December 1999

A Conceptual O-O Model for Internet-based Intrusion Detection Agents in Multi-Agent Systems

Felix Leung
City University of Hong Kong

Jess Yuen
City University of Hong Kong

Stephen Liao
City University of Hong Kong

Huaiqing Wang
City University of Hong Kong

A Conceptual O-O Model for Internet-based Intrusion Detection Agents in Multi-Agent Systems

Felix S. K. Leung, Jess H. K. Yuen, Stephen S. Y. Liao, Huaiqing Wang,
Department of Information Systems, City University of Hong Kong,
isfelix@is.cityu.edu.hk, isjess@is.cityu.edu.hk, ishongko@is.cityu.edu.hk, iswang@is.cityu.edu.hk

Abstract

UML is one of the most popular modeling languages in today's industries. This paper works with UML in order to introduce the conceptual O-O model for Internet-based Intrusion Detection Agents. Firstly, we introduce the reason for choosing agent-based technology for Intrusion Detection system. Next, we work on the classification of the proposed Intrusion Detection agents. Last of all, by using a scenario on IP spoofing, we illustrate how the agents work effectively.

Introduction

Many companies are accustomed to conducting their business on the web. The widely use of network connectivity through the Internet makes computer systems more vulnerable to attacks. These attacks often exploit flaws in either the computer systems or the company private data. Although many security solutions have been introduced to combat this special threat, most of these solutions involve a large expense in terms of time and money in both building and maintaining such an Intrusion Detection System (IDS).

This paper adopts the agent technology approach in this fraud detection issue. Besides constructing a conceptual model for the Intrusion Detection agents which is the focus of this paper, we have also worked out a paper on an intelligent multi-agent architecture in which the proposed detecting agents will be integrated with it [5]. By associating the detecting agents and the intelligent architecture, an Internet-based Intrusion Detection System can be built accordingly. The abnormal system operating conditions will be actively detected and diagnosed by these proposed agents. Agents will continuously monitor the system 24 hours a day 7 days a week and will alert security officers immediately when a security violation occurs.

Why use Agents?

A software agent is a computer program which acts in an environment autonomously and goal-orientedly on behalf of a person or an organization (authority)[8]. Based on our experience from the multi-agent systems in APACS [2] and intelligent agent assisted decision support system [3], we found that software agents are suitable for use in a wide variety of applications. They are well suited for use in applications that involve distributed computation or communication between components. This explains why agent-based technology is so common in the Internet. Furthermore, using intelligent agent technology in intrusion detection is one of the most active fields in recent years [1,6,7]. That is why intelligent agent techniques are believed to be applicable and promising on improving security on the Internet.

Modeling Techniques

Our modeling technique is based on the previous accomplishments of the O-O System research [10]. The expressions for object-oriented modeling used in this paper are explained in the Unified Modeling Language (UML) which is the unification of Booch, OMT and OOSE methods. Our study uses UML to represent and model the various types of agents. Each category of the Agents is treated as a class. The entire agents are organized hierarchically as shown in Figure 1. The top-level class is the Agents. This class consists of three sub-classes. They are the Network, Server and Client agents. The Client Agent interacts with the system users. The Network Agent monitors the system status. The Server Agent handles the input and output from the information repository. Last of all, there is a Communication Manager class associated with the Agents class. This class provides the service of inter–communication among different agents.

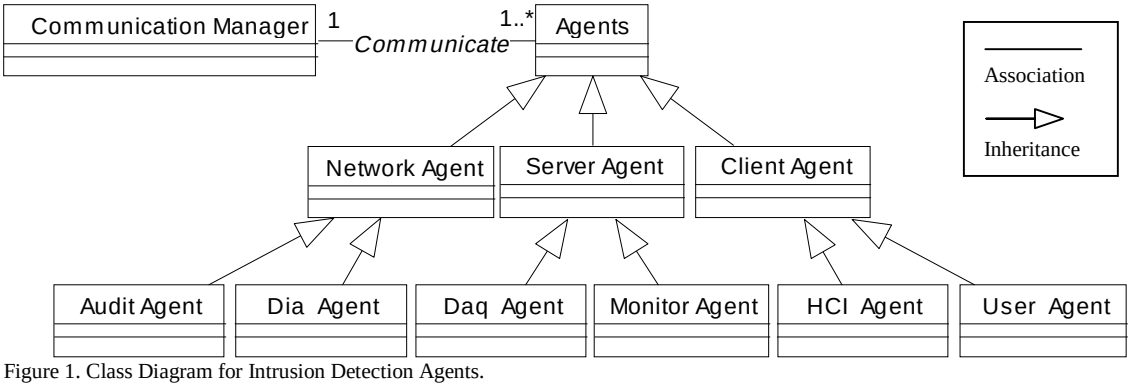

Figure 1. Class Diagram for Intrusion Detection Agents.

