https://doi.org/10.31891/2219-9365-2022-69-1-8
УДК 004.891

Vera TITOVA
https://orcid.org/0000-0001-8668-4834
Yurii KLOTS
https://orcid.org/0000-0002-3914-0989
Nataliia PETLIAK
https://orcid.org/0000-0001-5971-4428
Mariia KAPUSTIAN
https://orcid.org/0000-0001-9200-1622
Khmelnytskyi National University

FUZZY INFERENCE SUBSYSTEM FOR CLASSIFYING THREATS TO COMPUTER INFORMATION

This article was analyzed the threats to computer data in computer systems and classified these threats by their attributes. The relationships between threat classes, attributes, and related security methods and tools have defined the mathematical model of the computer threat classification problem.

Based on the model analysis was concluded that the computer threats classification problem belongs to difficult formalized problems and requires for its solution methods of intellectual analysis, one of which is the subsystem of logical inference implemented in this article.

Keywords: Computer Threats, Mathematical Model, Information Security, Computer Systems

Віра ТІТОВА, Юрій КЛЬОЦ,
Наталія ПЕТЛЯК, Марія КАПУСТЯН
Хмельницький національний університет

ПІДСИСТЕМА НЕЧІТКОГО ВИСНОВКУ ДЛЯ КЛАСИФІКАЦІЇ ЗАГРОЗ КОМП'ЮТЕРНІЙ ІНФОРМАЦІЇ

Однією з ключових проблем комп'ютерної безпеки сьогодні є необхідність ефективної протидії комп'ютерним загрозам. Загрози можуть бути як ненавмисними, так і навмисними. Найбільшу небезпеку становлять навмисні погрози. Крім того, комп'ютерні дані обробляються за допомогою різних компонентів архітектури комп'ютера: апаратних, програмних, комплексних. Тому актуальним завданням захисту комп'ютерних даних є захист усіх компонентів архітектури комп'ютера від загроз, як навмисних, так і ненавмисних.

У даній статті проаналізовано загрози комп'ютерним даним в комп'ютерних системах та класифіковано ці загрози за їх атрибутами. Зв'язки між класами загроз, атрибутами та відповідними методами та інструментами безпеки визначили математичну модель проблеми класифікації комп'ютерних загроз.

На основі аналізу моделі зроблено висновок, що проблема класифікації комп'ютерних загроз належить до складних формалізованих задач і потребує для свого вирішення методів інтелектуального аналізу, одним з яких є реалізована в даній статті підсистема логічного висновку.

Ключові слова: комп'ютерні загрози, математична модель, інформаційна безпека, комп'ютерні системи

Introduction

One of the key challenges in computer security today is the need to effectively counteraction computer threats. Threats can be both unintentional and intentional. The greatest danger is intentional threats. In addition, computer data is processed using various components of computer architecture: hardware, software, complex [1-4]. Therefore, the urgent task of computer data protection is to protect all computer architecture components from threats, both intentional and unintentional.

Today, there are many ways to protect computer data from threats in computer systems. Among them are [1-4]:

- ✓ anomaly detection methods are methods of finding and identifying elements, events or observations that don't correspond to the expected behavior (patterns);
- ✓ signature and heuristic methods of detecting malware, based on comparing the contents of suspicious programs and files with known samples of malware;
- ✓ access control methods. Access control can be performed in relation to the user and in relation to the data. The most common user access control is a registration procedure in which the user needs to enter his ID and password. Data access control is that each user can match a profile that specifies the allowed operations and file access modes.

Problem definition

Each group of methods has both advantages and disadvantages. Anomaly detection methods require the use of machine learning or artificial intelligence, which complicates their software and hardware implementation. Signature and heuristic methods can recognize a threat if it has occurred before. Access control methods require the use of additional cryptographic protocols to prevent password and ID hacking and can create difficulties when different users need to share certain data. The use of these methods in combination would eliminate the disadvantages of one group due to the advantages of others and increase the effectiveness of computer data protection in general.

However, using a hybrid system that includes all of these methods requires a lot of resources. Therefore, it is more appropriate to create a protection system in which one or another group of methods will be involved depending on the threat identified class.

