DOI: 10.14529/ctcr160303

ALGORITHMIZATION OF REFERENCE SECURITY MODELS OF CORPORATE AUTOMATION SYSTEMS BASED ON FORMAL SECURITY MODELS

V.S. Luzhnov, *ua9stz@gmail.com,*
A.N. Sokolov, *ANSokolov@inbox.ru*
South Ural State University, Chelyabinsk, Russian Federation

The paper considers the process of algorithmization of reference security models implemented on the basis of the existing formal security models. Main approaches to practical implementation of reference security models in a key of identifying potential areas for improvement are studied. The paper describes the analysis of constraints of models for synthesis based on their formal reference model amenable to implementation in a software algorithm for subsequent practical security analysis of real systems. On the basis of a formalized model graph is built which combines multiple information security vulnerabilities and attack methods of realization of the consequences for the security systems on the basis of which controllable models of real systems can be created. An algorithm of the semi-automatic analysis of the security of corporate automated systems is developed.

Keywords: information security, automation systems, reference security models, algorithmization of formal models, automation security systems, analysis of the security of automation systems.

Introduction

The main assessment tool is reference security models (RSM) when analyzing the security of the corporate automation systems (AS) and studying their peculiarities from the point of view of information security and information protection. Implementation of information protection measures in AS includes getting the actual system within RSM framework [1, 4, 5]. The process of getting the actual system within RSM framework in the manual mode is difficult and requires the collection and processing of large volumes of data aspects of the AS operation. That means there is a perspective to automate the process of collecting information about these aspects in the context of identifying potential vulnerabilities and threats to information security in the AS.

1. Reference security models

RSM serves as a list of security requirements to the AS, describes the information flows in AS, structures used by the access control policy contains a formal description of the potential operation of vulnerabilities and materializing information security threats. The basic RSM that determines the methods and forms of AS protection against security, integrity, availability information threats and the detection AS parameters and structures are [1, 2, 4]:

- discretionary access control models;
- isolated software environment model;
- the security model of information flow;
- role-based access control model
- logical security management model.

Models of these types have the necessary properties of the adequacy and abstraction for analytical and research purposes. Fig. 1 represents a formal classification of these models [3]:

Practical implementation represents using several theoretical and methodological approaches. One such approach is that all the processes of information security in AS can be described by the subjects' access to clearly defined objects or groups of objects. An example of such approach is Harrison-Ruzzo-Ulman model [2, 3]. In this model AS with discretionary access control is described as set of matrices, each of which corresponds to the AS. To change the properties of the AS and its transition in the various states one can use commands of changing matrices' accesses.

