Multi-Agent Approach to Network Intrusion Detection*

(Demo Paper)

Martin Rehak
Center for Applied Cybernetics
FEE, Czech Technical
University in Prague

Michal Pechoucek
Department of Cybernetics
FEE, Czech Technical
University in Prague

Pavel Celeda
Institute of Computer Science
Masaryk University

Vojtech Krmicek
ICS, Masaryk University

Martin Grill
CESNET, z. s. p. o.

Karel Bartos
CESNET, z. s. p. o.

ABSTRACT

Our demo presents an agent-based intrusion detection system designed for deployment on high-speed backbone networks. The major contribution of the system is the integration of several anomaly detection techniques by means of collective trust modeling within a group of collaborative detection agents, each featuring a specific detection algorithm. The principal role of anomalies is to provide the input into the trust modeling stage of the detection, where each agent determines the flow trustfulness from aggregated anomalies. The aggregation is performed by extended trust models that model the trustfulness of generalized situated identities, represented by a set of observable features. The system is based on traffic statistics in NetFlow format acquired by dedicated hardware-accelerated network cards, and is able to perform a real-time surveillance of the gigabit networks.

Categories and Subject Descriptors

I.2.11 [**ARTIFICIAL INTELLIGENCE**]: Distributed Artificial Intelligence—*Intelligent agents*

General Terms

Security

Keywords

trust, intrusion detection, network behavior analysis

1. INTRODUCTION

Network Intrusion Detection Systems are designed to protect the computer networks by observing the network traffic and notifying the operators when a possible attack happens. **CAMNEP** is a system that performs an online analysis of traffic statistics by a group of collaborative detection agents, each of which embeds an anomaly detection model. This model predicts the status of the traffic and determines the anomaly of each flow by comparing the observed traffic features with the prediction. Direct deployment of such anomaly detection techniques is not practical, as they suffer from very high error rate. The traffic model is rarely perfect, and given the relatively low ratio of anomalous traffic in the volume of normal traffic, most investigated incidents turn out as misclassified legitimate traffic (false positives). CAMNEP addresses this problem by the use of classic agent techniques, specifically **trust** and **reputation**, to improve the quality of individual agent's classifications.

The information provided to the detection agents uses the NetFlow format, which aggregates the information about network flows, unidirectional components of TCP connections (or UDP, ICMP equivalent) identified by common source and destination IP address and ports, together with the protocol, and delimited by the time frame used for data acquisition. The system does not use the content of the transmitted data. It is designed to detect the attacks that are significant from the network perspective, such as horizontal scanning (used to map the network for on-line hosts, and used for worm and malware propagation), vertical scanning (used to determine the services offered by a host), denial of service attacks and other relevant events.

2. AGENT-BASED IDS ARCHITECTURE

In our approach, we have decided not to develop a novel detection method, but rather to integrate several existing methods [2] with an extended trust models of a specialized agent. This combination allows us to correlate the results of the used methods and to combine them to improve their effectiveness. The solution consists of several layers:

Traffic Acquisition and Preprocessing Layer: The components in this layer acquire the data from the network using the hardware-accelerated NetFlow probes and perform their preprocessing. This approach provides the real-time overview of all active unidirectional connections on the observed network. In order to speed-up the attack detection,

*This material is based upon work supported by the European Research Office of the US Army under Contract No. N62558-07-C-0001. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the European Research Office of the US Army. Also supported by Czech Ministry of Education grants 1M0567 and 6840770038

Cite as: Multi-Agent Approach to Network Intrusion Detection (Demo Paper), M. Rehak, M. Pechoucek and P. Celeda, *Proc. of 7th Int. Conf. on Autonomous Agents and Multiagent Systems (AAMAS 2008)*, Padgham, Parkes, Müller and Parsons (eds.), May, 12-16., 2008, Estoril,Portugal,pp.1695-1696.

the preprocessing layer aggregates meaningful global and per-flow (or group of) characteristics and statistics.

Cooperative Threat Detection Layer: This layer principally consists of specialized, heterogeneous agents that identify the attacks in the preprocessed traffic data by means of their extended trust models [1]. Their collective decision regarding the degree of maliciousness of a flow with certain characteristics uses a simple reputation mechanism.

Operator and Analyst Interface Layer: This layer handles the interaction with the network operator. The main component is an intelligent visualization agent that helps the operator to analyze the output of the detection layer, by putting the processed anomaly information in context of other relevant information.

