UDC 621.565.94:004.2

MACHINE LEARNING IMPLEMENTATION FOR THE CLASSIFICATION OF ATTACKS ON WEB SYSTEMS. PART 1

K. Smirnova[1], A. Smirnov[2], O. Olshevska[3]

[1,3]Odessa National Academy of Food Technologies, Odessa, Ukraine
ORCID: [1]0000-0002-3818-8083, [2]0000-0002-9459-6292, [3]0000-0002-4512-3915
Scopus ID: [3]57192687506
E-mail: [1] smirnova.kathrin@gmail.com, [2] smyrnov.aleksandr.dev@gmail.com,[3] olshevska.olga@gmail.com

Abstract: The possibility of applying machine learning is considered for the classification of malicious requests to a Web application. This approach excludes the use of deterministic analysis systems (for example, expert systems), and based on the application of a cascade of neural networks or perceptrons on an approximate model to the real human brain. The main idea of the work is to enable to describe complex attack vectors consisting of feature sets, abstract terms for compiling a training sample, controlling the quality of recognition and classifying each of the layers (networks) participating in the work, with the ability to adjust not the entire network, But only a small part of it, in the training of which a mistake or inaccuracy crept in. The design of the developed network can be described as a cascaded, scalable neural network.

The developed system of intrusion detection uses a three-layer neural network. Layers can be built independently of each other by cascades. In the first layer, for each class of attack recognition, there is a corresponding network and correctness is checked on this network. To learn this layer, we have chosen classes of things that can be classified uniquely as yes or no, that is, they are linearly separable. Thus, a layer is obtained not just of neurons, but of their microsets, which can best determine whether is there some data class in the query or not.

The following layers are not trained to recognize the attacks themselves, they are trained that a set of attacks creates certain threats. This allows you to more accurately recognize the attacker's attempts to bypass the defense system, as well as classify the target of the attack, and not just its fact. Simple layering allows you to minimize the percentage of false positives.

Keywords: Neural network, machine learning, intrusion detection system, protection of web applications, information security.

1. Introduction

The security of web applications today is one of the key tasks in the context of information security. Most sites which are available at the Internet have different vulnerabilities and are periodically attacked.

The main source of security threats for web applications are malicious users. That is, people motivated, as usual, by commercial interests. Attacks on web applications can be divided into targeted and untargeted groups. Targeted attack is an attack with a pre-selected goal and task (for example, to get a database of the prices of a product from a competitor that has not yet gone on sale, or personal data on credit cards of users of this competitor). An untargeted attack differs in that there is a definite statement of the problem, but the goal is maximally flexible (for example, any sites on which credit card data can be in a certain geo-segment of the Internet).

One of the urgent tasks in the field of information security is the creation the system for detecting non-standard, zero day attacks vector. The implementation of this task is complicated by the fact that in carrying out targeted attacks, it is almost impossible to predict all possible bundles of attack vectors and tools for impact on network objects, which leads to errors in the operation of intrusion detection systems. Another complication is that targeted attacks are mainly carried out by intruders. Highly qualified in the field of web security [4-6].

The spread of attacks on web applications is associated with two main factors: the lack of proper support for site security and a low threshold for the entry of potential attackers. In most cases, the site does not use specialized means of monitoring, detecting and preventing intrusions, the quality of design and software implementation is not paid enough attention, there are no specialists in information security in the application support staff. The proliferation of a variety of utilities and security

scanners for web applications, a large number of thematic forums and prompt publicity about the discovery of new vulnerabilities causes a low threshold for the entry of potential attackers.

2.Theoretical part

There are several approaches for identifying something: finding patterns (example, algorithmization, setting rigid frames) and a machine learning as an option for learning more intelligent actions than finding a template in the text.

If we consider a neural network "as it is" to solve such problems, in the case of one layer, we get problems of linear separability of the perceptron, which was described by Minsky [1]. In the case of multilayeredness and even a rigid threshold function, we get the problem of the unknown stage of the neural network - we can not be sure how correctly the input recognizes the first and second layers and, also, that the correct result is not the result of an erroneous separation of two similar entities.

To solve such problems it is necessary to evade standard approaches and build the mechanisms that based on fundamental principles, but the essence of them are bypassed.

