MODELLING FOR ENSURING INFORMATION SECURITY OF THE DISTRIBUTED INFORMATION SYSTEMS

Alexander A. Grusho, Elena E. Timonina and Sergey Ya. Shorgin
Institute of Informatics Problems,
Federal Research Center "Computer Science and Control"
of the Russian Academy of Sciences
Vavilova 44-2, 119333, Moscow, Russia
Email: grusho@yandex.ru, eltimon@yandex.ru, sshorgin@ipiran.ru

KEYWORDS

Information security of the distributed information systems, models of the permitted interactions, statistical models of interactions

ABSTRACT

In the paper the concept of the permitted interactions is defined, i.e. such interactions are necessary for the tasks which are legally started at present. Any other interactions are considered as forbidden.

The main objective is definition, what interactions are permitted during this period of time. For the solution of this problem it is offered to model the needs for interactions depending on existence of legally started tasks. Such modeling is possible on the basis of meta data about the used tasks and their information requirements.

The main idea of control is that the started task appeals to meta data for the permission of interaction with other task, necessary for her decision. On the basis of meta data a need of such interaction is defined and permission which can't be forged or bypassed is given.

INTRODUCTION

The malicious code and harmful influences (Rieck et al.(Eds), 2013; Skorobogatov and Woods, 2012) can move through the distributed information system (DIS), using independently organized interactions of the DIS components. This assertion is true for the distributed DIS components. Therefore it is expedient to control all interactions of the DIS components. First of all it concerns to interactions of software applications. The set of software applications is part of a set of tasks which can be realized in DIS. In this paper software applications are also called tasks.

In the paper the concept of the permitted interactions is defined, i.e. such interactions are necessary for the tasks which are legally started at present. Any other interactions are considered as forbidden.

For such security policy it is necessary to develop special means of its realization. It is easy to construct mechanisms of control of network flows with use of cryptography. However the main objective is definition of component interactions which are allowed during this period of time. For the solution of this problem it is offered to model interactions depending on existence of legally started tasks. Such modelling is possible on the basis of meta data about the used tasks and their information requirements.

The main idea of control is that the started task appeals to meta data for the permission of interaction with other task, necessary for her decision. On the basis of meta data the need of such interaction is defined and permission which can't be forged or bypassed is given. Really interactions are implemented through network by means of sessions and information flows in network.

Usually security of information flows is supported by Firewalls, Proxy servers, Intrusion Detection Systems. These mechanisms work when there can be malicious flows. The paper presents new security mechanism which can be used instead of traditional measures. This is due to the strong limitation for existence of non needed information flow.

In the paper the ways of creation of the required meta data is considered. Historically the first method for creation of meta data are statistical (it was used in Secret Net). However with development of information technologies other ways for creation of meta data were found, tools are developed for their realization.

Emergence of such new methods is connected with constantly arising situations in which the initial statistical method doesn't give the adequate answer.

Control methods of information flows have a long story. They are correctly realized in security policies MLS and Biba (TCSEC, 1985). However these policies are formulated only in terms of information flows. Real security policies consider interactions of all DIS components and are formulated at the levels of tasks (software applications), and hosts (Grusho et al., 2014).

But all mechanisms of their realization are at the lower level of hierarchy (network, computer system). Therefore we define a mapping of interactions of components of the top level to the lower level.

Certificates of open keys (Menezes et al., 1997) which allow a wide arbitrariness in the organization of network interactions are used long ago in problems of the organization of secure communication sessions in networks. Sometimes it is useful. Tracking of such connections with the help of audit allows to indirectly observe leakages of valuable information, or interaction with the risk hosts including a malicious code.

On the opposite side there is the system of permitted connections with the help of a priori set of keys for

Proceedings 31st European Conference on Modelling and Simulation ©ECMS Zita Zoltay Paprika, Péter Horák, Kata Váradi, Péter Tamás Zwierczyk, Ágnes Vidovics-Dancs, János Péter Rádics (Editors)
ISBN: 978-0-9932440-4-9/ ISBN: 978-0-9932440-5-6 (CD)

symmetric cryptography.

In the paper we offer the intermediate way of the organization of communication when session keys are created by the cryptographic center as a result of the positive decision on a possibility of interaction of hosts. This way is more suitable for cases when security policy is defined by interactions of the current business tasks, and demands frequent changes.

