Nonlinear Phenomena in Complex Systems, vol. **17**, no. 3 (2014), pp. 263 - 271

Reflexive Control over Intruder Using Deception Systems

D. S. Lavrova,* E. Y. Pavlenko,† and A. I. Pechenkin‡
Saint-Petersburg State Polytechnic University,
29 Politechnicheskaya Str, 195251 Saint-Petersburg, RUSSIA
(Received 31 March, 2014)

Confrontation between a security administrator and an intruder is presented as an information security conflict. An approach to formalization of this conflict on the basis of Lefebvre's algebra of conflicts has been proposed. Possible behavior strategies of conflict participants have been analyzed and identified those being most effective in terms of protection. These strategies are proposed to be implemented by using deception systems. A generalized model of IS security threats has been developed which links information security offenders of various types to critical objects of the protected IS. It has been also identified a subset of critical IS objects in order to arrange "traps" in the deception system implementing reflexive control over external intruder. A concept of the adaptive deception system based on maximizing the length of the graph describing the actions of the attacker in a deception system has been suggested.

AMS Subject Classification: 68U35
Keywords: conflict of information security, deception systems, information security, Lefebvre's algebra of conflicts

1. Introduction

In the context of widespread computerization, information has become a critical resource, that gives rise to significant increase in attempts to breach the security of information systems [1]. In order to improve the efficiency of automated systems information security, a complex approach based on combination of a priori and a posteriori information protection means is frequently used. Often protection means are supplemented by the others, implementing indirect protection by setting the attacker in a state of a priori uncertainty. An example of such means of protection is deception systems. Deception mechanism implements control over an intruder, therefore, in the process of studying the attacker behavior this mechanism can be extended and supplemented in order to increase the degree of information protection. To study the attacker behavior it is necessary to consider options of his actions in a confrontation, a conflict, whose subject is providing information security.

2. Formalization of information security conflict

When it is necessary to ensure information security of an information system (IS), an intruder is regarded as a party opposed to defense mechanisms of the IS. Since the protective mechanisms are set by the IS security administrator, there is a confrontation between the security administrator and the intruder, which can be presented as a conflict between two parties. The conflict between two disparate security professionals, which can not be resolved "peacefully", will be called a conflict of information security (ISec conflict). It is impossible to resolve the ISec conflict "peacefully" due to the contradiction of goals of the security administrator and the attacker: the former aims to ensure security and prohibit illegitimate access to the IS infrastructure, while the latter wants to obtain information about the infrastructure of the protected system, acting illegitimately and

*E-mail: lavrova.daria@gmail.com
†E-mail: evpavlenko92@gmail.com
‡E-mail: alexander.pechenkin@ibks.ftk.spbstu.ru

hacking or bypassing the IS security mechanisms.

The object (goal) of the conflict is the infrastructure of the information system. The participants of the conflict are the security administrator and the intruder. A formal description of the ISec conflict is necessary to increase the information system security, as mathematically describing hacker's potential strategies and their development we can extend the functionality of security mechanisms. In order to formally describe such a process, one should correctly choose mathematical tools which will further enable to describe the properties of the process in the most abstract and adequate way.

For a formal description of the conflict, where the parties copy each other thinking process, trying to impose on each other a certain pattern of behavior and can change behavioral strategies, the best option is to combine the tools of Lefebvre's algebra of conflicts and the Game Theory. The advantage of Lefebvre's algebra of conflicts mathematical tools as applied to a formal description of a conflict is the possibility to imitate the opposing parties' thinking process and to describe reflexive control the process of transferring the grounds for taking the wrong decisions by the adversary [2].

In accordance with the concept of conflict description used in Lefebvre's algebra [3], to describe the conflict between a security administrator A and a hacker H, the following symbols should be introduced:

- S-objective situation, represented as some foothold for confrontation. In relation to an information security conflict, a foothold is the infrastructure of the protected system including physical and logical structures of the system, as well as a set of integrated protection means;
- administrator (A) perception of the foothold S, the displaying of S on the set of knowledge of A, represented as S_A. The security administrator does not have a complete set of information about the system's security, as his set of knowledge is limited to the used protection means, therefore, there always remains a non-zero risk of having undetected or previously unknown security problems;
- intention of the security administrator I_A, which is to ensure the information security of the protected system in the context of opposition to the hacker and detecting the attempts of breaking the system security;
- doctrine D_A, representing a set of measures and actions to ensure the security of the system ant the information stored in it;
- resolution of the problem of ensuring the system information security R_A obtained by application of the doctrine D_A to S_A.

