Journal of Computing and Information Technology - CIT 22, 2014, 3, 145–150
doi:10.2498/cit.1002388


# Application of Case-based Methodology for Early Diagnosis of Computer Attacks

Gulnara Yakhyaeva and Olga Yasinskaya

Department of Information Technologies, Novosibirsk State University, Russia

In this article we consider the mathematical foundations and software implementation of the early diagnosis of computer attacks. For this we used the JSM method of automatic hypothesis generation and the theory of case-based models.

This software outputs hypotheses about the properties and expected consequences of a new computer attack. The system analyses a set of properties of the computer attack known to the user. For this we use the Base of the cyber attack's precedents, described in the language of fuzzification of Boolean-valued models. Each potential property of the new attack is studied by using the JSM method. This process builds sets of positive and negative hypotheses concerning each property, giving a set of properties and consequences characteristic of the attack that has yet not happened at the time of analysis.

The developed algorithm has polynomial complexity.

*Keywords:* information security, computer attack, case of the computer attack, case-based model, fuzzification of the case-based model, JSM-method, JSM-reasoning

## 1. Introduction

Technology helps improve communication by allowing easy, rapid exchange of information. However, the convenience of digital networks has a downside. As enterprises use computers and digital networks more and more, cyber crimes can do greater damage. Every day almost 200,000 pieces of malicious code infect 150,000 computers in corporate and state networks. According to the Internet Crime Complaint Center (IC3), cyber crimes caused losses in the United States of more than $550 million in 2009, almost twice as much as in the previous year.

Every year the number of detected cyber crimes worldwide increases dramatically. Russia and the U.S. are the largest malware contributors. A useful analysis of cyber crimes is the 2013 Data Breach Investigations Report released by the Verizon Enterprise risk team. This report combines the expertise of 19 organizations worldwide and covers more than 47,000 incidents, among which there were 621 confirmed data disclosures [1].

Because of these risks, companies must consider and implement well-developed information security systems, which are becoming one of the most important conditions to remain competitive and even viable. One of the most promising developments in this area is modeling information security by using ontologies as specifications of a given subject domain [2, 3].

Using this methodology, a team at Novosibirsk State University developed the RiskPanel software system [4], a workplace for experts to ensure corporate information security. This software system aims at implementing risk management in information security.

RiskPanel has a modular structure, allowing for new functionality to be added. This article describes a module that diagnoses computer attacks and provides risk management during the initial attack.

## 2. Mathematical Foundations of the Developed Approach

### 2.1. Case-based Models

The principal difference between the mathematical foundations of the proposed approach [5–7] and traditional methods of information-risk assessment is that in this approach we do not work with numerical estimates of risk probabilities, but instead with sets of cases on which these risks have worked. In the standard approach, information is first digitized (or fuzzificated) and then processed. Under the proposed approach, all available information, including the description of the domain ontology and empirical data, is first processed and then fuzzificated (converted to numbers in the interval [0, 1]). The proposed approach allows one to work with relevant data not yet distorted by digitization during all stages of information processing.

We will describe each case of computer attack by the algebraic system $\mathcal{U} = \langle A, \sigma \rangle$, where $A$ is the universe of the algebraic system, and $\sigma$ is its signature. Signature $\sigma$ is a set of concepts that describe the subject domain: the vulnerabilities, threats, countermeasures, consequences, and so on. We assume that all the cases of computer attacks have the same signature. For example, set $A$ and signature $\sigma$ would be denoted as $\sigma_A = \sigma \cup \{c_a | a \in A\}$. The algebraic systems by which we describe instances of the domain belong to the following class

$$\mathbf{K}(\sigma_A) = \{\mathcal{U} = \langle \{c_a^{\mathcal{U}} | a \in A\}, \sigma_A \rangle \, | c_a^{\mathcal{U}} \neq c_b^{\mathcal{U}} \text{ if } a \neq b\}.$$

Let $\mathcal{P}(X)$ denote the set of all subsets of $X$. Let $S(\sigma_A)$ denote the set of all sentences of the signature $\sigma_A$.

The algebraic system $A$, the model of some computer attack, is called the *case* of the considered subject domain. For each set of cases $E$ we define a case system $\mathcal{U}_E$.