In order to decide on the use of a particular method, the computer data protection system must contain a subsystem that will solve the problem of computer threats classification and determinate appropriate protection methods and tools. This article is devoted to the implementation of this subsystem.

Computer threats and protection methods classification

Among the whole set of threats, the following groups can be identified [5, 6]:
threats to data in memory;
threats to input data correctness;
threats to computer system stability;
threats to privileges and access;
denial of service;
attacks on the system;
threats to hardware components.
Mathematically, this can be written as follows [7]:

$$Y_i =< Y_1, Y_2, Y_3, Y_4, Y_5, Y_6, Y_7 >,$$

whereY_1– threats to data in memory; Y_2– threats to input data correctness; Y_3– threats to computer system stability; Y_4 – threats to privileges and access; Y_5– denial of service; Y_6 – attacks on the system; Y_7– threats to hardware components; – current threat class.

Attributes of threats can be represented as a set [7]:

$$A = \{a_1, a_2, a_3, ..., a_{19}\},$$

where a_1 - buffer overflow due to incorrect data using; a_2 - link to the deleted object; a_3 - format string error; a_4 - manipulation of command shell metacharacters; a_5 - intrusion into queries; a_6 - open access to system area; a_7 - manipulation of user scripts; a_8 - race files in multitasking systems; a_9 - privileges escalation; a_{10} - attack with symbolic links; a_{11} - DoS-attack (simple or distributed); a_{12} - replacement of a trusted network object; a_{13} - imposing the wrong route; a_{14} - network traffic analysis; a_{15} - network protocols scanning; a_{16} - incorrect hardware configuration; a_{17} - unauthorized use of developer tabs; a_{18} - hardware listening for data traffic; a_{19} - physical access to data.

The same attribute in combination with other attributes can define different classes of threats. At one point in time, there may be one or more classes of threats, and the attributes can change in the decision-making process. And with their change, one threat class can modifies to another or correlate with it. Based on the classification, the mathematical model of threat classification was built (1).

Set of threat protection tools and methods can be represented as:

$$P = \{p_1, p_2, p_3, ..., p_{19}\},$$

where p_1 - prohibition the code using in the stack area; p_2 - checking the variables dimensionality; p_3 - correct removal of objects, garbage removal; p_4 - string length limit; p_5 - shielding any characters; p_6 - checking

the request correctness; p_7 - restriction of access rights to system area; p_8 - prohibition of special characters in the request; p_9 - correctness of semaphore functions; p_{10} - launching applications with minimal privileges; p_{11} - antivirus tools using; p_{12} - using of separate directory for temporary files; p_{13} - using of standard tools to create temporary files; p_{14} - correct configuration of routers and firewalls; p_{15} - traffic limit; p_{16} - using of cryptographic protection methods, data encryption; p_{17} - using of Host-Based Intrusion Detection System; p_{18} - using of ingress-filtration and egress- filtration; p_{19} -ICMP-packages limit; p_{20} - detection and correction of incorrect hardware configuration; p_{21} - compliance with security policy.

One of the protection tools and methods can be applied to several threats at the same time, or several tools and methods can counteract one threat. The relationships between threats and protection tools and methods are presented in the following mathematical model (2).

