Ministry of education of the Republic of Belarus
Educational Institution
Belarusian state university of informatics and radioelectronics

UDK 004.056

Al-Zamili
Ali Hassan Waheed

Modeling the security of remote banking terminals

ABSTRACT

for the degree of master of science
on a speciality 1-98 80 01 «Methods and systems of information protection, information security»

_____

Scientific supervisor
T.V. Borbotko
Doctor of science, professor

_____

Minsk 2016

INTRODUCTION

The offer of banking products through a network of self-service terminals is becoming a mass phenomenon. As world practice shows 90% of banking services provided within the framework of traditional bank branches, it cannot be only automated, but also translated into the sphere of self-service with modern terminal devices.

This process requires special attention both from the legal support of its operations, and from the safe operation and maintenance of the terminal.

Existing in Belarus the clearing system for retail payments based on the use of electronic payment instruments is represented mainly by the settlement systems with the use of bank cards and electronic money.

The legal basis of the system make up the Banking Code of the Republic of Belarus, the normative legal acts of the National Bank, as well as developed in accordance with their local regulations and contracts to banks and other participants of the payment systems with the use of electronic payment instruments.

Settlement systems using electronic money are supported by appropriate technical, organizational and procedural safeguards to prevent, contain and detect threats to the security system, including malicious acts.

Software and hardware used in the system of settlements with the use of electronic money shall be subject to certification by the certification of software and hardware in the field of banking and technology in accordance with the legislation of the Republic of Belarus.

In order to ensure safe and reliable operation in operations with electronic money, banks must comply with safe operation standards and fulfill reserve requirements set by the National Bank.

Technical, organizational and information support of functioning in Belarus settlement systems with the use of plastic cards made of "National Processing Center" Joint-Stock Company "payment system" BelKart ".

The nature of the impact of the terminal can be very different, therefore, field of security threats is quite extensive. Classification and description of possible security threats, as well as the assessment of risks associated with them is one of the main topics of the graduation project, which today is quite a hot topic.

GENERAL DESCRIPTION OF THE WORK

Communication of operation with large scientific programs (designs) and themes

The theme of dissertational work matches to subsection 13 «Safety of the person, a society, the state» the priority directions of scientific researches of Byelorussia for 2016-2020, confirmed by the Decision of Ministerial council of Byelorussia on March, 12th, 2015, № 190. Work was carried out in formation establishment «Belarusian state university of informatics and radioelectronics».

The purpose and research problems

The purpose of dissertational work consists in working out of a program complex allowing to provide modelling of information security automatic teller machine.

For object in view achievement it was necessary to carry out following problems:

1. To analyze a problem of the informational security of automatic teller machine.
2. To develop the program complex allowing to provide modelling of information security automatic teller machine.

The personal contribution of the competitor

All basic results stated in dissertational work, are gained by the competitor independently. In common published works to the author belong: definition of the purposes and statement of research problems, sampling of methods of research, direct participation in their conducting, and also machining, the analysis and interpretation of the gained results, the formulation of leading-outs.

Approbation of effects of the dissertation

Substantive provisions and effects of the dissertation were discussed at XIV Belarus-Russian scientific and technical conference "Hardware components of protection of the information" (Minsk, 2016).

Publications on a dissertation theme

By results of the examinations presented to the dissertations, 1 operation, including 1 paper in collectors of materials of conferences are published.

THE BASIC CONTENT OF WORK

In introduction the urgency of a theme of work is proved. It is shown, that classification and the description of possible threats of safety and as the estimation of risks with them connected is one of the cores to those of the given degree project, that for today is enough vital topic.

In chapter one. The security of systems of banking terminals can be understood as their properties, which is expressed in the ability to resist attempts to harm the owners and users of the system at various disturbing (intentional and unintentional) impacts. In other words, under the security of the system one understand its protection against accidental or deliberate interference in the normal process of its operation, as well as the attempts of theft, modification or destruction of its components.

For many banks, there is a fact that a breach of the security of information in their end bank terminals can cause tremendous damage both to the banks and their customers. Therefore, these organizations have to pay special attention to security assurances, which leads to the need to implement comprehensive protection.

Unification of electronic payment messages, an increase of services and as a consequence the complexity of the information infrastructure increase the likelihood of threats to information security.

The cryptographic and organizational measures help to protect transactional data from interception and tampering.

Analysis of threats to the security of the personal payments indicates that they all in one way or another are aimed at taking money. Analyzing the system of interaction "client - automatic cash register," there are two classes of threats - technical and information, they are depending on the implementation and are divided into five sub-classes: physical, technological, computer, operating, social.

