Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 104 (2017) 35 – 42

Procedia Computer Science

ICTE 2016, December 2016, Riga, Latvia

System Integration and Security of Information Systems

Andrii Boiko[a], Vira Shendryk[a,]*

[a]*Sumy State University, 2, Rymskogo-Korsakova st., 40007 Sumy ,Ukraine*

Abstract

The frequency of unauthorized actions to information systems (IS) in the process of their integration is steadily increasing, which inevitably leads to huge financial and material losses. According to statistics, internal users of IS, commit more than half of all violations. All of this forms "a dangerous group of risk ". Existing approaches for IS security are mainly provided by specialized tools of differentiation of user access to information resources. At the same time each user is assigned certain rights, in accordance with which it is permitted/prohibited local access to information is stored in PC, or remote access via communication links to information available on other PC.

After analyzing we identified 2 major vulnerabilities: tools of differentiation of local access are not able to provide protection against the actions of offenders are not directly related to obtaining unauthorized access to IS resources and tools of differentiation of remote access does not provide protection from network by internal users of the system.

The results of this research will lead to an improvement of the process of ensuring effective protection against threats to information security in the IS.

Keywords: Information system; Intrusion detection system; Behavioral method; Signature method; Security of information systems

1. Introduction

In recent years, the frequency of unauthorized actions into information systems (IS) is constantly increasing, which inevitably leads to huge financial and material losses. There is an interesting fact; more than half of all violations committed by the company’s employees, i.e. internal IS users.

* Corresponding author.
E-mail address: andrii.a.boiko@gmail.com

doi:10.1016/j.procs.2017.01.053

It is known that last few years, IS protection from insiders is mainly provided by specialized tools of the differentiation of user access to information resources. With the help of these tools to each user are assigned specific rights, in accordance with this it is permitted (or prohibited) local access to information are stored in computer, or remote access via communication links to information on other computers[1].

Still it must be noted that this approach does not solve the whole problem of information sources protection from intruders are operating inside IS. This is caused by two main factors:

- Tools of differentiation of local access are not able to provide protection against the actions of offenders who are not directly related to obtaining unauthorized access to information system resources. For example, the user can intentionally install and run the malicious software on own workstation that allows to capture and analyze network traffic in the IS. Another example of the unauthorized activity when protection can't be ensured by tools of access control is data recorded to external devices or the printing of confidential information to which the user has legally access. To identify such actions in IS should apply the system of workstation active monitoring
- The tools of differentiation of remote access does not provide protection from network attacks that can be performed by internal users of the system. Such attacks are based on vulnerabilities that may happen in software-hardware server and desktop stations of IS. Examples of vulnerabilities are unstable passwords, incorrect software configuration, errors are presented in the application software, etc. The success of the network attacks can lead to a breach of confidentiality, integrity or availability of information in the system. To timely detect and block such attacks should be used detection tools, known as IDS-system (Intrusion Detection Systems)[2].

On this basis, it should be highlighted the main tasks of research:

- The development of organizational measures are needed to meet the requirements of data protection, organizational and administrative documentation projects
- The ensure compatibility of hardware and software processing tools of data protection on the protected workstation with installable protection tools in compliance with the requirements for the configuration mechanisms of closed software environment, and flow control (mandatory access)
- The organization of complex schemes of information backup to external devices
- The development of the efficient schemes of the operational and centralized management of configuration
- The development of regulations to ensure continuity and rapid recovery of functioning of the object of protection in the presence of a complex server groups, including the secure server and domain controller, database, a management server anti-virus tools and file server

Thus, the effective protection from insiders of information security requires the use of additional forms of protection, such as workstations active monitoring, as well as intrusion detection systems

2. The main methods of ensuring the security of information systems

In order to counter threats are listed in the previous, modern information systems include security engines that implement the adopted security policy. Security policy in accordance with the purpose and conditions of operation of the system can determine the rights of access to resources and regulate the procedure of auditing of user activity in the system of network communications protection, to formulate ways of restore the system after a random crashes, etc. For the implementation of the adopted security policy, there are legal, organizational, administrative and engineering measures to protect information (see Fig. 1).

The legal maintenance of information security is a set of laws, legal documents, regulations, instructions, manuals, requirements which are required in the information security system.

Engineering measures are a set of special authorities technical tools and measures which are operating together to perform a specific task on the Data Protection Act. To engineering tools is included screening rooms, the organization of alarm, security facilities with a PC.