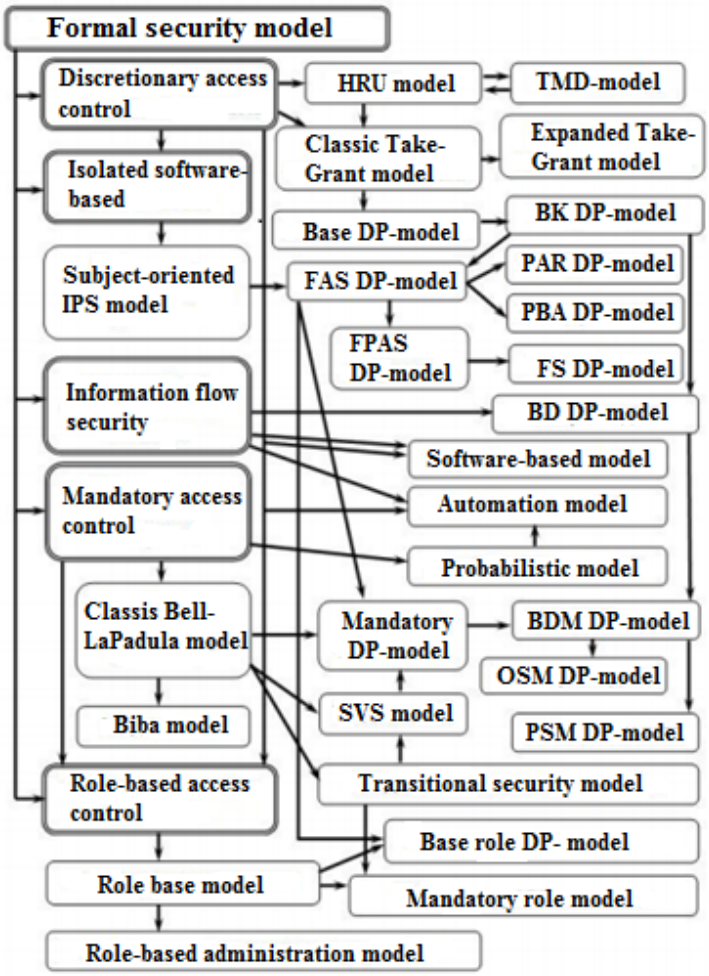

Fig. 1. Classification of RSM in AS

Another approach involves mandatory access control that is often described by terms of Bell-LaPadula classical model and special models based on it. [2, 3]. Bell-LaPadula classical model is an automation model presenting AS as an abstract system. An abstract system state is formalized by:

• a closed set of current access rights of subject to system objects;

• abstract functions, specifying the access level and the current access level for each subject and the level of confidentiality for each object;

• access matrix that gives an opportunity to unite discretionary and mandatory access control approaches to models.

Described classical models include special definitions of the elements and functions of the AS, in these models the following important features of the functioning of modern AS are not considered [3]:

• the ability of merging subjects and the transfer of access rights;

• the ability of the existence of subjects with zero trust level in AS, which must be provided with special working conditions;

• the ability of processing of conflict state of the system at the overlap of access subjects functions with zero and nonzero trust levels;

• the presence of hierarchical connectivity of entities in AS;

• the necessity of defining different access control rules and information flow control for specific sections of AS.

The third approach is taken with the purpose of providing a theoretical analysis of access rights leakage conditions and the implementation of prohibited information flows by memory or by time taking into account the essential features of modern AS. The approach is to obtain a set of formal security models of logical access control and information flow (the set of DP-models) [3].

The basis for all model of the set is DP-model developed with the application of regulations of the extended Take–Grant model, Bell-LaPadula model, SVS models, subject–oriented IPS model. It is used a classical approach that is each modeled AS is represented as an abstract system, where each system state is described by the graph accesses, and any transition of a system from one state to the next is carried out as a result of applying one of the rules of the graph accesses transformation.

Thus, using the existing main approaches to RSM in AS allows realizing complex algorithmic approach to conducting a practical security analysis of specific AS by means of software verification tools of the conformity of AS.

2. Mathematical models of security analysis

There are three main types of mathematical models that are mathematical tool of formalization and machine implementation in the form of the algorithm for security analysis that can be used for practical realization:

• models of information attacks designed to reproduce the essential properties and characteristics of attacks. Models of this type allow to research characteristics of a specific attack in the laboratory in order to determine what remedies can be used for attack neutralization;

• models of detecting information attacks, allowing to describe the process of detecting attacks on information resources of the AS;

• models of information security risk assessment of AS, which allow us to determine the efficacy of the entire security system.

In order to provide the mathematical tool of the researches described models can be formalized in a hierarchical tree (coherent acyclic graph) [7] $T = < M, N >$, where M – the set of vertices of the tree, N – the set of arcs of the tree. Each vertex of a tree T is associated with a particular security incident in the AS and the root of the tree represents the ultimate goal of the incident (information attacks). On the graph T there is an ability to make a lot of possible paths T_p, where each path $t_p \in T_p$ is a sequence of arcs $(n_{p1}, n_{p2}, \dots, n_{pn})$ such as $n_{pk} = (m_i, m_j), m_i, m_j \in M$, and final vertex of an arc n_{pk} is initial vertex of the arc n_{pk+1}. As the initial vertex of the path, there may be leaves of the tree T, as well as the final vertex – the root of the tree T. Thus, every element of the set T_p describes one of the possible scenarios of the incident (information attacks).

A special case of the models based on the described method of formalization is the model of attacks on information resources.

The proposed model of attacks on information resources consists of three basic sets: V – the set of information resources vulnerabilities of the automation system, A – variety of ways of implementing attacks on information resources, C – the set of consequences of the attacks on information resources. The main regulations of the reviewed models are given in [8].

To describe the relationship between elements of the sets A, V and C, it is necessary to define algebraic relation (ternary if $n = 3$) W:

$$W = A \times V \times C.$$

Then the element (a, v, c), belongs to the relation W, where $a \in A,\ v \in V,\ c \in C$, and this element is the logical structure "Attack on information resources, which is implemented by way of a via exploitation of the vulnerability v leads to the consequence c".

