Scientific and Practical Cyber Security Journal (SPCSJ) 6(1): 53-58 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

DEVELOPMENT OF THE STRUCTURAL AND ANALYTICAL MODELS FOR EARLY APT-ATTACKS DETECTION AND INTRUDERS IDENTIFICATION

Sergiy Gnatyuk, NAU Cybersecurity R&D Lab, National Aviation University, Kyiv, Ukraine
Zhadyra Avkurova, L.N. Gumilyov Eurasian National University, Nur-Sultan, Kazakhstan
Andriy Tolbatov, NAU Cybersecurity R&D Lab, National Aviation University, Kyiv, Ukraine
Yevheniia Krasovska, Professional College of Engineering and Management, National Aviation University, Kyiv, Ukraine
Bagdat Yagaliyeva, Yessenov University, Aktau, Kazakhstan
Oleksii Verkhovets, State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, Kyiv, Ukraine

ABSTRACT: Modern information and communication technologies (ICT) are vulnerable to APT-attacks (advanced persistent threats) and other relevant threats. APT-attack is a stealthy threat actor, typically a nation-state or state-sponsored group, which gains unauthorized access to ICT and remains undetected for an extended period. Early detection of APT-attack is very important for ICT of critical infrastructure sectors. But existed approaches don't allow to detect attacks effectively in cyberspace as fuzzy environment. In this paper, a method of linguistic terms using statistical data was used for structural and analytical models of parameters (both host and network parameters) as well as intruder model based on the defined host and networks parameters was developed. Based on this, logical rules can be developed to provide the functioning of IDS based on honeypot (or other) technology for APT-attacks detection and intruder type identification in ICT.

KEYWORDS*: APT-attack, Early Detection, Identification, Honeypot, Fuzzy Logic, Parameter, ICT.*

1. Introduction

The development of information and communication technology (ICT) creates new types of threats to information security, among which the intruder in computer systems and networks (for example, APT-attacks or other negative influences) occupies a prominent place. To effectively counter this threat, IDS (intruder detection system) are being developed to detect and identify an intruder. Early detection is important and not simple task for security side. Typical IDS should perform the following main functions [1]:

- monitor and analyze the activity of ICS (information and communication system) users;
- capture system configurations and vulnerabilities;
- assess the integrity of critical system files and data files;
- recognize activity patterns that reflect known attacks;
- perform statistical analysis to detect abnormal behavior;
- recognize violations of security policy by the system user.

2. Related papers analysis and problem statement

The IDS tasks can be divided into global and local. Global tasks is recognition of the violator (intruder) and legitimate user. The solution of this problem contains the following stages [2-3]: data collection, filtering, behavior classification – directly the process of recognizing the violator, report and response system. As can be seen from the main functions and tasks of IDS, one of the most important aspects of their functioning is not only the fixation of intrusion in ICS, but also its identification.

There are many studies related with APT-attacks early detection. In [4-5] the big data processing approach was proposed for APT-attacks detection. In [6-9] authors proposed malware and DoS-attacks detection system as well as game theory based approach for APT-attacks detection. Presented techniques have many advantages (indicators, correlation, high-speed and others), but they don't allow identifying intruders` category as well as don't give possibility to operate with fuzzy parameters. That is why, the ***main task*** of this study is creation the possibility for early APT-attacks detection using developed structural and analytical models based on network and host parameters as well as method of linguistic terms using statistical data.

3. Development of the structural and analytical models based on host and network parameters

Basic parameters for intruders identification

In the process of attack, the violator, acting on the system, changes certain parameters, creates or terminates its inherent processes, and so on. All these actions are reflected in the state of the system. Evaluating these parameters, you can detect the fact of intrusion into the system. The work of modern IDSs is based on this principle. Thus, the NIDES system performs audits of such processes as logging in, working with files and processes, administration and fixing errors and failures. Previous works describe the parameters by which the violator is identified by the developed system. These parameters (are host settings) include:

Host Parameters (HIDS): Username at login, *UID;* Login time, *Tlog;* Frequency of login requests, *Nlog;* Time spent logging in, *TSlog;* Intensity of actions, *I;* Processor time / CPU usage, *CPU;* The amount of RAM load, *Muse;* Number of executable files, *NEF;* The type of files used in the attack, *AtEF;* Number of failures and errors, *NEr;* Process / file execution time, *RTPr/F;* Unusual processes, *UPr;* File transfer to the system, *TrFin;* Files changes, *ModF;copying* / transferring files from the system, *TrFout;* Pressing the keyboard keys, *KS.*

Network Parameters (NIDS) – characteristics of *ARP-, IP-, ICMP-* and *TCP*-packages.

