MULTI-AGENT SECURITY SYSTEM BASED ON NEURAL NETWORK MODEL OF USER'S BEHAVIOR

N. Kussul, A. Shelestov, A. Sidorenko, V. Pasechnik,
S. Skakun, Y. Veremeyenko, N. Levchenko

Abstract: It is proposed an agent approach for creation of intelligent intrusion detection system. The system allows detecting known type of attacks and anomalies in user activity and computer system behavior. The system includes different types of intelligent agents. The most important one is user agent based on neural network model of user behavior. Proposed approach is verified by experiments in real Intranet of Institute of Physics and Technologies of National Technical University of Ukraine "Kiev Polytechnic Institute".

Keywords: neural network, multi-agent system, network security system, user behavior model, intrusion detection system.

Introduction

During last decades information technologies based on the computer networks play an important role in various spheres of human activity. Problems of great importance are entrusted on them, such as keeping, transmission and automation of information processing. The security level of processed information can vary from private and commercial to military and state secret. Herewith the violation of the information confidentiality, integrity and accessibility may cause the damage to its owner and have significant undesirable consequences. Thus the problem of information security is concerned. Many organisations and companies develop security facilities that require significant contributions. On the other hand, the impossibility of creating completely protected system is a well-known fact – it will always contain mistakes and «holes» in its realization.

To protect computer systems such accustomed mechanisms as identification and authentication, mechanisms of the delimitation and restriction of the access to information and cryptographic methods are applied. However they possess following drawbacks:

- exposure from internal users with malicious purposes;
- difficulties in access differentiation caused by information resources globalisation, which washes away differences between "own" and "foreign" subjects of the system;
- reduction of productivity and communication difficulties due to mechanisms for access control to the resources, for instance, in e-commerce;
- simplicity of passwords definition by making combinations of simple users' associations.

Therefore logging and audit systems are used along with these mechanisms. Among them are Intrusion Detection Systems (IDS).

The Intrusion Detection Systems

IDS are usually divided to systems detecting already known attacks (misuse detection systems) and anomaly detection systems registering the life cycle deviations of the computer system from its normal (typical) activity. Besides, IDS are subdivided to network-based and host-based types by information source. Herewith they can be as real-time (online), so offline.

Network-based IDS analyse network dataflow, protecting its participants, practically not affecting the productivity of their work. Network-based systems do not use information about processes from separate workstation. In turn, the host-based systems are installed on the separate computers and analyse information from their logging mechanisms.

If IDS is real-time an attack can be registered on the stage of its preparation and warned on the stage of its generation (that is more preferable). In this case there is no need to store large amounts of logged data. However the real-time host-based IDS may vastly influence upon the system productivity.

In contrast there are offline systems, which, as a rule, are activated at night or at any other time, when workstation load is low. Thereby, they do not use system resources, necessary for other tasks. Their drawbacks: to analyse information it is necessary to save sufficient amount of audit-data logged during observation, and reaction on attacks is greatly remitted.

At present a lot of IDS are developed. Among them are: Haystack, GrIDS, NIDES, ASAX, DARPA, EPIC2, snort and others. They have made the significant contribution to development of IDS. These systems are based on different algorithms. The main trends are:

- Building activity graphs (Graph-based Intrusion Detection System – GrIDS) in which nodes represent hosts and edges represent network activity among them. The detection technique is to compare graph to a known pattern of intrusive activity.
- Statistical deviation detection methods (Next Generation Intrusion Detection Expert System – NIDES). These systems are the prime examples of anomaly detection systems.
- Employing expert evaluations. In this approach more scalability is achieved by hierarchical arrangement of the expert systems (Extensible Prototype for Information Command and Control – EPIC2).

Main drawbacks of the described IDS are:

- high probability of the false positive and false negative warnings;
- primitive mechanisms of determining new, unknown in advance intrusions;
- unstable reaction to distributed attacks;
- need of human expertise during all the working time.

To eliminate such defects new approaches were developed. They allow to build completely or highly automated IDS [1]. These approaches are mainly directed on “intellectualisation” of IDS. Among them:

1. Use of neural networks [2,3], genetic algorithms, utilising variable-sized Markov chains [4] etc.
2. Systems based on agent approach [1,5].

It is known, that approximately 70% of attacks are initiated from the inside of network. It might be as password stealing, so using vulnerabilities of information security and the software. So, modern approaches actively use the user behavior model.

Developing IDS it is also necessary to take into account distributed nature of attacks on computer network. All these factors show agents approach to be more preferred for creating the security systems.

Agent paradigm

The agents system is meant to be the system of interacting agents. They are coordinated by general global purpose (the strategy) but autonomous enough to realize their own tasks within the framework of the general strategy (the own tactics).

