Automatic Classification of Attacks on IP Telephony

Jakub SAFARIK[1], *Pavol PARTILA*[1], *Filip REZAC*[1], *Lukas MACURA*[2], *Miroslav VOZNAK*[1]

[1]Department of Telecommunications, Faculty of Electrical Engineering and Computer Science, VSB–Technical University of Ostrava, 17. listopadu 15, 708 00 Ostrava-Poruba, Czech Republic
[2]Institute of Computer Science, Faculty of Philosophy and Science in Opava, Silesian University in Opava, Bezrucovo namesti 13, 746 01 Opava, Czech Republic

jakub.safarik@vsb.cz, pavol.partila@vsb.cz, filip.rezac@vsb.cz, macura@opf.slu.cz, miroslav.voznak@vsb.cz

Abstract. *This article proposes an algorithm for automatic analysis of attack data in IP telephony network with a neural network. Data for the analysis is gathered from variable monitoring application running in the network. These monitoring systems are a typical part of nowadays network. Information from them is usually used after attack. It is possible to use an automatic classification of IP telephony attacks for nearly real-time classification and counter attack or mitigation of potential attacks. The classification use proposed neural network, and the article covers design of a neural network and its practical implementation. It contains also methods for neural network learning and data gathering functions from honeypot application.*

Keywords

Attack classification, neural network, security, SIP attacks, VoIP attacks.

1. Introduction

The IP telephony environments based on Session Initiation Protocol (SIP) is a popular design for handling telecommunication services like calls, video calls and conferences. With the growing popularity of SIP protocol also raise a potential threat. The VoIP infrastructure based on SIP is very fragile to various kinds of attacks, which can lead to loss of money and other unpleasant consequences [1].

The partial solution of this situation is in properly set VoIP servers, encryptions and strict security policies. Nevertheless, the attacker can still corrupt whole IP telephony network and stole sensitive information, eavesdrop calls, stole caller identity or deny the service for legitimate users (DoS). Intrusion detection systems, network monitoring, and honeypot applications can detect these kinds of malicious activity in VoIP infrastructure. Some applications can also mitigate specific attacks. Even then, there is still a broad spectrum of attacks, which can impact VoIP servers. All information about these attacks is logged in some kind of detection mechanism. The automatic classification of this data can provide a tool for detection various types of attacks in the network and for the further successful mitigation.

The statistical analysis of attack data brings valuable information about attacks on VoIP but is not so suitable for attack classification. The solution of the attack classification is in evolutionary algorithms. This paper brings a proposal of a classification system for VoIP-based types of attacks. With properly classified regular and malicious traffic, it is possible to reduce the number of undetected attacks. Using this classification mechanism in a distributed monitoring network with a proactive reaction can lead to a diminishing impact of attacks on IP telephony networks.

2. Honeypot Network Concept

The classification engine based on neural network is only a part of solution for detecting malicious activity in an IP telephony infrastructure. A single honeypot application could bring valuable information. Combining different application at a different geographical location and network parts should provide more detailed data with other benefits.

But this exceeding numbers of running honeypots causes unwanted overhead in a data analysis and some kind of automatic mechanism must be used. Without this mechanism lead this situation only to decreasing profit from gathered data.

The concept of a honeypot network is shown in Fig. 1 and it's based on prepared nodes and a single server for data gathering and analysis. Neural network described in this paper is a module on the centralized server for classification of VoIP based attacks. More information about distributed honeypot network could be found in a previous article [2].

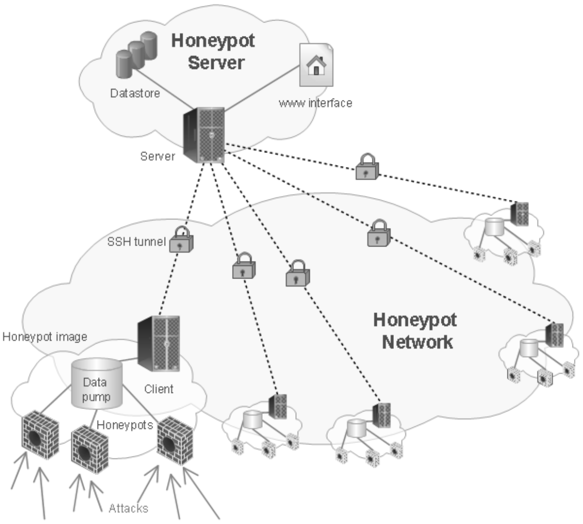

Fig. 1: The distributed honeypot network concept.

3. Neural Network

Neural networks are an attempt, which try to model information processing capabilities of the nervous system. Animal nervous system is composed of millions of interconnected cells in a complex arrangement. The artificial neural networks use the lower number of cells called perceptron.