The paper is structured as follows. Section 2 introduces two-level hierarchical model of DIS. Section 3 defines the problem of information security in DIS. In Section 4 we construct the special protocol which allows controlling information flows. In the Section 5 we consider the security assessment by means of the constructed protocol. In Section 6 we give examples of meta data formation. In Conclusion we shortly analyze the results.

TWO-LEVEL MODEL OF THE DISTRIBUTED INFORMATION SYSTEMS

The DIS two-level hierarchical model consists of the level of tasks and level of network. The network consists of hosts. The connection equipment allows to connect each host with everyone host without an interactions with other hosts. Communication is implemented only by means of sessions, for example, under the TCP protocol. In further considerations the network equipment will not be considered.

Hosts are computer systems and contain computing resources, information resources and software for the solution of various tasks.

The task is a facility for a transformation of information. It consists of source data which it can receive from other tasks, means of transformation of information, and the output data which will be used by other tasks. According to (Nilsson, 1971) a task can be divided into subtasks (operation of a reduction). Thus, a task A can generate a schedule of subtasks (Fig. 1).

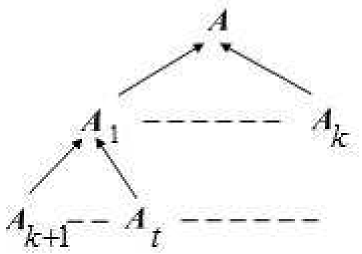

Figure 1: Graphic of subtasks

Let's note that subtasks carry out transformations of information, which results are used in the solution of an initial task A. Some tasks can be solved in other hosts.

Thus it is possible to consider that there is a mapping of a set of tasks and subtasks of a task A into a set of hosts. For any task A, a host on which it is solved, we will denote $H(A)$.

For the convenience tasks and hosts are named DIS components. Hosts on which tasks are solved form the level of network for tasks. All interactions of tasks (collection of information, distribution of information, starting) are carried out through network interactions.

As it was noted above, network interaction is implemented only through communication sessions. Each session is unambiguously defined by the identifiers (addresses, ports, etc.).

Thus, two-level decomposition of DIS (network, tasks) is constructed. Data transmission between hosts is implemented by means of information flows. Thus, each interaction of the DIS components is characterized by a set of information flows.

In traditional networks information flows can form transitive closure, i.e. information flows $V_1 \mapsto V_2$, $V_2 \mapsto V_3$ can generate information flow $V_1 \mapsto V_3$ (can be with a time lag). In certain cases such transitive closure is inadmissible from the point of view of information security. Therefore in DIS it is necessary to build the architecture preventing unauthorized closure of information flows.

INFORMATION SECURITY IN DIS

Let's consider questions of the information security in DIS. For generalizing the model (Grusho et al., 2014, 2015a), we will divide all information flows on admissible flows and non admissible flows.

The permitted interactions are defined by the scheme (Fig. 1), and the task A requests data for itself (ready, or demanding for calculations), i.e. the data flow is directed to A. Then for all levels of the reduction of the task A, and for network schedules the data flows are directed to A or to the following element of the network schedule. When the immediate task is solved, the user or the managing program starts a following task.

Admissible information flows are defined by the permitted interactions of tasks for hosts on which they are solved.

Experience in flows control in security policies (MLS and Biba (TCSEC, 1985)) shows that to construct an information security of DIS basing only on a concept of information flows is not enough because of a possibility of transitive closure of information flows. Therefore the information security models will be constructed on two bases:

- admissible/ non admissible information flows;
- isolation of tasks in computer systems.

Isolation of a task A in a computer system assumes that there is an isolated domain in computer system such that:

- in it there are all source data for solution of task A;
- there is no malicious code in it;
- if on a host two or more tasks are being solved, then their domains are guaranteed to be isolated from each other; necessary data exchange is possible only with the permission of some managing process $\mathcal{N}(H(A))$.

The concept of isolation of a task on a host allows to exclude non admissible transit of information flows. Basic element of providing information security is the model of tasks $\mathcal{N}$ on a host H_0. Model $\mathcal{N}$ is also a task containing a meta information about other tasks.

For its execution the task A on a host $H(A)$ has to address an immediate task A_1 as it follows from scheme of a reduction (Fig. 1). For this purpose the task A generates request for a possibility of the appeal of the task A to the task A_1, and addresses the managing program $\mathcal{N}(H(A))$. Each host H in DIS has in the managing task $\mathcal{N}(H)$ cryptographic facilities and a unique key $k(H)$ for communication with the managing task $\mathcal{N}$ on a host H_0.