$$Y_i = \begin{cases} Y_1, \text{ if A'} = \{a_1,a_2,a_{16},a_{17},a_{18}\} \\ Y_2, \text{ if A'} = \{a_3,a_4,a_5,a_6,a_7, a_{10},a_{18}\} \\ Y_3, \text{ if A'} = \{a_3,a_4,a_7,a_8,a_{17}\} \\ Y_4, \text{ if A'} = \{a_6,a_8,a_9,a_{10},a_{17}\} \\ Y_5, \text{ if A'} = \{a_1,a_2,a_3,a_8,a_9,a_{11},a_{12},a_{13},a_{16},a_{19}\} \\ Y_6, \text{ if A'} = \{a_4,a_5,a_6,a_7,a_{10},a_{11},a_{12},a_{13},a_{14},a_{15},a_{17},a_{18},a_{19}\} \\ Y_7, \text{ if A'} = \{a_{16},a_{17},a_{18},a_{19}\} \\ Y_1 \cup Y_2, \text{ if A'} = \{a_1,a_2,a_3,a_4,a_5,a_6,a_7, a_{10},a_{16},a_{17},a_{18}\} \\ Y_1 \cup Y_3, \text{ if A'} = \{a_1,a_2,a_3,a_4,a_7, a_8,a_{16},a_{17},a_{18}\} \\ Y_1 \cup Y_4, \text{ if A'} = \{a_1,a_2,a_6, a_8,a_9,a_{10},a_{16},a_{17},a_{18}\} \\ Y_1 \cup Y_5, \text{ if A'} = \{a_1,a_2,a_3,a_8,a_9,a_{11},a_{12},a_{13},a_{16},a_{17},a_{18},a_{19}\} \\ Y_1 \cup Y_6, \text{ if A'} = \{a_1,a_2,a_4,a_5,a_6,a_7,a_{10},a_{11},a_{12},a_{13},a_{14},a_{15},a_{16},a_{17},a_{18},a_{19}\} \\ Y_1 \cup Y_7, \text{ if A'} = \{a_1,a_2,a_{16},a_{17},a_{18},a_{19}\} \\ Y_2 \cup Y_3, \text{ if A'} = \{a_3,a_4,a_5,a_6,a_7, a_8,a_{10},a_{17},a_{18}\} \\ Y_2 \cup Y_4, \text{ if A'} = \{a_3,a_4,a_5,a_6,a_7, a_8,a_9,a_{10},a_{17},a_{18}\} \\ Y_2 \cup Y_5, \text{ if A'} = \{a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_9,a_{11},a_{12},a_{13},a_{16},a_{18},a_{19}\} \\ Y_2 \cup Y_6, \text{ if A'} = \{a_3,a_4,a_5,a_6,a_7,a_{10},a_{11},a_{12},a_{13},a_{14},a_{15},a_{17},a_{18},a_{19}\} \\ Y_2 \cup Y_7, \text{ if A'} = \{a_3,a_4,a_5,a_6,a_7,a_{10},a_{16},a_{17},a_{18},a_{19}\} \\ Y_3 \cup Y_4, \text{ if A'} = \{a_3,a_4,a_6,a_7, a_8,a_9,a_{10},a_{17}\} \\ Y_3 \cup Y_5, \text{ if A'} = \{a_1,a_2,a_3,a_4,a_7,a_8,a_9,a_{11},a_{12},a_{13},a_{16},a_{17},a_{19}\} \\ Y_3 \cup Y_6, \text{ if A'} = \{a_3,a_4,a_5,a_6,a_7,a_8,a_{10},a_{11},a_{12},a_{13},a_{14},a_{15},a_{17},a_{18},a_{19}\} \\ Y_3 \cup Y_7, \text{ if A'} = \{a_3,a_4,a_7,a_8,a_{16},a_{17},a_{18},a_{19}\} \\ Y_4 \cup Y_5, \text{ if A'} = \{a_1,a_2,a_3,a_6,a_8,a_9,a_{10},a_{11},a_{12},a_{13},a_{16},a_{17},a_{19}\} \\ Y_4 \cup Y_6, \text{ if A'} = \{a_4,a_5,a_6,a_7,a_8,a_9,a_{10},a_{11},a_{12},a_{13},a_{14},a_{15},a_{17},a_{18},a_{19}\} \\ Y_4 \cup Y_7, \text{ if A'} = \{a_6,a_8,a_9,a_{10},a_{16},a_{17},a_{18},a_{19}\} \\ Y_5 \cup Y_6, \text{ if A'} = \{a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_9,a_{10},a_{11},a_{12},a_{13},a_{14},a_{15},a_{17},a_{18},a_{19}\} \\ Y_5 \cup Y_7, \text{ if A'} = \{a_1,a_2,a_3,a_8,a_9,a_{11},a_{12},a_{13},a_{16},a_{17},a_{18},a_{19}\} \\ Y_6 \cup Y_7, \text{ if A'} = \{a_4,a_5,a_6,a_7,a_{10},a_{11},a_{12},a_{13},a_{14},a_{15},a_{17},a_{18},a_{19}\} \end{cases} \quad (1)$$