***Definition 1.*** Let $E \subseteq \mathbf{K}(\sigma_A)$ be a set of cases. The algebraic system $\mathcal{U}_E = \langle A, \sigma, \tau_E \rangle$, where $\tau_E : S(\sigma_A) \to \mathcal{P}(E)$, is called a *case-based system* (generated by set $E$). $\tau_E(\varphi) = \{\mathcal{U} \in E | \mathcal{U} \models \varphi\}$ for any sentence $\varphi$ of signature $\sigma_A$.

Most techniques for information risk-management use objective and/or subjective probabilities to eliminate risks [8]. The *objective probability* is the relative frequency of an event occurring over total observations or the ratio of favorable outcomes to the total observations. The *subjective probability* (or Bayesian probability) is a measure of sureness of an expert or group of experts that an event will occur. Contrasting objective probability, the Bayesian probability is a quantity that we interpret as a state of knowledge [9] or a state of belief [10].

The approach developed in this paper also uses objective and subjective probability to identify and evaluate risks. In our case, the objective probability is a function of the truth $\mu(\varphi)$ in the fuzzy model $\mathcal{U}_\mu$ (defined below), and the subjective probability is an estimation made by an expert. The approach compares the subjective knowledge of the expert to objective reality. If it does not exist, or if the expert knowledge is inconsistent, we forecast the consequences of the new computer attack.

### 2.2. Definition of the Problem Involving Early Diagnosis of Computer Attacks

Let the object domain knowledge be formalized in the form of the case-based model $\mathcal{U}_E$ defined by the signature $\sigma_A$. This model is a mathematical formalization of the knowledge base of computer-attack cases. To calculate the objective probabilities of the origins of different computer attacks, we define the notion of case-based model fuzzification.

***Definition 2.*** Model $\mathcal{U}_\mu = \langle A, \sigma_A, \mu \rangle$ is called *fuzzification* of the case-based model $\mathcal{U}_E$ (denoted $\mathcal{U}_\mu = Fuz(\mathcal{U}_E)$) if $\mu(\varphi) = \dfrac{\|\tau_E(\varphi)\|}{\|E\|}$ for any sentence $\varphi$ of signature $\sigma_A$. Let $\mathcal{U}_\mu \models_\alpha \varphi$ if $\mu(\varphi) = \alpha$.

Model $\mathcal{U}_\mu = Fuz(\mathcal{U}_E)$ gives us objective probabilistic estimates of events in this object domain. Consider the case of a new computer attack formalized by some model $\mathcal{N} \in \mathbf{K}(\sigma_A)$. The elementary diagram $\mathcal{D} = \{\varphi \in S_a(\sigma_A) | \mathcal{N} \models \varphi\}$ of this model is unknown. However we know some subset $S_\mathcal{N} \subseteq \mathcal{D}$ of this diagram. We must determine whether some sentence $\psi \in S_a(\sigma_A)\S_\mathcal{N}$ is true in model $\mathcal{N}$: in other words, does it belong to the elementary diagram $\mathcal{D}$?

### 2.3. JSM Method in the Language of Case-based Models

To answer the question posed at the end of the last section, we will use the JSM method of automatic hypothesis generation [11, 12].

The JSM method originated from the attempts to formalize John Stuart Mill's inductive logic by using the multi-valued logic of predicates. The JSM method is a theory of automated reasoning and a method for knowledge representation when solving forecasting problems in situations with incomplete information.

However it is difficult to describe the JSM method in the language of multi-valued logics for implementation in an algorithm so different formalisms are commonly used for computer implementation. The best known formalism used to effectively implement an algorithmic JSM method is Galois correspondences and formal concept analysis [13].

First, let us formally describe the JSM method of automatic hypothesis generation in the language of case-based models. This method has two stages: In the first stage the sets of atomic sentences which in principle can be prerequisites for the truth/falsehood of sentence $\psi$, are found by analyzing the known subject domain knowledge. (Traditionally such sets are called positive and negative hypotheses.)

In the second stage each of the resulting hypotheses is checked for compatibility with a set $S_{\mathcal{N}}$. Then the final answer to the posed question is given. (This procedure can be called rules for plausible reasoning.)

