IJWC
International Journal of Wireless Communication
Volume 1, Issue 1, 2011, pp-01-04
Available online at http://www.bioinfo.in/contents.php?id=109

NEW MOBILE AGENT-BASED INTRUSION DETECTION SYSTEMS FOR DISTRIBUTED NETWORKS

PRANITA JAIN, SANDEEP RAGHUWANSHI AND PATERIA RK
Department of Computer Science & Engineering, MANIT, Bhopal, India
*Corresponding author. E-mail: pranita.jain@gmail.com, sandeep8056@yahoo.co.in, r_k_pateriya@indiatimes.com

Abstract- This paper presents various distributed intrusion detection system (IDS), based on mobile agents, that detects intrusion from outside the network segment as well as from inside. Mobile agents are intelligent agents that can migrate among hosts. They can execute tasks autonomously in dynamic environments. Besides general definitions of these IDS system architectures, it includes an overview of several Network and Agent Based Intrusion Detection systems .The system shows a superior performance compared to central sniffing IDS techniques, and saves network resources compared to other distributed IDSs. The proposed model comprises three major components: The Network Intrusion Detection Component, the Mobile Agent Platform, and distributed sensors residing on every device in the network segment.
Keywords- Mobile Agents, Intrusion Detection, Distributed Systems.

INTRODUCTION

Security issues, such as network intrusion and virus infection, are becoming more and more serious with the growth of computer and network applications. In order to prevent information from malicious attackers, Intrusion Detection System (IDS) is used to detect various intrusions in network environment. Traditional IDSs have some drawbacks. i.e A central analyzer is a single point of failure. When an intruder manages to put it out of action (e.g. denial-of service attack), the whole network loses its protection.) , When all information is processed at a single location, the system is not scalable. The processing capacity of the analyzer unit limits the monitored network size and distributed data collection can lead to excessive data traffic over the network.

To overcome the above two limitations of traditional IDSs, some researchers suggest to use Peer-to-Peer (P2P) IDSs instead of hierarchical IDSs. In a P2P IDS, each host can send detection request to other hosts of the system to check whether there are suspicious activities, and estimate whether the network is intruded. Most current P2P IDSs only allow hosts of a system to obtain detection information from limited sources (e.g. direct-linked neighbours). This limitation may lead a system to make inaccurate decisions.

A different and interesting approach is taken by systems which utilize mobile agents to perform distributed intrusion. detection. The aim of this paper is to discuss various intrusion detection techniques based on mobile agents and also discuss advantages and possible drawbacks when applying mobile agents to intrusion detection systems. we also take into consideration the features gained from agent technology, such as autonomous components, which offer significant benefits.

MOBILE AGENTS

The development of distributed ID systems and the introduction of software agents to perform intrusion detection lead to the idea of using mobile agents. Mobile agents offer several potential advantages when used in ID systems that may overcome limitations that exist in IDS that only employ static, centralized components (as discussed above).

- ***Reducing Network Load*** - Instead of sending huge amounts of data (e.g. audit files) to the data processing unit, it might be simpler to move the processing algorithm (i.e. agent) to the data.
- ***Overcoming Network Latency***- Mobile agents are useful for applications that need to respond in real time to changes in their environment, because they can be dispatched from a central controller to carry out operations directly at the remote point of interest., When agents operate directly on the host where an action has to be initiated, they can respond faster than a hierarchical IDS that has to communicate

with a central coordinator located elsewhere on the network.

- ***Scalability-*** Distributed MA IDS architectures are one of several options that allow computational load and diagnostic responsibilities to be distributed throughout a network. As the number of computing elements in the network increases, agents can be cloned and dispatched to new machines in the network.
- ***Fault Tolerance-*** Mobile agents react dynamically and autonomously to the changes in their environment, which makes them robust, and fault tolerant. They have the ability to distribute themselves in the network in such a way as to maintain the optimal configuration for solving the particular problem. If a host is being shut down, all agents executing on that machine will be warned and given time to dispatch themselves and continue their operation on another host in the network.
- ***Asynchronous and Autonomous Execution-***Mobile agents operate asynchronously. Once a mobile agent is dispatched from the home machine, the home machine can disconnect from the network. The mobile agent executes autonomously without the intervention of the home machine .The home machine can reconnect at a later time and collect the agent.
- ***Protocol Encapsulation-*** Protocols enable components of a distributed system to communicate and co-ordinate their activities. However, protocols evolve over a period of time and new features such as better security may be introduced in the protocol. It is a cumbersome task to upgrade the protocol code at all locations in the distributed system. Mobile agents offer a solution to this problem. The mobile agent code can encapsulate the protocol. When a protocol is upgraded, only the mobile agent has to be altered.