$$P_j = \begin{cases} \{p_1, p_2, p_3\}, \text{if } Y_i = Y_1 \\ \{p_4, p_5, p_6, p_7, p_8\}, \text{if } Y_i = Y_2 \\ \{p_9\}, \text{if } Y_i = Y_3 \\ \{p_{10}, p_{11}, p_{12}, p_{13}\}, \text{if } Y_i = Y_4 \\ \{p_{14}, p_{15}, p_{16}, p_{17}, p_{18}, p_{19}\}, \text{if } Y_i = Y_5 \\ \{p_{16}, p_{17}, p_{18}, p_{19}\}, \text{if } Y_i = Y_6 \\ \{p_{20}, p_{21}\}, \text{if } Y_i = Y_7 \end{cases} \quad (2)$$

where P_j- subset of protection tools and methods to counter the current threat.

From the analysis of these models was concluded that the task of threats classification has the following features:

- ✓ there are a large number of possible solutions, which complicates the solution of the problem by a complete search of all available alternatives;
- ✓ input data can change in the process of solving the problem, and when changing at least one value it is necessary to go through all the available options first;
- ✓ input data is difficult to represent in the form of numerical data, and therefore the solution of the problem cannot be reduced to numerical calculations.

So, the task of threats classification is a difficult-formalized task [8]. To solve it, it is advisable to use intellectual analysis methods. The authors chose the logical inference subsystem, which is best suited for the implementation of production rules set, which is the mathematical model.

Logical inference subsystem for threats classification and determination appropriate protection methods

This subsystem was implemented using Matlab software. The neural network structure of this subsystem is shown in Fig. 1.

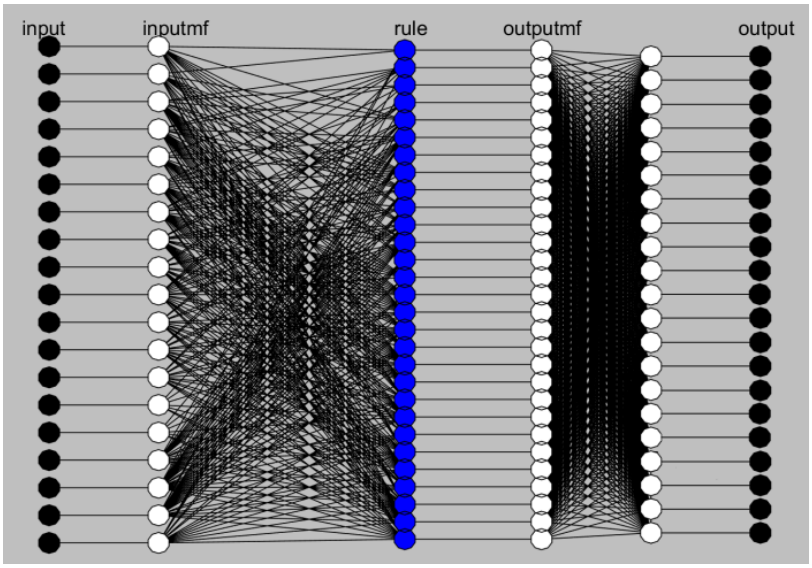

Fig. 1. Structure of logical inference subsystem for threats classification and determination appropriate protection methods

The number of inputs is 19, according to the number of threat attributes. The input data can be 0 or 1, depending on the manifestation of a particular threat attribute.

The number of outputs is 21 according to the number of protection tools and methods. The output data can be 0 or 1, depending on how much a particular method or tool is needed.

The set of rules determinate links between identified threat attributes and the protection tools and methods to be applied.

The results of the subsystem work are presented in Fig. 2. The value of p1 depends on both attributes a1 and a2. The value of p9 depends only on the value of the attribute a4 and is independent of the value of the attribute a5.