Note that a final (positive or negative) answer is not always possible. For example, there might be insufficient information to make a decision, such as when the set $S_{\mathcal{N}}$ is too small or one's knowledge of the subject domain (model $\mathcal{U}_E$) is inadequate. Inconsistent information can also complicate decision-making, in which case the inconsistent information would have to be filtered.

So, let the knowledge of the subject domain of information security be formalized as a case-based model $\mathcal{U}_E$ of a signature $\sigma_A$. Knowledge of the new attack is formalized in a set of sentences $S_{\mathcal{N}} \subseteq S_a(\sigma_A)$ of the same signature.

***Definition 3.*** Consider fuzzification $\mathcal{U}_\mu = Fuz(\mathcal{U}_E)$. The sentence $\varphi \in S(\sigma_A)$ is called the *concept of model* $\mathcal{U}_\mu$ if

1. $\varphi = \varphi_1 \& \varphi_2 \& \ldots \& \varphi_n$ where $\varphi_1, \ldots, \varphi_n \in S_a(\sigma_A)$;
2. $\mu(\varphi) > \mu(\varphi \& \xi)$ for any $\xi \in S_a(\sigma_A) \setminus \{\varphi_1, \ldots, \varphi_n\}$.

***Definition 4.*** Formula $\varphi$ is called a *positive hypothesis* in relation to property $\psi$ in model $\mathcal{U}_\mu$ if

1. $\varphi \& \psi$ – concept of model $\mathcal{U}_\mu$
2. $\mu(\varphi) = \mu(\varphi \& \psi)$.

***Definition 5.*** Formula $\varphi$ is called a *negative hypothesis* in relation to property $\psi$ in model $\mathcal{U}_\mu$ if

1. $\varphi \& \neg\psi$ – concept of model $\mathcal{U}_\mu$
2. $\mu(\varphi) = \mu(\varphi \& \neg\psi)$.

Thus, we understand the positive hypothesis as the maximum property set of computer attacks that are executed for some attacks during which property $\psi$ is executed, and are not executed on all attacks during which property $\psi$ is not executed. The negative hypothesis is defined similarly.

In practice, it is often difficult to define the threshold number of cases in which the positive or negative hypothesis must be performed for it to be considered informative [14]. To solve this problem, we can use the ratio of truth degrees of appropriate sentences $\dfrac{\mu(\varphi)}{\mu(\psi)}$ or $\dfrac{\mu(\varphi)}{\mu(\neg\psi)}$ as a metric, which allows us to quantify the informativeness of the positive and negative hypotheses.

Let us denote $\Gamma_+(\psi)$ and $\Gamma_-(\psi)$ for sets of all positive/negative hypotheses in relation to the property $\psi$ in model $\mathcal{U}_\mu$. Then, we check each hypothesis for compatibility with known information about the new attack.

**Rules for plausible reasoning:**

1. $\mathcal{N} \models \psi$ if and only if
   a) $\exists \varphi \in \Gamma_+(\psi) : \mathcal{N} \models \varphi$;
   b) $\neg\exists \varphi \in \Gamma_-(\psi) : \mathcal{N} \models \varphi$.
2. $N \models \neg\psi$ if and only if
   c) $\exists \varphi \in \Gamma_-(\psi) : \mathcal{N} \models \varphi$;
   d) $\neg\exists \varphi \in \Gamma_+(\psi) : \mathcal{N} \models \varphi$.

***Remark 1.*** Because model $\mathcal{N}$ is not fully defined, the expressions $\mathcal{N} \models \varphi$ and $\mathcal{N} \not\models \varphi$ are not mutually exclusive. In essence, the truth value of sentence $\varphi$ in model $\mathcal{N}$ may be undefined.

***Remark 2.*** There can be a situation when conditions b) and d) are both true. This situation suggests insufficient knowledge to make prediction. If a) and c) are true, then we have inconsistent knowledge.

Thus, we assume that computer attack $\mathcal{N}$ has (does not have) property $\psi$ if at least one positive (negative) hypothesis is compatible with condition $S_{\mathcal{N}}$ and all negative (positive) hypotheses are incompatible with this condition.