Importance of transition to agent paradigm is compared with importance of using object-oriented approach. Agent technology can be effectively applied in different areas of information technology, e.g. computer networks, software development, object-oriented programming, artificial intelligence, human-machine interaction etc.

Main advantages of intelligent agent systems are as follows.

- Distribution. Functional independence of system parts, ability of solving heterogeneous tasks from all domains.
- Intelligence. The ability to adapt to the changing environment.
- Scalability. Property that makes possible solving new tasks without bringing significant changes to the system architecture.

System structure and functionality

Integrated network IDS should detect different attack types (known and unknown) and anomaly activities. To meet these requirements it should contain various (rather autonomous) interactive modules. Such architecture can be implemented on the base of agent approach. An important role is played by User Agent that should monitor the user behavior and detect anomalies in its activity. Other types of agents are responsible for other aspects of security.

- User Agent. This agent allows detecting anomalies in user activity on base of neural network user model. It predicts user actions on the base of the model and compares them to real activity. But we should take into account that behavior of the same user differs for various operating systems. Consequently, User Agent is developed for each type of operating system available in the network (e.g. Win2000, 98, XP, Free BSD).
- Host Agent. Performs system calls processing and detects anomalies and known types of attacks. For example, it allows detecting “Trojan horse” attacks.
- Network Agent. Operates at the firewall and analyses the network traffic. The information extracted from packets is used to detect known attacks and anomalies in the network. It may be done utilising neural network and probability approaches (e.g. Bayesian networks and variable-sized Markov chains).
- Server Agents. Group of agents is responsible for the server security.
- Controller Agent. Responsible for anomalies analysis and detection of distributed attacks in scale of whole system, initialising agents, interaction with database and between various parts of the system.

The structure of proposed system is shown in Fig. 1.

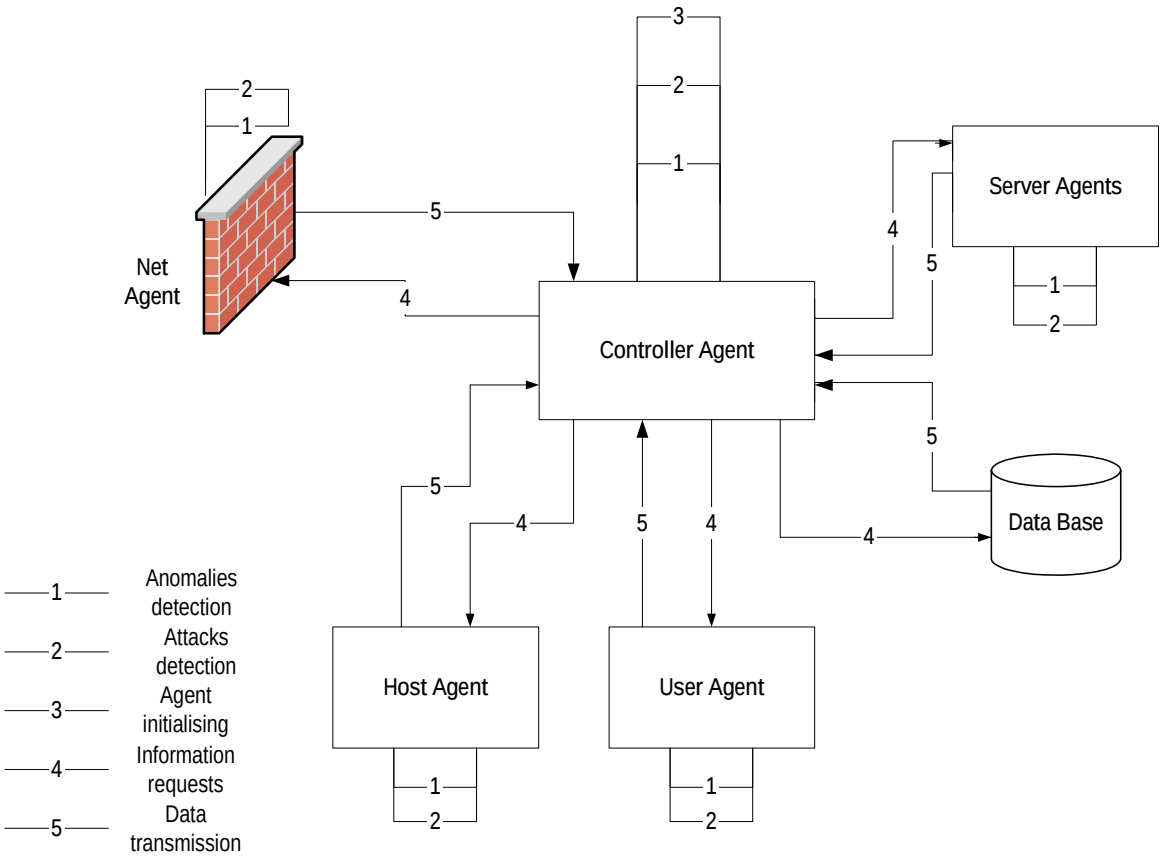

Fig. 1. System structure.