The task $\mathcal{N}(H(A))$ forms the encoded message on key $k(H(A))$ with a request to allow interaction of the task A with the task A_1. The task $\mathcal{N}$ checks need of the appeal to A_1 with the help of available for it meta data of the solution of the task A. At the positive decision $\mathcal{N}$ forms the encoded message for the task $\mathcal{N}(H(A))$ in which there is an address of the host $H(A_1)$, number of a port for communication with the task $\mathcal{N}(H(A_1))$ and a session key $k(A, A_1)$. The similar message is also formed for a host $H(A_1)$. The address of the host $H(A)$, port of the task $\mathcal{N}(H(A))$, permission for starting of the task A_1 for the benefit of the task A, and the common key for their communication $k(A, A_1)$ are specified in this message. After obtaining this information the host $H(A)$ initiates a session of the encoded communication with the host $H(A_1)$.

Completion of a session happens standardly. If there is a failure, then it comes to light by means of identification codes MAC (Message Identification Code). In case of need there is a restart of the protocol.If we have agents $\mathcal{N}(H)$ in every host, then there is no need to use all other protocols to control parameters of the net. All necessary control information can be gathered by secure interaction of available hosts with H_0. It can be done by several sets of meta data. One of them may be net control meta data. It helps to forbid service flows.

Cryptographical part of the model resembles well known protocol Kerberos, but it supports different functionality.

SECURITY ASSESSMENT BY MEANS OF THE PROTOCOL

For verification of security of system by means of the offered method it is necessary to prove the following.

1. All admissible information flows are implemented in system.
2. Non admissible information flows, including transit flows, are absent.
3. All failures are identified.

Assertion. Admissible information flows in network are generated by legal interactions of tasks according to the scheme of meta data in $\mathcal{N}$, and non admissible information flows are impossible.

Proof. In the task $\mathcal{N}$ there is information about the required interactions of the task A with other tasks from which it has to obtain source data. If at least one of such tasks A_1 is on other host, i.e. $H(A) \neq H(A_1)$, then according to Protocol A requests at $\mathcal{N}$ an interaction with the task A_1. The task $\mathcal{N}$ finds the host $H(A_1)$ and allows opening of the protected session between $H(A)$ and $H(A_1)$. Information flows of this session are admissible according to the definition. Besides $\mathcal{N}$ can initiate all service information gathering. It can be done by initiating a legal session with any available host. Even protocol "keep alive" (control of perimeter of net) can be constructed in such a way. That proves the first part of the assertion.

Let's assume that the host H wants to organize a session with host H' beyond of an authorization system $\mathcal{N}$ (according to the assumption the UDP connection is forbidden). However the port and, therefore, the software application on the host H' aren't defined. Standard ports in secure system are closed. Communication with any legal task is carried out by means of enciphering. Other ways of information transfer from host H to host H' don't exist in the considered system. Thus, non admissible information flow between hosts H and H', ignoring an authorization system, is impossible in the system, where interactions are under $\mathcal{N}(H)$ control.

It is necessary to check impossibility of unauthorized transitive closure of information flows. If the host H has the permitted session with a host H', and the host H' has the permitted session with a host H'', then two situations are possible.

- Host H' organizes a session with a host H'' for the task A which has generated a session between host H and host H'. Then it is possible a transit information flow from host H to a host H'' and vice versa. However these flows are necessary for the solution of the task A and therefore they are legal information flows.

- If the host H' organizes the permitted session with a host H'' for the decision of a task A', unconnected with the task A, then in the assumption of domains isolation concerning the task A doesn't get into information flow from host H' to a host H''. Also information concerning to task A' doesn't get into information flow from the host H' to the host H. So it follows that there is no exist non admissible transit closure of information flows.

The assertion is proved.

FORMATION OF META DATA

The protocol forbids any connections which aren't reflected as legal in meta data. Therefore questions of completeness, consistency, a possibility of modification, and scalability are connected with the organization of meta data.

Questions of the organization of meta data are connected with possible examples of interrelation of tasks. Without applying for completeness, we will give several such examples.

Example 1. Addressing of a task A to database. In meta data it perhaps the access of the task A to the database on subject T. T is a parameter of the task A. The protocol will organize a session with the host containing the DBMS, but the access is possible only about subject T.