The function of a single animal neuron is well known and serves as a model for an artificial one. But the fundamental for consciousness and complex behaviour lies in interaction between neurons. The Massive and hierarchical networking of the brain with an incredible processing rate has not yet been completely elucidated. The artificial neural network tries to handle these complex and self-organizing networks handle with various topologies. Different versions of neural network topologies are known today, and each one has its pros and cons [3].

For a VoIP based attack classification was used a feed-forward MLP (Multilayer Perceptron) neural network. This type of neural network consists of multiple layers.

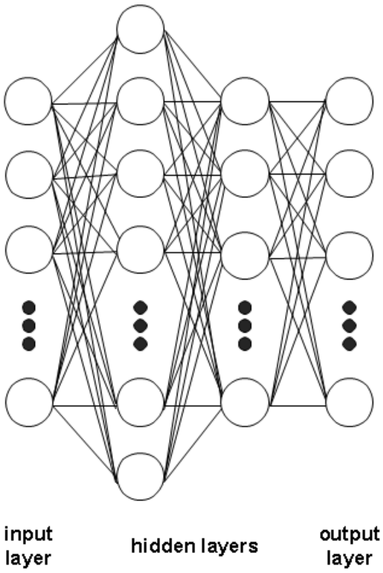

Fig. 2: MLP neural network topology.

In a MLP neural network topology, each neuron in one layer is connected to every perceptron in forward layer. This connection is so-called synapses and its purpose will be discussed later.

As shows the Fig. 2, 4 layer type of network was used. First layer serves as input layer. Each input neuron has a value of a single input parameter. All parameters for input neurons then form a single case for neural network analysis. Inner two hidden layers then solve the given problem. In this case, it is an attack classification. Each neuron itself solves a part of a solution. The last layer of the neural network is an output layer, and it represents the final set of solutions. Each output neuron is then a single class of learned attack.

3.1. Perceptron

The perceptron itself is a more general computational model than McCulloch-Pitts units. The innovation is an introduction of numerical weights and a special interconnection pattern. The activation function of neuron impact the potential of the neuron and it is also then input information transmitted to other neurons in forward layer. Inputs for this activation function are real inputs $x_1, x_2, \ldots, x_n$ from previous layers with the associated weights $w_1, w_2, \ldots, w_n$.

The output is between 0 and 1, where 0 means inhibition and 1 excitation. The final value at output (y) depends on perceptron's activation function. The activation function used for attack recognition was sigmoid, a real function $S_c : \Re \longrightarrow (0, 1)$.

$$y = S_c(z) = \frac{1}{1 + e^{-cz}}, \tag{1}$$

$$z = \sum_{i=1}^{n} w_i x_i. \tag{2}$$

As shows the Eq. (2), z parameter is a sum of output x from the previous layer multiplied by weight w of the connection. Parameter c represents a skewness of the sigmoid function (typically is 1, 0). Higher values of c bring the skewness of sigmoid closer to the step function [3], [4].

4. Backpropagation

Backpropagation represents a mechanism for neural network learning. In a feed-forward mode is information transferred from the input layer to the output layer. The backpropagation algorithm looks for the minimum error function in weight space. The combination of weights with a minimum error function is then considered as a solution of the learning problem. The solution of the learning problem is then saved in memory of neural network via weight adaptation process.

This weight adaptation is done on a training set of input with known correct outputs. With a specific learning rate is then corrected each connection weight to obtain a lower value of an error function. The backpropagation error is always counted backward as in feed-forward, so from higher layer to lower layer.

$$\delta_j = \sum_{k=1}^{n} \delta_k y_k (1 - y_k) c w_{jk}. \tag{3}$$

As show Eq. (3), backpropagation error (δ) for connection in one layer (indexed as j) is count as a sum of connections to higher layer (indexed as k). Parameter y represents the output of neuron, x its inputs. Finally c is an expected output and w weight of the connection. Then is this backpropagation error used to count a change for weight update, as shows Eq. (4) and Eq. (5):

$$\Delta w_{ij} = \eta \delta_j y_i, \tag{4}$$

$$w_{ij} = w_{ij} + \Delta w_{ij}. \tag{5}$$

The parameter η serves as a learn rate parameter for selecting a proper step of correction in one backpropagation iteration [3], [4]. w_{ij} represents connection weight from the previous layer i to actual layer j (Fig. 3).

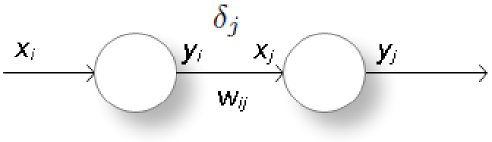

Fig. 3: Indexing between layers.

5. Practical Implementation

5.1. Neural Network Parameters

As was mentioned above a multilayer perceptron neural network was used for VoIP attack classification. The final neural network contains 10 input layer neurons which correspond to specific input parameters. The two hidden layers contain 16 and 12 neurons. The output layer, where each neuron specifies one class of attack type, contains 6 neurons.