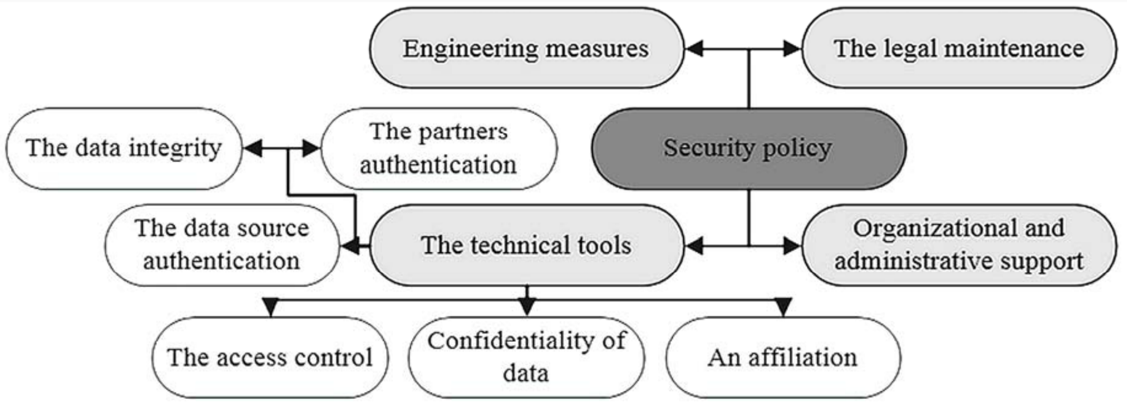

Fig. 1. The structure of security policy.

Organizational and administrative support of the information security is a regulation of industrial activity and the relationship between performers in the legal and regulatory basis in the way that disclosure, leakage and unauthorized access to information becomes impossible or significantly hampered by carrying out organizational activities. [3,4] Measures of this class include: the selection and training of personnel, the definition of job descriptions of employees, organization of access control, security of premises, the organization of information security with the conduct of control of personnel information, determining the order of storage, redundancy, destruction of confidential information, etc.

The technical tools of protection include the hardware, software and cryptographic protection, which make difficult to attack, and help detect the fact of its occurrence, and help to get rid of the consequences of an attack.

Technical tools of security subsystems in modern distributed information systems have the following main features:

- The partners authentication on the interaction, which allows to ensure in the authenticity of the partner when the connection is established
- The data source authentication, which ensures in authenticity of the source of the message
- The access control to protect against unauthorized use of resources
- Confidentiality of data, which provides protection against unauthorized information
- The data integrity for detection and, in some cases, and prevent change of information when its storage and transfer
- An affiliation, which provides proof of the belonging information to a certain person

Table 1. Relationship between the security features of IS and mechanisms for their implementation.

Security service	The encryption	The digital signature	An access control	The integrity control	Authentication mechanism	Traffic additions	The notarization
The partners authentication	X	X			X		
The data source authentication	X	X					
The access control			X				
Confidentiality of data	X					X	
The data integrity	X	X		X			
An affiliation		X		X			X

The following mechanisms are used to implement these functions:

- The encryption converts information into a form that is inaccessible to unauthorized users understanding
- The digital signature transports the properties of the real signatures to electronic documents
- An access control mechanism that control how users access to resources on the basis of such information as the database access control data, passwords, security label, access time, the access route, and the duration of access
- The integrity control mechanisms that control the integrity of a single message, and the message flow and use it to control the amount of special tags, message sequence numbers, cryptographic methods
- An authentication mechanism, which decide whether or not a user in what he claims on the basis of requirements of passwords a user, authenticating devices or biometrics
- The mechanisms of traffic additions are added to the message flow additional information, which “masks” useful information from the attacker
- The notarization mechanisms that serve to certify the authenticity of the source of information

3. The intrusion detection system

Detection systems are designed to detect attacks and counter network attacks from intruders. Intrusion Detection Systems (ISD) are specialized software and hardware with a standard architecture[5], which includes the following components (see Fig. 2):

