# Information Security Protection in Software Testing

Yubin Wang, Jinyu Yao
Information Security Department
The First Research Institute of the Ministry of Public Security
Beijing, China
e-mail:wyb1227@hotmail.com

Xiaoxue Yu
Information Technology Department
The People's Insurance Company(Group) of China Limited
Beijing, China
e-mail: yuxiaoxue@picc.com.cn

***Abstract*—At the present, information security protection for software testing is faced with serious situation. There are risks of software information interaction and transmission throughout the life cycle in software testing process. Lack of information security protection and technical support will result in important information leakage, such as the source code leakage, etc. By analyzing the leakage way of software information, a method in accordance with the information security requirements is elaborated which composed by technology framework, Controlled library, and test data security etc. The method is throughout the life cycle of software testing process in order to ensure the security of software testing.**

***Keywords- software testing; information security; security policy***

## I. INTRODUCTION

The specificity and its sensitive information on industry which was contained in software easily leads to the following security hidden dangers in the process of software testing: information being tampered, forged, stolen, intercepted. Security events lead to the information loss and leakage, causes the spread of the virus in the software information, even causes huge losses. How to ensure the information security in software has become an important problem to solve in the way approaching to information.

The aim at information security in software is to ensure that the information has the following characteristics: authenticity, confidentiality, integrity, availab ility, controllability, identification, non-repudiation. Large amounts of test data and documents which related to the sensitive information of the testing software are produced in the process of software testing. The information security is very important to the sensitive information on industry. In this paper, according to the technical requirements in software testing, the demand for information security is analyzed in testing process, and then combined with knowledge of information security, at last information security problems are discussed in the process of software testing.

## II. SOFTWARE TESTING PROCESS AND SECURIY PROBLEMS

Software testing process includes [1]: the testing requirement analysis, testing to plan, testing design and implementation, testing execution, testing summary etc. Information security protection is needed in each phase of testing process. The independent software testing process of information security problems is shown in Figure 1:

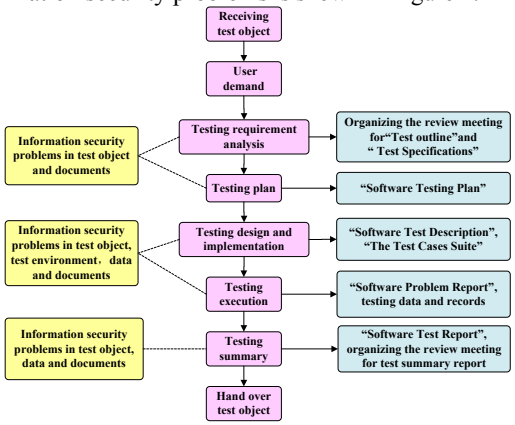


Figure 1. Software testing process of information security problems

Intellectual property rights and related information on software which submitted by the client was strictly confidential in testing procedure though test institutions in the requirements for industry standard for many countries, including protection for electronic / paper storage and transmission of the testing results. Because of the constraints on test condition and environment, test environment in the third party testing was provided by the client and confirmed by the assignee, the classified information having the security risk in the interaction and transmission. Security solution currently: formulate the regulations and procedures; did the security training and sign the confidentiality agreement to the relevant test personnel; the storage and transmission of test object and related documents was stored and transferred by optical media. The solution was lack of information security policy and technical support, has potential security risk.

978-1-7281-0169-9/18/$31.00 ©2018 IEEE
DOI 10.1109/CIS2018.2018.00106

## III. INFORMATION SECURITY POLICY IN SOFTWARE TESTING PROCESS

According to the security problems of software test process, security policy is elaborated throughout the life cycle of software testing process.

### *A. Testing requirement analysis and Testing plan*

In the test requirement analysis phase, test group receives the test object of the assignee, and then test to charge distributes test object to test members according to division of project. The information security protection for test object: ensure the security of test object of the storage, use and distribution etc; prevent the information to be stolen, tampered and loss; guarantee the secret of the related documents of intellectual property and industry sensitive information.

Concrete process can be embodied as receiving the electronic test object and copying it into the device with component CA authentication though encryption device such as security USB flashed to drive, receiving the paper test object of strict regulations.

In the process of testing requirement analysis, transfer and integration exist in documents and other information, the security and integrity of information and documents in the transmission processed should be ensured. The test environment for receiving test object device should be at least meeting the standard that security environment of classified system of two levels. If the test object comprises industry sensitive information, the test environment for receiving test object device should be at least meeting the standard that security environment of classified system of three level [2]. By the same token, according to the security level of tested object, the secure computing environment for high security level tested object should be physically isolated from Internet, as far as possible to ensure the safety of the tested object.

In the test plan process, test group should complete the test plan document. The security of information on the course of transmission should be ensured. At the same time, the confidentiality and integrity of software tested to plan is needed to be ensured.