Unfortunately, the introduction of agents and agent platforms may also cause the following problems

- ***Security*** - Security risks in a mobile computing environment are two fold. Firstly a malicious mobile agent can damage a host. For example a virus can be disguised as a mobile agent and distributed in the network causing damage to the host machines that execute the agent. On the other hand a malicious host can tamper with the functioning of the mobile agent.
- ***Code Size -*** An IDS is a complex piece of software and agents that implement its functionality might get rather large. Transferring the agent's code over the network may take some time, but it is only needed once, when each host stores agent code locally. Claims that agents get especially large when they encode operating system dependant parts, but one might consider putting these routines into the agent platform and offer a generic interface to agents
- ***Performance -*** Agents are often written in scripting or interpreted languages to be easily ported between different platforms. This mode of execution is very slow compared to native code. As an IDS has to process a large amount of data under very demanding timing constraints. the use of MAs could degrade its performance.

AGENT BASED INTRUSION DETECTION

In this approach not only the workload will be divided between the individual processors, but also he IDS will be able to obtain an overall knowledge of the networks working condition. Having an overall view of the network will help the IDS to detect the intrusion more accurately and at the same time it can respond to the threats more effectively. In this approach, servers can communicate with one another and can alarm each other.

In order to respond to an attack, sometimes it can be sufficient enough to disconnect a subnet. In this type of system in order to contain a threat, the distributed IDS can order severs, routers or network switches to disconnect a host or a subnet. One of the concerns with this type of system is the extra workload that the IDS will en-force on the network infrastructure. The communication between the different hosts and servers in the network can produce a significant traffic in the network. The distributed approach can increase the workload of the net-work layers within the hosts or servers and consequently it may slow them down.

There are two approaches in implementing an agent based technology. In the first approach, autonomous distributed agents are used to both monitor the system and communicate with other agents in the network. A Multi-agent based system will enjoy a better perception of the world surrounding it. A multiagent based IDS where they have considered four types of agents: Basic agent, Coordination agent, Global Coordination agent, Interface agents. Each one of these agents performs a different task and has its own

subcategories In a work reported by Ramachandran el the idea of neighborhood-watch is implemented for the net work security. There are three different types of agents All the agents are defined in PERL (Practical Extraction and Report Language

INTRUSION DETECTION SYSTEMS

Only a few research projects have already attempted to incorporate some ideas of mobile agent technology into intrusion detection systems. Although the architectural description is interesting no implementation has been provided so far. The following subsection briefly describes the various intrusion detection models based on mobile agents

SPARTA

Sparta [5] (which is an acronym for Security Policy Adaptation Reinforced Through Agents) is the name of a project sponsored by the European Union. It is a system whose primary aim is to detect security violations in a heterogenous, networked environment. Sparta is an architectural framework which helps to identify and relate interesting events that may occur at different hosts of a network. In addition to the detection of interesting patterns, Sparta can also be utilized to collect statistical data (i.e. extreme value or sum of attribute values) of certain events. The network overhead of the travelling agents is negligible and the processing overhead at
each node is reasonably low.

MICAEL

Micael is another agent based approach, where decision making, distributed, autonomous agents have the role of investigating intrusions. Its architecture consists of the following elements.

Sentinels are static agents existing on every host. They do not have any knowledge about different attacks, but they are against distributed attacks.(DoS etc.).

Detachments are mobile agents to investigate intrusions. When a possible attack is detected, they are moved to the related host and start to examine log files in detail. In case they decide that there is an attack, they can perform various actions from disconnecting the host to counterattacking to the intruder.

Headquarter*s* are centralized agents collecting data from sentinels and creating new detachments if needed. Micael is a successful implementation of the agent based approach with several advantages. Its agents are not used only collect data, they can also react to incidents.

APHIDS

APHIDS, that employs mobile agents to perform monitoring and analysis in a distributed and timely manner. This architecture delegates data capture and detection tasks to existing monitoring systems. Distributed search and analysis tasks are implemented with mobile agents, and the system provides a high level scripting facility to define how analysis results from these agents should be combined and reported. APHIDS is able to discover and utilize greater amounts contextual information when processing an incident, allowing it to potentially make more informed decisions.