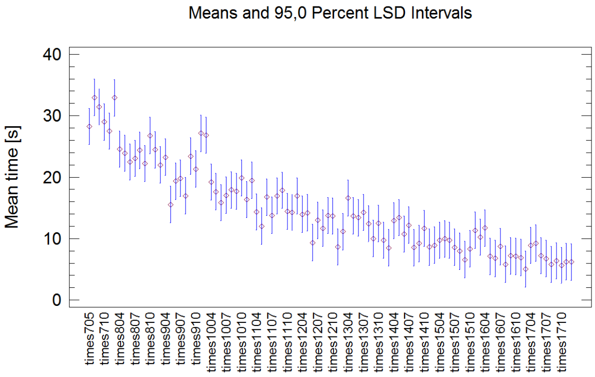

Fig. 4: 100 Backpropagation cycles mean time for different configurations of hidden layers.

The inner structure of neural network is based on tests of convergence for 100 backpropagation cycles. These tests prove different mean times of learning for different structures as shows Fig. 4. The impact of a structure is evident only for backpropagation learning. Because forward MLP classification use already learned neural network. This neural network then classifies the attack regardless of the inner structure of neural network. The test shows statistically significant difference between learning time of neural networks. Best results have a configuration with 16 neurons in first hidden layer and 10 neurons in second hidden layer.

The higher number of neurons in these layers is possible to decrease the mean time needed for neural network learning, but the memory requirement also raises. From a statistical point of view, there is not a statistically significant difference between learning mean times for neural network backpropagation learning with a confidence interval of 5 %. Final neural network configuration uses the following number of neurons 10 16 12 6 (from input to the output layer).

Other specific parameter for this neural network is a skewness of an activation function. This activation function is a sigmoid function with skewness set to 1, 0.

5.2. Data Source for Classification

The data for classification with neural network is collected with an open-source honeypot application Dionaea. This multi-service oriented honeypot was used for its PBX emulation feature. It is possible to monitor and emulate typical behaviour of a SIP PBX with Dionaea.

The Dionaea attack log contains only information about malicious traffic. Because it is a honeypot application, no legitimate calls are connected with it, and even no regular end-point device tries to register to it and make calls. So it contains only information about malicious traffic.

All attack data store Dionaea in a sqlite database file. This database consists of several tables. Each table contains various information. This information is bind on traffic or protocol emulated by the honeypot. Most of this information is based on a request, response mechanism. So selecting a single line from the database for classification is valueless. All data about SIP attacks must be aggregated from different tables. Then is prepared a list of detected attacks. Each row in this list is a specific attack detected on an emulated SIP server. From all accessible attack features was created an array of 10 parameters. These individual 10 parameters serve as an input for a neural network classification and are following: used transport protocol (tcp – 0, udp – 1), connection count, REGISTER message count, INVITE message count, ACK message count, BYE message count, CANCEL message count, OPTIONS message count, SUBSCRIBE message count and connection rate. The connection count parameter is the number of connection made in one SIP session on the server. The connection rate is then a ratio of received SIP messages to connection count.

5.3. Backpropagation Algorithm

For a neural network learning was used a backpropagation algorithm. Whole network is evaluated as learned, when the network correctly identify more than 95 % samples of the training set. So the confidence interval for neural network learning is always lower than 5 %.

On the beginning of backpropagation learning are weights of connections randomly selected from the interval (-1, 1). When all weights are randomly set, the backpropagation algorithm starts. After each 100 cycles of backpropagation learning is checked the successfulness of attack classification. When is successfulness higher than 0, 95, the neural network learning is done. Otherwise, continues more backpropagation learning cycles.

There is also a possibility that the learning algorithm is stucked in a local minimum, and final successfulness cannot reach desired 0, 95. If the neural network is not successfully learned after 2 500 000 backpropagation cycles, the learning starts again with a randomly selected connection weights.

5.4. Training Set

The training set is one of most important parts of neural network learning. If the items in the training list are not a specific representative of an attack group, attack cannot be successfully classified.

As a source for the training set were used a real malicious traffic. Honeypot captured these attack data for a period of two months. All these attacks were aggregated and then one by one classified by human into six classes. These classes are call testing, client registration attempt, flood attacks, registration attempts, PBX scanning and the last unknown group.

When were all attacks classified, specific representatives of each class were chosen for the training set. The final training set contains 78 attacks, which means that each attack class has 13 subjects.

To increasing the impact of a SIP message counters are all parameters powered to four. After a successful backpropagation learning is possible to classify single attacks. As a final attack class is then chosen the output layer neuron with the highest potential.

