SOCIETY FOR SCIENCE AND EDUCATION
UNITED KINGDOM

TNC TRANSACTIONS ON NETWORKS AND COMMUNICATIONS

VOLUME 7, NO. 2
ISSN: 2054 -7420

About Some Methods for Software Security

Shafagat Mahmudova
Institute of Information Technology of ANAS, Baku, Azerbaijan
shafagat_57@mail.ru

ABSTRACT

This study reviews software security, etc. It studies the methods for the analysis of software security. The problems of software protection are identified. The risks for software projects, their management, determination and categories are studied. Software development process includes the construction of an agreed structure for software development. The design of large distributed systems uses many programming languages, which in turn causes certain difficulties. That is, security in these cases is not provided. Software security is a set of measures aimed at its protection. Security in software exploitation is also a key issue. Software security is understood as its functioning without any problems. Information security threats arise in the process of software exploitation.

Keywords: Software; security; analysis methods; risks.

1 Introduction

In modern era, the information society is increasingly gaining momentum. Computers affect all the processes ongoing in the society, including research and economy, changing human behavior in general and shaping new areas. The study of new technologies and their introduction to different areas leads to the creation and progress of new systems and software.

The fight against terrorism and criminals has sharply increased in modern times. The wave of terrorist acts around the world has created a need for improved detection and preventive security systems and software.

One of the main challenges facing the most states is the development of new principles and approaches to the prevention of smuggling and terrorist incidents, the creation of different systems, and the establishment of software centers or national security, international integration, and so forth.

Improvement of search, disclosure and identification of crimes against any individual, society and the state is of particular importance. Solution of these issues requires new global approaches and the application of the most up-to-date technologies. Any evidence obtained from research or effective search should be used successfully in real time [1].

The national law enforcement system enables solving a wide range of issues facing the state security system and defense agencies of the country:

Search for suspects or criminals potentially involved in illegal incidents and dangerous acts (against citizens' lives, government agencies, etc.);

DOI: 10.14738/tnc.72.6334
Publication Date: 20th March 2019
URL: http://dx.doi.org/10.14738/tnc.72.6334

Identification and detection of the participants in the incidents is one of the key challenges of law enforcement, national security and defense systems of the country;

Successful solution of these issues at the state level is possible with the use of up-to-date software;

Development of a distributed system for the collection and storage of multimedia data (images, videos, etc.) is of crucial importance;

Interactive search of suspects in the databases crated based on the data collected from the investigations and operational search activities is essential, etc.

Software development process includes the construction of an agreed structure for software development [2].

Effective development of an algorithm and the precise determination of the data structure play a key role in software development. The algorithm of the problem and the data structure are the key aspects that affect the effectiveness. Thus, the structure of the data becomes more difficult to change than its algorithm.

The design of large distributed systems uses many programming languages, which in turn causes certain difficulties. That is, security in these cases is not provided [3].

Software security is a set of measures aimed at its protection.

From this point of view, the study of software security methods is of particular importance.

Security in software exploitation is also a key issue.

2 Software Protection Problems

Software security is understood as its functioning without any problems (failures, errors, etc.). The exploration of software protection issues shows that the following problems should be considered [4]:

detection of errors during software functioning;

identification of the points originating the errors;

determination of the number of existing software errors;

differentiation of software errors from software failures;

determination of probable outcomes as a result of activating destructive programs during software exploitation.

Information security threats arise in the process of software exploitation. Currently, one of the malicious acts against information on computer systems is a virus. The more software develops, the more types of viruses are created. Over recent years, computer viruses have damaged both hardware and software. The amount of these damages is about 1 mln. USD. On November 21, 1988, the most dangerous Morris virus was disrupted ARPANET network within 24 hours. The restoration of the network cost millions of dollars.

Technological safety model of software often bases on a common concept of security in the infosphere [5]. The following issues should be considered in this regard:

developing the theoretical basis for the practical solution of technological safety of software;

creating secure information technologies;

expanding control system to ensure security of computer info sphere.