Intrusion Detection Agents

Like other intelligent agent systems we had built [2,3], our proposed agents enjoy autonomy, social ability (agents communicate with other agents), reactivity, and pro-activity. The Intrusion Detection agents will help the system to identify unauthorized use, misuse, and abuse of computer systems. Besides these detection, the other role of our intelligent agent is to alert a system security officer that a potential security violation is occurring. As such it is a reactive, rather than a proactive form of system defense [7].

The Intrusion Detection agents are described as follows:

- **Audit Agent**: Different Audit agents will specialize in different intrusion detection areas such as IP Spoofing, Virus, etc. It is an expert agent with a rule-based decision mechanism [6]. The function of an audit agent is to compare and analyze between its knowledge and the current data from an User agent. It is able to determine whether the user's current behavior is acceptable or not. If it detects a suspicious situation, it will send a suspicious message out to other agents in the system.
- **Diagnosis Agent (Dia Agent)**: The Diagnosis agent is usually in a waiting mode. It takes as input the output of the Audit agent and starts its diagnostic process.
- **Data Acquisition Agent (Daq Agent)**: The function of the Data Acquisition agent is to retrieve data from the information repository. It is a repository interface agent. When it receives a request from the other agents, it will co-operate with them by providing appropriate historical data, security rules, operation rules, etc.
- **Monitor Agent**: The Monitor agent analyses the requests that are handled by the information repository. It monitors all the write requests on the information repository.
- **Human Computer Interface Agent (HCI)**: This agent acts as a front end between the system security officers and the system. This agent displays the system running status to the system security officers. In the meantime, the system security officer may interact with the system for making decisions or requests via this agent
- **User agent**: The function of the User agent is to capture all the necessary data from the users. It encapsulates the current raw data from the users in such a way so as to allow other agents to handle it. Other agents can use this data to analyze a user's activities. As attacks by unauthorized third parties have been identified as one of the five areas in attacking agent systems [1,4], our User agents will provide the functions of encryption which safeguard point-to-point communication between agents. It ensures a secure communication.

Scenario

To illustrate how we envision such Intrusion Detection agents working cooperatively, we will consider an Internet protection scenario as shown in Figure 2. We will assume the intrusion detection agents are running on our intelligent multi-agent architecture [5] and protect against spoofing attack. Although spoofing can occur with a number of different protocols, we choose IP spoofing to illustrate our model because our proposed agents and architecture are using Internet-based systems. Also, a number of IP spoofing attacks have been recorded recently. One of the simplest ways to prevent IP spoofing is to disallow any trust relation between the internal and external network. However, extending a trust relationship across public networks is what worldwide organizations are looking for. Those organizations have increasingly come to use Internet/Intranet for their management and transactions with their trading partners [6]. As a result, both internal and external (Internet) users will be authorized to access the system while access control is needed as one of our security requirement [9].

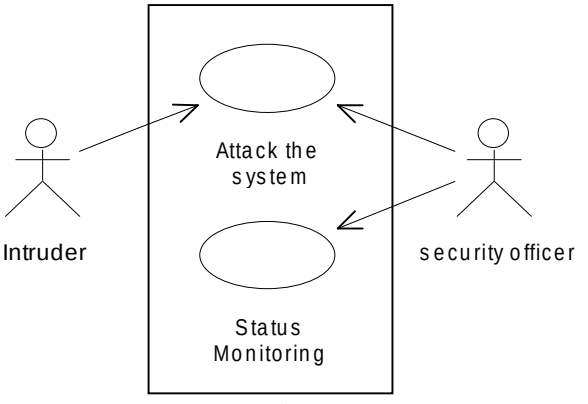

Figure 2. Use Case Diagram for Intrusion Detection Systems

Model of Security Process

An actual operation on IP spoofing detection involves numerous phases and sequences. In the start-up phase, each Audit agent queries the Daq agent to retrieve necessary knowledge.

The following are some rules that an Audit agent employs for IP spoofing detection:

- If packet transmitting within an internal network which should not be passed according to the claimed source and destination address, then it should be recognized as counterfeit.
- A packet coming from the Internet that contains the source address of a host inside the private network should be regarded as IP spoofing.
- If a host address on the Internet is known to be sending fraudulent packets, then block all traffic to and from that host.

- Outgoing packet whose source address is not in the

At the running phase as shown in Figure 4, when an internal user attempts to login the system, a User agent will be created for that particular user. The User agent encapsulates the real-time data package from the users and sends the encrypted data to corresponding expert agent (Audit agent) via the Communication Manager. When the Audit agent receives the data frame from the User agent, it will perform the checking base on the rule defined in the start-up phase. For example, the Audit agent will check whether the destination IP address (IP-To) for the current package falls into one of its subnet IP addresses (IP-My) or not as shown in Figure 3.

Once a suspicious current package is found, the Audit agent will broadcast what it has found to other Dia agents via the Communication Manager. Then the Dia agent does inferencing on the current situation. Eventually, if the final current suspicious level is higher than the predefine threshold, the Dia agent will send a message to the Monitoring agent and stop all the services for that current user. It will also inform the security officer of a possible intrusion via the HCI agent.

internal network should be regarded as IP spoofing.