The administrator's decision making process can be presented as follows:

$$\frac{I_A}{S_A} D_A \to \frac{R_A}{S_A}. \tag{1}$$

Similarly, we introduce the symbols of terms for describing the conflict for the hacker:

- hacker (H) perception of the foothold S, the displaying of S on the set of knowledge of H, represented as S_H. At the initial stage, the hacker set of knowledge of the system can be either empty, or contain information obtained from public sources, as well as from the insiders of the system. In the course of the conflict this set can be expanded, replenishing with both false and true information;
- hacker's intention I_H, which is to break the information security of the target system and hide the traces of harmful effects on the system;
- doctrine D_H, representing a set of actions and means aimed at violating the system's security;
- resolution of the problem of breaking the system's information security R_H obtained by application of the doctrine D_H to S_H.

The hacker H, based on his experience and skills, is able to imitate the decision taken by the administrator, which is indicated by $\overleftarrow{AH}$.

In order to take a decision ensuring success, H should imitate reasoning of and must follow the procedure described by the formula (1). It should be noted that the hacker H does not possess S_A. He possesses something that can be described as "perception of S_A from the point of view of H", which is secondary perception of the objective situation S. Likewise, the hacker H is not in possession of I_A and D_A; he holds only "I_A from the point of view of H" and "D_A from the point of view of H". The introduction of the symbols S_{AH}, I_{AH}, D_{AH} and R_{AH} makes possible a formal description of hacker's (H) imitation of administrator's (A) reasoning as follows:

$$\frac{I_{AH}}{S_{AH}} D_{AH} \to \frac{R_{AH}}{S_{AH}}. \tag{2}$$

Next, the hacker must project the decision obtained as a result of imitation $\frac{R_{AH}}{S_{AH}}$ to the set of his knowledge about the system:

$$\frac{R_{AH}}{S_{AH}} \to \frac{R_{AH}}{S_H}. \tag{3}$$

Now the hacker, by applying his doctrine, must devise a solution, which is to define a set of actions enabling him to breach the target system's security:

$$\frac{R_{AH}}{S_H} \to \frac{R_{AH} I_H}{S_H} D_H \to \frac{R_H}{S_H}. \tag{4}$$

The decision making process with the imitation according to $\overleftarrow{AH}$ can be presented in the following way:

$$\frac{I_{AH}}{S_{AH}} D_{AH} \to \frac{R_{AH}}{S_{AH}}$$

$$\to \frac{R_{AH}}{S_H} \to \frac{R_{AH} I_H}{S_H} D_H \to \frac{R_H}{S_H}. \tag{5}$$

In this conflict, the administrator A is defeated, as the hacker H managed to copy the thinking process of A. It is obvious that in this conflict can occur more complex chains of imitating adversary's thinking process, in particular, the administrator can as well imitate hacker's imitation process of adversary's reasoning. Thus, the conflict will be won by the party, that will be able to predict adversary's way of thinking in the most precise way.

One of the most effective behavior strategies in a conflict is modeling adversary's decisions by transferring to him the reasons, on the basis of which he could logically infer his own, but predetermined by the other party, decision [3]. The transfer of reasons between the administrator and the hacker implies getting A involved in the process of reflection of the situation by H, thus A starts to control the process of decision making. In reference [3] it is determined that any "deceptive movement" (provocation and intrigue, disguise and jokes, making false objects and lie in general in any context) are realizations of reflexive control.