The most common types of threats today include technological threats. The most numerous in the number of incidents of fraud statistics is "skimming" - the kind of fraud in which the offender is using technical means to access data of the card account of the legitimate card holder, and then can manipulate them on his own.

In the second chapter. Questions of information security (IS) are studied in various countries for a long time. It can be noted that nowadays there is a common point of view on the conceptual foundations of information security. Its essence lies in the fact that the approach to information security must be comprehensive, combining measures of the following levels:

- legislation (laws, regulations, standards);
- administrative (general action taken by management);
- procedural (safety measures implemented by the staff);

- software and hardware (specific technical measures).

By providing information security, there are two aspects: the formal - to determine the criteria, that should be met by secure information technology, and practical - the definition of a particular set of security measures in relation to the consideration of information technology.

The development of measures against security threats - the faithful, but a long, expensive and not always effective way for the company. Standardization of the practical aspects of the security is held for a long time and is reflected in various recommendations, guidelines and standards as the international level (ISO, BSI), and regional (STB). In order to achieve an acceptable level of information system security today is sufficient to use a hybrid approach - along with private study, research use international, implementing a simplified approach to risk analysis.

Continuous monitoring and statistics allows you to develop a series of measures to counter the most common types of threats. The video surveillance system, the choice of location of the ATM, the system of notification of incidents, failover - this is an incomplete list of activities that are mandatory to be implemented during the installation of automatic cash register.

The level of both technical software today is quite high, the availability and diversity of the market due to high demand from both companies and from individuals, often the only thing standing ownership of a technology can be a financial factor. In this situation, the likelihood that the technology acquired to protect the information will not be studied in detail by someone else and used to attack is minimal. With these facts, it should be remembered that tools such as monitoring the state, administrative measures, control of removable media, as well as many other standard security measures described in this chapter, will reduce the risk of cyber-attacks and the implementation of technical

In the third chapter. To claim that the information system is 100% secure using a set of standard safety features is not possible, usually the concept of acceptable level of safety is used. The main instrument of control and evaluation of the level of safety is a technique for risk assessment of information security. Using these tools one can get varying degrees of detail to obtain information about existing of vulnerabilities exploited system. Risk assessment techniques are generally described in the standards of foreign origin, such as BS 7799, ISO 17799. In order to simplify and accelerate their implementation, a number of software products implementing the algorithms described in them were created (COBRA, RiskPAC, SSADM, CRAMM, etc).

Structurally ATM consists of the functional units of the model, modify its developments by the manufacturer. The open architecture and modular design also allows ATM to develop common approaches to the training of personnel servicing the device. The accumulation of statistical data as well as data on incidents and their

decision can help to create the actual theoretical foundation for the analysis and training on safety.

IS mode in such systems is provided:

- on the procedural level - through the development and implementation of sections of the instructions for staff dealing with information security and physical protection measures;

- on the software and the technical level - the use of tested and certified solutions, a standard set of countermeasures: backup, virus protection, password protection, firewalls, encryption, and so on.

The program complex, along with theoretical knowledge on information security, allows the user to test the skills of designing the security system in terms of effective use of allocated funds.

CONCLUSION

The thesis analyzes the security problems of ATM, methods of protection against the most likely threats, measures to optimize the number of security features, as well as approaches to assess information security risks and minimize them.

During the study of statistical data as well as information reports and publications of different organizations involved in the protection of information in banking and in the public networks, the classification of the most likely threats to automated teller machines.

In the planning and implementation of the security of bank terminals special attention is paid to the complexity of the developed protection.

This information is used to develop an electronic textbook, which in addition to the study of text and media materials allows to work out the practical security of the ATM with given limiting conditions.

Electronic textbooks are developed in Macromedia Flash environment 8 using a programming language ActionScript 2.0.

Got and fastened with textbook knowledge will help the user to better navigate in the protection of ATM.

Developed in the course of the master's work, workbook features a new approach to the classification of threats to information security, a large number of practical aspects of security that are relevant today, as well as the originality of information in electronic form.

LIST OF PUBLICATIONS

1. Алзамили Али Хасан Вахид Программный комплекс моделирования системы безопасности АТМ терминалов / Алзамили Али Хасан Вахид, Т.В. Борботько // XIV Белорусско-российская научно–техническая конференция "Технические средства защиты информации": Тезисы докладов, 25 -26 мая, 2016, Минск: БГУИР, 2016. — С. 22-23.