This again raises the question of probabilistic assessment of this assumption. Intuitively, as more cases support this assumption, the assumption will become more likely true. Quantitatively, this can be expressed by the following metrics:

$$\frac{\mu(\bigvee_{\varphi\in\Gamma'}\varphi)}{\mu(\psi)}$$

and

$$\frac{\mu(\bigvee_{\varphi\in\Gamma''}\varphi)}{\mu(\neg\psi)},$$

where $\Gamma' \subseteq \Gamma_+(\psi)$, $\Gamma'' \subseteq \Gamma_-(\psi)$ – sets of hypotheses compatible with the set of sentences $S_{\mathcal{N}}$.

## 3. Software Implementation of the Developed Approach

Within the RiskPanel information risk management system, we developed a module for diagnosing early computer attacks.

We used OntoBox to organize and work with a case database [15, 16]. OntoBox is a powerful, flexible system used to represent, store, and process data formatted as ontologies. It is very modular and allows for mobile knowledge bases, an advantage when developing difficult information systems. This technology is based on the idea of using "smart" tools of mathematical logic to solve massive tasks of building information resources.

OntoBox uses an object-oriented data structure, whose basic concepts are the class, object, and property. The class is a set of objects, and any object can belong to multiple classes. There are two types of properties: t-properties and o-properties. T-properties have a value (string, integer, etc.), while o-properties have an object value. OntoBox is designed for use as data storage and organization built in a Java application.

We used OntoBox firstly because it allows organization of data in treelike structures. For this purpose one can simply create a class and define its o-property, whose values are objects of this class. This approach gives flexibility to the developed system. For example, while detecting a new type of virus, there is no need to rewrite the data structure of the system modules; in Ontobox, one can simply add the new type of virus as a sub-object in the "Virus" object describing the connections between objects.

To describe attack cases in OntoBox, we created seven categories of attributes (classes): symptoms, threats, vulnerabilities, consequences, losses, countermeasures, and configuration. Each of these attribute categories is represented in OntoBox as a treelike structure, and each attack case in the database is characterized by attributes from these categories. When considering a concrete case, its attributes are read from the database.

We represent the architecture of the software module for diagnosing early computer attacks by using several major classes, most prominently for interactions between the interface and data. Filling $(+)$ and $(-)$ lists of cases from a database uses the special class. Separate classes provide treelike-structured data models for each of the attribute categories. User actions are processed by classes that implement a standard event-listener pattern. JSM reasoning is implemented using another class. As hypotheses are created, a class using the Chein algorithm [17] receives a set of all concepts for the entrance model $\mathcal{U}_\mu$. The time complexity of this algorithm is $O(\|E\|^3\|S_a(\sigma_A)\|\|\Gamma\|)$, where $E$ is a set of all attack cases, and $\Gamma$ is a set of all concepts in the model $\mathcal{U}_\mu = Fuz(\mathcal{U}_E)$. Finding a set of positive and negative hypotheses requires $O(\|\Gamma\|^2)$ operations. Performing JSM reasoning and obtaining the final answer requires $O(\|\Gamma\|^2)$ operations. Thus, we have $O(\|E\|^3\|S_a(\sigma_A)\|\|\Gamma\|+\|\Gamma\|^2+\|\Gamma\|$, which gives the final algorithmic complexity of the developed approach: $O(\|E\|^3\|S_a(\sigma_A)\|\|\Gamma\| + \|\Gamma\|^2)$.