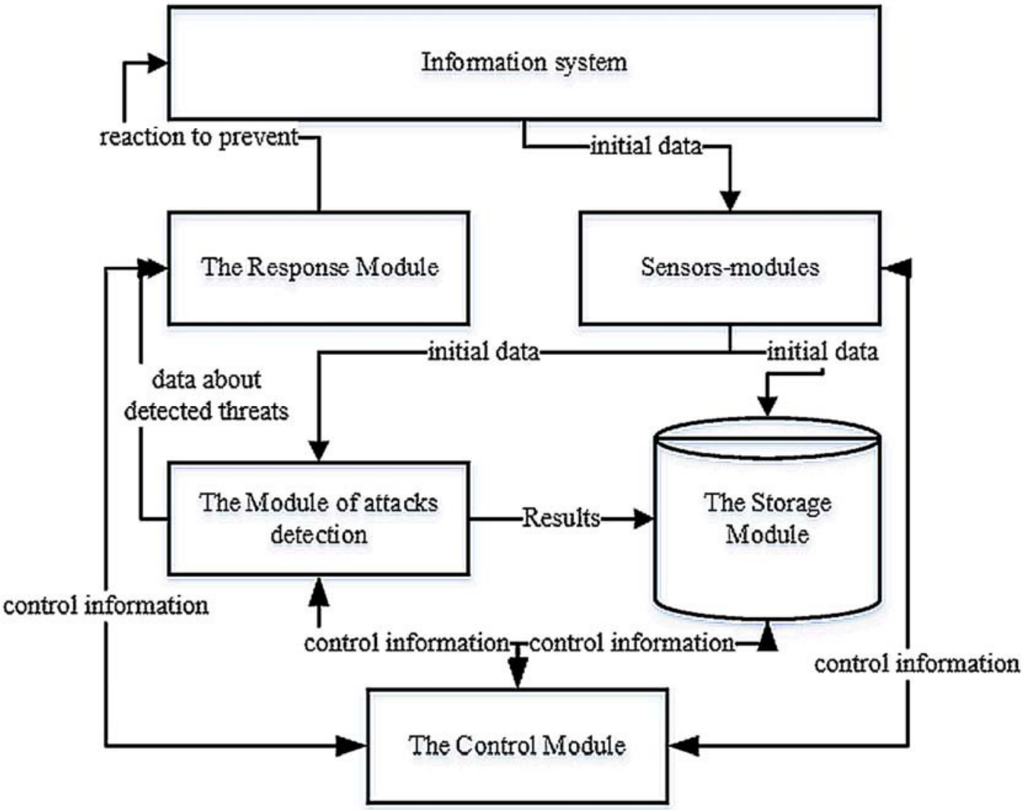

Fig. 2. The typical architecture of intrusion detection systems.

- Sensors-modules to collect the necessary information about the network traffic in IS

- The Module of attacks detection that performs data processing are collected by sensors to detect phishing attacks
- The Response Module to detected attacks
- The Storage Module of Configuration Information, as well as information about detected attacks. That unit usually performs a standard database (e.g. MS SQL Server, Oracle or DB2)
- The Control Module of Components of intrusion detection system

The two types of sensors are needed to be used in the intrusion detection system - the network and host. Networked sensors are designed to collect information about the data packets are transmitted in the IS segment, where the sensor is installed. Host sensors are installed to the IS servers and are designed to collect information about the data packets that are received by the server with the sensor.

The information is collected by the network and host sensors, further will be analyzed by the intrusion detection system to identify the potential violators of attacks. The data analysis can be carried out by two main groups of methods - signature-based and behavioral [6].

Signature methods describe every attack in the form of a special model, or signature. As the signature attacks can be: character string, semantic expression in a special language, a formal mathematical model, etc. The algorithm of the signature method concerns to find the source of attack signatures in the data collected by the network and host intrusion detection system sensors. In the case that the required signatures is founded, intrusion detection system records the fact of the information attack, which corresponds to the signature found. The advantage of the signature methods is their high precision and obvious disadvantage - the inability to detect the attacks that are not identified by the methods of signature.

Behavioral methods, unlike signature, is based on models of IS with regular process operation and not based on information attacks models. The principle of behavioral methods is to detect discrepancies between the current modes of the operation of IS and full-mode model is laid down in the method parameters. Any such discrepancy is considered as an information attack. The advantage of this type of methods is the ability to detect new attacks without the need for constant change operating parameters of the module. The disadvantage of this group of methods is the difficulty of creating accurate models of the normal mode of IS functionality.

After identifying the attack in the IS the intrusion detection system has the ability to take specific response action to block it. For the implementation of these actions is responsible the response module of intrusion detection system. The responding in intrusion detection system can be in active and passive form. To passive methods of response refers simply notify the administrator of the intrusion detection system about detected attacks. To the active can be included the following methods:

- The block of TCP-connection, in which the attack was realized. Such a closure is realized by sending special subjects TCP-connection segment with the RST flag set
- The launch of an external program with a given certain parameters. The presence of such response functions of the module allows to administrator of intrusion detection systems complements existing methods of responding with their own methods, are implemented in the form of external software
- The reconfiguration of firewall with the purpose of blocking traffic is coming from the offending host. Currently, the vast majority of the existing DOE has the appropriate external interfaces, which provide the interaction with the firewall of intrusion detection system. An example of such an interface is OPSEC interface for firewall CheckPoint FW-1[7,8]

According to the fact that the intrusion detection systems can themselves act as a malicious attack objects, these systems must be equipped with its own security subsystem.

