Fast Learning Neural Network Intrusion Detection System

Robert Koch[1], Gabi Dreo[2]

Universität der Bundeswehr München
Werner-Heisenberg-Weg 39, 85577 Neubiberg, Germany
{Robert.Koch, Gabi.Dreo} @UniBw.de

Abstract. Assuring the security of networks is an increasingly challenging task. The number of online services and migration of traditional services like stocktrading and online payments to the Internet is still rising. On the other side, criminals are attracted by the values of business data, money transfers, etc. Therefore, safeguarding the network infrastructure is essential. As *Intrusion Detection Systems (IDS)* had been in the focus of a numerous of researches for the last years, several sophisticated solutions had been found. Very capable IDS are based on neural networks. However, these systems lack of an adaptability to dynamic changing environments or require a protracted learning phase before they are operational. The approach is to overcome these restrictions by introducing a modular neural network based on pre-processed components supplemented by static policies. By that, it is possible to overcome long-lasting learning phases.

1 Introduction

The availability of services, communication lines and the network infrastructure is of essential relevance. For that, failures, attacks and other kinds of anomalies have to be detected as soon as possible. Beside firewalls, IDS are key elements for securing network infrastructures nowadays. Traditional IDS analyze the network traffic for the appearance of known patterns. Either only the headers of the packets are analyzed or also the payload, whereas analyzing the whole payload is not always possible due to performance reasons. Furthermore, pattern-based analysis is hardly able to detect new and unknown attacks.

Newer approaches examine the network infrastructure as a whole. *Network Security Situational Awareness (NSSA)* considers all information about the network, not only intrusions. The security engineer is aware of what is happening on the network [1]. In *Network Behavior Analyses (NBA)*, anomalies are detected by evaluation of the network traffic statistics. Newer routers and switches are able to generate and allocate statistics about the traffic flow through the device. Important protocols are *NetFlow* (RFC 3954) from Cisco which is now under further vendor-independable development known as *Internet Protocol Flow Information Export* (RFC 3917) on the one side, and sFlow (RFC 3176) on the other. By using flow information it is possible to detect unknown and new threats

because of the divergence of the statistics to the normal network behavior in the case of an attack. Very efficient systems for the evaluation of the data are based on neural networks. Due to their ability to find behavioral patterns in the attack which could be learned [2], detection of yet unknown attacks is possible. *Modular Artificial Neural Networks (MANNs)* and hierarchical ones are better adaptable to dynamic environments. Modular networks divide the task into multiple subproblems while in a hierarchical network every node can be a neural network on its own. By combining NBA techniques with neural networks it is possible to perform online-learning and to recognize new and unknown threats.

Anyway, there are still major shortcomings: Depending on the respective realization, neural networks suffer from long lasting learning phases. Things are getting worse if the learning phase is carried out in a manipulated, non-isolated environment, because that can force the network to accept attack behavior in the final system. After finishing the learning phase, they are only able to adapt to changing environments by introducing special structures and methods. Therefore, neural networks with fast and secure learning phases are needed.

An overview of current researches will be given in the next paragraph, while section 3 describes our proposed approach.

2 Current Research

There are numerous studies in the area of IDS. Simple pattern-matching based IDSs are very efficent for detecting malicious traffic, but only known and available patterns could be found. Therefore, IDSs based on neural networks have been investigated which are able to detect new and unknown attacks. Anyway, after the network is trained, adaptability to changing environments is hard to accomplish. Possibilities to overcome these restrictions are enabled by the concepts of modular and hierarchical systems. In [3], Berg and Spaanenburg show that compositionality of MANNs is possible under further conditions, parallel and cascade (de-)composition are shown. Zhang et al. use hierarchical networks to construct a modular IDS [4]. The structure of the system consists of multiple layers and classifiers. First, a serial structure is used, later on some of the shortcomings of the serial structure are solved by using a parallel structure. Basically, an anomaly classifier detects either the packet is "normal" or not. Suspect packets are stored in a database and structured by a clustering algorithm. After exceeding a threshold value, a new classifier is trained.

For building neural networks with faster learning abilities, Moraga [5] shows that by including knowledge of the problem in the design phase, the effectiveness of the network can be increased. Doing that, he was able to construct the neural network without the need for a learning phase. Almgren et al. [6] reduce the learning data by allowing the algorithm to decide which data should be used next. By addressing the dynamics of the environment, some appendages for realizing online-learning capabilities in neural networks are done. Potter proposed a *Learning Intrusion Detection System* based on a blackboard architecture [2]. A learning layer is introduced as an additional layer in a multi-tier concept,

which is able to maintain and update the training data for the network. By using multiple agents it should be more efficient in a dynamic environment.

NBA and NSSA are concepts to examine the current state of the whole network. Rehak et al. present an approach for NBA to reduce the error rate and the number of false positives. This is done by designing a framework for the integration of different anomaly detection algorithms. By this a value for the trustfullness of the current traffic is generated. *Extraction Method of Situational Factors for NSSA* [1] describes methods for the evaluation of *situational factors*, for example a special type of intrusion.