The set A_i is the subset of the set A and it is connected with each vulnerability $v_i \in V$ and includes attacks on information resources, exploiting the vulnerability v_i. The following relation is satisfied:

$$0 < |A_i| < |A|,$$

i.e., the vulnerability v_i cannot be used for the realization of all attacks on information resources from the set A. There is no such vulnerability, based on which none of the attacks on information resources could be implemented.

Each information attack $a_j \in A$ is connected with the set V_j that is the subset of the set V and includes the vulnerability exploited by the attack a_j. The following relation is satisfied:

$$0 < |V_j| < |V|,$$

i.e., the attack a_j can not exploit all the vulnerabilities of information resources of the automation system. There is no such attack that does not exploit the vulnerability of information resources of the automation system.

Each information attack $a_j \in A$ is connected with the set C_j that is the subset of the set C and includes consequences caused by the attack a_j. The following relation is satisfied:

$0 < |C_j| < |C|$,

i.e., the attack a_j can not lead simultaneously to all effects included in the set *C*, however, the attack a_j leads to one consequence at least.

Every consequence $c_k \in C$ is connected with the set A_k that is the subset of the set A and includes attacks on information resources of the automation system, which lead to the consequence c_k. The following relation is satisfied:

$0 < |A_k| < |A|$,

i.e. there is no such consequence that does not lead to the attack. The consequence is not the result of the realization of the attack included in the set A.

3. Mathematical model of attacks on information resources

Taking into account the formalization, described mathematical model can be presented as the graph $G = < L, E >$, where L – the set of graph nodes, $E \subset L^2$ – the set of graph arcs. There is a relation $T \in \{E \times W\}$ for graph G such as every arc of the set E complies with one or more than one elements of the relation W. Applying the relation T one interprets every arc of the graph G as one of the types of modeled attack on information resources of the automation system. In the relation T, some elements of the set W can comply at the same time with one arc $e \in E$ on conditions that the elements are attacks leading to the identical consequences, i.e.:

$(\forall e \in E), (\forall w' \in W), (\forall w'' \in W)\ \exists\ (e, w') \in T, \exists\ (e, w'') \in T \leftrightarrow c' = c''$,

where $w' = (a', v', c')$, $w'' = (a'', v'', c'')$ – the elements that belong to the set W, $a' and\ a''$ – ways of attack realization, $v'\ and\ v''$ – vulnerabilities, $c'\ and\ c''$ – consequences of attack realization.

Some arcs can be included in the graph node G when in the relation *T* elements of the set *W* describing attacks on information resources of automation system that lead to the identical consequences comply with every arc. Thus, graph nodes G can consolidate different stages of the attack on information resources that lead to identical consequences. An example of described graph G is in Fig. 2.

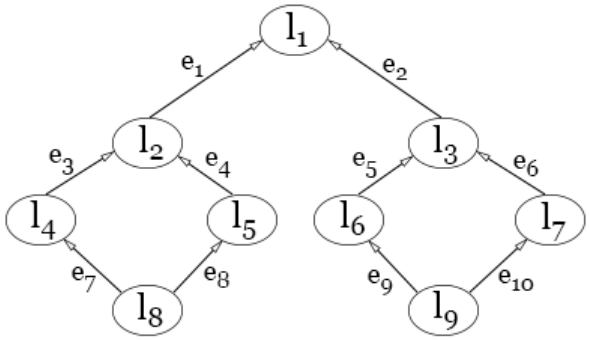

Fig. 2. An example of the graph:
$l_1 \ldots l_9$ – nodes of the graph G, $e_1 \ldots e_{10}$ – arcs of the graph G

The following relation T is applied to the graph:

$T = \{(e_1, (a_1, v_2, c_1)), (e_2, (a_2, v_1, c_1)), (e_3, (a_2, v_1, c_2)), (e_4, (a_3, v_4, c_2)), (e_5, (a_4, v_3, c_3)),$
$(e_6, (a_5, v_5, c_3)), (e_7, (a_5, v_6, c_4)), (e_8, (a_6, v_7, c_5)), (e_9, (a_7, v_7, c_6)), (e_{10}, (a_8, v_3, c_7))\}$.

4. The algorithm for security analysis of AS

On the basis of the described mathematical model of attacks on information resources, we can realize algorithms and software for the conduction of security analysis of automation systems.

The following set of instructions is an example of such security analysis algorithm:

1. To make lists of vulnerabilities, ways of realization of threats and impacts from their implementing for developing a model of attacks on information resources. These lists are the basis for forming the sets *V*, *A*, *C*.