When neural networks describes, the most often there is a multi-layered perceptron by Rosenblatt [2] or his converted version - Rummelhart's multi-layer perceptron [3].

Today in the tasks of machine learning is to solve the problem of class separation that are applied networks with many hidden layers, which improves the quality of classification quite well, but does not help with solving another problem - abstraction.

Let's pretend that we need to classify the type of attack, for example, a SQL injection, but with a more detailed report, with an association, and most importantly, the target with which the attacker does it, whether it is the desire to upload executable code to the server or to read the contents of the database. What does the standard multilayer perceptron model offer us? She suggests choosing an approximate number of neurons per layer empirically and for learning to use the methods of back propagation errors. But for this we need to create an excessive number of P-elements of the network. This approach will not give us the flexibility if, for example, in attack a malefactor combined vectors and tried to immediately gain access to various resources, and in learning will force to repeat many actions due to the inability to generalize certain characteristics, which will be discussed further.

How can the network be improved? To begin with, it must be separated from the view that the biological progenitor of the mathematical model of the McCulloch-Pits is the same aggregate of neurons as the multilayer perceptron [2]. The human brain is divided into zones, there are a lot of zones, the zones are interconnected with each other and neurons perform not only a generalizing effect, but, among other things, they also have a transport function. It follows that the aggregate of neurons and synapses that a person answers for recognizing images will distinguish this image from where information does not come from, and the transport function points to such a brain design and, therefore, has the opportunity to interact not only with the neurons of its group, but also with the neurons of other groups. Therefore, for the problem under consideration, let's imagine the brain as a network of networks.

What gives such an approach in practice? In practice, we can reduce the training sample, improve the quality of generalization, improve the quality of training and, most importantly, keep the processes open and understandable for analysis regarding the buildup of hidden layers, which is one of the main criteria for the safeness of artificial intelligence.

3. Practical part

Let's pretend that we are faced with the task of writing a classifier of attacks on a web application. Threats for simplicity of presentation will be considered from the world list OWASP 10.

Each type of attack separate on the elements to compile a training sample and plan the topology of the future network.

For example, SQL Injection: SQL Syntax, SQL Symbols, SQL injection type, SQL resource. This is separation of one of the most common and most dangerous vectors of attack on 4 criteria, which are important enough for classification.

If we use a standard multilayer perceptron to detect these attacks, the training sample should contain complete queries that describe the entire attack. Accordingly, the number of synaptic connections will increase, and generalize these attacks as signs - will not work. Moreover, if it is necessary to train the network to find an attempt to access the resource in this type of attacks, as well as to do it in LFI / RFI, for example, it will be necessary to find examples of a large number of attacks that contain access to resources for each class. From the above it becomes clear that from the compilation of such an excessive training sample, the instructor's time suffers the quality of the classification and the ability to generalize. Because of excessive synaptic connections, the speed of such a network is greatly reduced on each layer, and if it is necessary to add another neuron that would like to learn the simple difference between JS Code injection and XSS Injection, it will be necessary to teach it the full attack vector with, redundant examples, which makes the scaling of such a network an extremely time-consuming task.

Consider this task from the point of view of the network of networks. Let's imagine that for each attack from the OWASP 10 list there are 3 subtypes, and for each motive, there are separate markers of attributes.

For each subvector we will create and train a perceptron with the required number of S-elements, one A- and one P-element, which will answer only 1 or 0 to incoming data, producing the most primitive classification of data. In addition, in the same layer, we will construct, similarly to the first layer, additionally the necessary number of neurons with the required number of S-elements, one A-element and one P-element. These neurons will teach the signs that are necessary to classify the attacker's motive. For example, a neuron that tells us about an attempt to access data from a disk will learn the hierarchy of all the directories of the unix / windows / linux / freebsd file system of similar systems. And the neurons, which will have to catch the attempt to transfer part of the data in the encoded form - all encoding techniques.