### *B. Testing design and implementation*

In the testing design and implementation, prepared test data should be complete and ready, established test environment should be effective and controllable, designed test case achieves the aim of "visible, controllable", and carried out a task with information security. The established test environment is not only almost the same as the real environment, but also need was paid attention to the safety of it [3]. The testing environment equipment should conform to the requirements of classified protection for information system, including that physical location of test environment is properly selected; physical access control measures are perfect; network topology is safe; technology measures of regional boundary, communication network, computing environment and application of access control policy are in accordance with the requirements for classified protection of information system. The technology framework of information security for test environment is shown in Figure 2.

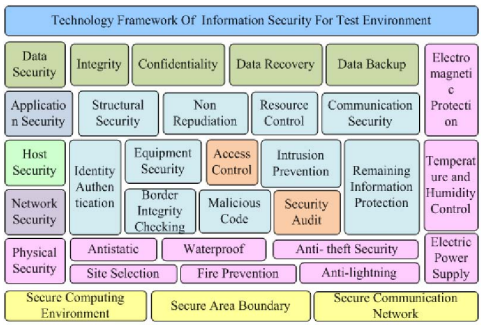


Figure 2. Technology framework of information security for test environment

### *C. Testing execution*

#### *1) Information security protection policy:*

The test environment should be set up at this process. From the view of information security, the test environment security area planning should be roughly divided into core zone, DMZ (demilitarized zone), application server zone, security management area, user terminal zone and Internet access zone [4]. If the test object of high security level or containing important sensitive information, test environment protection area should not include Internet accessed zone, or physically isolated from internet access zone. Security area classification in software testing environment is shown in Figure 3:

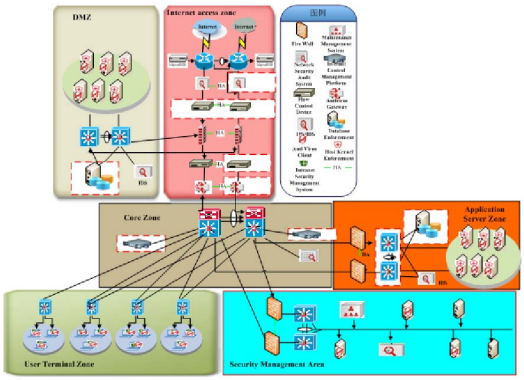


Figure 3. Security area classification in software testing environment

Computers, mobile storage media are required to be used in the testing process in the laboratory and field. The objectives needed for information security protection: computer (work), mobile storage media, test object, test data, test records and documents.

In the process of testing, the security should be focusing on receiving, issuing destruction of test object of the first test and regression test. The test object is contained by software tested software, software plan documentation, software requirements specification, user manuals and other related document.

After testing group receiving test object of the first round of the test, the authenticity and availability of test object

should be confirmed. If the test object is available, then do digital signature on it. The digital signature can prevent the tampered or forged original documents and signature from being verified, to ensure consistency of the test object in the whole test process. The test project leader does the digital signature, adopts corresponding signature according to the file format. Establish exclusive controlled library for test object, control the version and content of test object. Control library diagram is shown in Figure 4.

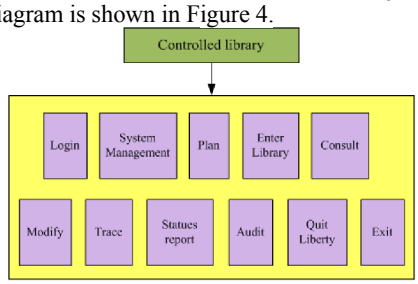


Figure 4. Control library diagram

In the distribution of test object, strictly control the user s of controlled library, encrypt test object of sharing mode, and ensure information integrity and confidentiality [5]. Limit the scope of users with encrypted permission after decrypting to test object, project team uses specific user named in the controlled library allocated by project leader, to receive and save test project in the specific regions in working server respectively.

In the first round and regression, a number of test data, test scripts and test records are generated to form a series of test process documents. The relationship of these records and documents within software is closely, embodies the fairness, justice and test level of testing. Before test execution, communicate with research and development personnel to confirm the data used in test and the usability of test script, and then the test projected leader uses digital signature for the above information on shared mode encryption, give the tester the permissions of decryption, and tester have permissions to read the related information.

In test execution, the original test record is in strict management, test execution personnel and test supervisor are full-time people, but not the same individual. Tester uses digital signature for the original test case suite and the relevant documents with shared mode encryption, and then gives the decryption permission. The test leader integrates the test record. After the review of test ware, the test ware version needed to be controlled, digital signature and encryption used on it by the test leader is to ensure the sensitive information security. After regression testing, test leader confirms and reviews for all the problems having been zero, uses digital signature and then stores the test ware by disk.

The feasible information security policy is established combined with the technical methods: encrypt the tested software program files to prevent illegal modification, use and copy the program; encrypt the data and electronic files to ensure confidentiality, authenticity and integrity of electronic document; use digital signature on the related technical documentation to ensure the electronic file that comes from the author; use access control to effectively control the illegal users to access electronic files or data. The date security policy is shown in Figure 5.

