playing a central role. Crycryption technologies include symmetric encryption (such as AES) and asymmetric encryption (such as RSA), which are suitable for efficient data encryption, key management and digital signature, respectively. The hash function (such as SHA-256) ensures data integrity and authenticity by generating a unique data summary. In terms of access control, multi-factor authentication (MFA), role-based access control (RBAC) and attribute-based access control (ABAC) effectively improve the accuracy of authentication and the degree of refinement of authority management. In addition, security audit and monitoring technologies, such as log management systems, exception detection systems, and intrusion prevention systems (IPS), are able to detect and respond to security incidents in a timely manner. Emerging technologies such as blockchain, zero-trust architecture, and Security Automation and Response (SOAR) further enhance data security, access control rigor, and security event processing efficiency, providing more comprehensive and advanced solutions in the software engineering security field.

3 Challenges for software engineering security

As a complex and increasingly prominent research field, its importance is increasing with the rapid progress of technology. Given that software systems have been widely penetrated into various industries and become the core cornerstone of supporting business operations and data processing, their security issues are directly related to the stability of system operation and the security of data assets. Specifically, the safety problems in software engineering can be summarized into the following core aspects:

3.1 Security vulnerabilities and design defects: a major threat to software security

Security vulnerabilities constitute the most common and serious threat among software security problems. Such vulnerabilities often result from improper processing in the design or maintenance process, providing a way for attackers to easily penetrate the software system and steal sensitive private data, thus posing a significant threat to the information security of users. In addition, in the field of software engineering, design defects can also not be ignored as a common safety problem. These defects, including errors and omissions, are usually apparent in the early stages of the software development cycle, and are often caused by the neglect or lack of sufficient attention to security issues (Wang Cui, Kong Yali, 2024) [2].

3.2 Ensure input authentication and authentication, and prevent application attacks

Inadequate input validation mechanisms may provide an opportunity for malicious users to attack an application using input malicious data. Therefore, developers must ensure that all input data undergo a rigorous and accurate verification and filtering process to effectively defend against common security threats such as cross-site scripting attacks (XSS) and SQL injection attacks. In addition, building a sound software application requires an effective authentication and

authorization mechanism designed to ensure that only authorized users can access and execute specific functional modules. On the contrary, the lack or improper implementation of authentication and authorization mechanism may directly cause serious security problems such as unauthorized access behavior and illegal promotion of authority (Wang Junxiang, 2023)[3].

3.3 Sensitive data storage and transmission: encryption protection and configuration security

In the process of storing and transmitting sensitive data, the implementation of encryption and protection measures is an indispensable security strategy. Unencrypted data is easily a target for theft or tampering, thus causing a significant risk of data leakage and integrity damage. In order to ensure the safe transmission and storage of data, the application program and server configuration needs to go through a strict audit process and security parameter setting, in order to fundamentally eliminate the potential system vulnerabilities and attack vectors. Given that the default configuration often fails to achieve the optimal safety state, refined configuration adjustment must be made to effectively improve the safety protection efficiency and robustness of the entire system (Tan Junyang, 2020)[4].

3.4 malicious code poses another major challenge to software security

Malicious software is characterized by its malicious purpose of system attack and data destruction. It spreads through a variety of complex transmission mechanisms such as telephone hijacking, virus infection and Trojan horse penetration, showing extremely high hidden performance. It is often latent in the deep structure of software release and is difficult to be detected by conventional means. Therefore, strengthen the software security review and testing process, and use the code depth analysis, real-time monitoring behavior, advanced information security technology, to effectively identify and remove potential malicious code, ensure the security of the software system stability, has crucial academic and practical significance (lee, 2020)[5].

To sum up, software engineering security faces multiple challenges from both traditional and emerging fields. To meet these challenges, it is necessary to deeply study software engineering safety technology and methods, strengthen safety protection measures, and improve the security and reliability of software system. At the same time, more security education and training are also needed to improve the security awareness and skill level of developers and users.

4 Security problem solving strategy for software engineering based on information security technology

4.1 Establish and improve the computer software security supervision mechanism

In the process of computer application, users often use various technical means to manage the computer system, and in this process, users often ignore the management of the computer system. The computer system is composed of many software, and once the software security problems, will directly affect the rights and interests of the computer. Therefore, in the process of software development, the relevant personnel should increase the management of the software system, in timely maintenance and repair of security problems, in order to reduce the risk of vulnerabilities in the system.