Since the process of detection and identification of the violator takes place in conditions of uncertainty, and some of the parameters of the IDS are unclear, the operation of such a system should be based on fuzzy logic. To identify the violator, we can use the logical-linguistic approach and the basic model of parameters, partially described in [10], which will be the basis for the construction of the developed IDS. For example, to detect the process of port scanning in section [11] used linguistic variables (LV) "Number of virtual channels" and "Age of virtual channels", and in section [12] LV "Number of simultaneous connections", "Query processing speed", "Delay between requests" and 'Number of packets with the same sender and recipient address"– to detect DDoS attacks and spoofing.

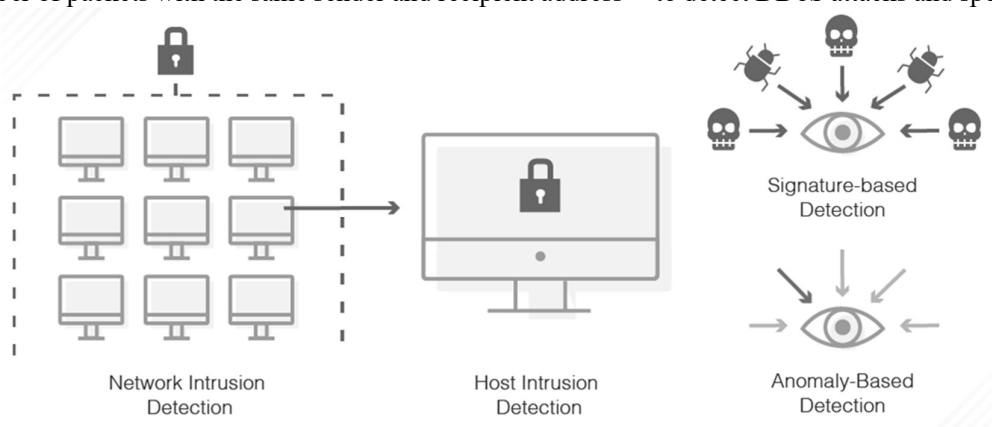

Figure 1. Difference between HIDS and NIDS

The process of detecting and identifying the violator requires determining the necessary parameters and their properties. In this regard, the main purpose of this work is to build models of standards required for the operation of IDS in a vaguely defined, poorly formalized environment.

Method of linguistic terms using statistical data

Consider the method of linguistic terms using statistical data (MLTS) [13], where as a measure of belonging of the element to the set is an estimates of the frequency of use of the concept, which is given by a fuzzy set to characterize the element. To do this, the values of the linguistic variable (LV) are placed on the universal scale [0; 1] $X=\{x_1, x_2, \dots, x_n\}$. The method is based on the condition that the same number of experiments falls into each interval of the scale, but this is usually not followed in practice. An empirical table is compiled in real conditions, in which experiments can be unevenly distributed over intervals. Some of them may not be involved, and then the data is processed using a matrix of prompts. May it is necessary to estimate in values of LV deviations of the parameter $\Delta B \in [0, B]$ (where B is the maximum possible deviation), which characterizes the current measurements. Next for $n = 5$ determine the value of LV $\{x_1, x_2, x_3, x_4, x_5\}$. Interval $[0, B]$ and $\Delta B/B$ (estimated ratio) divided

into k segments (for example, 5), on which the statistics characterizing frequency of use by the expert of the value of drugs for the display of the conclusions gathers. Then the data are entered into the table and processed to reduce the errors made during the experiment: the table is removed individual elements on the left side and on the right side of which there are zeros in the row. The tooltip matrix is a string whose elements are calculated by the formula:

$$k_j = \sum_{i=1}^{n} b_{ij} = \sum_{i=1}^{5} b_{ij},\ j = \overline{1,5}. \quad (1)$$

Next, in the resulting row of the matrix, the maximum element is selected $k_{\max} = \max k_j$, and then all elements of the table are converted by expression

$$c_{ij} = b_{ij} k_{max} / k_j,\ i = \overline{1,5}; j = \overline{1,5}, \quad (2)$$

and for columns, where $k_j = 0$ the linear approximation is applied $c_{ij} = (c_{ij-1} + c_{ij+1})/2,\ i = \overline{1,5}; j = \overline{1,5}$.

