Academic Journal of Science and Technology
ISSN: 2771-3032 | Vol. 14, No. 1, 2025

A Study of Software Security in Software Engineering

Liuwen Kong*

School of Computing, Engineering & Physical Sciences, University of the West of Scotland, Glasgow, G72 0LH, UK
*Corresponding author: kongliuwen2024@outlook.com

Abstract: In the field of software engineering, software security has increasingly become a key research field, especially in aviation, automobile, medical and other industries that require high system stability. With the wide application of software intensive systems, ensuring software security is not only related to the normal operation of the system, but also related to public safety. This paper will discuss the importance of software security in software engineering, the latest research progress at home and abroad, and the application in DevSecOps practice, and look forward to the future development trend and challenges.

Keywords: Software engineering; software security; research that.

1. Introduction

With the rapid progress of science and technology, software has penetrated into all areas of our lives, from smart phone applications in daily life, to information systems for commercial operations, to aviation, medical and transportation equipment related to life safety. In this digital era, the reliability and security of software have become unprecedented important. Software security is not only related to the confidentiality of data, but also directly related to the safety of users' lives and property. For example, the "heart bleed" vulnerability event in 2015 exposed serious security problems in the OpenSSL library, affected millions of websites around the world, and put hundreds of millions of user data at risk. Such events remind us that the importance of software security cannot be ignored and must be paid attention to and guaranteed in the whole life cycle of software engineering.

2. Background of Software Security Research and Progress at Home and Abroad

The origin and development of software security research is a microcosm of modern science and technology, which evolves with the rapid progress of information technology. With the popularization of the Internet and the deepening of digital transformation, the complexity and scale of the software system is increasing, and with it, the complexity and diversity of security threats are also growing exponentially. In this context, the importance of software security research is gradually emphasized, which is not only related to the privacy of personal data, but also related to the security of national critical infrastructure.

The research on software security at home and abroad has made remarkable progress in the past decade. Internationally, the airborne software security analysis framework proposed by the General Airworthiness Administration of the United States provides a solid theoretical basis and practical guidance for security in the field of software engineering. This framework integrates software safety analysis into all aspects of the software life cycle, emphasizes the necessity of safety consideration at the beginning of design, and provides an effective tool to ensure the safety of software in key areas such as aviation.

In China, the research force represented by CodeWisdom team of School of Computer Science and Technology of Fudan University has taken the lead in the field of software security. At the international conference ISSTA in 2024, the team published a series of research results, which covered software testing, analysis and other aspects, such as open source software license analysis, automatic driving system simulation test, etc. The paper on license analysis of open source software proposed LiVo method, which effectively guaranteed the legitimacy and security of open source software by detecting and repairing violations of license modification terms. These research results have had a profound impact on the world, and also promoted the in-depth research on software security in China.

3. Application and Practice of Software Security in DevSecOps

In the practice of software development and operation and maintenance integration (DevSecOps), software security has become the key factor to ensure the success of the project. The core idea of DevSecOps mode is to integrate security into every stage of software development, from demand analysis to software deployment, to ensure that security always goes hand in hand with agile development, and to improve the security of the entire software life cycle. In this way, the software team can identify and solve security problems when the software is still in its early stage, and avoid paying high repair costs in the later stage.

Microsoft's Security Development Lifecycle (SDL) is a widely known practice framework, which emphasizes the need for security assessment and design at every stage of software development. SDL includes threat modeling, code review, security testing and other steps to ensure that the software has good security from the beginning of design. The Software Assurance Maturity Model (SAMM) of OWASP (Open Web Application Security Project) provides more comprehensive guidance for organizations. It covers four key links: planning, implementation, measurement and improvement, and aims to improve the organization's software security capabilities.

In terms of enterprise practice, Huawei has made remarkable achievements in the implementation of DevSecOps. Huawei has built a data security and privacy protection design for the whole life cycle. It applies the

security concept to every aspect of software development, including data isolation, data encryption, data redundancy and privacy protection design. This practice ensures that software can always effectively respond to security challenges in the process of design, development, testing and operation and maintenance, and reflects the important role of software security and reliability engineering.

