Journal of Discrete Mathematical Sciences & Cryptography
DOI : 10.1080/09720529.2016.1226619

Formalization of the problem of protection against reconnaissance in conflict systems

M. A. Styugin *
Department of Research
Siberian State Aerospace University
Department of Space and Information Technology
Siberian Federal University
79 Svobodny av, Krasnoyarsk 660041
Russia

A. A. Kytmanov †
T. N. Yamskikh §
Department of Space and Information Technology
Siberian Federal University
79 Svobodny av, Krasnoyarsk 660041
Russia

Abstract

This paper attempts to identify recent trends in counteraction to the intruder`s penetration into the system at reconnaissance stage as the sphere of information security. The problem of actions interrelation, agents` information awareness and system transition from one state into another is formulated.

Based on the functional model, formalization of the three tasks is presented. The first task formulates the conditions in which the system can not transform into undesirable state for a given set of indiscernible elements. The second task formalizes the way to achieve a safe state in the system and allows one to formulate the optimization problem. The third task formalises the conditions under which the system agents actions may be indiscernible to each other.

The scope of study for functional steganography is defined. Exponential complexity of agents actions factorization in a system is proved. The definition of absolutely indiscernible actions is provided.

E-mail:* **styugin@gmail.com
†*E-mail:* **aakytm@gmail.com**
§*E-mail:* **ytanya.08@mail.ru**

Keywords: *Information security, Hidden actions, Active systems, Structure of information awareness, Moving targets defence.*

Mathematics Subject Classification (2010): *93A30, 90C35*

1. Introduction

The recent trend of research in the area of information security is ever more shifting to the field of information awareness management in conflict systems. This trend is quite reasonable. Vulnerabilities are not embedded deliberately in an information security system (except the cases when a defender is interested in). Inevitable presence of vulnerabilities is caused by the complexity of current information systems. It was discovered that successful attacks become more simple with the increasing complexity of a system. This law-like regularity was called "The Adam And Eve Paradox" [1]. Information asymmetry between attacker and defender is a significant restriction in the area of security. This is when a defender's time to develop the system is limited while an attacker`s is normally not. Furthermore an attacker has access to information about the software vulnerabilities and shortcomings which are found after the system development process has been completed.

Recently there appeared a lot of researches dedicated to overcoming this asymmetry. The majority of them address to protection technologies based on Moving Target Defense (MTD). The principle of this technology consists in transforming the system from a static type to a dynamic one [2, 3]. Temporarily changing its structure an information system makes the research process difficult for an attacker. Information obtained in the process of reconnaissance becomes irrelevant the next moment.

The first research works in this area appeared about five years ago. At the same time one can observe the significant increase in a number of research papers in this field within the last couple of years. There were proposed such solutions as defense of networks from remote scanning [4, 5], defense from DDoS-attacks [6], virtualization technologies protected from research [7], etc. Some solutions based on MTD were accepted as standards in the area of software development, e.g. Address-Space Layout Randomization (ASLR) [8], which has been used in all common operating systems over the last couple of years.

However, formalization of processes for obtaining information while interacting with the system (i.e. information about the system itself) can be considered as a constraining factor to extend the research in this area. Thus, we cannot define precisely which particular elements of an information system need to be hidden and how to hide them; what information will be revealed to an intruder in the process of interaction with the system; if a defender can be sure that the system is adequate enough to declare security; how agents can hide their actions in the system and how to oppose it, etc.

These have undoubtedly been the most frequent causes of concern in researches that have been carried out for formalizing the general problem of protection against reconnaissance [9], formalizing the process for information flow analysis with graphs [10], proposing an algorithm to design self-complicating systems [11]. In this paper we formalize the notion of action taking into account shifts in the agent`s awareness and structure two problems of protection from research on the model designed. The first problem deals with restrictions for agents to achieve specific conditions due to their awareness, the second one concerns hiding agents` actions in the system. The scope of functional steganography is defined in a similar way to classic (content) steganography.