Next, calculate the value of MF (membership function) by the formula

$$\mu_{ij} = c_{ij} / c_{imax},\ c_{imax} = \max_j c_{ij},\ i = \overline{1,5}; j = \overline{1,5}. \quad (3)$$

The described method uses data from statistical studies. Their processing is quite time consuming, because to build a MF of one term it is necessary to conduct statistical studies of all terms of LV. We construct a model of standards of linguistic variables for fuzzy parameters of violator identification from the set of parameters (host and network). Model contains (4) as well as Table 1 and Table 2.

DIO = <UID, Tlog, Nlog, TSlog, I, CPU, MUse, NEF, AtEF, NEr, RTPr/F, UPr, TrFin, ModF, TrFout, KS, ARP, IP, ICMP, TCP>. (4)

Models of intruders host and networks parameters

The system must monitor certain parameters of the IS (Table 1), record them and identify violator.

Table 1 – Host parameters for violator identification and their characteristics

Parameter	Blur	Human				Bot	
		Misinformer	*Spammer*	*Cracker*	*Hacker*	*Spam-bot*	*Bot-hackers*
UID	-	+	-	+	+	-	+
Tlog	+	Depending on the time of day (*)	-	*	*	-	*
Nlog	+	Above average (***)	-	***	***	-	High
TSlog	+	***	-	***	***	-	***
I	+	Within the norm	Within the norm	Within the norm	Within the norm	Above the norm	***
CPU	+	***	***	***	***	***	***
MUse	+	***	***	***	***	***	***
NEF	+	Not within the norm	-	Not within the norm	Not within the norm	-	Not within the norm
AtEF	-	Scripts and PHP scripts	PHP scripts	Executa-ble files	Scripts	PHP scripts	Scripts
NEr	+	***	***	***	***	***	***
RTPr/F	+	Differs from the typical time (**)	**	**	**	**	**
UPr	-	Present	Present	Present	Present	Present	Present
TrFin	-	Present	Present	Present	Mostly absent	Present	Mostly absent
ModF	-	Present	Absent	Present	Mostly	Absent	Mostly present

TrFout	-	Absent	Absent	Mostly present	Present	Absent	Present
KS	-	It is fixed	It is fixed	It is fixed	It is fixed	It is not fixed	It is not fixed

Network part works with network traffic and detect attacks associated with low-level impact on network protocols, and can detect attacks on multiple network hosts. Network VDS is based on an intelligent traffic analyzer, which processes each frame of data passing through it, in order to search for prohibited signatures that indicate attacks. Network data, network traffic is received from a network adapter operating in a promiscuous mode (i.e. receiving all packets on the network).

Consider ***network parameters*** (with the characteristics of the TCP / IP protocols) in more detail:

Table 2 – Network parameters for intruder identification and their characteristics

Parameter	Blur	Human				Bot	
		Misinformer	*Spammer*	*Cracker*	*Hacker*	*Spam bot*	*Bot hackers*
ARP- request	-	Doesn't meet the allowed (****)	****	****	****	****	****
IP- fragment	-	****	****	****	****	****	****
ICMP- message	-	****	****	****	****	****	****
TCP- package	-	****	****	****	****	****	****

ARP request is monitored by the following parameters: IP address of source; source hardware address; network interface that limits the ARP request.

IP-fragment: source address; receiver address; protocol field; offset field; length; header length; MF bit; identification.

ICMP message: source IP address; IP address of the receiver; ICMP field type; ICMP identifier; ICMP sequence number.

TCP-package: source IP address; IP address of the receiver; TCP source port; TCP receiver port; bits of the TCP code.

All these network parameters, provided the correct configuration of the interconnection policy, clearly indicate the attack, and therefore belong to the group of clear.