Even there exist multiple implementations, there are still major drawbacks. Neural networks have to be trained for the operational environment. Furthermore, attacks from the inside of the local network, for example by manipulating a switch or performing a replay attack, are hardly to detect and can undercut the integrity of a neural network based system in the learning phase.

3 The Idea: Fast Learning Neural Network IDS

To overcome the long learning phases and the resulting threat of learning attack behavior as valid behavior, we use a MANN. Fig. 1 gives an overview of the system. The traffic as well as the flows which are to be analyzed will be processed by the MANN. Further on, the data available by routers, switches and network scans will be used to implement policy-based rules about the network structure.

Unlike existing approaches, the initial MANN will be constructed by the usage of pre-processed modules. These modules are devided into two groups: service- and infrastructure-oriented. The former ones are designed and trained to detect anomalies in the network traffic of different services, like the hypertext transfer protocol, by learning the protocol-specific communication behavior in a secured environment. The later ones are used to detect changes in the network infrastructure like connecting new devices. In the inital network, only a few infrastructure-oriented pre-processed modules could be used, because for these modules, a generalization is not possible.

To overcome the lack of knowledge in the beginning, static data is used to monitor the network structure. For example, this could be the switch and port a host is connected to. By the use of policies, the allowed and restricted possibilities to integrate new devices and services into the network can be specified. While these are strict guidelines for the early operation of the IDS, it allows to detect the endangerment of learning forbidden network operations. If a violation of a policy is detected by the system, it informs the operator who can decide to stop or to continue the learning process of the neural network. After the learning phase of the infrastructure-oriented modules, a finer classification is available, for example by using typical load distribution, response times, etc.
Normally, the NBA is not able to detect slowly driven attacks, because of the necessity to excess a threshold to raise an alarm. The *Infrastructure and Service Policies Module* can also be used for the detection of slowly driven attacks, if they are violating the given policies. Therefore, several violations of policies are

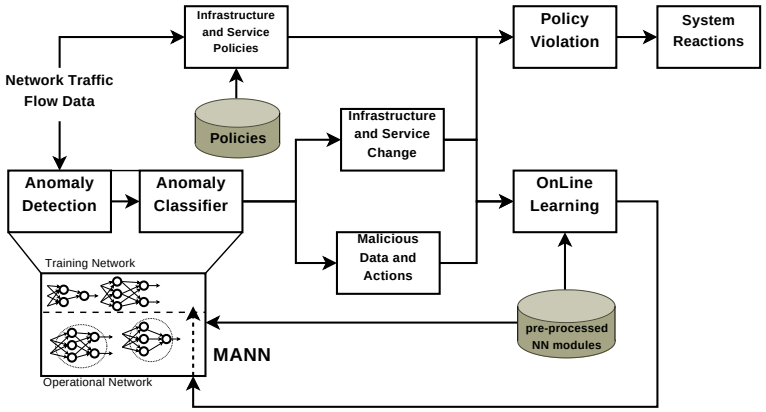

Fig. 1. Overview of the System Structure. Pre-processed modules are used to build the inital operational MANN. Additional MANN components are trained before transferred to the operational network. The policy module defines additional strict rules.

secured in a long term matrix and evaluated by using a time lapse function. Detected anomalies are forwarded to the MANN for further investigations.

Summarized, the IDS will consist of an initial neural network and an additional component for monitoring static policies. The initial system is generated by composition of the selected pre-processed modules. In the beginning these are the modules that are responsible for the services in the network, while the infrastructure is described by the policies set. Only the training network is modified during the learning phase and transferred to the operational network to discrete points in time. providing the possibility to execute a roll-back of the training network. Hereby, the initial learning effort and furthermore the endangerment of a manipulation of the learning phase is reduced to a minimum.

References

1. Wang, H., Liang, Y., Ye, H.: An Extraction Method Of Situational Factors For Network Security Situational Awareness, International Conference on Internet Computing in Science and Engineering, 2008.
2. Dass, M., Cannady, J., Potter, W.: A Blackboard-Based Learning Intrusion Detection System: A New Approach LNAI 2718, IEA / AIE 2003
3. Berg, A., Spaanenburg, L.: Modular and Hierarchical Specialization in Neural Networks, Journal of Electrical and Electronics Engineering, Volume 3, Number 1, 2003
4. Jiang, J., Zhang, C., Kamel, M.: Intrusion detection using hierarchical neural networks, Pattern Recognition Letters 26, Elsevier 2005
5. Moraga, C.: Design of Neural Networks, Knowledge-Based Intelligent Information and Engineering Systems, Lecture Notes in Computer Science, Volume 4692/2008
6. Almgren, M., Jonsson, E.: Using Active Learning in Intrusion Detection, Proceedings of the 17th IEEE Computer Security Foundations Workshop, CSFW04