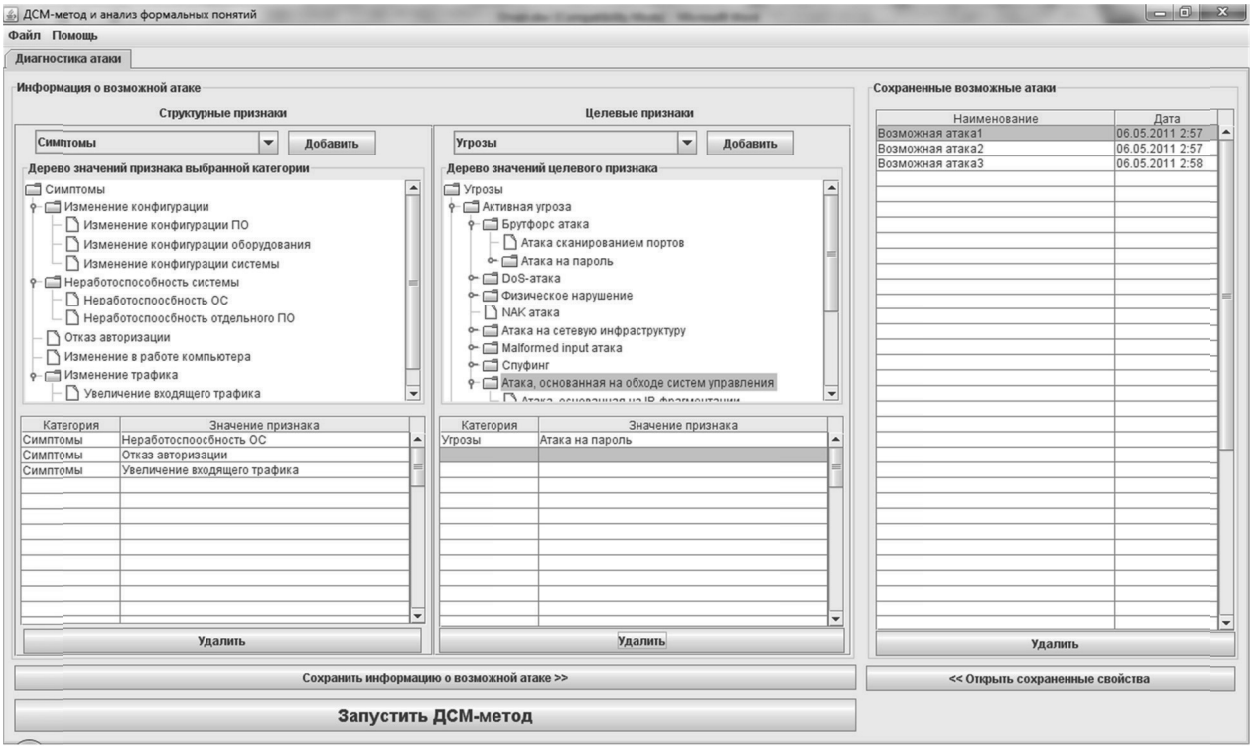


*Figure 1.* General view of the "Attack Diagnosis" tab.

Figure 1 shows the module interface of the "Attack Diagnosis" tab. To input data into the main algorithm, the user must fill in two tables. The first table is filled in with known information on the new computer attack (structural attributes); the second table is filled in with the attributes, which the program determines whether the attack possesses (target attributes) or not. For this purpose, we divided part of the "Attack Diagnosis" tab, called "Information about possible attack", into two parts. The "Information about possible attack", entered at the left, are the attributes of the attack noticed by the user at the moment. From a drop-down list, the user can select from the attribute categories: symptoms, threats, vulnerabilities, consequences, losses, countermeasures, and configuration. Information on the attribute categories and their possible values are stored in the OntoBox database file.

The "Start JSM method" button executes the JSM method for the input information on the possible attack and target attributes. This process constructs hypotheses based on cases, the information about which is stored in an OntoBox database file.

The module produces a window with three tables. The first table contains the target attributes the new computer attack will possess, while the second table contains those it will not possess. The third table contains the target attributes that could not be classified.

We put the developed system into test mode to forecast known cyber attacks. Its forecasting accuracy was 87.5%.

## Acknowledgment

The research for this paper was financially supported by the Ministry of Education of the Russian Federation (project no. 2014/139) and was partially supported by RFBR (project no. 14-07-00903_a).

## References

[1] The 2013 Data Breach Investigations Report: `http://www.verizonenterprise.com/DBIR/2013/`, [Accessed: March 2014].

[2] D. E. PALCHUNOV, The solution of the problem of information retrieval based on ontologies. *Bisnes-informatika*, **1** (2008), 3–13.

