Research on Software Testing Security

Yan Li

Xi'an Fanyi University, Xi'an, 710105, China China

18058909@qq.com

Keywords: Software Testing, Security, Testing Process

Abstract: the Leakage of Software Information, Related Documentation and Other Important Software Information That Occurs in the Process of Software Testing Presents a Threat to Software Security. the Analysis of the Security Threats That May Exist in the Testing Process and Information Security Protection Method for Guaranteeing Software Testing Security Are Presented in This Article.

1. Introduction

The software testing is a process that is conducted with a manual or automated method to perform or evaluate a system or system component in order to verify whether the software has met the specified requirements, or to identify whether there are any differences between the desired and actual results. As a specialized technology, software testing was not developed along with the generation of computer. In the early stages of software development, people paid little attention to the importance of software testing. As people understand the significance of software testing in a more and more in-depth way, the proportion of the software testing phase to the whole software development cycle is increasing day by day.

Different software contains different industrial information. Some software even contains confidential documents of industries, the susceptibility of the industrial information which is included in the software, and vulnerability of information systems may easily lead to the leakage related sensitive information. However, there will exist a large number of test data and documents in the software online testing process, and also, sensitive information and privacy data of the tested software are involved in the process. Certain security risks come along with the test process: information may be tampered, forged, embezzled, or intercepted; a security incident may easily cause information loss, disclosure, even make the virus spread in the software system, resulting in huge losses. Therefore, the information security protection is extremely important for the software of industrial confidentiality. For this reason, such features should be guaranteed at the same time in the software online test process: availability, confidentiality, authenticity, integrity, controllability, non-repudiation, and identifiability. Software testing should be designed on the basis of the requirement specification, design documents, so that a safe test environment can be set up to ensure test safety.

2. The Technology and Process of Software Testing

As shown in Fig. 1, existing software testing technologies are usually divided into static testing technologies and dynamic testing technologies. A static test is a process in which the defects that may occur in the program code are detected or the program code is evaluated without executing the code. Static testing includes static testing that is primarily performed by manual code review, code walkthrough, desktop inspection, and static analysis that is mainly performed by automatic software tools. In a broad sense, static tests include software requirements analysis and technical review at the design stage.

Copyright © (2019) Francis Academic Press, UK DOI: 10.25236/ISMHI.2019.058

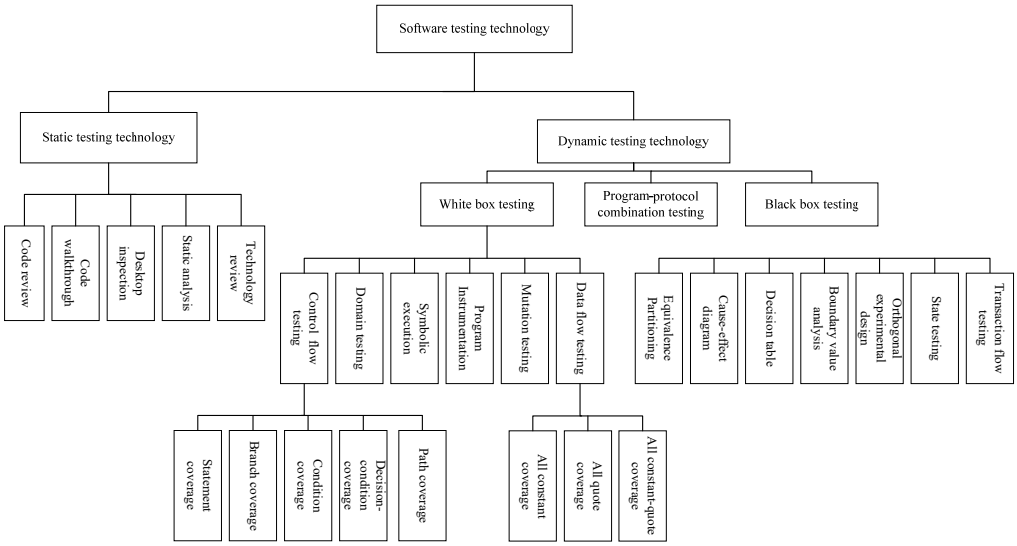

Fig.1 Classification of the Software Testing Technologies

The dynamic test detects the defects by checking the dynamic behaviors and running results of the program through running the program on sampled data. Dynamic testing includes the production of testing cases, program running and program verification, which are the core contents, as well as document preparation, data management, operating procedures and tool applications and other ancillary work. The most important issue for dynamic testing is the strategy for producing testing cases. It is the key to the effectiveness and efficiency of dynamic testing. The testing case includes input data and expected result. Generally speaking, when a test case is produced, due to the difficulty of constructing the expected result, the input data is the focus or the only product, and called test data. The following discussion is based on the statement above.