Suppose that the administrator A has a single (first) rank reflection, and the hacker H has a zero rank. This means that A can perform reflexive control over H. In general terms, this can be represented as transfer of picture F, specially planned by A for H, to H:

$$F_{HA} \to F_H. \tag{6}$$

Picture F consists of a set of elements S_{HA}, I_{HA}, D_{HA}, R_{HA}. Reflexive control in an information security conflict implies the transfer of one or more elements of this set to the opponent. Lefebvre's algebra presents some examples of reflexive control over the adversary:

- reflexive control by transferring false information about the foothold, $S_{HA} \to S_H$;
- reflexive control by forming the intention of the adversary $I_{HA} \to I_H$;
- reflexive control by forming the doctrine of the adversary, $D_{HA} \to D_H$, characterizing intentional "training" of the opponent in order to develop his association with achieving the target;

- reflexive control by transferring the resolution, $R_{HA} \rightarrow R_H$, an example of which may be an incorrect tip;
- forming the target by transferring the picture of the foothold $I_{HA} \rightarrow S_{HA} \rightarrow S_H \rightarrow I_H$;
- reflexive control by converting $S_{HAH} \rightarrow S_{HA}$, transferring supposedly your own view of the situation to the adversary;
- reflexive control by converting $I_{HAH} \rightarrow I_{HA}$, which includes convincing the adversary of acts that will not be committed (a deceptive trick);
- reflexive control by converting $D_{HAH} \rightarrow D_{HA}$, which includes convincing the adversary of using some doctrine, which will affect the hacker's conclusions, meanwhile the doctrine will not be used, but the hacker's logic, based on false information, will be obtained;
- reflexive control by the chain $I_{HAH} \rightarrow S_{HAH} \rightarrow S_{HA} \rightarrow I_{HA}$, which also includes transferring to the adversary supposedly your own view of the situation in order to form the wrong target;
- neutralization of the adversary's deduction, a technique used when it is impossible to avoid the disclosure of the true picture of the situation, in order to form some equally probable targets that can "confuse" the attacker.

In practice, implementation of such illustrations (we call them strategies) of reflexive control over the intruder can be resolved with the use of deception systems.

3. Deception systems as a tool for implementation of reflexive control

Deception systems are a promising mechanism supplementing the existing mechanisms for protection of information in computer networks, due to misleading information security violators [4]. Applying deception systems will not only disorient the intruder, but also maximize the amount of data obtained about his behavior, goals and skills through the use of reflexive control strategies.

Since a lie in any form is in itself the realization of reflexive control, therefore deception systems mechanism implements a priori reflexive control over the hacker. Deception systems mechanism allows implementing directly only the strategy of transmitting false information about the foothold. Therefore, to improve the performance and effectiveness of the information system protection one should consider approaches to implementation of the remaining reflexive control strategies, described earlier, through the mechanism of deception systems.

However, before considering and suggesting possible approaches to the implementation of the strategy, it is necessary to give reasons for choosing the strategies to be realized on the basis of probable targets of the hacker. The necessity is based on the risk that inappropriately large amount of time and material resources will be spent on developing and implementing the strategies without any significant increase in protection level of the IS.

Thus, the model of IS threats should be implemented. In this case, IS means not a certain IS, but a general definition, according to reference [5]: "Information system is a set of technical, software and organizational support, as well as personnel, aimed at timely providing the right people with adequate information."

4. Generalized model of information system security threats

Threats to IS security can be divided into four categories, according to their occurrence:

- Physical level
  - Embedding instrument bugs;

  - Deactivating IS components;
  - Destruction of material data storage items;
  - Invading communication lines;
  - Using photo and video equipment.
- Network level
  - Disturbing equipment availability;
  - Network traffic interception;
  - Network traffic modification.
- Operating system (OS) level
  - Installing malicious software;
  - Disrupting stable performance of system processes and services;
  - Impact on information resources (copying, editing, deleting information).
- Application level
  - Disrupting applications;
  - Impact on information resources of applications;
  - Applications modification.

According to IS security threats it is necessary to identify the most important - critical - objects, access to which the intruder will definitely want to get. Critical objects are classified as follows:

- Hardware
  - Computers;
  - Network hardware;
  - Material data storage devices.
- Software
  - Operating system services and processes;
  - Software applications.
- Information resources
  - Network traffic;
  - Files;
  - Information from data base (DB);
  - E-mail messages;
  - Logins / passwords.