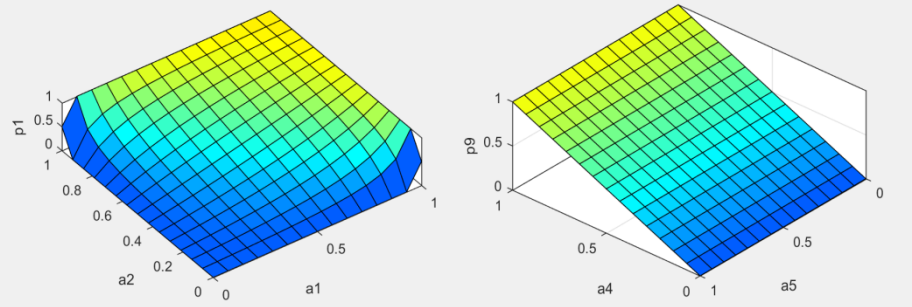

Fig. 2. The results of the logical inference subsystem work are presented in the response surface form

Conclusions

The article considers the threats to computer data in computer systems and their classification. Based on the classification, the mathematical model for determining the current threat class was proposed.

The methods and tools of counteracting threats were also considered and the relationships between them and classes of threats were determined.

These models became the basis for the design of the threat classification subsystem of the computer data protection system. The implementation of this subsystem will increase the efficiency of the computer data protection system and will avoid high needs in computer resources during the operation of this system.

REFERENCES

1. Informatsiyna bezpeka v komp'yuternih merezhah: navch. posib./ O.A. Smirnov, O.K. Slobodenyuk, S.A. Smirnov, K.O. Buravchenko, T.V. Smirnova, L.I. Polischuk. – Kropivnitskiy: Vidavets Lisenko V. F., 2020. – 295 s.

2. Zahist informatsiyi v komp'yuternih sistemah ta merezhah: navch. posib./ S.G. Semenov, A.O. Podorozhnyak, O.I. Balenko, S.Yu. Gavrilenko – H.: NTU «HPI», 2014.– 251 s.

3. Kompleksna bezpeka informatsiynih merezhevih sistem. Navchalniy posibnik/ A.G. Mikitishin, M.M. Mitnik, P.D. Stuhlyak. – Lviv, «MagnolIya 2006», 2016. – 256 s.

4. Informatsiyna bezpeka: navchalniy posibnik/ [Yu. Ya. Bobalo, I. V. Gorbatiy, M. D. Kiselichnik, A. P. Bondarev ta in.]; za zag. red. d-ra tehn. nauk, prof. Yu. Ya. Bobala ta d-ra tehn. nauk, dots. I. V. Gorbatogo. – Lviv: Vidavnitstvo Lvivskoyi politehniki, 2019. – 580 s.

5. Korpan Ya.V. Klasyfikatsiia zahroz informatsiinii bezpetsi v kompiuternykh systemakh pry viddalenii obrobtsi danykh / Ya.V. Korpan // Myr nauky y ynnovatsyi. – Nauchnyi myr, 2015. – T. 17, № 2. – s. 39-46.

6. Korpan Ya.V. Kompleks metodiv i zasobiv zakhystu informatsii u kompiuternykh systemakh / Ya.V. Korpan // Reiestratsiia, zberihannia i obrobka danykh. – 2015. – Vyp. 1. – T. 32. – s. 31-35.

7. Titova V. Yu. Klasyfikatsiia modelei zahroz v kompiuternykh systemakh/ V. Yu. Titova, Yu. P. Klots, S. O. Savchuk // Herald of Khmelnytskyi National University. Technical sciences. – 2020. – № 2. – S. 201-203/

8. Lokaziuk V. M. Zasady system pidtrymky pryiniattia rishen na osnovi kompiuternykh system ta yikh komponentiv : navch. posib./ V. M. Lokaziuk, O. V. Ivanov, V. Yu. Titova; Khmelnyts. nats. un-t. – Khmelnyts.: Honta A.S., 2010. - 338 c.

9. Martseniuk, V. P., Sverstiuk, A. S., Kozodii, N. V., & Kravchyk Yu, V. (2019). Vykorystannia paketu R dlia kompiuternoho modeliuvannia kontaktiv antyheniv z antytilamy v kiberfizychnykh imunosensornykh systemakh na priamokutnii reshittsi. Visnyk Khmelnytskoho natsionalnoho universytetu. Tekhnichni nauky (4), 97-105.