The complete software testing work should run through the entire software life cycle, meaning in two respects: (1) there are software testing works on different stages of software development; (2) The various steps of software testing exist throughout the whole software life cycle.

Figure 2 depicts the distribution of the software testing steps at different stages in the software life cycle (The left-to-right order shown in Fig. 2 represents the before-to-after time order). According to the software testing process, the software testing work is divided into plan, which refers to the test plan, design, which refers to the test design, and the implementation, including evaluation, which refers to the implementation of the test and the determination of results, evaluation of testing results and tested software. The Figure 2 shows that the software testing is conducted continuously during software development. This fact reflects the principle of software testing: start software testing as soon as possible, and do the work continuously.

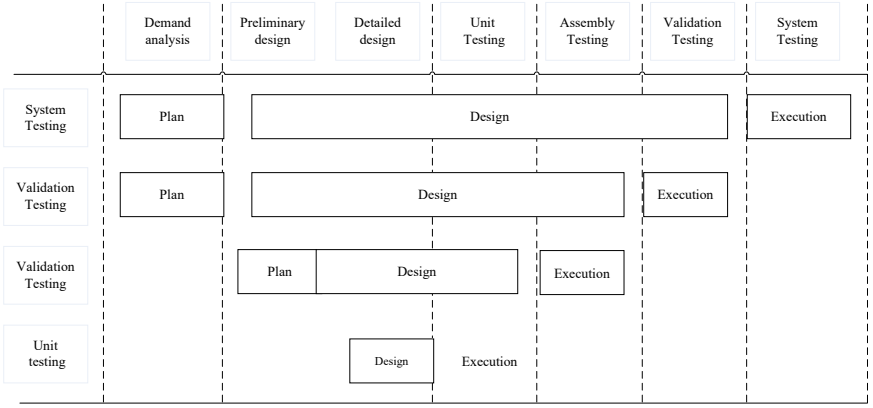

Fig.2 Activity Distribution in the Phases of Software Testing

3. Information Security Issues in Software Testing

The software testing process includes test requirements analysis, test planning, test design and implementation, test execution, test summary, and so on. All phases in the testing process require information security protection. The entire independent software testing process is shown in Figure 3.