2. Construction of a functional model

In this section we present mathematical notions and illustrate their interpretations in terms of real objects. This method allows one to understand the formalized model more clearly.

Consider the set $T = \{T^1, \dots, T^m\}$ of vectors

$$T^i = (a_1^i, \dots, a_n^i)^T, \quad i = 1, \dots, m, \quad a_j^i \in A_j,$$

where each A_j is a finite subset of a set of positive integers $\mathbb{N} = \{1, 2, \dots\}$, consisting of n_j elements $\left(\| A_j \| = n_j \right)$.

Definition 2.1: We call the vectors T^i by states, and the set T by set of states.

Interpretation: The state of any real system can be represented by means of its elements' states. E.g., a system with distribution of users rights to access can be described by means of such entities as roles, which states are sets of access rights; files with discrete set of their content; users with the states of their roles, etc.

Let I_K be a vector of length n, consisting of s zeros and $n - s$ "ones", namely

$$I_K = I_{(k_1,\dots,k_s)} = (1,\dots,1,\overset{k_1}{0},1,\dots,1,\overset{k_s}{0},1,\dots,1)^T \in (\{0,1\})^n,$$

where the zeroes are in positions with numbers $k_1,\dots,k_s$ with $1\leqslant k_1 < \dots < k_s \leqslant n$. Let $I_{\overline{K}}$ be a vector $I_{\overline{K}} = I_n - I_K$, where $I_n = (1, ..., 1)$ is the unit vector of the length n.

By T_K^i we denote a vector $T^i * I_K$, where operation $*$ means termwise multiplication of vector elements:

$$(a_1,\dots,a_n)^T * (b_1,\dots,b_n)^T = (a_1b_1,\dots,a_nb_n)^T.$$

Thus vector T_K^i is obtained from vector T^i by substituting coordinates with numbers $k_1, ..., k_s$ into zeros.

Definition 2.2: We say that the states T^i and T^j from T are K-equivalent and denote $T^i \overset{K}{\sim} T^j$, if $T^i * I_K = T^j * I_K$.

Interpretation: Within any real system some elements stay indiscernible. It can be either the whole element or some of the element's states. Hence an agent might not notice system transformation from one state to another. Thus two states stay equivalent for a particular individual. E.g., modifying the contents of a file, which is not accessible for the individual.

Let $M = \{1,\dots,m\}$, and $M_{\neq}^2 = \{(i,j) : i,j \in M, i \neq j\}$ be a set of ordered pairs of elements from M with distinct coordinates.

Definition 2.3: Denote the ordered pair (T^i, T^j) by F^{ij}, where $(i,j) \in M_{\neq}^2$. We say that F^{ij} defines transformation from the state T^i into the state T^j and denote it by $F^{ij} : T^i \to T^j$. Define composition of transformations $F^{ij} \circ F^{jk}$ by $F^{ij} \circ F^{jk} = F^{ik}$.

It is convenient to represent a set of states with a specified set of transformations with a directed graph. Its vertices correspond to states and its edges correspond to transformations between states.

Definition 2.4: We say that the transformation F^{ij} is K-enabled, if the states T^i and T^j are not K-equivalent, but they are $\overline{K}$-equivalent, i.e. $T^i * I_K \neq T^j * I_K$ and $T^i * I_{\overline{K}} = T^j * I_{\overline{K}}$ hold.

Definition 2.5: If B is a subset of $M_{\neq}^{2}$, we denote the set

$$F_K^B = \left(\{F^{ij} : (i,j) \in B, F^{ij} \text{ — } K - \text{enabled}\}, \overset{K}{\sim} \right)$$

by F_K^B and call it by the *set of the agent B-K*.