4. Structural and analytical models

System login time, Tlog. This parameter is based on the fact that the activity of the ICS and users of this system depends on the time of receipt. Usually, the usual greater activity of users to log in is detected on the last day, less – at night. Still, other statistics are possible, determined by the mode of operation of the organization to which the ICS belongs. The nature of these parameters is unclear, due to which it is impossible to conclude the message's illegal activity unambiguously. Thus, in organizations working from 08.00 to 16.00, the probability of who is the user who logs in – the message is lowest at 08.00 and increases over time, reaching a maximum in the years after 16.00. However, it should be changed that in the concepts of honeypot-technology, this parameter loses weight, as any activity on them is considered criminal. Let's evaluate the LV "Level of legitimacy over time". Determine the value of the linguistic variable $\{x_1, x_2, x_3\}$, corresponding {legitimate, suspicious, illegitimate}. That is $T_{Tlog} = \bigcup_{i=1}^{3} T^i{}_{Tlog} = \{legitimate, suspicious, illegitimate\}$, we use statistics for $B = 24$ hours. It is advisable to divide the total interval into 4 intervals [00:00;06:00], [06:00;12:00], [12:00;18:00], [18:00;24:00].

Table 3 – Data for LV *Tlog*

The value of LV	Interval			
	№1	№2	№3	№4
High	0	8	6	1
Middle	2	1	2	3

Low	6	1	1	4

Using expression (1), we define $k_j = \|8\ 10\ 9\ 8\|$, where k_{max} = 10, and in accordance with (2) calculate:

$$\|c_{ij}\| = \begin{Vmatrix} 0 & 8 & 6,66 & 1,25 \\ 2,5 & 1 & 2,22 & 3,75 \\ 7,5 & 1 & 1,11 & 5 \end{Vmatrix}.$$

Calculate the MF by formula (3):

$$\|\mu_{ij}\| = \begin{Vmatrix} 0 & 1 & 0,83 & 0,16 \\ 0,66 & 0,26 & 0,59 & 1 \\ 1 & 0,13 & 0,15 & 0,66 \end{Vmatrix}.$$

For $\bigcup_{i=1}^{3} \mu_{ij}$ accordingly, we find the evaluation relationship $\bigcup_{i=1}^{3} \Delta B_i / B = \{0,25;\ 0,5;\ 0,75;\ 1\}$, and we obtain the following fuzzy numbers:

$$L = \{0/0,25;\ 1/0,5;\ 0,83/0,75;\ 0,16/1\},$$

$$P = \{0,66/0,25;\ 0,26/0,5;\ 0,59/0,75;\ 1/1\},$$

$$N = \{1/0,25;\ 0,13/0,5;\ 0,15/0,75;\ 0,66/1\}.$$

Schedule MF terms LV *Tlog* is shown in Fig. 2.

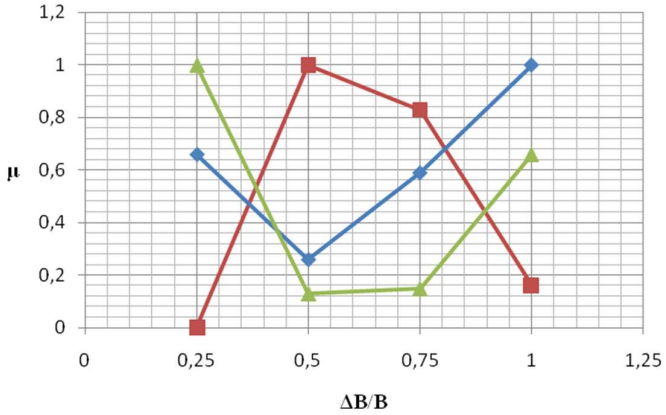

Figure 2. Linguistic standards of fuzzy numbers for *Tlog*

Analogically, using (1) - (3), structural and analytical models for other defined parameters (4) can be formed and presented.

5. Conclusions

In this paper, defined linguistic variables were introduced as well as structural and analytical models of parameters *Tlog, Nlog, TSlog, I, CPU, Muse, NEF, NEr, RTPr/F* were built. Also, for each described linguistic variables, MF were calculated and schedules of their terms were constructed. The formed standards are necessary for formation the system of logical rules allowing to provide functioning of IDS for APT-attacks detection and intruder category identification. Also, the intruder model based on the defined host and networks parameters was developed. These results can be used in sectors of critical infrastructure because APT-attacks are directed on them frequently.

The obtained results will be further used to build an IDS system (or other cyber threat detection system) based on honeypot technology or cloud architecture [14-17]. In the future, authors plan to create the rules system for effective detection the fact of intrusion in ICS and identification of the person (category) of the intruder.