3 Analysis Methods for Ensuring Software Security

Various analysis methods are used for ensuring software security. These methods perform various functions. Some of the analysis methods are presented in figure 1 [6].

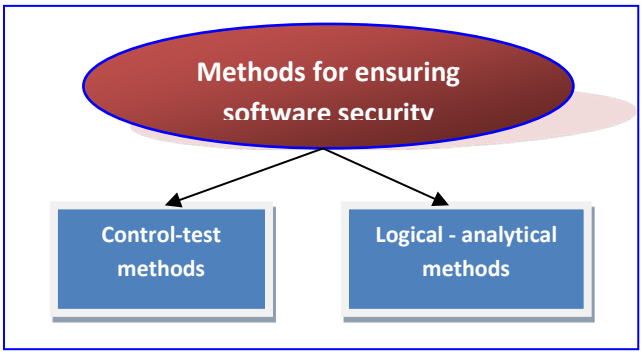

Figure 1. Methods for ensuring software security

The execution of software is controlled through control-test methods. These methods are widespread since they do not require formal analysis, enable the use of current hardware and software tools, and allow for the development of ready-to-use methods in a short period of time [7].

A software model is built through logical and analytical methods during the security analysis, and the correspondence of the model of the explored software with the software model in the group is officially proven [8]. In the simplest case, a machine code (bits) can be a software model. And the existence of the viruses in the software can be verified by detecting their attack signatures. Attack signature is a feature of a computer virus [8]. It often uses formal models.

The models related to the software analysis process [10] are presented in figure 2.

Lexical verification analysis model studies the classification of various lexemes of the objects of the software submitted in the search, recognition and executed codes. A lexeme is a sequence of possible symbols of the programming language assigning a sense for a translator [11]. In this case, the lexemes become the signatures.

At present, the search for signatures is performed in the following groups:

- virus signatures;
- signatures of the software system elements;
- signatures of "suspicious functions".

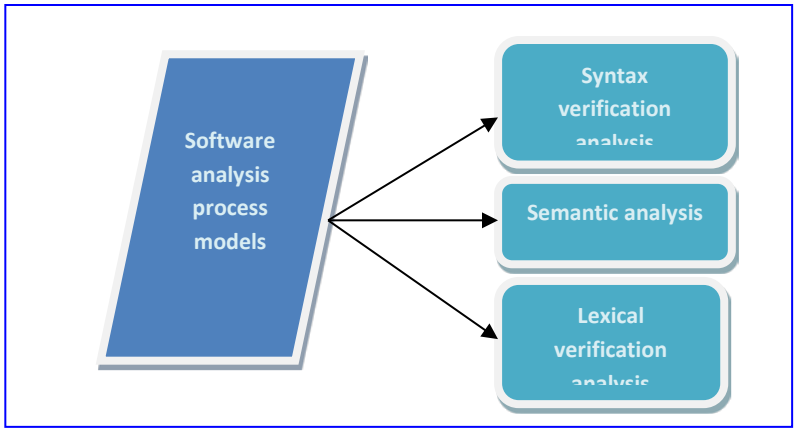

Figure 2. Software analysis process models

Syntax verification analysis model classifies the syntax structures of search, recognition, and software, and builds an algorithm corresponding to own structure of the software.

Semantic analysis examines the semantics of software functions (procedures) in the operating system of the computer. Unlike previous types of statistical analyses, semantic analysis focuses on the study of the software dynamics. Semantic analysis model is the most effective type of analysis, which also requires a lot of effort.

The principles of ensuring software security are as follows:

restrictions of software tools access, and the failure to change them;

implementing full scan of malware, and performing preventive testing;

ensuring software identification since its exploitation in terms of monitoring and security maintenance;

replacing separate modules of software without changing its structure;

performing a strict accounting and cataloging of all accompanying software;

performing statistical analysis of data about all processes, working operations and software functionality;

applying additional tools in case of revealing new and unexpected information security threats for software protection;

etc.

The information on the method for automated detection of errors and elimination of defects to ensure software security is provided in [12]. The mentioned study analyzes the methods for detecting and elimination of software defects.