Interpretation: Any action within a system can be denoted by transformation of its elements' states. An individual cannot observe some states of the elements, so he/she cannot make a shift, modifying the system elements. This claim contradicts classical idea in the area of information security because of "blind" attacks. One should be more careful when using the term "observability" referring to protection against reconnaissance. E.g., if an attacker has write access to a file, but no read permission, he might get indirect channel of leakage in time. While putting data he/she checks whether errors occur in the program or whether it requires more time to run. A significant number of blind injection attacks to brake codes and ciphers are performed using this approach. If the state of an object is not observable at all, it can be used in future to produce other actions, that will provide information whether it has been transformed to a target state or not. Thus we cannot consider the situation when an individual produces any actions with absolutely unobservable elements.

Definition 2.6: We say that the state $T^q \in T$ is *B*-*K*-attainable for the state $T^p \in T$, if there exists sequence $F^{pi_1}, F^{i_1 i_2}, \ldots, F^{i_r q}$ of F_K^B such that

$$F^{pi_1} \circ F^{i_1 i_2} \circ \ldots \circ F^{i_r q} = F^{pq} : T^p \to T^q .$$

Let $F = \left\{ F_{K_1}^{B_1}, \ldots, F_{K_l}^{B_l} \right\}$ be a collection of agents' sets.

Definition 2.7: We say that the state $T^q \in T$ is *F*-attainable for the state $T^p \in T$, and denote $T^p \xrightarrow{F} T^q$, if there exists sequence of states $T^p = T^{p_0}, T^{p_1}, \ldots, T^{p_r} = T^q$ from *T* such that for any $i \in \{1, \ldots, r\}$ there exists $j \in \{1, \ldots, l\}$ such that the state T^{p_i} is B_j-K_j-attainable for the state $T^{p_{i-1}}$.

Let $T^0 \in T$ be an initial state, and T^N be a certain subset of *T* called *undesirable set of states*.

Definition 2.8: For certain *T*, $T^0 \in T$ and *F* by attainability set we call the set of *F*-attainable states for T^0:

$$T^A = \{T^q : T^q \in T, T^q\, F - \text{attainable for } T^0\}.$$

Definition 2.9: We call the collection $\langle T, T^0, T^N, F\rangle$ by investigated system.

Definition 2.10: By investigated system graph we call directed graph with the set of vertices corresponding to the set of system states and with the set of edges corresponding to the set of all transformations, that are *K*-enabled for at least one agent in a system.

Denote:

$$\| \langle T, T^0, T^N, F\rangle \| = \begin{cases} 0, T^A \cap T^N = \varnothing, \\ 1, T^A \cap T^N \neq \varnothing. \end{cases}$$

Interpretation: For a certain system a set of undesirable states could be a set of states with unauthorized access to resources or denial-of-service states. By identifying all the actions in the system, we are able to define weather it can transform to undesirable state, e.g. due to security policy violation.

For such investigated system we can describe the following "protection against reconnaissance" tasks.

Task 1: Which conditions applied to investigated system provide the equality $\| \langle T, T^0, T^N, F\rangle \| = 0$?

Task 2: If for the given investigated system $\| \langle T, T^0, T^N, F\rangle \| = 1$, how can we get $\| \langle T, T^0, T^N, F\rangle \| = 0$ by modifying equivalence relations (and, therefore, agents sets)?

Task 3: Under which conditions applied to investigated system, the problem of matching of the given transformation in a system to a certain agent's action is intractable (computationally complex) or unfeasible when we are limited by the equivalence relations of certain agents?

3. Formalization of the first task

Consider the system with one agent:

$$\left\langle T, T^0, T^N, \left\{F_{K_1}^{B_1}\right\}\right\rangle$$

Theorem 3.1: *If* $\forall T^j \in T^N : T^j \overset{\overline{K_1}}{\nsim} T^0$ *then* $\left\|\left\langle T, T^0, T^N, \left\{F_{K_1}^{B_1}\right\}\right\rangle\right\| = 0.$

Proof: The proof follows from the fact that any attainable state $T^i \in T^A$ satisfies $T^j \overset{\overline{K_1}}{\sim} T^0$.