However, it should be noted that a single use of intrusion detection systems do not allow completely solve the problem of protection against unauthorized activities of internal users of IS. This is primarily connect with the fact that the intrusion detection systems detect only the information attacks that can be detected by analyzing only the data packets circulating in the IS. This fact does not allow intrusion detection systems to detect unauthorized actions of those users who are not connected to a network of IS traffic. As mentioned above for detecting and blocking such action is necessary to use an active monitoring system, described below.

4. The system of the active monitoring of IS work stations

The systems of active monitoring of IS work stations, as well as intrusion detection systems are designed to detect and block phishing attacks, but not at the network level but at the level of the IS work stations. The architecture of active monitoring systems is similar to structure of the intrusion detection system. The sensors of active monitoring system are installed into the workstations of IS users and allow to collect information about all events are taking place. An example of such information may be:

- About the applications are running at workstations
- About the users are working at the station at the current time
- On file access to applications
- About the network traffic that is generated by IS applications, and others

The collected information is fed into the analysis module of active monitoring system where data processing is carried out. The security administrator must pre-configure of analysis module of active monitoring system, i.e. define requirements that allow or deny IS users perform various operations at the workstations. The totality of these requirements is a security policy in active monitoring system, which can be a part of a whole organizational security policy. For example, according to some defined security policy work with printers or access to certain files can be prohibited to some users.

Any event that fixed by sensors of active monitoring system and violates the previously given policy, is considered as an information attack. The security policy in active monitoring system may include a different group of requirements, which are formed based on two basic principles:

- “Everything that is not forbidden - is allowed” The security policy of active monitoring system is built on the basis of this principle, can clearly defines the prohibited actions of users. At the same time all other actions are performed by users is allowed. In order to identify violations of this policy uses signature analysis methods
- “Everything that is not allowed - not allowed” The security policy of active monitoring system, is built on the basis of this principle, explicitly defines only permitted user actions. All other actions under this policy are violations for which behavioral analysis techniques are used

In case of detected violations, the security policy of active monitoring system can implement passive and active response methods. Passive methods include alert the security administrator about discovered unauthorized user activity. This notification can be done by displaying a message on the administration console, or send an e-mail. Active methods mean blocking the actions of users who violate the specified security policy. As well as intrusion detection systems, active monitoring system can combine active and passive methods of response.

The systems of active monitoring should also be equipped by own security subsystem which helps to protect the active components of the monitoring system from unauthorized intruders effects.

Active monitoring systems can be used as an autonomous and functionally independent tools of protection for the detection of violations of IS security policy. However, to ensure a comprehensive approach to information security in IS, it is need to joint use of intrusion detection systems and active monitoring of the IS work stations.

5. The integrated use of the system of detection and IS active monitoring

Initially, consider the functional differences between the intrusion detection system and an active monitoring system based on the following parameters: type of sensor used, the type of collected data, methods of attacks detection and respond to them (see Table 2).

Table 2. Compare intrusion detection system and an active monitoring system.

The type of protection Score comparison	The Intrusion Detection Systems	The system of active monitoring of IS workstation
The type of sensors	Network sensors installed at the IS segments; Host sensors installed on the IS servers;	Host sensor installed on workstations IS users
The type of data collected	Information about the data packets are transmitted in IS	Information about the events on the users' workstations
Methods of attacks detection	Behavioral method are based on the detection the deviations from the characteristics of network traffic in IS;	“Everything that is not allowed – Forbidden”;
	Signature method, are based on the identification the network traffic in certain patterns of information attacks;	“Everything that is not forbidden – Allowed”;
Response methods	The active method that provides the block of network attacks which are detected;	The active method that provides the block of user actions that violate the security policy.
	The passive method that provides administrator notification of detected violations;	

The data are presented in the Table. 2 shows that systems of active monitoring of IS workstation are an additional tool for intrusion detection systems, and provide detection of the attacks, which are implemented by internal users of IS. Independently the intrusion detection system cannot detect such attacks due to their lack of collection and analysis information mechanisms at the level of workstations. On the other hand, information are collected by the sensors in the system of active monitoring can serve as evidence in the investigation of incidents are related to those violations of information security in IS, which have been identified by tools of intrusion detection systems.