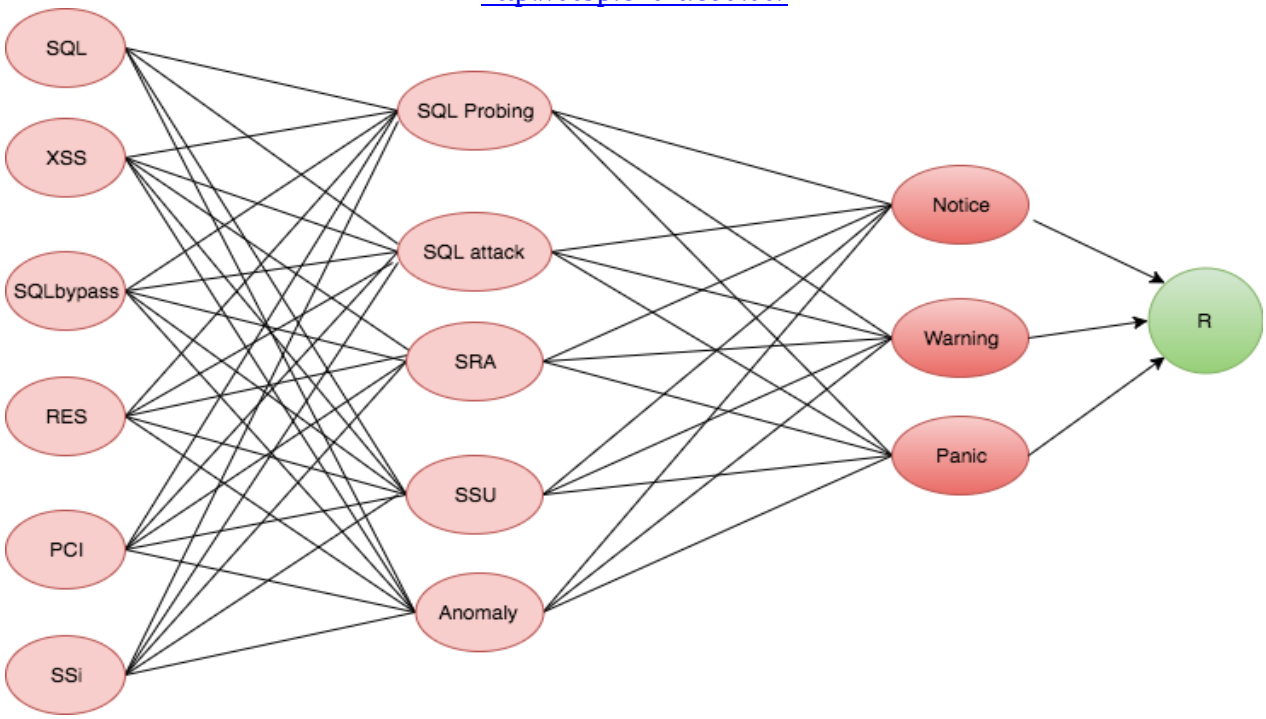

Fig. 1 – Scheme of the proposed neural network

The second neural network will be trained on a sample, which was obtained on the basis of the first network. It is now possible to generalize previously impossible things. SQL Syntax, SQL Symbols will give the SQL Injection class at the output, while individually each of them does not. In this case, for example, SQL Synax + SQL recource (SQL Synax + Resource accessing) can also give a positive conclusion.

Conclusions

Thus, the training of the second network is already on the basis of the trained first network and allows the teacher to select a sample that will not only reduce false alarms, but will also allow the second network to build a cascade of the third or fourth networks in which the threat assessment training can be conducted.

The proposed approach makes it possible to improve the quality of training of the neural network, to simplify the creation of a training sample, examples, to speed up the classification process due to the absence of redundant neural connections where this can be avoided. The approach does not pushed for using only combinations of single-layer perceptrons - more than one hidden layer is allowed.

Also, this approach allows to debug a neural network with the ability to view in detail the outputs of each of the networks, in order to identify which of them introduces an error in the operation of the entire system, which would not be possible with a single multilayer perceptron. However, before using a multi-layer perceptron, it should try to break the problem into steps that could be solved by a simple single-layer perceptron.

Recent research in the field of in-depth training describes and proves empirically the assertion that networks trained separately in layers, taking into account architecture, show much better results in all areas than networks trained by the method of back propagation of the error alone with the calculation of an approximate adjustment of the weights for convergence of output requirements to input vectors.