Theorem 3.1 might be interpreted as follows: if for any undesirable state there exists attainable state, indiscernible for the only agent, then the system will never transform into this state, given that indiscernible elements were not initially in undesirable state.

Similarly one can consider the system with more than one agent (several agents):

$$\langle T, T^0, T^N, F\rangle,\ F = \left\{F_{K_1}^{B_1}, \ldots, F_{K_l}^{B_l}\right\}.$$

Theorem 3.2: *If* $\forall T^j \in T^N : T^j \overset{\overline{K}}{\nsim} T^0$ *where* $\overline{K} = \overline{K_1} * \ldots * \overline{K_l}$, *then* $\left\|\left\langle T, T^0, T^N, \left\{F_{K_1}^{B_1}\right\}\right\rangle\right\| = 0.$

Proof: The proof is similar to the proof of Theorem 3.1, taking into account that none of the agents can change the element from the subset of indiscernible for any agent elements at any stage (i.e. coordinates corresponding to "1" coordinates of the vector $\overline{K} = \overline{K_1} * \ldots * \overline{K_l}$).

Let us now introduce the notion of reduced graph to simplify operating with graphs.

Definition 3.1: Let us call an island a set of system states, each of which is *F*-attainable for the others. We will use the notion of reduced graph to denote a graph of the system in which each island is identified with a vertex, and each edge, coming in- or out of any state of the island, accordingly, comes in- or out of the vertex, corresponding to this island.

Denote by O a collection of all islands in the system. Now we are able to construct a graph O_G which vertices are elements of the set O and the transition from O_a to O_b exists if, and only if there exists transition $F^i j$ such that $T^i \in O_a$, and $T^j \in O_b$.

Theorem 3.3: *If $T^0 \in O_g T^N \in O_h$, where O_g and O_h are vertices of the reduced graph of the system, denoting the islands of the system, then $\left\|\left\langle T, T^0, T^N, \left\{F_{K_1}^{B_1}\right\}\right\rangle\right\| = 1$ if and only if there exist a path from O_g to O_h in the graph O_G.*

Let us consider an example. There are 4 modules within a system. These modules interact with each other. Let us denote only two states for each module: "0" means that module is not compromised and "1" means that module is compromised. Thus, vector (x_1, x_2, x_3, x_4), where $x_i \in \{0,1\}$ identifies the state of the system. Suppose that attacker has an access to the first module and he can further compromise it sequentially as he knows the rules of their interacting. Thus we can mark down all F-attainable actions in the system. Let us suppose that compromising of the last module is an undesirable state of the system. Thus, Theorems 3.1 and 3.2 postulate that it is possible to make the system safe by making this state indiscernible for an attacker and defining the vector $I = (*, *, *, 0)$, if the initial state of the system is $T^0 = (*, *, *, 0)$.

However it can be unfeasible to make the fourth element of the system indiscernible. Then, in accordance with the Theorem 3.3 we can build a graph of islands and protect from research crucial elements which break graph paths.

4. Formalization of the second task

If, in a real system, we obtain $\left\|\left\langle T, T^0, T^N, \left\{F_{K_1}^{B_1}\right\}\right\rangle\right\| = 1,$ we can transform it to the state $\left\|\left\langle T, T^0, T^N, \left\{F_{K_1}^{B_1}\right\}\right\rangle\right\| = 0$ by means of changing the vector I_K. To make some system elements undesirable for the agent we replace one with zero in the vector I_K at the corresponding position.

For the vector

$$I_K = I_{(k_1,\ldots,k_s)} = (1,\ldots,1,\overset{k_1}{0},1,\ldots,1,\overset{k_s}{0},1,\ldots,1)^T \in (\{0,1\})^n,$$

let us denote K_0 as a set

$$K_0 = \{k_1,\ldots,k_s\}$$

of zero coordinates places in the vector I_K. Consider the family of the sets K':

$$K' = K_0 \cup A \text{ where } A \text{ — non-empty subset } \overline{K_0} = \{1,\ldots,n\} \setminus K_0.$$

Thus, vector $I_{K'}$ is a vector I_K which has all zero coordinates of the vector I_K and some "1" coordinates of the vector I_K are replaced with zeros. Each vector $I_{K'}$ defines its equivalence relation $\overset{K}{\sim}$.