AAFID

The Architecture for Intrusion Detection Using Autonomous Agents (AAFID) implements a hosts based hierarchical design to deal with disadvantages of centralized systems. The system consists of three layers, each layer calls methods of the layer below. At the base level *agents* collect information, search for suspicious packets and forward collected data to *transceiver*, which exists in the upper layer and once in every host. Transceivers are like agent managers, they control and configure agents on the host, and channel information, most probably exclude unnecessary parts of the collected information and forward it to *monitors*. In the higher level, each monitor collects data from one or more transceivers and analyzes their input. In the AAFID architecture, agents are used to collect and preprocess information which is needed do detect intrusions in the system. They are not intelligent programs, but due to genetic programming they inherit their experience. In addition transceivers and monitors is aimed to make the system scalable, which allow detection of distributed attacks. The major disadvantage of AAFID architectures is the delay in the detection of the intrusion caused by the layers between agents and the monitor and also monitors are the single point of the failure.

JADE- Java Agent Development Platform

Network forensics analysis requires tools that effectively look through massive amount of scattered data to gather relevant evidence. This is graphical interface, mobility, message communication and parallel behaviours of the agent platform to first, implement a user interface wherein the analyst can specify the data to be collected from distributed systems. Second, dispatch distributed agents to heterogeneous locations to gather data. Third, display the collected result in a format that is useful to analyze network events. applications, does not enable knowledge sharing among agents. The meta-learning

approach tries to reduce this limitation by integrating a number of remote agents.

MAIDS

MA-IDS[6] employs MA technology to coordinately process information from each monitored host, and then completes global information extraction of intruder actions MAIDS was developed by Iowa State University is a distributed IDS based on MA technology. It build a model for an intrusion activity with Software Fault Tree Analysis (SFTA), and transform the SFT model into Intrusion Detection model by the use of Colored Petri net(CPN). Intrusion detections in MADIDF are not only relied on direct-linked neighbours of a particular host, but also other hosts in the network. In this way, the original host can obtain more information to achieve a more accurate decision.

MA may enhance the performance of IDS and even offer IDS some new capabilities, however, these benefits is not easy obtained. We could learn from these existing systems that there are three main research areas in IDS with MA technology: MAIDS can gather information not only from neighbours of the compromised host but from more other hosts in the network that can lead to more accurate final decision.

CONCLUSION

Although the possible advantages of mobile agents seem impressive at first, only a few systems use them to perform security related tasks. In this paper, we have discuss various approaches for intrusion detection in distributed network based on mobile agents.

In network-based IDS, agent based systems play an essential role. In such systems a distributed processing architecture is a must and system has to collect information from different components within the network. Implementing such architecture, one should avoid increasing the network traffic.

IDA employs mobile agents mainly for tracing purposes while Micael and Sparta have more ambitious aims. In these systems, mobile agents actually carry out the event correlation. Mobile agent paradigm provides mechanisms for the peer-to-peer networks by default. Another important distinction between two theories is that the agent induced client can move and talk to the server locally rather than over network, which reduces the amount of communication. The advantages may be better throughput, bandwidth utilization, faster completion time, smaller delays, lower cost and better performance. MADIDF can gather information not only from neighbours of the compromised host but from more other hosts in the network that can lead to more accurate final decision.

REFERENCES

[1] G. B. White, E. A. Fisch, and U. W. Pooch. Cooperating security managers: A peer-based intrusion detection system. *IEEE Network*, pages 20–23, January/ February 1996.

[2] C. Krugel and T. Toth. A survey on intrusion detection systems. Technical Report TUV-1841-00-11, University of Technology, Vienna, 2000.

[3] P. A. Porras and P. G. Neumann. Emerald: Event monitoring enabling responses to anomalous live disturbances. In *Proceedings of the 20th National Information Systems Security Conference*, October 1997.

[4] X. Wang, J. Zheng, K. Xiao, X. Xue, and C. Toh. A mobile agent-based p2p model for autonomous security hole discovery. In *Proceedings of the Fifth International Conference on Computer and Information Technology*, pages 723ñ727, 2005.

[5] C. Krugel and T. Toth. Sparta - a security policy reinforcement tool for large networks. In *submitted to I-NetSec 01*, 2001.

[6] Li, C., Song, Q., Zhang, C.: Ma-ids architecture for distributed intrusion detection using mobile agents. In: Proceedings of the 2nd International Conference on Information Technology for Application (ICITA 2004), 2004

[7] W. Jansen and T. Karygiannis. Mobile agents and security. Special Publication 800-19, NIST, 1999.

[8] Duarte de Queiroz, J., Fernando Rust da Costa Carmo, L., Pirmez, L.: Micael: An autonomous mobile agent system to protect new generation networked applications. In: 2nd Annual Workshop on Recent Advances in Intrusion Detection, 1999.