To demonstrate this, consider the case of sharing use the intrusion detection system and system of active monitoring in a specific example. Assume that the ISD has recorded the fact of a network attack in the one of the IS servers. At the same time intrusion detection system has determined that the attack was carried out with the IP-address that belongs to the internal user workstation where installed the sensor of active monitoring system. Knowing only one IP-address does not allow to prove that user of workstation is involved to the conducted attack, because the station address can be intentionally distorted by the infringer. In this case, to confirm or refute the user guilt in the incident, the collected data by the sensor of active monitoring systems can be used.

Examples of data that can be provide by the information security tools to investigate the incident, are: the user login, which works with the station at the time of the attack, the list of applications are running at the station, network traffic information are generated by running applications, etc. The analysis of these data will allow to determine the degree of user’s guilt in the incident. Furthermore, if user who originally fell under suspicion is not guilty, the analysis of information from other sensors of active monitoring system will reveal the true disturber.

6. Conclusion

The current strategy of information systems protection is should be partially reviewed. According to the fact that for a long time, this problem was solved only with the tolls of access control, so completely protect the IS from insiders it was not possible. It connects to the fact that the functionality of these tools do not allow to protect the IS from the internal network attacks, as well as the actions of internal users of IS, which is not directly related to the violation of the access rules restricting to the information resources of IS.

To protect information security from internal threats it is need to use ISD and active monitoring system. The sensors of ISD are installed at servers of the intrusion detection system and IS workstation and perform the functions of detection the network attacks by analyzing network traffic. The sensors of active monitoring system are installed on users workstations of IS and allow to detect and block the actions of users who violate the specified policy. The sharing use of intrusion detection systems and active monitoring systems allow to use a comprehensive approach in the protection against internal attacks and significantly improve the level of information security in IS.

References

1. Siponen M, Willison R. *Information security management standards: Problems and solutions*. Information & Management. 46 (5); 2009. p. 267-270.
2. von Solms SHB. *Information Security Governance–compliance management vs operational management*. Computers & Security. 24 (6); 2005. p. 443-447.
3. Chang SE, Ho CB. *Organizational factors to the effectiveness of implementing information security management.* Industrial Management & Data Systems. 106 (3); 2006. p. 345-361.
4. Kenkre PS, Pai A, Colaco L. Real time intrusion detection and prevention system. In: *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014*. Springer International Publishing; 2015. p. 405-411.
5. Nazareth DL, Choi J. *A system dynamics model for information security management*. Information & Management. 52 (1); 2015. p. 123-134.
6. Chari SN, Cheng PC. BlueBox: *A policy-driven, host-based intrusion detection system.* ACM Transactions on Information and System Security (TISSEC). 6 (2); 2003. p. 173-200.
7. Srinivasan T, Vijaykumar V, Chandrasekar R. *A self-organized agent-based architecture for power-aware intrusion detection in wireless ad-hoc networks*. International Conference on Computing & Informatics. IEEE; 2006. p. 1-6.
8. Chebrolu S, Abraham A, Thomas JP. *Feature deduction and ensemble design of intrusion detection systems*. Computers & Security. 24 (4); 2005. p. 295-307.

Andrii Boiko is a Ph.D. student of computer science at the Sumy State University, Sumy, Ukraine. He has a Bachelor of Computer science at Sumy State University in 2013. He received his Master’s Degree of Information Technology of Design (Diploma with distinction) in 2014. At November 2014 till present he is a PhD student at the Sumy State University. Research direction is creation information technologies of information processing within the information systems integration of enterprise with a multiple production. Contact him at andrii.a.boiko@gmail.com.

Vira Shendryk started her academic career in Sept. 2002 at the Sumy State University, Ukraine. She was a visiting scholar at McMaster University, Canada in 2012 and was a visiting research fellow at the Department of Computer Science of the Faculty of Technology and Society, the Malmo University, Sweden in 2013. Her research interest is focused on the field of Information Systems and Decision Science particularly in decision making under uncertainty. She has written over 100 journal articles and conference papers and presentations. She has also been a Member of the Editorial Review Board of international multi-disciplinary quarterly journal Information Technology and Economics, which focuses on the intersection of Information Technology and Economics and was Member of Programme Committees the International Conference on Information and Software Technologies (ICIST 2014, Lithuania) and Advanced Information Systems and Technologies (AIST 2012-2014, Ukraine).