Let us assign a nonnegative real number $a \geqslant 0$ to each set A. We will call this number by weight transformation coefficient.

For each agent the set $M_{\neq}^2$ is permanent, and the sets of B'-enabled transformations (subsets of $M_{\neq}^2$) will change with K' so that sets $F_{K'}^{B'}$ will be the subsets of F_K^B.

Let us formulate the optimization problem.

Given the family of agents' sets $F = \left\{ F_{K_1}^{B_1},\ldots,F_{K_l}^{B_l} \right\}$ with $\| \langle T, T^0, T^N, F \rangle \| = 1$ it is required to find a family of sets $A_{F'} = \{A_1,\ldots,A_l\}$ with minimal weight $a_{F'} = a_1 + \ldots + a_l$ so that $\| \langle T, T^0, T^N, F' \rangle \| = 0,$ where $F' = \left\{ F_{K_1'}^{B_1'},\ldots,F_{K_l'}^{B_l'} \right\}$. In other words we should find

$$a_{\min}(F') = \min_{F' : \| \langle T, T^0, T^N, F' \rangle \| = 0} a_{F'}.$$

When transforming the states of real systems to the T set the main problem is to find independent elements being components of the vector $T^i = (a_1^i,\ldots,a_n^i)^T$. Independence is the absence of changes in one element's state with changing the state of the others. E.g., the state of the web-server will depend on the state of the virtual machine it is placed in. However, two virtual machines on the same computer are most likely to be independent.

In real systems indiscernibility of states can be achieved in several ways:

1. Restriction of access to an element by making it unobservable. It is the most obvious and simple way but certainly it is not always practicable for different parts of the system interact with each other and may not be isolated at all times. Unobservability makes an element isolated.
2. Changing an element's conception quicker than the time required for the response from the element to an agent. Reconnaissance and recognition of elements' states requires some time. For example the time for remote scanning of hosts in a network or read time of connection parameters within one session. When elements are turned into constantly changing ones then obtaining a correct image of a system or its elements may be impracticable. That solution is more realistic to implement from the technical point of view and was referred to as MTD technology in the introduction. The drawback of such systems lies in the inability to defend the MTD itself from research as it remains stereotypic. One of the options to solve that problem is a decentralized self-complicating information system in modification principles of which are not programmed during the design stage [14].
3. Setting up a functional "disguise" and making the system's functional element indiscernible. In that case it becomes unclear what each element actually is (solution to the second task). Hence, as it is impossible to distribute elements of set T correctly those elements become indiscernible. One of the innovative ways to solve that problem is set out as an example of establishing an absolutely indiscernible data transfer channel [15].

5. Formalization of the third task

There are two fundamental approaches to data hiding in the area of cryptography. The first approach uses perfect ciphers. Ciphertext is literally meaningless for a cryptanalyst as it does not provide any information about the original message. The second approach is based on hypothesis that attacker can use only polynomial time algorithms. Thus there is a class of hardly compromised cryptographic primitives. The complexity of their compromising increases very fast (non polynomial) depending on some parameters (generally, key size). Within this paper we will consider data hiding in terms of computation complexity and elements indiscernibility for agents.

The first part of the problem consists in possibility to compare transition in a system with the action of an agent in condition of complete information about the system. Let us consider a system with three agents and an action F^{14}. Action F^{14} does not belong to any set of agents' actions. But after transition in a system action F^{14} may be represented as a composition of agents' actions. Let us suppose,

$$F^{14} = F^{12} \circ F^{23} \circ F^{34}, F^{12} \in F_{K_1}^{B_1}, F^{23} \in F_{K_2}^{B_2}, F^{34} \in F_{K_3}^{B_3}.$$

Definition 5.1: Trivial action is an action that could not be represented as a composition of other actions which do not contain the action itself.