REFERENCES

1. M. Khosravi and B. T. Ladani, "Alerts Correlation and Causal Analysis for APT Based Cyber Attack Detection", in IEEE Access, Vol. 8, pp. 162642-162656, 2020.
2. Denning D.E. "An Intrusion-Detection Model", IEEE Transactions On Software Engineering, February 1987, Vol. SE-13, No. 2, pp. 222-232.
3. Hu Z., Odarchenko R., Gnatyuk S., Zaliskyi M., Chaplits A., Bondar S., Borovik V. "Statistical techniques for detecting cyberattacks on computer networks based on an analysis of abnormal traffic behavior", International Journal of Computer Network and Information Security, Vol. 12, Issue 6, pp. 1-13, 2020.
4. Y. Qi, R. Jiang, Y. Jia and A. Li, "An APT Attack Analysis Framework Based on Self-define Rules and Mapreduce", 2020 IEEE Fifth International Conference on Data Science in Cyberspace (DSC), 2020, pp. 61-66, doi: 10.1109/DSC50466.2020.00017.
5. D. Liu, H. Zhang, H. Yu, X. Liu, Y. Zhao and G. Lv, "Research and Application of APT Attack Defense and Detection Technology Based on Big Data Technology", 2019 IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC), 2019, pp. 1-4, doi: 10.1109/ICEIEC.2019.8784483.
6. X. Liu, L. Li, Z. Ma, X. Lin and J. Cao, "Design of APT Attack Defense System Based on Dynamic Deception", 2019 IEEE 5th International Conference on Computer and Communications (ICCC), 2019, pp. 1655-1659, doi: 10.1109/ICCC47050.2019.9064206.
7. S. -P. Hong, C. -H. Lim and H. J. Lee, "APT attack response system through AM-HIDS", 2021 23rd International Conference on Advanced Communication Technology (ICACT), 2021, pp. 271-274, doi: 10.23919/ICACT51234.2021.9370749.
8. Y. Su, "Research on APT attack based on game model", 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), 2020, pp. 295-299, doi: 10.1109/ITNEC48623.2020.9084845.
9. M. Zaliskyi, R. Odarchenko, S. Gnatyuk, Yu. Petrova. A. Chaplits, "Method of traffic monitoring for DDoS attacks detection in e-health systems and networks", CEUR Workshop Proceedings, Vol. 2255, pp. 193-204, 2018.
10. A. Paradise et al., "Creation and Management of Social Network Honeypots for Detecting Targeted Cyber Attacks", in IEEE Transactions on Computational Social Systems, vol. 4, No. 3, pp. 65-79, Sept. 2017.
11. Svarovskiy S. "Approximation of membership functions for linguistic variables", Mathematical issues of data analysis, pp. 127-131, 1980.
12. M. Zuzcak and P. Bujok, "Causal analysis of attacks against honeypots based on properties of countries", in IET Information Security, Vol. 13, No. 5, pp. 435-447, 9 2019, doi: 10.1049/iet- ifs.2018.5141.
13. W. Zhang, B. Zhang, Y. Zhou, H. He and Z. Ding, "An IoT Honeynet Based on Multiport Honeypots for Capturing IoT Attacks", in IEEE Internet of Things Journal, Vol. 7, No. 5, pp. 3991-3999, May 2020, doi: 10.1109/JIOT.2019.2956173.
14. Gnatyuk S., Berdibayev R., Avkurova Z., Verkhovets O., Bauyrzhan M. "Studies on cloud-based cyber incidents detection and identification in critical infrastructure", CEUR Workshop Proceedings, 2021, Vol. 2923, pp. 68-80.
15. Gnatyuk S., Berdibayev R., Smirnova T., Avkurova Z., Iavich M. "Cloud-Based Cyber Incidents Response System and Software Tools", Communications in Computer and Information Science, Vol. 1486, pp. 169-184, 2021.
16. Maksim Iavich, Sergiy Gnatyuk, Giorgi Iashvili, Andriy Fesenko, Cyber security European standards in business, Scientific and practical cyber security journal, 2019
17. Iavich M., Gnatyuk S., Odarchenko R., Bocu R., Simonov S. (2021) The Novel System of Attacks Detection in 5G. In: Barolli L., Woungang I., Enokido T. (eds) Advanced Information Networking and Applications. AINA 2021. Lecture Notes in Networks and Systems, vol 226. Springer, Cham. https://doi.org/10.1007/978-3-030-75075-6_47