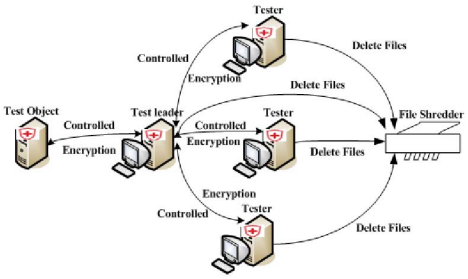


Figure 5. Date security policy

The implementation of the above policy is of great benefit to protect the client sensitive information and intellectual property rights during the whole testing process, guarantee that the trade secrets will not be leaked, reflect the justice, fairness and independence of testing institution.

*2) Software information security test*

More attention should be paid to the software information security test of testing process. Protect the security of important information on software through the information security terminal tool for the testing process. With the security testing tool to check the software if there are a buffer overflow, array bounds, unreachable code and memory leak which may be attacked by hackers. Modifying the program defects by the developer can reduce software vulnerabilities, improve software security.

If the test software has user permission settings, the security mechanism of user management and authority management should be used, the test content includes identity identification and authentication for user login; protect the user identity uniqueness and password complexity, support role assignment and permission management, establishment and management access control list, etc.

If testing the application software with the database, consideration should be given to the database backup and recovery function and initialization function. Although the database management system itself has the backup and restore function, developer still need to consider the recovery log planning, the safety audit opening, the date size estimation of data backup and recovery, the using way of backup files and log files, etc.

If testing the encryption software, the test data transmission and storage encryption and data encryption function should be considered. If the data type conversion and precision are lost in the software processing, the integrity, equivalence and consistency of the testing data should be considered. According to a variety of possible unusual data situations, performance testing should be considered for example the watchdog reset test.

In strength information security in software testing, security vulnerability scanning is the use of host and network

vulnerability scanning procedures to test the software whether it has vulnerability [6]. Before the security vulnerabilities caused serious harm, find these vulnerabilities and inform the developer to prevent it. Simulate attack testing including spoof, replay, message tampering, denial of service, internal and external attacks, trap, Troy horse, etc. Ping of death, Teardrop, UDP Mood and SYN Flood are typical attack methods in denial of service. Capture data onto the data communication and data interaction process, analyze the data by sniffer packet, and then use it for safety testing.

### *D. Testing summary*

In the testing summary, ensure the confidentiality and integrity of the information on the software test report. In order to ensure the test objective and fair, guarantee the authenticity, integrity and non-repudiation of the information contained in the test report. When the test report relates to the software intellectual property or contains sensitive information, its confidentiality should be ensured.

In filling process, electronic document produced in test should be stored by disk; the paper documents with related procedures should be stored in the archive room. When the test is end and document delivery is completed, all related project files (documents stored in the target machine, working machine and removable storage media) should be removed immediately. The file which needs to be destroyed should be smashed through file shredder, carrying the point of completely deleted, nonrenewable and no trace. The paper document should be returned or destroyed, if it should be returned to developer, the proof of return / receipt should be issued and signed by the developer and tester together, conforming to the destroy procedure when destroy the file.

## IV. CONCLUSION

The confidentiality, integrity, availability, non repudiation and identification of software should be considered in the process of software. Therefore, test record and defect to report should be carefully analyzed and counted in security risk assessment; the several aspects above also should be taken into comprehensive consideration. The related problems are tracked down each stage of software testing, judging the software whether reach the safety requirements.

Software testing is not fully tested, it usually only proves what the procedure is wrong, and cannot prove that the procedure is right. The problem which lacks of testing approach, testing tools, and professional testing team still exist in software testing industry of our country. Therefore, version tracking is needed in the software which was put into produce; revise, upgrade and improve the software constantly with the combination of business requirement and modern technology. Only in this way, the software can stand the test of time; level of information security in software testing can be improved.

## ACKNOWLEDGMENT

First and foremost, I would like to show my deepest gratitude to my supervisor, Yong jiang who has provided me with valuable guidance in every stage of the writing of this thesis. Without his enlightening instruction and patience, I could not have completed my thesis.

Second, I shall extend my thanks to leaders from the ministry of public security of network security bureau to direct my job and works, thanks for the strong support of the project 2017YFC0820706.

Third, I thank my family members that have given me their constant encouragement and support in my academic terms.

Last but not least, I'd like to thank all of my workmates for their encouragement and support.

## REFERENCES

[1] Kaner C.1essons learned in software testing.John Wiley&Sons,Inc.2001.

[2] GB/Z 28828-2012.Information security technology - Guideline for personal information protection within information system for public and commercial services.

[3] GJB 2725A-2001. General requirements for the competence of calibration and testing laboratories.

[4] Tipton H F.Information security management.Auerbach Publications.2002.

[5] PARK J, SANDHU R. Towards usage control models: beyond traditional access control.ACM Symposium on Access control Models and Technologies,2002' 2(3): 57-64.

[6] Hongbiao Zhao.Information Safety . Beijing:Tsinghua University Press,2004.