6. Conclusion

In typical nowadays IP networks are used some form VoIP services. The SIP protocol is an open-source standard for this purposes and also one of the most used protocols for handling VoIP services. This situation leads to higher exposition of this text based protocol to the various types of attacks. Previous researches in our lab prove a high vulnerability of a SIP server to different types of attacks [4], [5].

One way for improving security of whole IP telephony infrastructure lies in deployment of a monitoring mechanism. This monitoring mechanism based on distributed net of monitoring nodes can detect malicious activity in the network. With a possibility to change firewall rules or network routing even mitigate potential threats. The proposal is described above, and the main part of a monitoring node is a honeypot application. In case of a SIP protocol monitoring, this honeypot application is open-source Dionaea.

But to improve network security from data gathered at different honeypots, some kind of analysis must be made. Classification by humans is very precise, but also time consuming and expensive. An automatic classifying mechanism could bring a solution for the problem of VoIP attack classifying.

With a properly learned neural network, it is possible to classify various types of attacks. This article aims at describing a neural network design for VoIP attack classification.

One of the biggest disadvantages of this solution is that it cannot recognize a new type of attack. Whole neural network topology and learning set are prepared only for specific types of attacks. But even with this functionality is possible to use this neural network as a classifying module in distributed monitoring networks.

Future plans for this neural network attack classification lie in deploying other types of neural networks and testing its fitness for IP telephony attacks classification. One of the challenges is also in an implementation of self-learning mechanisms.

Acknowledgment

The research leading to these results has received funding from the Grant SGS no. SP2013/94 and has been partially supported by the project No. CZ.1.07/2.3.00/20.0217 "The Development of Excellence of the Telecommunication Research Team in Relation to International Cooperation" within the frame of the operation programme "Education for competitiveness" financed by the Structural Funds and from the state budget of the Czech Republic.

References

[1] SAFARIK, J., M. VOZNAK, F. REZAC and L. MACURA. Malicious Traffic Monitoring and its Evaluation in VoIP Infrastructure. In: *2012 35th International Conference on Telecommunications and Signal Processing (TSP)*. Prague: IEEE, 2012, pp. 259–262. ISBN 978-146731118-2. DOI: 10.1109/TSP.2012.6256294.

[2] VOZNAK, M., J. SAFARIK, L. MACURA and F. REZAC. Malicious Behavior in Voice over IP Infrastructure. In: *Recent researches in communications and computers proceedings of the 16th WSEAS International Conference on Communications*. Kos Island: WSEAS, 2012, pp. 178–182. ISBN 978-1-61804-109-8.

[3] ROJAS, R. *Neural Networks*. New York: Springer-Verlag, 1996. ISBN 35-406-0505-3.

[4] HEATON, J. *Introduction to Neural Networks for JAVA, 2nd Edition*. St. Louis: Heaton Research, 2008. ISBN 16-043-9008-5.

[5] REZAC, F., M. VOZNAK, K. TOMALA, J. ROZHON and J. VYCHODIL. Security Analysis System to Detect Threats on a SIP VoIP Infrastructure Elements. *Advances in Electrical and Electronic Engineering*. 2011, vol. 9, no. 5, pp. 225–232. ISSN 1336-1376.

[6] VOZNAK, M. and J. SAFARIK. SIP Proxy Robustness against DoS Attacks. In: *Proceedings of the Applied Computing Conference 2011, (ACC '11)*. Angers: Neuveden, 2011, pp. 223–227. ISBN 978-1-61804-051-0.

About Authors

Jakub SAFARIK received his M.Sc. degree in telecommunications from VSB–Technical University of Ostrava, Czech Republic, in 2011 and he continues in studying Ph.D. degree at the same university. His research is focused on IP telephony, computer networks and network security. He is with CESNET as a researcher since 2011.

Pavol PARTILA received the M.Sc. degree from University of Zilina, Faculty of Electrical Engineering in 2011. Currently, he is working toward the Ph.D. degree at the Dpt. of Telecommunications, VSB–Technical University of Ostrava. Topics of his research interests are Speech processing, speech quality and VoIP.

Filip REZAC was born in 1985. He received M.Sc. degree in telecommunications from VSB–Technical University of Ostrava, Czech Republic, in 2009 and he continues in studying Ph.D. degree at the same university. His research is focused on IP telephony, computer networks and network security. He is with CESNET since 2009 as a researcher.

Lukas MACURA is a Ph.D. student with Dpt. of Telecommunications at Faculty of Electrical Engineering and Computer Science, VSB-Technical University of Ostrava. He is also administrator of SIP infrastructure within CESNET where he is employed as a researcher with Dpt. of Multimedia, CESNET, Czech Republic.

Miroslav VOZNAK was born in 1971. He holds the position as an associate professor with Department of Telecommunications, VSB–Technical University of Ostrava, Czech Republic. Topics of his research interests are the Next Generation Network, IP telephony, speech quality and network security. He is with CESNET since 1999, currently in R&D department.