In order to design the generalized threats model we should classify the sources of threats, i.e. intruders:

- Hackers deliberately attacking IS
  - External;
  - Internal - legitimate IS users, acting beyond user permissions;
- Suppliers of software and hardware, expendable materials, services etc., and contractors carrying out installation, commissioning of equipment and its repair
- Legitimate IS users acting without malicious intent.

The generalized model of IS security threats is presented in Figure 1.

Greatest interest represents the reflexive game with an external attacker, because for him the set of possible strategies used is somewhat broader and requires reflection of a lower rank. Therefore, further in describing the concept of adaptive deception systems and reflexive control strategies, the intruder will mean an outside attacker.

5. Choosing reflexive control strategies for implementing in a deception system in order to increase IS protection

On the basis of classified threats, from the range of reflexive control strategies we have selected those which can be realized through deception systems mechanism without any difficulties:

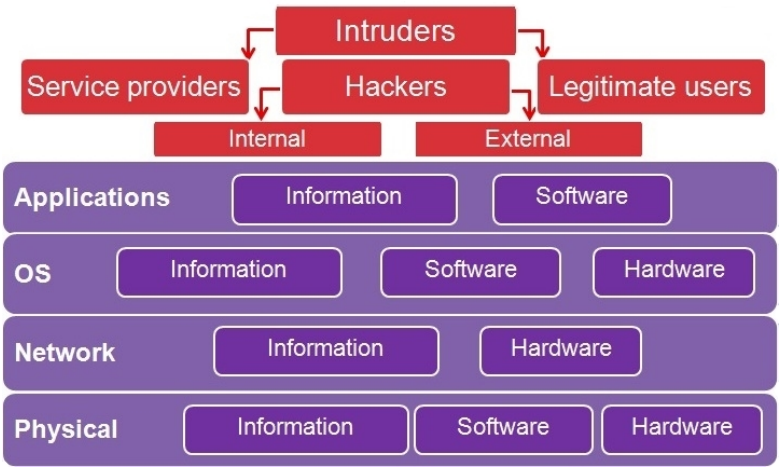

FIG. 1: Generalized model of IS security threats(in color).

- The strategy of transferring false information about the foothold $S_{HA} \to S_H$.
- The strategy of reflexive control by forming the target of the adversary $I_{HA} \to I_H$.
- The strategy of forming the target by transferring the view of the foothold $I_{HA} \to S_{HA} \to S_H \to I_H$.
- The strategy of reflexive control by converting $S_{HAH} \to S_{HA}$.
- The reflexive control strategy through the chain $I_{HAH} \to S_{HAH} \to S_{HA} \to I_{HA}$.

In relation to providing IS security, under transferring false information about the foothold should be understood transferring element $S_H A$ to the hacker, thus forming hacker's false perception of the protected IS infrastructure. This can be achieved by adding excessive elements both to the IS network infrastructure (hosts, ports, network protective means) and to the inside infrastructure (a set of "installed" software, folders with data, etc.).

With the use of deception systems we can implement the strategy of reflexive control by forming adversary's target ($I_{HA} \to I_H$). In this case, some desired action is enforced on the hacker by the security administrator, and it is done in such a way that the hacker is sure that he himself took the decision to commit this action. An example of such reflexive control in the situation when an hacker is exploring the network infrastructure of the protected IS can be opening of some port, whose scanning will guarantee hacker's getting into a "trap", provided the hacker tended to scan ports when analyzing network infrastructure. Another example of reflexive control is allocating in the IS a file or a folder with an "important", catching hacker's attention title (for instance, passwords.txt), in other words, some information for designated users. In using the strategy of forming the target by transferring the view of the foothold, the following transfer takes place $I_{HA} \to S_{HA} \to S_H \to I_H$. Such reflexive control is a more complicated process, as it includes goals of various importance. In an information security conflict the administrator's "global" goal is formed before the beginning of the conflict, and this is IS protection. Specific goal may be to "force" the hacker to attack some specially formed target (for instance, one of the servers). Forming hacker's target to attack the desired object is done by displaying false information on the foothold. Thus, initially the administrator selects the object which must become the hacker's