As the user logs on, Controller Agent creates correspondent User Agent and initialises it. During the user session agent controls the user's activity on the base of neural network behavior model. At the same time it picks data for behavior model correction. When the session is finished it sends data for database update. In

the case of anomaly detection User Agent informs Controller Agent about suspicious activity. Host Agents and Server Agents detect system anomalies and known attacks.

Experimental results

Efficiency of suggested approach is confirmed by experimental results. We have built neural network user behavior model for operating system FreeBSD [3]. For this purpose we applied the feed forward neural network that was trained to predict a command by given number of previous ones. The experiments were carried out Intranet of Institute of Physics and Technologies of National Technical University of Ukraine "Kiev Polytechnic Institute". About 4000 user behavior models were analysed. Experimental results confirmed such models to be capable to detect anomalous user activity. Taking into account this experience we propose to spread given approach on other operating systems.

Neural network user behavior model was applied for operating system Windows 98. Initial information for neural network was process sequences run in the system. Neural network was to predict running process by the previous ones. The criterion for the optimal neural network prediction is to distinguish appropriate user from others (Fig. 2).

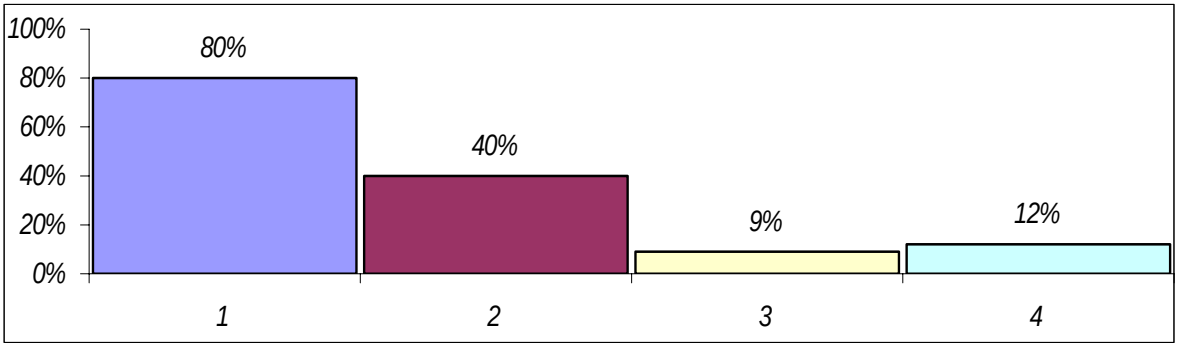

Fig. 2. Indexes of predicted processes for different users.

1 - Index of predicted processes for legal user on training set.
2 - Index of predicted processes for legal user on testing set.
3 - Index of predicted processes for illegal user #1.
4 - Index of predicted processes for illegal user #2.

Prediction errors for process for one session are shown in Fig. 3.

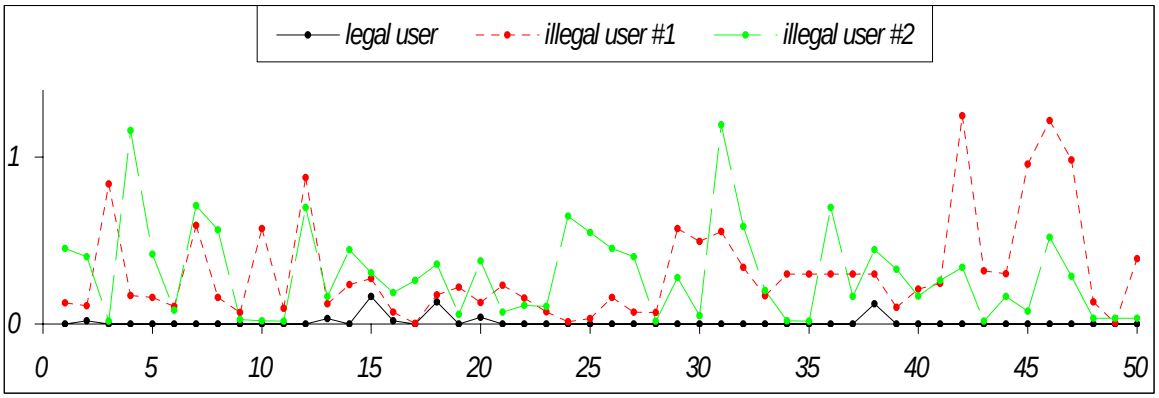

Fig. 3. Prediction errors for processes.