2. Based on the conditions $0 < |A_i| < |A|, 0 < |V_j| < |V|, 0 < |C_j| < |C|, 0 < |A_k| < |A|$ и $W = A \times V \times C$ the great number of possible combination of elements of the sets V, A, C is formed.

3. The resultant set is filtered to exclude inappropriate elements to the ternary relation $W = A \times V \times C$.

4. As result of filtering the set W' is formed, containing the possible and impossible elements-combinations (a_i, v_j, c_k). Then, it is held the second stage of filtering for exclusion elements describing an impossible attack scenario from the set W'. For its implementation a plurality of elements $(a, v), (a, c), (v, c)$ that are impossible combinations of attacks and vulnerabilities, attacks and consequences, vulnerabilities, and consequences respectively are formed.

5. Based on the formed sets the set W' is filtered to W that is appropriate for developing attacks model.

6. On the basis of the set W the graph $G = < L, E >$ is constructed by forming the set $T \in \{E \times W\}$ taking into account the following rule: in the set T, at the same time some elements of the set can correspond to one arc $e \in E$ only under the condition that these items represent attacks that lead to the same consequences.

7. As a result, the set *T* contains all possible scenarios of attacks on information resources. To implement the security analysis, ratio $0 < r_i < 1$ и $\sum_1^i r_i = 1$ is for each consequence of the set *C* that is directly proportional to the damage of system resources from ensuing consequences. Every consequence is different from zero, while the total ratio of all the consequences is not more than 1.

Based on the generated ratios in the set *T* there is a search of such paths in a graph where the sum of the consequences ratio is maximum, i.e. finding ways of implementing information attack that lead to the greatest damage of information system.

Conclusion

The result of the analysis of RSM of AS and studying the available mathematical tool is the formal algorithm for security analyzing of AS. The algorithm is developed using basic approaches to the analysis of the AS security based on the classic RSM and it allows us to study AS security in various states.

References

1. Shcherbakov A.U. *Sovremennaya komp'yuternaya bezopasnost'. Teoreticheskie osnovy. Prakticheskie aspekty* [Modern Computer Security. Theoretical Basis. Practical Aspects]. Moscow, Knizhniy mir Publ., 2009. 352 p.

2. Devyanin P.N. *Modeli bezopasnosti komp'yuternykh sistem. Upravlenie dostupom i informatsionnymi potokami* [Models of the Security of Computer Systems. Access and Information Flow Management]. Moscow, Akademiya Publ., 2013. 338 p.

3. Devyanin P.N. *Modeli bezopasnosti komp'yuternykh sistem* [Models of the Security of Computer Systems]. *Prikladnaya diskretnaya matematika* [Applied Discrete Mathematics], 2009, no. 2. 190 p.

4. Luzhnov V.S., Sokolov A.N. [Security Analysis of Automated Systems Based on the Model of Attacks on Information Resources]. *Sbornik trudov I Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii "Voprosy kiberbezopasnosti, modelirovaniya i obrabotki informatsii v sovremennykh sotsiotekhnicheskikh sistemakh 'Inform–2015'"* [Proc. 1st Int. Sci. Conf. "Problems of Cyber Security, Simulation and Data Processing in the Modern Socio-Technical Systems"]. Kursk, 2015. (in Russ.)

5. Luzhnov V.S., Sokolov A.N. [Software Security Analysis of Automated Systems. Problems and Prospects]. *Sbornik trudov XIII Vserossiyskoy nauchno-prakticheskoy konferentsii studentov, aspirantov i molodykh uchenykh* [Proc. 13th All-Russian Conf. of Students, Graduate Students and Young Scientists]. Chelyabinsk, 2015. (in Russ.)

6. Serduk V.A. *Razrabotka i issledovanie matematicheskikh modeley zashchity avtomatizirovannykh sistem ot informatsionnykh atak* [Development and Research of Mathematical Models of the Automated Systems of Protection of Information Attacks]. Moscow. 2004.

7. Schnier B. *Modelirovanie ugroz bezopasnosti* [Modeling Security Threats]. Available at: https://www.schneier.com/paper-attacktrees-ddj-ft.html (accessed 18 March 2016).

8. Serduk V.A. [A Mathematical Model for Estimating the Level of Security of Data Transmission Networks]. *Modeling. Theory, methods and tools*. Novocherkassk, 2002, pp. 31–34. (in Russ.)