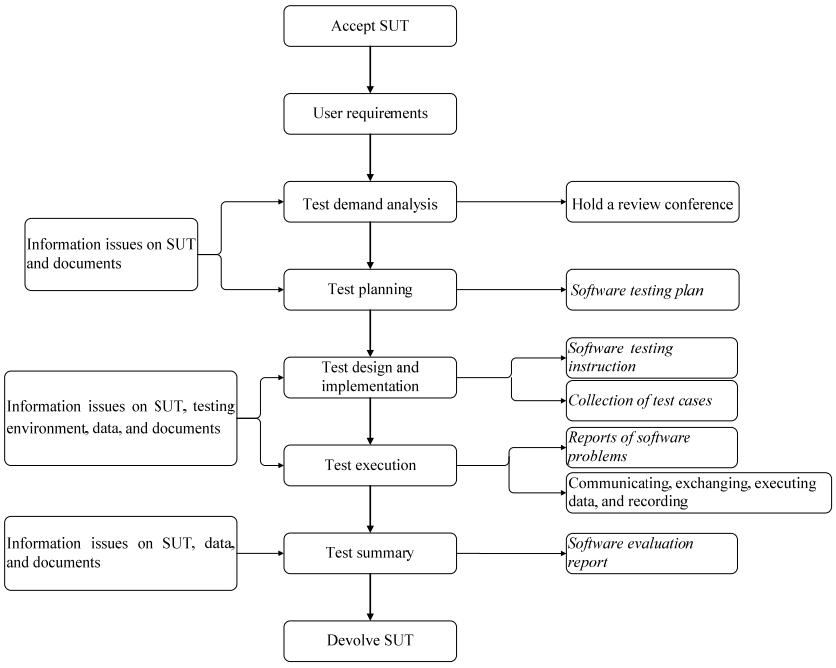

Fig.3 Software Test Flow Chart

Many of the national industry standards require clearly that the evaluation agency should encrypt the file format which is submitted by software users, program code, software copyright and other information in the software testing process, protect the media where test results are stored effectively, and protect the paper test information and its transmission security. Due to the differences between testing environments and the limitations of environmental factors, current software testing platforms are generally based on the information system provided by evaluation agency, requiring the tester to inspect and recognize technical site. The confidential information, test results and important documents involved in some of the tests, and the use and transmission of important data and documents transmission are prone to safety risk points. In this regard, the design for a solution to the security problems is presented in the article, and relevant risk control process is shown in Fig. 2. Through this design, risk points of the test process are put forward clearly, the storage and transmission of relevant secret documents or important data should be encrypted, and the risks in the test process are generally eliminated. In addition, people who take part in the test and the relevant personnel from the entrusted units should also receive confidential training, and sign a confidentiality agreement, preventing the occurrence of security risks the management means.

In the test demand analysis phase, the test project team accepts SUT (Software Under Test) submitted by the measured side, and the test pieces are distributed to testers by the test leader in accordance with their division of work. The security protection for information of SUT: Ensure that the security of SUT during storage, distribution, use and other phases. Ensure the information is not embezzled, tampered, or lost. Ensure the dissemination and content of controllable information. Ensure the confidentiality of document contents that is related to intellectual property protection, or contain industrial confidential information. The test project team should complete the preparation of the test plan documents in the test planning process. The testers should ensure the security of information in the transmission process. At the same time, the confidentiality and integrity of the software test plan should be guaranteed. While the testers test and implement the design, prepared test data should be complete, the establishment of the test environment should be effective, and the

designed test cases should be controllable and visual, ensuring an effective protection of security is set up for information. While testers are implementing the test, the original test records should be under strict control, the test executive and the test supervisor should be full-time, and these two jobs should not be done by a same person concurrently. The test team members should make and digital signatures and share encryption on the original test cases which they are responsible, related documents and other, send them to the test project leader after giving decryption authority to him or her, and it is the leader's duty to integrate test records. While summarizing the test, testers should ensure the confidentiality and integrity of the information in the report or evaluation. To ensure the objective and impartiality of the test, it is necessary to ensure that the information contained in the test report is of authenticity, completeness, and non-repudiation. When the test report involves software intellectual property, or contains sensitive information, it is necessary to ensure that the sensitive information is not disclosed.

4. Conclusion

Software information security should ensure that the authenticity confidentiality, integrity, availability, controllability, and non-repudiation, and identifiability of information. Software testing should be based on the requirements of the software specifications, design documents, and other information, to build a safe test environment, ensuring the safety of testing. A large number of test data and documentation are produced during testing, involving sensitive information and privacy data test of the software. For this reason, the formation security protection is extremely important for software that contains the industrial confidential information,. For the independent third-party testing of software, information security technology alone is not enough, we should take trinity measures, including information security technology, security control methods, system construction, to set a goal for information security guarantee in all domains, and to build a corresponding guarantee system, so that the security of information system can be ensured fundamentally.

References

[1] Yang R, Xu Q, Au MH, Yu Z, Wang H, Zhou L. Position based cryptography with location privacy: A step for Fog Computing. Future Generation Computer Systems, 2018, 78(2).799-806.

[2] Alrawais A, Alhothaily A, Hu C, Cheng X. Fog computing for the Internet of Things: Security and privacy issues. IEEE Internet Computing, 2017, 21(2).34-42.

[3] Toosi AN, Calheiros RN, Buyya R. Interconnected cloud computing environments: challenges, taxonomy, and survey. ACM Computing Surveys, 2014, 47(1).1-47.

[4] Weyuker E J. Evaluation Techniques for Improving the Quality of Very Large Software Systems in a Cost- Effective Way. The Journal of Systems and Software, 1999, 47(11). 97- 103.

[5] King S, Hammond J, Chapman R, et al. Is Proof More Cost- Effective Than Testing? IEEE Transactions on Software Engineering, 2000, 26(8) : 675- 686

[6] Chen X, Proulx B, Gong X, Zhang J. Exploiting social ties for cooperative D2D communications: A mobile social networking case. IEEE/ACM Transactions on Networking, 2015, 23(5).1471-1484.

[7] Chen H Y, Tse T H, Chen T Y. TACCLE: A Methodology for Object-Oriented Software Testing at the Class and Cluster Levels. ACM Transactions on Software Engineering and Methodology, 2011, 10(4).96-109.