Definition 5.2: A simple composition is a representation of action that could not be denoted with the smaller number of elements. I.e., if there exists representation $F^{14} = F^{15} \circ F^{54}$, then $F^{14} = F^{12} \circ F^{23} \circ F^{34}$ is not simple.

Suppose in our case representation $F^{14} = F^{12} \circ F^{23} \circ F^{34}$ is simple. We can conclude that system transformation F can be performed only with collaborative actions of agents 1, 2 and 3. However, it is not so, as each of these actions can be non trivial. Let us show the whole composition of actions (Figure 1).

Each action is marked with the number of agents composing the set of actions it belongs to.

Thus, action F^{12} may be represented as a composition $F^{15} \circ F^{52}$, where $F^{15} \in F_{K_2}^{B_2}, F^{52} \in F_{K_1}^{B_1}$. In its turn, action F^{15} may be represented as a composition $F^{17} \circ F^{75}$, where $F^{17} \in F_{K_1}^{B_1} F^{17} \in F_{K_2}^{B_2}, F^{75} \in F_{K_1}^{B_1}$.

As a result, we can represent action F^{14} as composition:

$$F^{14} = ((F^{17} \circ F^{75}) \circ F^{52}) \circ (((F^{29} \circ F^{98}) \circ F^{86}) \circ F^{63}) \circ F^{34}.$$

Each action in this composition is an element of the set $F_{K_1}^{B_1}$. Consequently, agent 1 can perform transformation F^{14} independently.

$$\begin{tikzcd}
 & & F^{14} = \overset{3}{\overline{F}}{}^{12} \circ \overset{2}{\overline{F}}{}^{23} \circ \overset{1}{\overline{F}}{}^{34} \arrow[dl] \arrow[dr] & & \\
 & \overset{2}{\overline{F}}{}^{15} \circ \overset{1}{\overline{F}}{}^{52} \arrow[dl] & & \overset{2}{\overline{F}}{}^{26} \circ \overset{1}{\overline{F}}{}^{63} \arrow[dr] & \\
\overset{1,\,2}{\overline{F}}{}^{17} \circ \overset{1}{\overline{F}}{}^{75} & & & & \overset{2}{\overline{F}}{}^{28} \circ \overset{1}{\overline{F}}{}^{86} \arrow[dl] \\
 & & & \overset{1}{\overline{F}}{}^{29} \circ \overset{1}{\overline{F}}{}^{98} &
\end{tikzcd}$$

Figure 1

Decomposition of a simple chain of nontrivial actions

Analyzing real systems, when we see the transition, we generally, compare it with the simplest composition. However, it could be considered incorrect in terms of digital forensics. In this case there occurs an important question whether a single agent or a group of agents could perform this action or not.

If each element of a system has more than one state, that is, $\| A_i \| = n_i \geqslant 2$ for each $i = 1, \ldots, k.$ such system can be called nondegenerate

Theorem 5.1: *Complexity of the task to attain the state of nondegenerate system increases exponentially with the number of system elements.*

Proof: Note that the number N of vectors $(a_1, \ldots, a_k)$ of the length k, where $a_i \in A_i, \| A_i \| = n_i \geqslant 2,$ can be estimated by

$$N = n_1 \cdot \ldots \cdot n_k \geqslant 2^k.$$

Thus, since complexity to find connected vertices is defined by the number of graph's vertices, complexity to define elements attainability will be not less than $O(2^k)$.

The third task may be specified as follows. Suppose there occurred transformation from state T_0 to $T' \in T_N$. We need to find all the paths executing this transformation. Solution of this task allows us to define whether the given transformation is performed by the single system agent or not.