target, then he displays it so that the target for the attack of this object lay "on the surface" in order to acquire information resources, then he acts in such a way that the hacker could not understand that this target is specifically formed. Practical implementation of reflexive control by converting $S_{HAH} \rightarrow S_{HA}$ can be performed by deliberate giving relevant technical documentation about the IS infrastructure. It is also possible to use reflexive control strategy through the chain $I_{HAH} \rightarrow S_{HAH} \rightarrow S_{HA} \rightarrow I_{HA}$. As in one of the previously considered strategies, the target is transmitted to the hacker by transferring to him the administrator's view of the foothold. In this case, the hacker, analyzing the view of the foothold, must come to false (needless to say) conclusions. For example, the security administrator can concentrate a large amount of protective means around one of the network hosts, thereby causing the hacker to believe that this host contains very important confidential information, while it does not. As the deception system will be a software tool, some "emulation" of the protected system, the selected strategies will be implemented at all levels, except for physical. (However, reflexive control over the intruder can be performed at a physical level as well). In order to structure the future deception system implementing reflexive control over the intruder, we should identify which strategies will be realized at certain levels and what IS objects they will affect.

- Transferring false information about the foothold
  - Open ports;
  - Host;
  - Network protocol.
- Reflexive control by forming the target of the adversary
  - Network traffic;
  - Open ports;
  - OS;
  - Services and software;
  - Vulnerability.
- Forming the target by transferring the view of the foothold
  - Network traffic;
  - Open ports;
  - Vulnerability;
  - Files.
- Reflexive control by converting $S_{HAH} \rightarrow S_{HA}$
  - Network traffic;
  - Files.
- Reflexive control through the chain $I_{HAH} \rightarrow S_{HAH} \rightarrow S_{HA} \rightarrow I_{HA}$
  - Network traffic;
  - Files.

6. The concept of the adaptive deception system for reflexive control over the intruder

The concept of the adaptive deception system can be represented as a series of stages that are closely related to each other.

1. Constructing the configuration of the deception system. The peculiarity of this stage is that the infrastructure of the deception system must comply with the infrastructure of the real system. Since the hacker can take advantage of competitive intelligence and find out, at least, the number of employees in the organization, the number of hosts in the deception system must meet this number, otherwise the deception system can be at serious risk of being compromised.

2. Identifying a set of the most probable objects for an attack. This is done by sampling from a variety of critical objects in the deception system to form the attacker's target, which can

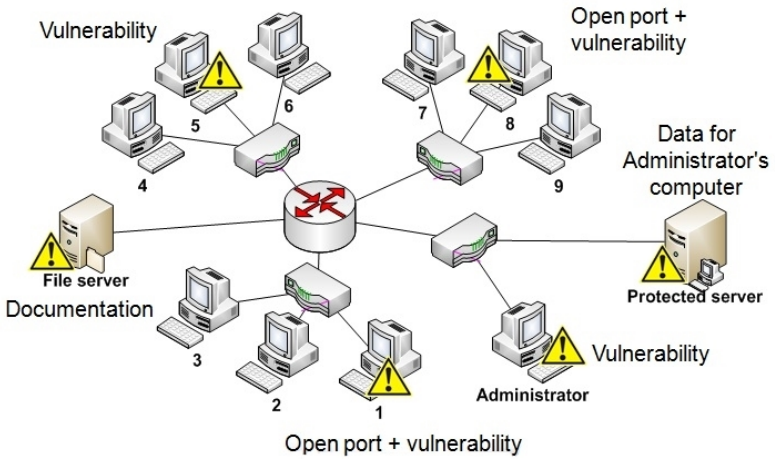

FIG. 2: Example of the configuration of the deception system with "traps" (in color).

be, for instance, the administrator's computer or the protected server.

3. Constructing the graph of maximum length to each target. The nodes of the graph are objects of the deception system and the edges of the graph are the hacker's actions. Such graph must be constructed in order to force the hacker to spend as much time as possible in the deception system for collecting the necessary information about him.

4. Classifying the nodes of the graph according to the criticality index of compromising. It is obvious that, for example, a "trap" emulating the administrator's computer will require a more complicated realization than an ordinary network host, therefore, neutralizing the threats of disclosure will require a substantially larger number of operations.