Received 20 March 2016

УДК 004.056 **DOI: 10.14529/ctcr160303**

АЛГОРИТМИЗАЦИЯ ЭТАЛОННЫХ МОДЕЛЕЙ ЗАЩИЩЕННОСТИ КОРПОРАТИВНЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ НА БАЗЕ ФОРМАЛЬНЫХ МОДЕЛЕЙ БЕЗОПАСНОСТИ

В.С. Лужнов, А.Н. Соколов

Южно-Уральский государственный университет, г. Челябинск

Рассмотрен процесс алгоритмизации эталонных моделей защищенности автоматизированных систем, реализованных на основе существующих формальных моделей безопасности. Изучены основные подходы практической реализации эталонных моделей защищенности с позиций выявления потенциальных направлений их улучшения. Проведен анализ ограничений моделей в целях синтеза на их основе формальной эталонной модели, поддающейся реализации в виде программного алгоритма для последующего проведения практического анализа защищенности реальных систем. Выбран математический аппарат и проведена формализация синтезированной модели. На базе формализованной модели построен граф, объединяющий множества уязвимостей информационной безопасности, способов реализации атак и последствий для защищенности систем, на основе которого возможно создание управляемых моделей реальных систем. Сформулирован алгоритм проведения в полуавтоматическом режиме анализа защищенности корпоративных автоматизированных систем.

Ключевые слова: информационная безопасность, автоматизированные системы, эталонные модели безопасности, алгоритмизация формальных моделей, безопасность автоматизированных систем, анализ защищенности автоматизированных систем.

Литература

1. Щербаков, А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты: учеб. пособие / А.Ю. Щербаков. – М.: Книжный мир, 2009. – 352 с.

2. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учеб. пособие для студ. высш. учеб. заведений / П.Н. Девянин. – М.: Издат. центр «Академия», 2013. – 338 с.

3. Девянин, П.Н. Модели безопасности компьютерных систем. / П.Н. Девянин // Прикладная дискретная математика. – Томск: НИТГУ, 2009. – № 2. – 190 с.

4. Лужнов, В.С. Анализ защищенности корпоративных автоматизированных систем на основе модели атак на информационные ресурсы / В.С. Лужнов, А.Н. Соколов // I Международная научно-техническая конференция «Вопросы кибербезопасности, моделирования и обработки информации в современных социотехнических системах «Информ–2015»: сб. тр. – Курск: Изд-во КГУ, 2015.

5. Лужнов, В.С. Программные средства анализа защищенности автоматизированных систем. Проблемы и перспективы / В.С. Лужнов, А.Н. Соколов // Безопасность информационного пространства: сб. тр. XIII Всерос. науч.-практ. конф. студентов, аспирантов и молодых учёных / сост. А.Н. Соколов. – Челябинск: Издат. центр ЮУрГУ, 2015.

6. Сердюк, В.А. Разработка и исследование математических моделей защиты автоматизированных систем от информационных атак / В.А. Сердюк. – М.: РГТУ им. К.Э. Циолковского, 2004.

7. Шнайер, Б. Моделирование угроз безопасности / Б. Шнайер. – https://www.schneier.com/paper-attacktrees-ddj-ft.html.

8. Сердюк, В.А. Математическая модель оценки уровня защищённости сетей передачи данных / В.А. Сердюк // II Междунар. науч.-практ. конф. «Моделирование. Теория, методы и средства». – Новочеркасск, 2002. – С. 31–34.

Лужнов Василий Сергеевич, аспирант, ассистент кафедры безопасности информационных систем, Южно-Уральский государственный университет; ua9stz@gmail.com.

Соколов Александр Николаевич, канд. техн. наук, доцент, заведующий кафедрой безопасности информационных систем, Южно-Уральский государственный университет; ANSokolov@inbox.ru.

Поступила в редакцию 20 марта 2016 г.

ОБРАЗЕЦ ЦИТИРОВАНИЯ

Luzhnov, V.S. Algorithmization of Reference Security Models of Corporate Automation Systems Based on Formal Security Models / V.S. Luzhnov, A.N. Sokolov // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». – 2016. – Т. 16, № 3. – С. 25–31. DOI: 10.14529/ctcr160303

FOR CITATION

Luzhnov V.S., Sokolov A.N. Algorithmization of Reference Security Models of Corporate Automation Systems Based on Formal Security Models. *Bulletin of the South Ural State University. Ser. Computer Technologies, Automatic Control, Radio Electronics*, 2016, vol. 16, no. 3, pp. 25–31. DOI: 10.14529/ctcr160303