4. Theoretical Foundations and Practical Applications of Software Security

Software security is a core issue in software engineering, and its theoretical foundation and practical application are the key to ensure software reliability and user trust. In the whole process of software development, the consideration and practice of security covers various stages such as design, coding, testing, maintenance, etc., and is closely connected with the engineering of software reliability. In terms of theoretical research, software security analysis frameworks and metric models provide a scientific basis for quantifying security performance, enabling software engineers to systematically assess and improve software security.

Software security analysis frameworks, such as the airborne software security analysis framework provided by the U.S. General Aviation Administration, provide a structured system for software security analysis, including security analysis methods for design, development, testing and maintenance. These frameworks emphasize the consideration of security factors at the early stage of software design, through threat modeling, risk assessment and security design, to ensure that the software has security from the source.

The construction of measurement model is another important part of software security research. They provide a set of indicators to quantify the security and vulnerability of software. For example, the definition and measurement model of software security can help engineers to evaluate the security quality of code according to these indicators, so as to timely discover and repair potential security risks in the development process. In practice, the security measurement model can be applied to the continuous integration and continuous delivery (CI/CD) process, and the security status can be fed back in real time through automated tools, making security inspection a natural part of the development process.

In the software development phase, code review and static code analysis are two common practical methods, which can detect potential security vulnerabilities in code, such as buffer overflow, SQL injection and insecure password storage. Dynamic analysis, such as fuzzy testing, penetration testing and security scanning, is also an important tool in the testing phase. They can find security problems in software runtime by simulating real attacks.

Another focus of the software testing phase is security testing, which covers both functional security testing and penetration testing to ensure that the software is able to withstand or alert to malicious attacks. In addition, security practices should not be overlooked during the maintenance phase of software, which includes regular security audits, vulnerability management, and timely deployment of security patches. Software reliability engineering is particularly important in this phase, which ensures that the software can maintain normal operation in the event of an attack or failure through redundant design, error detection and recovery mechanisms.

In the application of software practices, enterprises such as Huawei ensure that software always complies with security norms during development and operation and maintenance by building a full life-cycle security design. This includes data security and privacy protection design, such as data encryption, data segregation, and privacy protection technologies, which are taken into account in the early stages of software design to ensure that the software has good security in every aspect.

For example, Huawei uses threat modeling to identify potential security risks, and develops corresponding protective measures based on risk levels. In the coding phase, static code analysis tools are used to conduct deep scans of code to eliminate possible security risks. In the testing phase, Huawei conducts not only functional tests, but also rigorous security tests, such as penetration tests and security audits, to ensure that the software meets security standards before going live. In the operation and maintenance phase, Huawei monitors system security in real time through automated tools to ensure that security incidents are detected and handled at the first opportunity.

The combination of theoretical foundation and practical application of software security makes software security move from concept to practice, and improves the security level of software and the trust of users. With the progress of technology and the evolution of security threats, software security research will continue to deepen, and constantly put forward new theories and methods to cope with more complex and changing security challenges. At the same time, the successful cases in enterprise practice will also provide valuable practical experience for academic research and promote the overall improvement of software security.

5. Conclusion

In the face of the future, software security research will continue to integrate the latest technological trends, such as intelligent analysis and big language modeling, to cope with increasingly complex application scenarios and security threats. At the same time, researchers and engineers need to explore new theories and methods to improve the accuracy and efficiency of software security analysis. Through continuous innovation and practice, software engineering will be able to better guarantee the security of software and provide a solid foundation for the digital transformation of society.

References

[1] He Yuling Application of software engineering technology in system software development [J] Computer Products and Circulation, 2018, (03): 34

[2] Zhang Yalin, Geng Xiangyi Research on software security assurance framework based on software engineering idea [J] Computer Knowledge and Technology, 2009, 5 (31): 8731-8732

[3] Niu Aimin, Ye Dongsheng Application of software security technology in engineering [J] Computer Engineering and Design, 2007, (20): 5063-5065