Methodology for Detecting Traces of Preparation for Cyber Attacks

Alexey N. Nazarov
Dept. of Intelligent Information Systems and Technology,
Moscow Institute of Physics and Technology,
Moscow, Russia

Abhishek Vaish
Department of IT,
Indian Institute of Information Technology,
Allahabad, India

Ilia M. Voronkov
Dept. of Intelligent Information Systems and Technology,
Moscow Institute of Physics and Technology, InterEVM
Moscow, Russia

Sunakshi Singh
Department of IT,
Indian Institute of Information Technology,
Allahabad, India

Nitish Kumar Ojha
Department of IT,
Indian Institute of Information Technology,
Allahabad, India

***Abstract*— This article proposes the order of description and classification of digital traces of the attacking object and new methodical recommendations for creating a protection function to counter cyber attacks.**

***Keywords*— cyber attacks traces, protection function, infocommunication**

I. Introduction

With the advancement of the internet connection facility there has been increase in the human computer interaction. Although it has benefited us in plethora ways but at the same time it poses security threat to our information asset [1]. So the main idea is to safeguard it from the possible intrusions [2]. Intrusion is basically an attempt to invade the system illegally and compromise the confidentiality, integrity, and authenticity of system [3]. The frameworks which act as a defense mechanism in order to recognize the possible attempt of intrusions are called intrusion detection system (IDS). IDS is a software or a hardware or concatenation of both which is considered as most promising in detecting intrusions [4], [5]. The basic problem of IDS is to identify and report malicious events from that of normal activities in a protected system [6]. Intrusion detection system can be broadly classified into host based intrusion detection system and network based intrusion detection system. The complexity of countering cyber attacks is primarily due to their high adaptability and adaptability is an important feature for Intrusion detection System Therefore, only the use of intelligent tools and countermeasures systems [7] can be a real defense against malicious intrusion.

We can assume that the life cycle of a cyber attack consists of reconnaissance followed by vulnerability exploitation and hiding in the normal traffic. Later on the attack traces are covered without generating tracks after the successful data infiltrations [8], [9].

Literature as well as practical experience suggests that the most effective way to handle counteraction against cyber attacks is their suppression at the stage of their preparation, design or, generalizing - early stage.

The possibility of organizing a global monitoring of selected risk objects in the web-space was investigated, for example, in articles [10], [11].

The complexity and variety of infocommunication technological operations, protocols leads to the fact that the practical task is to determine the identifying features (traces) of initiators of cyber attack, including terminal endings (gadgets, devices) and their owners with their individual user features at the stage of preparation or the intent of a cyber attack.

In this regard, the formal formulation of the scientific task of developing models and methods for collecting, processing and structuring information necessary for realizing the technology for identifying physical devices and users is based on an analysis of the ”traces” left by them in the information space.

II. Literature Review

For an arbitrary risk object, as a part of the information and telecommunication system, which undergoes a cyber attack in the web space, there is generally [12], [13], [14] a complete (in the cause-effect sense) system (list) of protection functions. Each protection function in general is a condition for suppressing an attack. The system of protection functions allows, on a universal methodical basis, to combine and supplement methods, tools, and information security technologies from various subject areas that do not intersect in their physical and natural essence, including regulatory legal acts.

In articles [12], [13], [14], [15], [16] methods for assessing the risk of cyber attack have been developed, formalized on the logical and probabilistic basis of the protection function and the success (failure) function of the risk object on the basis of known protection functions, and the conditions for

the success of confrontation with attack (attainability) are obtained.

The meaning of the protection function X1 is the prevention of conditions that generate destabilizing factors (DF) in the overall structure of the risk of cyber attack, it is responsible, among other things, for solving the task of identifying physical devices and cyber attackers, based on the analysis of the signs (attributes) of preparing such an attack or "traces" left by them in the information web space.

In articles [12], [13], [14], [15], [16] approaches of creation of systems of counteraction to cyber attacks on a cloud basis with application of methods of an artificial intelligence and on the basis of a neuro-fuzzy formalism are investigated. There is a need for a new development of these approaches in terms of formal statements of research tasks for algorithmic and programmatic synthesis of the $X1$ protection function for different devices and intruders at the stage of preparing a cyber attack.