For each message comes from User Agent **do**
  If (IP-To is not equal to IP-My)
    Then generate a suspicious broadcast message to Dia Agent
  End if
End For

Figure 3. A simple pseudo-code in Audit Agent for IP spoofing

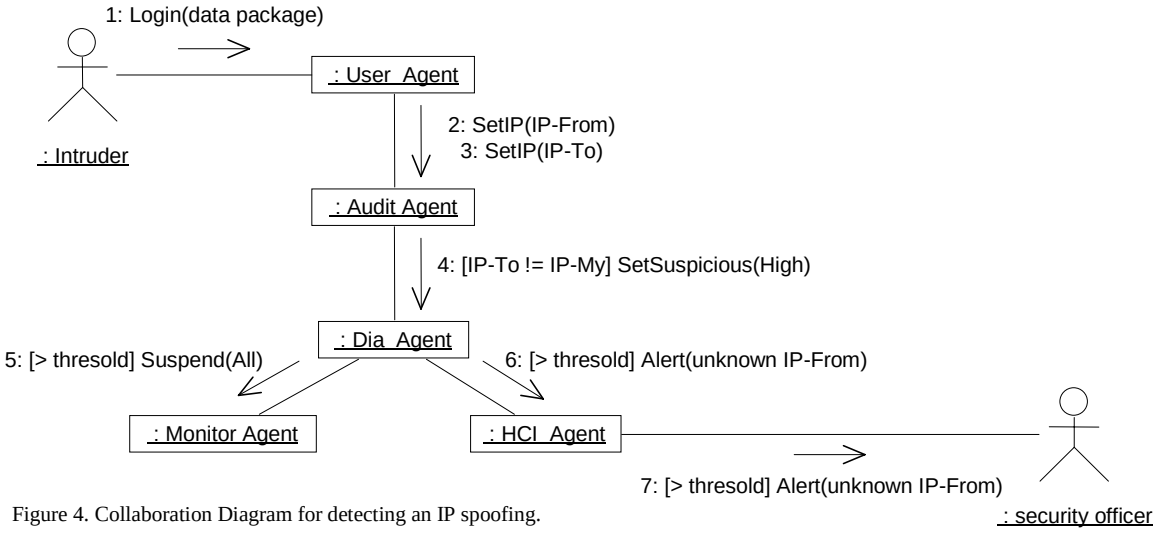

Figure 4. Collaboration Diagram for detecting an IP spoofing.

Conclusion

In this paper, we have proposed a conceptual model for Internet-based Intrusion Detection Agents. The application of agent-base technology enables our Intrusion Detection Systems to enjoy a level of flexibility and scalability that is not evident in traditional detection systems. It is possible to achieve the same detection result through a non-agent based system. However, a much greater effort is required when compared with an agent-based system that performs the same result. As the system profiles change over time, the detection system will change with them to allow newer activities, and possibly disallow earlier actions. Only an agent-based system can provide such an architecture for adding or removing a component (Agent) easily. We are now undertaking further research on a new type of agent which can perform the real-time learning on intrusion. There will be an agent proposed to learn about the intrusions during the systems run-time and use that knowledge in future decision making.

Reference

[1] Foner, L. "*A Security architecture for Multi-agent Matchmaking*". MIT Media Lab, Cambridge, MA, 1996.

[2] H. Wang, et al, "*APACS: a Multi-agent System with Repository Support*", Knowledge-Based Systems, 9 (1996) pp329-337.

[3] H. Wang "*Intelligent agent assisted decision support systems: integration of knowledge discovery, knowledge analysis, and group decision support*", Expert Systems with Applications, Vol. 12, No. 3, pp 323-335, 1997.

[4] Hohl, F. "*An Approach to Solve the Problem of Malicious Hosts*". University of Stuttgart, Department of Computer Science, 1997.

[5] J. Yuen, F. Leung, H. Wang, S.Liao, "*A Multi-Agent Architecture for Internet Security*", Feb 1999.
(Submitted to Americas Conference on Information Systems 1999)

[6] Lin Zeng, Huaiqing Wang, Matthew Lee, "*Intelligent Security System: Using Multi-Agent to Improve Internet Security*", Proceedings of Association for Information Systems 1997 Americas Conference (AIS'97), Indianapolis, Indiana, US, Aug 1997.

[7] Mark Crosbie, Gene Spafford, "*Defending a Computer System using Autonomous Agents*", Technical Report, Purdue University, Department of Computer Sciences, Mar 1994.

[8] Nwana, H.S. "*Software Agents: An Overview*", Knowledge Engineering Review, Vol.11, No.3, 205-244, Cambridge University Press, 1996.

[9] Parker D. "*A new framework for information security to avoid information anarchy*", Proceeding of IFIP/Sec'95, 1995.

[10] S.Liao, L. C. Chang, W.Y. Liu, "*An O-O Systems for the Reuse of Software Design Items*", Journal of Object-Oriented Programming (Accepted in Aug 1997).