Let's show how it is supported by functionality of Oracle DBMS. The addressing to the task A_1 with parameter T (the appeal to the DBMS with a request from the task A) is equivalent to creation of the user process on a host $H(A_1)$. In Oracle DBMS the user process generates the server process isolated by means of TCB (Trusted Computing Base) (Oracle7 and Trusted Oracle7, 1994). For an isolation of server processes the mechanisms of implementation of discretionary and mandatory security policies are used (TCSEC, 1985). In this regard restriction of T is implemented by the standard policies of access control which are built in the DBMS. The trust to these functions is determined by certification documents (Oracle7 and Trusted Oracle7, 1994).

Example 2. Formation of meta data by means of models of business processes.
Formation of meta data about interactions of tasks can be made on the basis of business process modelling methods. A set of advanced methods is developed for business process modeling: IDEF, ARIS, UML, BPMN, etc. (Samuylov et al., 2009).

The methodology of the functional simulation of IDEF0 considers system as a set of actions, each of which will transform some object or a set of objects. These actions correspond in the considered terminology to tasks and information transforms. Application of IDEF0 is presented in the form of hierarchy of the charts connected by cross-references. These models, in particular, allow to estimate distribution of resources for implementation of the target task.

For creation of models an automation software, for example, of BPwin and ERwin (Samuylov et al., 2009) are created. For creation of sequential diagrams it is possible to use methodology of IDEF3 (Samuylov et al., 2009). The methodology of IDEF3 is supported by software of the Computer Associates companies, etc.

The methodology of ARIS assumes several abstraction layers and serves for the complex description of activities of the enterprizes. In this methodology the set of models for the adequate description of system and its processes is created. Software tools are created to support of ARIS which are added by modeling languages of UML, BPMN and etc.

Example 3. Meta data for tasks with uncertainty.
It is the most difficult to apply the offered approach of support of information security in DIS to tasks with uncertainties. An example of uncertainty is the question to the task $\mathcal{N}$: "Whether the task A can be solved by means of the task A_1?" For the consideration of such questions it is possible to use semantic methodology. Semantic methods are based on the description of ontologies. The ontology is understood as (Samuylov et al., 2009) hierarchical data structure containing meanings of information and their communications. The formal language of descriptions of ontologies is the standard of Web Ontology Language (Samuylov et al., 2009).

Example 4. The description of admissible communications of tasks by means of data mining.
This method of formation of an authorization system is connected with search of such tasks which can be the useful in the analysis of the task A. This method has common features with the example 3. However complication of search in comparison with an example 3 consists that there is no accurate description of the required ontologies. Therefore for creation of an algorithm of the decision about admissible communications for this class of tasks more thin methods of data mining are necessary (Finn (Eds)., 2009).

Example 5. Statistical method of formation of meta data.
Let some time the DIS, servicing technological processes of the organization, works in the free mode. Meta data are created by results of observation over interactions of tasks in DIS in the free mode. In some time point all interactions of solvable tasks in each of information technologies are fixed. The received mold of interactions defines meta data for monitoring of further interactions.

In case of such method of formation of meta data next errors are possible:

- some operation modes of information technologies can demand further additional requests for information resources or the software. I.e. in this method we get a bigger number of non admissible interactions, than it is necessary;

- in the free mode some interactions could be excessive, and can generate information flows, dangerous to functioning of information technologies.

Example 6. A method of bans for formation of meta data.
Let's assume that all interactions are permitted, except some set of couples of the forbidden interactions (bans). Theory of bans in discrete probability spaces developed since 2011 year (Grusho A. and Timonina E., 2011). Bans form the graph in which vertices are tasks, and edges are bans. This method is rough, but it allows to enter dynamics into system of permissions of interactions. For example, the monitoring system registers events which can be signs of the attacks to assets of the organization. Then for support of information security it is necessary to block urgently any accesses to these assets. At the same time remaining assets need to be still available not to block operation of DIS (Grusho et al., 2015b).

CONCLUSION

Simulation in DIS is widely used for the organization and optimization of computation. An example of successful usage of models for the analysis of behavior of a network is MiniNet [(Lantz et al., 2010). The main idea of efficiency of MiniNet consists that experiments are made on the reduced, cut down information on a traffic.