III. Proposed Solution

A. Statement of probabilistic rule criterion for identification of signs of (traces) preparing a cyber attack

The process of preparing the cyber attack A targeting the chosen risk object Y and using physical devices in the cyber space, begins long before the immediate onset of the attack this is define as preparation time T. An intruder using physical tools and devices develops an attack plan, collects tools and prepares resources for an attack. In the process of preparing an attack, physical tools, devices and the attacker they leave signs (attributes) or "traces" in the cyber space.

During this time T, it is necessary to detect the "traces" with high probability due to the fact that T exists in the attack life cycle. With properly designed $X1$ - control function, taking into account the "traces" of preparing a cyber attack, the probability value P of the successful identification of the "trace" in the time T should be large, close to 1.

B. Modeling the risk of identifying a "trace"

An attacker prepares a cyber attack A targeting risk object Y in the cyberspace to achieve his criminal goal, leaving "traces" due to technological features compelling the information to register. Consequently, "traces" and their characteristics are parameters that depend on the risk object.

The process of preparing for a cyber attack should also take into account the specifics of the high-tech sub-processes Scanning port, Social engineering, Gathering information about the host machine, Vulnerability scan, Interception, Wiretapping, Emanation analysis, Traffic analysis, Reverse engineering or Spoofing like used at an early stage on the preparation of the cyber attack. And "traces" must take into account the high-tech elements of the attack, and should be somehow connected with the risk object Y.

The semantics of the essence of the risk object Y, its parameters and characteristics are inextricably linked with the process of preparing a cyber attack by an attacker. The objects of the web-space with which the risk object interacted (private offices on the banks portals, Internet shops, sites for everyday goods, personal interests sites, payment sites for various consumer services, housing and utilities, etc.) are of interest to the attacker, because there he can find useful information (personal data, accounts, etc.) to prepare a cyber attack against the risk object. And in this sense, the components of the risk object, such as data objects, logical and physical records, files, information elements, data processing and retrieval procedures, relationships between elements, interface tools, program modules, utilities, etc. are the initial data both for the preparation of the cyber attack, and for the formation of the aggregate information array of "traces" of preparation for it. Such information arrays are the basis for creating a virtual model of a physical device, tools of a cyber attack and an attacker. Such information arrays are taking into account the technological features of the risk object.

There are a large number of standards, specifications for infocommunication interaction in the web-space. Recommendation ITU-T Y.4455 (10/2017), concerning the architectural features of the Internet of things, allows at the architectural level to develop gradations of the $X1$ control function, taking into account the specifics of the "traces" and virtual models. This in turn allows us to formulate neuro-fuzzy statements of the development tasks for new technological solutions in the cloud environment to identify the "trace".

Using the latest achievements in the field of artificial intelligence is becoming a powerful tool for countering cyber attacks.

C. Implementation of the Approach - formalizing the interests of an attacking object

With the existing literature it reveals that the interaction between the elements of information risk object is process oriented in general to a tree-like hierarchical structure. This is the inherent advantage to use fuzzy sets that allows to formalizing, develop algorithmic for such processes, taking into account technological features of the risk object.

Developing the control system inspired by the approach of Prof. Ryzhov A.P. [17], [18] it can be assumed that the feature of the attacking object is a set of linguistic variables, based on the logs of the attacker device (for example, smartphone) and third parties the construction of the attacking object is sufficient to solve a particular problem(Early detection).For example, Activity in terms of "active", "medium activity", "not active"; Preferences of the content type in terms of "voice", "pictures", "video"; Preferences for the size of content in terms of "large", "medium", "small"; Time preferences in terms of "morning", "day", "evening", etc.