This task can be solved by considering the graph with edges which correspond to the only agent with traditional algorithms of graph-based pathfinding. If transformation is not attainable for each separate agent (without collaboration) we can start a new task of state attainability by the pair of agents, etc.

Theorem 5.2: *If there exists system with N states and t agents, then complexity of the task whether j* $\in (1, \ldots, t)$ *of agents* $F_{K_S}^{B_S} = \left\{ F_{K_{s_1}}^{B_{s_1}}, \ldots, F_{K_{s_j}}^{B_{s_j}} \right\}$ *can perform transformation from state* T^0 *to* $T' \in T^N$ *in cooperation, is* $O\left(N \cdot C_t^j + \sum_S \| F_{K_S}^{B_S} \| \right)$, *where the sum is taken over all j-element sampling* $s_1, \ldots, s_j$, *and* $\| F_{K_S}^{B_S} \|$ *denotes the number of elements in the set of enabled actions for agents* $F_{K_{s_1}}^{B_{s_1}}, \ldots, F_{K_{s_j}}^{B_{s_j}}$, *and* $C_t^j = t! / (j!(t-j)!)$ *are binomial coefficients.*

Proof: There exists a graph for each sampling of *j*-elements set from *t*-elements set, so the complexity of pathfinding algorithm in the oriented graph between two fixed vertices equals the sum of the number of vertices and the number of edges.

The top value of this computation complexity can be obviously estimated with the variable

$$O\left(\left(N + \max_S \| F_{K_S}^{B_S} \| \right) \cdot C_t^j \right).$$

As a result we can conclude that the problem to compare transformations in a system with the agents' actions may be computationally complex even when we have all the information about the system and its agents. It allows agents perform "hiding" actions in the systems with the large number of elements.

The second part of the task is defined as infeasibility to compare transformation with the specified agents' actions if we are limited with equivalence relation of some agents. In other words a researcher is placed "inside" the system and, as an agent, tries to recognize an agent or a group of agents changing the state of the system. This task is always solvable if he is equipped with complete information and has unrestricted computational resources. However, the task can have no solutions from the agents 'point of view as some system elements are indiscernible. I.e., transformation in a system performed by specific agents with functional decomposition can be unobservable.

As a result the system can suddenly appear to be transformed to a new state for some agents. The most suitable notion to denote this problem is "functional steganography".

Definition 5.3: We will call actions F^{jk} and F^{st} *K*-equivalent $(F^{ij} \overset{K}{\sim} F^{pq})$ if $T^i \overset{K}{\sim} T^j$ and $T^p \overset{K}{\sim} T^q$.

Definition 5.4: Functional steganography subset for the *B*-*K* agent is a set of actions $F_K^{B(\mathrm{st})} \subset F_K^B$, so that for each action $F^{ij} \in F_K^{B(\mathrm{st})}$ and each agent *B′*-*K′* from $F \setminus F_K^B$ there exists action F^{pq} so that $F^{ij} \overset{K'}{\sim} F^{pq}$ and

$$F^{pq} \in F \setminus \left(F_K^B \setminus \big(\bigcup_{\substack{B' \neq B \\ K' \neq K}} F_{K'}^{B'} \big) \right).$$

The scope of functional steganography consists in finding transitions in a system represented as functional decomposition of an agent's actions, indiscernible by other agents.

Some practical tasks can be solved with the help of such subsets. E.g., hiding actions of security administrator in information system. The following conclusion can be useful for this task:

Corollary 5.1: *If one of the agents in a system has access to all system elements and the set of non empty indiscernible actions is available to other agents, then functional steganography subset for this agent is never empty.*

This approach can be implemented in policies of access control. E.g., discretionary access control where all object are independent a priori (like a HRU security model). In this case, indiscernibility can be considered as absence of read permission in the access matrix.

An action F^{ij} of agent *B*-*K* is *absolutely indiscernible* (indiscernible for all other agents) if for each agent *B′*-*K′* from $F \setminus F_K^B$ there exists action F^{pq}, so that $F^{ij} \overset{K'}{\sim} F^{pq}$ and $F^{pq} \notin F_K^B$ (i.e., no other system agent can identify this action as an action of agent *B*-*K*).