In the process of security management of computer software engineering, the government is not only the rule-maker, but also the guardian of information security. As an important software user,

the government itself is also faced with complex and changeable information security threats. In order to protect national security, social order and public interests, the government must actively assume the responsibility of supervision, and establish a comprehensive and efficient safety supervision mechanism through the formulation and implementation of relevant policies and systems.

4.2 Strengthen the protection of users' personal information

Users are the ultimate users of computer software and the main disseminators of the virus. In the process of software use, we should strengthen the guidance of user operation, and users should also take the initiative to strengthen the security awareness. Users should follow the principle of minimization when handling personal privacy data, that is, to upload only the necessary data to the network, and to ensure the use of strong password and encryption technology to protect the confidentiality and integrity of personal data. During using the Internet, users should not log in to illegal websites or download software installation packages of unknown sources, so as to reduce the risk of virus and malware infection. When installing the software, the user should carefully review every step during the installation process to ensure that the unauthorized or unneeded bundled software is not installed. By strengthening the awareness of self, the virus refused outside the personal computer.

4.3 Reasonable application of cryptography technology and strengthen professional skills training

Cryptography is a common technical means in the process of computer application. Using cryptography technology can effectively improve the efficiency of solving software engineering security problems. In the process of software development, the relevant personnel should reasonably apply the cryptographic technology. In the development of design software, the function and function of the software should be reasonably planned, and then according to the user needs to choose the appropriate password for development and design. In the security management of the computer system, the password technology should also be reasonably applied, such as the classification management of different accounts and passwords used by users, to improve the security of the system. At the same time, in the process of software engineering project development, it is necessary to strengthen the attention to the professional skills training of software engineering project developers to ensure that relevant personnel can master various skills related to their work. At the same time, in the process of software engineering project development, it is necessary to strengthen the computer technology application ability and network security awareness training work, so that the relevant personnel can master the computer network technology application methods and application skills, improve the level of computer network technology.

4.4 Strengthen the safety review and supervision of software engineering projects

In the process of the software engineering project development, it is necessary to strengthen the safety review of the software engineering project, so as to find out and solve the existing problems and deficiencies in time. At the initial stage of the project development, the technology and content involved in the project should be understood in detail to ensure that there will be no problems in the development process of the software engineering project. After the completion of the software engineering project development, the software engineering project should be accepted in time to

ensure that the software engineering project can complete the acceptance work within the specified time, so as to improve the security of the computer system. In addition, network security supervision is one of the more important work in the field of current information security technology. In the process of network application, we should strengthen the importance of network security supervision. In order to reduce the situation of computer information leakage, relevant personnel need to regularly check and monitor the network security situation, and deal with problems in time. Relevant departments can establish the relevant network supervision platform to effectively supervise the computer information system. At the same time, in order to avoid some criminals through the network for malicious attacks and other activities, the relevant departments can also establish a network security firewall to protect the computer information system.

5 Conclusions and outlook

At present, although China's computer software development and information security technology has made some achievements, but there are still many problems. These issues need to be properly addressed, especially in the software engineering field. In the process of software development and design, the relevant personnel must improve the importance of information security problems, strengthen the application and research of information security technology, and reduce the adverse impact of software engineering security problems on computer application as far as possible. This paper focuses on the in-depth integration of security problems and information security technology in software engineering, and puts forward a series of solutions to the main security problems existing in software engineering, aiming to integrate effective information security technology into software engineering and provide certain reference for relevant personnel.

About the Author

Yuanhaocheng Li, Research direction: Mathematics, Finance, Computer Science.

References

[1] Chen Xingyu. Research on Information Security Protection of Computer Network based on Big Data Technology [J]. Cyberspace Security, 2024,15 (4): 236-239.

[2] Wang Cui, Kong Yali. Research and analysis of database programming technology based on computer software engineering [J]. Software, 2024,45(5): 89-91.

[3] Wang Junxiang. Application of data encryption technology in computer network information security [J]. Digital Communication World, 2023(7): 141-143.

[4] Tan Junyang. Discussion on information system integration technology and software development [J]. Technology and Market, 2020,27(6): 102, 104.

[5] Li Kuan. Research on the application of system integration technology in information management system [J]. Information and Computer (theoretical edition), 2020,32(5): 5-7.