References

[1] Mynskyi, M., & Peipert, S. (1971). Perseptrony;
[2] Roenblat, F. (1965). Pryntsypy neirodynamyky. Pertsentron i teoryia mekhanyzmov mozgha. M;
[3] Rumelhart, D. E., & Mcclelland, J. L. (1986). Parallel distributed processing: Explorations in the microstructure of cognition: Foundations (Parallel distributed processing);
[4] Makkalok, D., & Pytts, U. (1956). Lohycheskye yschyslenyia ydei, otnosiashchykhsia k nervnoi deiatelnosty. Avtomaty. M.: YL. œ;
[5] Goseva-Popstojanova, K., Anastasovski, G., & Pantev, R. (2012, November). Using multiclass machine learning methods to classify malicious behaviors aimed at web systems. In Software Reliability Engineering (ISSRE), 2012 IEEE 23rd International Symposium on(pp. 81-90). IEEE;
[6] Schellekens, C. H. (2014). Alert classification of web application attacks: using Bayesian networks to classify alerts from anomaly based intrusion detection systems;
[7] Joseph, A. D., Laskov, P., Roli, F., Tygar, J. D., & Nelson, B. (2013). Machine learning methods for computer security (Dagstuhl Perspectives Workshop 12371). In Dagstuhl Manifestos (Vol. 3, No. 1). Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.

Література

[1] Минский М., Персептроны [Текст] / М. Минский, С. Пейперт. – М.: Мир, 1971. – 261 с.
[2] Розенблат Ф. Принципы нейродинамики. Перцентроны и теория механизмов мозга / Ф. Розенблат. – М. : Мир, 1965. – 478 с.
[3] Rumelhart D. E. Parallel distributed processing: Explorations in the microstructure of cognition: Foundations (Parallel distributed processing) / D. E. Rumelhart, J. L. Mcclelland. – Cambrige : The MIT Press, 1987. – 7 p.
[4] Маккалок Д. Логические исчисления идей, относящихся к нервной деятельности / Д. Маккалок, У. Питтс // Автоматы – М. : ИЛ, 1956.
[5] Goseva-Popstojanova K. Using multiclass machine learning methods to classify malicious behaviors aimed at web systems / K. Goseva-Popstojanova, G. Anastasovski, R.Pantev // Software Reliability Engineering (ISSRE), 2012 IEEE 23rd International Symposium. – IEEE, 2012. – C.81–90.
[6] Schellekens C. H. Alert classification of web application attacks: using Bayesian networks to classify alerts from anomaly based intrusion detection systems / C. H. Schellekens. – Eindhoven : Technische Universiteit Eindhoven, 2013. – 90 p.
[7] Joseph A. D. Machine learning methods for computer security (Dagstuhl Perspectives Workshop 12371) / A. D. Joseph [et al.] // Dagstuhl Manifestos. – Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2013. – Т. 3. – №. 1.

UDC 62–5:504.003.13

INCREASING THE LEVEL OF ENVIRONMENTAL EFFICIENCY OF INDUSTRY IS THE IMPORTANT RESULT OF ITS FUNCTIONING CONTROL

S. A. Voinova [1], D. V. Dets [2]
[1,2]Odessa National Academy of Food Technologies, Odessa, Ukraine
[1]ORCID: 0000-0003-0203-0599
E-mail: [1]voinova_s@yahoo.com

Abstract: The modern complex state of the natural environment, caused by the harmful impact of the rapidly developing world industry on it, is considered. It is pointed out the acute urgency of the utmost reduction of the harmful effects of industry. It is noted that the world's power engineering is the most active source of harmful effects increasing with acceleration on living and non-living nature. The ecological essence of the concept of energy saving is revealed. It is shown that high-quality control of the operation of technical objects is a productive means of increasing the level of ecological efficiency of enterprise *operations. A chain of interrelated circumstances that determines the strict dependence of the degree of environmental friendliness of a technical object on the quality of the control process of its operation is considered. The issues of ecological modernization of the enterprise as a means of increasing the ecological efficiency of its* enterprise *activities are considered. There are specified the components of the company's environmental efficiency in accordance with the state standard.*

Keywords: Environment, environmental friendlines, harmful impact, power engineering, energy saving, technological efficiency, ecological efficiency, functioning, technical object, control.

Introduction

World production is represented by a complex of industries that are closely interconnected by the channels of material and technical exchange and channels of energy supply - electricity and heat. The set of technical objects (TO) which included in it