[3] D. E. PALCHUNOV, Knowledge search and production: creation of new knowledge on the basis of natural language text analysis. *Filosofiya nauki*, **4**(43) (2009), 70–90.

[4] D. E. PALCHUNOV, G. E. YAKHYAEVA, A. A. HAMUTSKYA, Software system for information risk management "RiskPanel". *Programmnaya ingeneriya*, **7** (2011), 35–50.

[5] D. E. PALCHUNOV, G. E. YAKHYAEVA, Interval fuzzy algebraic systems. *Proceedings of the Asian Logic Conference 2005*, (2006) World Scientific Publishers, pp. 23–37.

[6] G. E. YAKHYAEVA, Fuzzy model truth values. *Proceedings of the 6th International Conference Aplimat*, (2007) Bratislava, Slovak Republic, pp. 423–431.

[7] D. E. PALCHUNOV, G. E. YAKHYAEVA, Fuzzy algebraic systems. Vestnik NGU. it Seriya: Matematica, mexanica, informatica, **10**(3) (2010), 75–92.

[8] S. A. PETRENKO, S. B. SIMONOV, *Controlling of the information risks*. DMK Press, Moscow, 2005.

[9] E. T. JAYNES, Bayesian Methods: General Background. In *Maximum-Entropy and Bayesian Methods in Applied Statistics* (J. H. JUSTICE, Ed.), (1986) pp. 1–25. Cambridge, Cambridge Univ. Press.

[10] B. DE FINETTI, *Theory of probability (2 vols.)*. J. Wiley & Sons, Inc., New York, 1974.

[11] O. M. ANSHAKOV, T. GERGELY, *Cognitive Reasoning*. A Formal Approach Series, Springer, 2010.

[12] S. O. KUZNETSOV, Machine Learning on the Basis of Formal Concept Analysis. *Automation and Remote Control*, **62**(10) (2001), 1543–1564.

[13] S. O. KUZNETSOV, Galois Connections in Data Analysis: Contributions from the Soviet Era and Modern Russian Research. In *Formal Concept Analysis: Foundations and Applications* (B. GANTER, G. STUMME, R. WILLE, Eds.), (2005) pp. 196–225. Lecture Notes in Artificial Intelligence (Springer), State-of-the Art Ser., Vol. 36262005.

[14] O. M. ANSHAKOV, The JSM method: A set-theoretical explanation. *Automatic Documentation and Mathematical Linguistics*, **46**(5) (2012), 202–220.

[15] A. A. MALIH, A. V. MANCIVODA, Ontobox: ontologies for objects. *Izvestia Irkutskogo gosydarstvennogo universiteta*, **2**(2) (2009), 94–104.

[16] A. MALYKH, A. MANTSIVODA, Query Language for Logic Architectures. In *Perspectives of System Informatics: Proceedings of the 7th International Conference*, (2010) pp. 294–305. Lecture Notes in Computer Science, Vol. 5947. Springer-Verlag Berlin Heidelberg.

[17] S. O. KUZNETSOV, S. A. OBIEDKOV, Comparing performance of algorithms for generating concept lattices. *Journal of Experimental and Theoretical Artificial Intelligence*, **14**(2-3) (2002), 189–216.

*Received:* March, 2014
*Revised:* September, 2014
*Accepted:* September, 2014

*Contact addresses:*
Gulnara Yakhyaeva
Department of Information Technologies
Novosibirsk State University
Russia
e-mail: gul_nara@mail.ru

Olga Yasinskaya
Department of Information Technologies
Novosibirsk State University
Russia
e-mail: yasinskaya.olga@gmail.com

GULNARA YAKHYAEVA is an Associate Professor in the Department of Information Technologies at the Novosibirsk State University, Russian Federation. She is a senior researcher at the Institute of Discrete Mathematics and Informatics. Her research areas include knowledge representation and reasoning and also uncertainty and fuzziness representation and reasoning.

OLGA YASINSKAYA received her MS degree in Engineering and Technology from Novosibirsk State University in 2012. Currently, she is a Ph.D. student at the Faculty of Information Technologies at the Novosibirsk State University. Her research in Ph.D. is focused on application of fuzzy logic in the field of information security. Other research interests include risk management, software engineering and data mining.