5. Specifying a set of strategies for each class of nodes. Each strategy will use a different set of "trap" for implementation, and this depends on the criticality index of compromising the object of the deception system.

6. Setting a number of "traps" for each strategy of each class.

7. Selecting and placing initial "traps", as using all the "traps" in the initial configuration of the deception system does not make sense.

8. Preparing a set of "traps" in case of compromising. This set will be used in case of arising a threat of compromising the deception system, to distract the hacker.

9. Extending the hacker's actions graph to maximum length. It is an emulation of unused "traps" for forcing a path similar to the graph of maximum length upon the hacker in order to get as much information about the hacker and his operations as possible. An example can be the configuration of the deception system (see Fig. 2), where exclamation marks show allocated "traps".

Figure 3 represents three scenarios describing the hacker's actions. Violet color demonstrates the graph of maximum length constructed initially, whereas pink and red show actions directed at bringing the graph to maximum length in conditions of compromising "traps" of various criticality indices: host and administrator's computer. The most complicated case is bringing the graph to maximum length in conditions of compromising the "trap" imitating the administrator's computer. Operations to neutralize the threat of compromising include "turning" the logic of "traps", as when the hacker directly attacks the administrator's computer, it is necessary to create an impression that it is not the administrator's computer, but a regular network host, as a result the graph will change

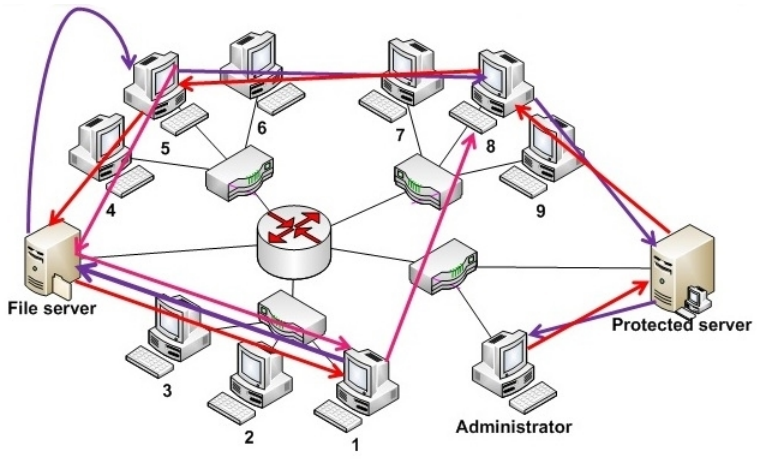

FIG. 3: Scenarios of the hacker's actions (in color).

its direction to the opposite, and computer #1 will emulate the administrator's computer which is the ultimate target of the hacker.

7. Conclusion

This paper presents the concept of the deception system for reflexive control over the intruder. For further formalization of information security conflict it is necessary to develop a hybrid mathematical model including the strategies of Lefebvre's algebra of conflicts. This will mathematically describe the principles of reflexive control over the intruder and realize algorithms and techniques for implementing these strategies in practice.

References

[1] D.P. Zegzhda. From information security to cybersecurity. Change of the paradigm. In: *Materials of the Conference "Information security. Regional aspects. InfoBEREG-2013"*.

[2] M.A. Eremeev, I.E. Gorbachev, G.U. Poterpeev, A.V. Kravchuk. Concealing information resources using deception systems. In: *Proceedings of the Conference "Theoretical and applied issues of developing and improving automated military control systems"*. Vol. 1. Pp. 140-147, 2013.

[3] V.A. Lefebvre, G.A. Smolyan. Lefebvre's algebra of conflicts. 1968. Computer Network Security, Lecture Notes in Computer Science, vol. 7531. Pp. 299-308 (2012).

[4] I.V. Kotenko, M.V. Stepashkin. Deception systems for protecting information resources in computer networks. Proceedings of SPIIRAS, 2004, Issue 2, Vol. 1, p. 211-230. Lecture Notes in Computer Science, vol. 3222. Pp. 9-21 (2004).

[5] W.S. Davis, D.C. Yen. The Information System Consultant's Handbook. Systems Analysis and Design. (CRC Press, 1998). Lecture Notes in Computer Science, vol. 4610. Pp. 372-384 (2007).