In this paper it is offered to use the simulation based on the reduced information on solvable tasks and their interactions for implementation of the security policies connected to control of information flows on a network. Component interactions of DIS which generate information flows on a network are modelled. The security policy is built on the basis of division of all of information flows on a network on the admissible flows and non admissible flows. Permission is created due to the model of the allowed interactions in case of decision of legal tasks in DIS. This information by means of the special protocol allows controlling information flows.

The permitted interactions are defined by meta data of tasks and their communications. In the paper ways of creation of meta data about permitted interactions of tasks are considered.

Acknowledgements

This work was supported by the Russian Scientific Foundation (grant No. 16-11-10227).

REFERENCES

Grusho, A. and E. Timonina. 2011. "Prohibitions in discrete probabilistic statistical problems". *Discrete Math. and Appl.* 21, No.3, 275–281.

Grusho, A., N. Grusho, S. Shorgin and E. Timonina. 2014. "Secure architecture of the distributed systems". *Systems and means of informatics* 24, No.3, 18-31.

Grusho, A., N. Grusho, S. Shorgin and E. Timonina. 2015. "Possibilities of Secure Architecture Creation for Dynamically Changing Information Systems". *Systems and means of informatics* 25, No.3, 78-93.

Grusho, A., M. Levykin, E. Timonina, V. Piskovski and A. Timonina. 2015. "Architecture of consecutive identification of attack to information resources". *2015 7th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, Brno, 265-268.

Lantz, Bob, Brandon Heller and Nick McKeown. "A Network in a Laptop: Rapid Prototyping for Software-Defined Networks". *9th ACM Workshop on Hot Topics in Networks*, October 20-21, 2010, Monterey, CA.

Menezes, Alfred J., Paul C. van. Oorschot and Scott A.. Vanstone. 1997. *Handbook of Applied Cpyptography*, CRC Press LLC, 780 p.

Nilsson, Nils J. 1971. *Problem-Solving Methods in Artificial Intelligence*, New York: McGraw-Hill Pub. Co., 255 p.

Final Evaluation Report Oracle Corporation's Oracle7 and Trusted Oracle7. Report No. CSC-EPL-94/004. C-Evaluation No. 07-95. 5 April 1994.

Rieck, K., P. Stewin and J.-P. Seifert (Eds). 2013. "Detection of Intrusions and Malware, and Vulnerability Assessment". *Proc. of 10th International Conference, DIMVA 2013*, LNCS 7967, Springer Berlin Heidelberg, 207 p.

Samuylov, K.E., A. V. Chukarin and N. V. Yarkina. 2009. *Business processes and information technologies in management of the telecommunication companies*, Moscow: Alpina Pablisherz, 2009. 442 p.

Skorobogatov, S. and Ch. Woods. 2012. "Breakthrough Silicon Scanning Discovers Backdoor in Military Chip". *Cryptographic Hardware and Embedded Systems - CHES 2012* LNCS 7428. Springer, Heidelberg, 23-40.

TCSEC. Department of Defense Trusted Computer System Evaluation Criteria. 1985, DoD.

Finn, V.K. (Eds), 2009. *Automatic Hypotheses Generation in Intelligent Systems*, Moscow: KD "LIBROKOM", 528 p.

AUTHOR BIOGRAPHIES

ALEXANDER A. GRUSHO, Professor (1993), Doctor of Science in physics and mathematics (1990). He is Head of laboratory in Institute of Informatics Problems, Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences (FRC CSC RAS) and Professor of Moscow State University.

Research interests: probability theory and mathematical statistics, information security, discrete mathematics, computer sciences.

His email is `grusho@yandex.ru`.

ELENA E. TIMONINA has graduated from the Moscow Institute of Electronics and Mathematics and obtained the Candidate degree (PhD) in physics and mathematics (1974). She is Doctor in Technical Science (2005), Professor (2007). Now she works as leading scientist in Institute of Informatics Problems, Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences (FRC CSC RAS).

Research interests: probability theory and mathematical statistics, information security, cryptography, computer sciences.

Her email is `eltimon@yandex.ru`.

SERGEY Ya. SHORGIN, Professor (2003), Doctor of Science in physics and mathematics (1997). He is Deputy Director of Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences (FRC CSC RAS) and principal scientist of Institute of Informatics Problems of FRC CSC RAS. Research interests: probability theory and mathematical statistics, information security, communication systems modeling, computer sciences.

His email is `sshorgin@ipiran.ru`.