It is pertinent to mention that the set of linguistic variables is determined by the task (that is, we will not be bothered by the abstract completeness of the set of linguistic variables, but it will be important to understand how to build them). Formally, by analogy with the approach in [18], we will assume that the attacking object is described by a finite set of attributes $A = \{A_1, ...A_n\}$. Each attribute A_q is associated with a set U_q of its "physical" values and a set $\{a_{1q}, ...a_{n_q q}\}$

of linguistic values $1 \leq q \leq n$ (that is, a sign is a linguistic variable). To each such linguistic value a_{wq} the membership function $\mu_{a_{wq}}(u_q)$ in the universal set U_q $(1 \leq w \leq n_q)$ is mapped. Sets U_q are defined by a set of available data. This data-set are presented in the format established by law, including Internet service providers. For example, the data-set provided by Data Processing Company [18] includes recording all actions with a smart-phone (log) of 800 users in 4 weeks. The data-set presented in the format ¡identifier, transaction¿, where the transaction is in the format ¡transaction start time, application, the end time of the transaction¿, where the application is the name of one of the applications installed on the user's smart-phone, with which the work occurred at the specified time. From such a data-set we can extract various data (sets U_q), for example, the average number of calls, the average number of telephone usage per day / week and above them (sets U_q). Further to build linguistic values the features of interest can be described as A_q, $(1 \leq q \leq n)$.

Let L_i, $(1 \leq i \leq N)$ is defined as the communication channels through which the attacking object prepares a cyber attack, and the channels used to measure the attack. It can be calls, sms, chat rooms, instant messengers, social networks, etc. The Units of measurement will be time (for calls), number of characters (for sms and instant messengers), time spent in the application, etc, and may vary based on the purpose specifics of the attack against the risk object.

We denote by Δt some time interval for monitoring the list of potential attacking objects, "natural" for the problem. This time interval should be correlated with the above-mentioned time interval for the preparation of a cyber attack - T, in the sense that the aforementioned probabilistic identification criterion is fulfilled.

We will consider this Δt interval equal to the day [18]. We divide the day into elementary units - minutes and denote by Δt_j, $(1 \leq j \leq 1440)$ the time interval corresponding to the j-th minute.

Let $v_{i,j}^k$ denote the number of units spent by the k-th attacking object on the i-th channel on the j-th minute $(1 \leq k \leq K)$. For time $v_{i,j}^k$ is 0 or 1, for other units of measure (for example, symbols), this can be averaged over the typing time.

D. The partition of the universal set - Classification

Suppose we are interested in understanding the readiness of an attacking object to gather and process information about a risk object at a certain time of day. Since the attacker and his assistants are people, they must sleep, eat, relax, etc. The question arises how many such meaningful time intervals exist? There is no general answer; therefore, it is correct to choose the number of natural intervals that will ensure full coverage a universal set [0, 1440]. Result is determined by different indicators - and we will use, similarly to [18], the class imbalance and the degree of fuzziness.

To do this, we collect all the activities of all components of the attacking object for a certain time, that is, calculate for each Δt_j value

$$\overline{v}_j^k = \Sigma_{i=1}^N \overline{v}_{i,j}^k,$$

where $\overline{v}_{i,j}^k = 1$ if the k-th component of the attacking object used the i-th communication channel in time Δt_j and $\overline{v}_{i,j}^k = 0$ if the k-th component of the attacking object had no activity in a period of time Δt_j. To split the time of day, we select a "typical" attacking object (for example, the cluster center after clustering the attacking objects) and clustering the received objects $\overline{v}_j$,$(1 \leq j \leq 1440)$ with the standard c-means algorithm for a different number of clusters and calculate the clustering quality.

IV. Conclusion

The high urgency of suppressing the cyber attack at an early stage of its preparation is due to the practical need to minimize the likelihood of damage to the risk object. Determination of the fact of preparing a cyber attack on the basis of signs becomes decisive in the practical application of the arsenal of methods and tools of ensuring information security. "Knowledge" of new attacking influences and the use by an attacker of the latest achievements in the field of infocommunications predetermine the need for innovative development.

The requirement-criterion for the interval of time for identifying the fact of preparing a cyber attack on the "footprints" is formulated that allows developing new methodological recommendations for creating the protection function $X1$ in the overall structure of the risk of a cyber attack.

Due to the high technological level of the process of preparing a cyber attack with the help of physical devices and tools, formal, methodological developments are urgently needed to identify the signs of such preparation of a cyber attack on the basis of "traces", which left by technological subprocesses when an attacker performs actions using physical devices, preparing a cyber attack. The information content of such "traces", forms and formats for the representation of such information content is of scientific interest.