As a result, reasoning by analogy with cryptography, we could define absolutely indiscernible agents' actions in a system and indiscernible agents' actions based on computing complexity of pathfinding in graphs, growing very fast (non polynomial) depending on the number of system elements.

6. Conclusion

The present paper resolved the problem of interdependence between awareness and agents' actions into a formalized model. The model enables defining attainability of undesirable states in the system from one agent's point of view. Methods provided herein can be used to develop system topology in accordance with Moving Target Defense which is currently widely applied in information security solutions. It can assist in establishing the systems protected from penetration or promote solving the task of functional indiscernibility in system dynamics and hiding agents' actions in the system (functional steganography).

Acknowledgement

The current research was supported by the grant from the Russian Foundation for Basic Research (project 16-29-09456-ofi_m, the first author) and by the grant from the President of the Russian Federation for young scientists, (project MD-197.2017.1, the second author).

References

[1] M. Kraft, D. Rohret, M. Vella and J. Holston, The adam and eve paradox. *8th International Conference on Information Warfare and Security*, 2013. pp. 275–283.

[2] Jajodia et al, Moving Target Defense. Creating Asymmetric Uncertainty for Cyber Threats. *Series: Advances in Information Security.* London: Springer, 2011.

[3] Jajodia et al, Moving Target Defense II. Application of Game Theory and Adversarial Modeling. *Series: Advances in Information Security.* London: Springer, 2013.

[4] M. Carvalho, R. Ford, Moving-target defenses for computer networks. *IEEE Security and Privacy*, Vol 12 (2014), pp. 73–76.

[5] G.D. JafarHaadiJafarian, E. Al-Shaer, Openflow random host mutation: Transparent moving target defense using software-defined networking. *Proceedings of the 1st Workshop on Hot Topics in Software Defined Networking (HotSDN)*, 2012. pp. 127–132.

[6] J. Quan, A. Stavrou, MOTAG: Moving Target Defense against Internet Denial of Service Attacks. *Proceedings of Computer Communications and Networks (ICCCN 2013)*, 2013. pp. 1–9.

[7] A. Paulos et al, Moving target defense (MTD) in an adaptive execution environment. *8th Annual Cyber Security and Information Intelligence Research Workshop: Federal Cyber Security R and D Program Thrusts, CSIIRW 2013*, 2013. pp. 39–47.

[8] J. Li, R. Sekar, Address-space randomization for windows systems. *Preceedings of 2006 Annual Computer Security Applications Conference (ACSAC)*, 2006. pp. 34–46.

[9] M. Styugin, Protection against system research. *Cybernetics and Systems*, Vol. 45 (2014), pp. 362–372.

[10] M. Styugin, Protection Systems against Unauthorized Access by Modifying the Structures Awareness Subjects (in Russian). *Bezopasnost Informatsionnykh Tekhnology*, Vol. 4 (2014), pp. 105–111.

[11] M. Styugin, The New Method of Security Development for Web Services Based on Moving Target Defense (MTD) Technologies. *Proceedings of the International Conference on Network Security and Communication Engineering (NSCE2014)*, 2014. pp. 130–136.

[12] V. Lefebvre, The Structure of Awareness. Beverly Hills: Sage, 1977.

[13] D. Novikov, A. Chkhartishvili, Reflexion and Control: Mathematical Models. London: CRC Press, 2014.

[14] M. Styugin, N. Parotkin, Multilevel Decentralized Protection Scheme Based on Moving Targets *International Journal of Security and Its Applications*, Vol. 10 (2016), pp.45–54.

[15] M. Styugin, Absolutely Indiscernible Data Transfer Channel *Proceedings of The 14th European Conference on Cyber Warfare and Security*, 2015. pp. 34–46.

Received February, 2016