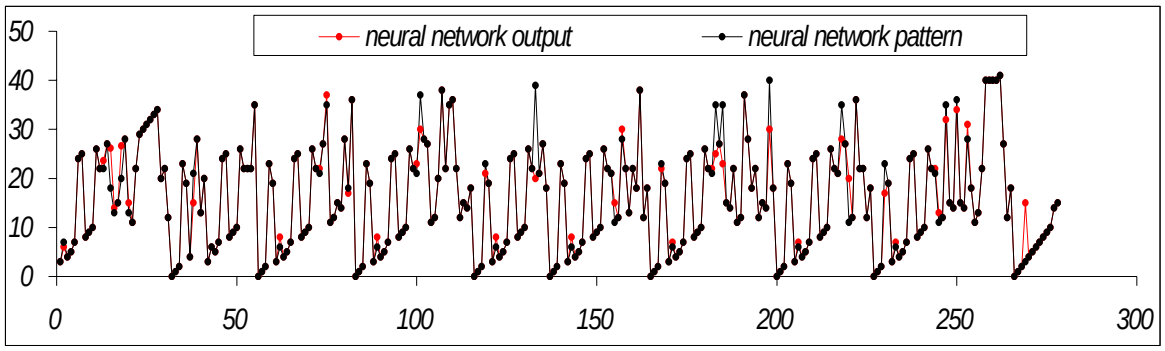

Fig. 3. Predicted process.

These results show the possibility of neural network to distinguish different users' behavior. Also other experiments were carried out in order to find optimal number of processes (premises) for correct prediction. Best results were achieved by predicting every 6-th command in sequence.

Conclusion

The above approach takes advantage of both intellectual methods of intrusion and anomaly detection and multi-agent architecture. The use of neural networks enables detection previously unknown attack types, while agent-based architecture provides features of intelligence and scalability as well as possibility to work in a heterogeneous environment. Currently, research of user behavior model demonstrates effectiveness of such approach.

Bibliography

1. V.Gorodetski, O.Karsaev, A.Khabalov, I.Kotenko, L.Popyack, V.Skormin. Agent-based model of Computer Network Security System: A Case Study. Proceedings of the International Workshop "Mathematical Methods, Models and Architectures for Computer Network Security". Lecture Notes in Computer Science, vol. 2052, Springer Verlag, 2001, pp.39-50.
2. James Cannady, James Mahaffey. The Application of Artificial Neural Networks to Misuse Detection: Initial Results.
3. A.M. Reznik, N.N. Kussul, A.M. Sokolov. Neural network identification of the behavior of the users of computer systems. Cybernetics and computational techniques, 1999, vol.123, pages 70-79.
4. A.M. Sokolov Computer System Intrusion Detection utilizing second-order Markov chain. Artificial Intelligence. Vol. 1, pp. 376-380. (in russian)
5. Jai Sundar Balasubramaniyan, Jose Omar Garcia-Fernandez, David Isacoff, Eugene Spafford, Diego Zamboni. An Architecture for Intrusion Detection using Autonomous Agents http://citeseer.nj.nec.com/balasubramaniyan98architecture.html.

Author information

Natalia Kussul - PhD, Head of Space Information Systems Department, Space Research Institute NASU-NSAU; 40 Glushkov Ave, 03187 Kiev, Ukraine; e-mail: inform@space.is.kiev.ua, nkussul@dialektika.kiev.ua

Andrey Shelestov - PhD, Senior Scientist, Space Research Institute NASU-NSAU; 40 Glushkov Ave, 03187 Kiev, Ukraine; e-mail: inform@space.is.kiev.ua

Anton Sidorenko – Bachelor in Applied Mathematics; System Developer, Space Research Institute NASU-NSAU; 40 Glushkov Ave, 03187 Kiev, Ukraine; e-mail: inform@space.is.kiev.ua

Vladimir Pasechnik - Bachelor in Applied Mathematics; System Developer, Space Research Institute NASU-NSAU; 40 Glushkov Ave, 03187 Kiev, Ukraine; e-mail: inform@space.is.kiev.ua

Sergey Skakun - Bachelor in Applied Mathematics; System Developer, Space Research Institute NASU-NSAU; 40 Glushkov Ave, 03187 Kiev, Ukraine; e-mail: inform@space.is.kiev.ua

Natalia Levchenko - Bachelor in Applied Mathematics; System Developer, Space Research Institute NASU-NSAU; 40 Glushkov Ave, 03187 Kiev, Ukraine; e-mail: inform@space.is.kiev.ua

Yuri Veremeyenko - Bachelor in Applied Mathematics, Physics and Technology Institute, National Technical University of Ukraine "Kiev Polytechnic Institute"; 37 Peremogy Ave, 03057 Kiev, Ukraine; e-mail: yur@pth.ntu-kpi.kiev.ua