The aspects of creating the model of interests of the attacking object are investigated. Applicability of theoretical results from the field of fuzzy sets in this case is due to technological capabilities to understand the digital interests of the attacking object a set of linguistic variables defined on the log of the device (for example, smart-phone) of the attacker and third parties from the attacking object, sufficient to solve a particular task.

To solve the task of identifying the attacking object of the information space on the basis of an analysis of its traces in the web space, an order is proposed for describing and classifying the digital tracks of the attacking object.

References

[1] Chaipa, Sarathiel, and Mariki M. Eloff. "Towards the development of an effective intrusion detection model." Information Security for South Africa (ISSA), 2017. IEEE, 2017.

[2] I. Brahmi, S. Ben Yahia, H. Aouadi and P. Poncelet, Towards a multiagent Based Distributed Intrusion Detection System Using Datamining Approaches, System, pp. 173-194, 2012.

[3] Mukherjee, Saurabh, and Neelam Sharma. "Intrusion detection using naive Bayes classifier with feature reduction." Procedia Technology 4 (2012): 119-128.

[4] Gaddam, RaviTeja, and M. Nandhini. "An analysis of various snort based techniques to detect and prevent intrusions in networks proposal with code refactoring snort tool in Kali Linux environment." Inventive Communication and Computational Technologies (ICICCT), 2017 International Conference on. IEEE, 2017.

[5] Basics of Intrusion Detection Systems HackThis!! 2016. URL: https://www.hackthis.co.uk/articles/basics-of-intrusion-detection-systems

[6] Shafi, K., H. A. Abbass, and W. Zhu. "An adaptive rule-based intrusion detection architecture." Proceedings of the 2006 RNSA security technology conference. Canberra, Australia. 2006.

[7] Nazarov A.N. Intellectual information security on a cloud basis / Proceedings of the III Interregional Scientific and Practical Conference "Perspective directions of domestic information technologies. Crimea, Sevastopol, 19-23.09.2017. - P.26-28.

[8] LogRhythm, The APT lifecycle and its Log Trail, Tech. rep. Jul 2013.

[9] D. R. Gardner, "Breaking the Kill Chain: Stopping Data Breaches with Privileged Access Management — CA Technologies", 2015.

[10] Volkov D.A., Nazarov A.N., Nazarov M.A. The Global Threat - Shadow Internet // Collection of annual scientific papers of the International Conference "Management of the Large-Scale Systems Development" (MLSD'2014), Moscow: ICS RAS.-2014-P.452-459.

[11] Nazarov A.N., Nazarov M.A., Pantiukhin D.V., Pokrova S.V., Sychev A.K. Automation of monitoring procedures in the web-space based on the neural-fuzzy formalism // T-comm.-T.9- 2015.- No. 8.- P. 26-33.

[12] A. N. Nazarov. Estimation of information safety level of modern infocommunication networks on basis of logic-probability approach// Automation and Remote Control, Volume 68 Issue 7, 2007, pp. 1165-1176.

[13] A. N. Nazarov. Logical-and-probabilistic model for estimating the level of information security of modern information and communication networks // Telecommunications and Radio Engineering, USA, 2010, Vol. 69, 16, pp. 1453-1463.

[14] Nazarov A.N., Sychyov K.I. Models and methods for calculating the performance indicators of the hub equipment and the structural and network parameters of the next generation communication networks. - 2-nd ed., Revised and additional. - Krasnoyarsk: Publishing house of "Polikom" Ltd., 2011. - 491 p.

[15] Nazarov A.N. Evaluation of security against information attacks / / Telecommunications.-2016.- Vol. 5.- p.23-33.

[16] A. N. Nazarov. Syntez of security functions against cyber-attacks // T-comm. 2017.-VOL. 11, no.9, pp. 80-85.

[17] A. N. Nazarov. Identification of the preparation of a cyber-attack// T-comm. 2018,- in press.

[18] Ryzhov A., Novikov P. On one model of digital habits, Intelligent Systems. Theory and applications. Vol. 21, Issue. 4, 2017, pp. 91-102.