2.1 System Use-Case

In order to illustrate the capabilities of the system from the user (e.g. network administrator or incident analyst) perspective, we will present the analysis of one particular attack detected by the system. Specifically, we will present an TCP vertical scan attack (SYN and CONNECT scan).

The main concept introduced by the system is the trustfulness of the flow (a value in the $[0, 1]$ interval, aggregated from the individual trustfulness as reported by the agents), which is determined for each flow. The system then uses this value to build a histogram of the traffic in each observation interval over the trustfulness spectrum (as shown in Figure 1). Trustfulness is an estimate of flow legitimacy. The flows that are accumulated at the left side of the histogram are therefore considered as malicious, while the bulk of the legitimate traffic is on the right side of distribution.

The major functionality of the system is its ability to acquire the real-time traffic statistics, aggregate them in a meaningful manner and classify them by their trustfulness. In practice, this means that the administrator can concentrate its attention to the set of flows identified by the system as untrusted – in our pilot deployment on a university campus, this meant that instead of analyzing 50000 lines of data (one for each flow), the operator can efficiently investigate up to 5 incidents that occurred in the given period.

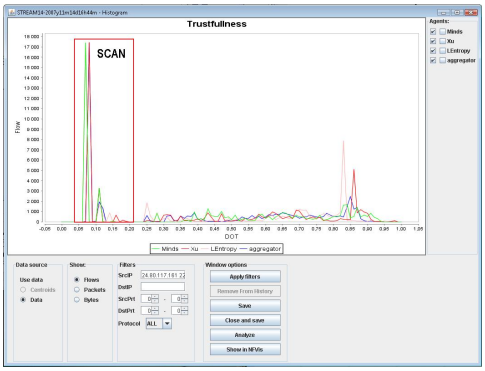

Figure 1: Traffic histogram during an attack (highlighted peaks with the trustfulness around 0.1). Note that the attack traffic (including the response) is clearly separated from the rest of the legitimate traffic.

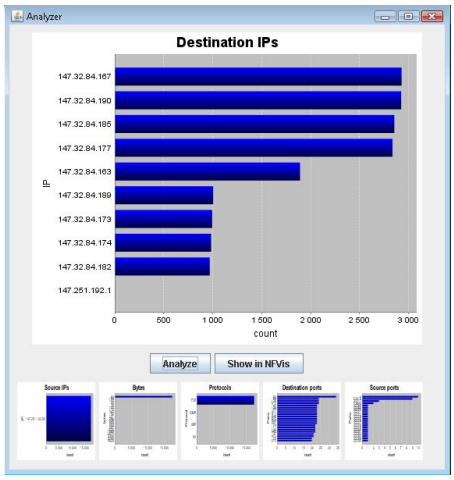

Figure 2: Properties of the leftmost scan peak in the analysis interface. Note that all the packets share the same source IP address and size (60 bytes). Destination IP addresses (i.e. scan victims) are shown, with the number of flows towards them.

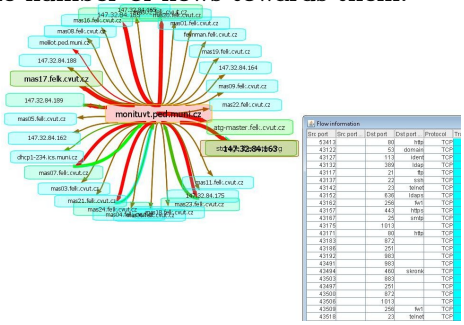

Figure 3: Operator's view of the attack through the *Visio Agent* with applied filtering.

3. CONCLUSION

The deployment of the system significantly changes the requirements on the work of the network operator or incident analyst. Currently, the network traffic statistics (and other logs) are studied reactively, when the consequences of the attack are perceived or when the administrators investigate a third-party complaints. CAMNEP deployment enables the operators to perform a real-time surveillance, and to act proactively. The fact that the system effectively clusters the flows by similarity and ranks the clusters with trustfulness aggregated from data also significantly facilitates the analysis of basic incident types, and decreases the qualification requirements on the analysts.

4. REFERENCES

[1] M. Rehak and M. Pechoucek. Trust modeling with context representation and generalized identities. In *Cooperative Information Agents XI*, number 4676 in LNAI/LNCS. Springer-Verlag, 2007.

[2] M. Rehak, M. Pechoucek, K. Bartos, M. Grill, and P. Celeda. Network intrusion detection by means of community of trusting agents. In *IEEE/WIC/ACM International Conference on Intelligent Agent Technology (IAT 2007 Main Conference Proceedings) (IAT'07)*, Los Alamitos, CA, USA, 2007. IEEE Computer Society.