4 Possible Risks for Software Projects

One of the important issues is the security of online software. Risks play a major role in software security [13]. The risks affect the schedule or resources required for the project implementation.

Some of the probable risks for software projects, their control and categories are listed below [14, 15]:

Risks for the software products under construction;

Business risks associated with the manufacturer in the organization.

Risk Management.

Determination of the risks. The possible risks for the project, developed product and business are identified;

Risk analysis. The sequence of the risks of probable hazardous situations is estimated;

Risk planning. The measures to be taken to prevent the risks or to minimize their effect on the project are scheduled;

Risk monitoring. The measures are taken for continual assessment of risk probabilities and reduction of the consequences of hazardous situations.

The list of possible categories of risks is as follows:

Technological risks. Searched in the software and hardware of the system;

Personnel-related risks. Connected with the members of the manufacturers team;

Organizational risks. Occur in the organization where the project is implemented;

Instrumental risks. Related to the use of CASE tools and support for the software organization process;

System requirements risks. Associated with the requirements of the developed system;

Assessment risks. Related to the assessment of the software system and the resources required for the project implementation.

Risk analysis.

Risk prevention strategies. These strategies necessitate taking the measures that minimize the probability of the risks' consequences. For example, the strategy for removing potential defective components;

Strategy minimization. It is aimed at reducing the possible damages associated with risks. For example, the strategy for the reduction of the damages caused by the illness of the members of manufacturers team;

"Emergency" situations planning. These strategies require an action plan. Thus, in case of emergency situation, the action plan has to be fulfilled.

5 Conclusion

This study reviewed the problems of software protection. Software security analysis methods were studied. Some of the probable risks for the software projects, their control and categories were highlighted.

This study strongly recommended to use the capabilities of cryptography to ensure software security. It can increase the reliability of software. Infringement of the data confidentiality can affect software security. Therefore, data receipt and signals processing performed in the process of confidential data processing can require in-depth studies, which proves the relevance of this study once again.

REFERENCES

[1] For the protection of information it is proposed to use face recognition technology, Information security journal, 10.29.2008, retrieved from

[2] http://www.itsec.ru/newstext.php?news_id=51127#sthash.HQGrMBJh.dpuf. Bakhtizin, V.V. and Glukhova, L.A. (2010), Software Development Technology, Minsk: BSUIR.

[3] Gromov, Yu.Yu., Ivanova,O.G., Belyaev, M.P. and Minin,Yu.V. (2013) Programming Technology. FSBEI:TSTU.

[4] Kadan, A.M. Methodology and programming technology, retrieved from http://mf.grsu.by/Kafedry/kaf001/academic_process/048/28

[5] Efimov, A.I. and Palchun, B.P. (1995) On the Technological Security of the Computer Informational Sphere, Information Security Issues, vol., 3, pp. 86-88.

[6] Kazarin, V. (2003) Security of computer systems software, Moscow: MSUL.

[7] Software security analysis methods, retrieved from https://studbooks.net/2043842/informatika/metody_analiza_bezopasnosti_programmnogo_obespecheniya

[8] Sereda, S. A. Software and hardware systems for software protection. ER, retrieved from http://www.ase.md/~osa/publ/ru/pubru427.html.

[9] Signature, retrieved from https://ru.wikipedia.org/wiki/ Signature

[10] Yashchenko, V. V. (2003) Introduction to cryptography, M.: MTSNMO: CheRo.

[11] Lexeme, retrieved from https://ru.wikipedia.org/wiki/ LEXEM

[12] Jeesoo, K. T. and Hwankuk, K. (2018) Antomatic Vulnerability Detection and Remediation Method for Software Security, International journal of wireless information networks, vol. 10, pp. 117-129.

[13] Mihailescu, M. S. and Nita, M. P. (2016) Software security techniques: Mircea cel Batran, Naval Academy Scientific Bulletin, vol., 19, 8 p.

[14] Georg, V. (2018) Winning with Open Process Innovation. MIT, Sloan management review, vol., 59, pp. 53-56.

[15] Timoti, L. The main risks of a software development project, retrieved from https://econ.wikireading.ru/78462