In Proceeding of The World Multiconference ***on SYSTEMICS, CYBERNETICS AND INFORMATICS (SCI)*** and, The International Conference on ***Information Systems Analysis and Synthesis (ISAS) -*** ORLANDO, FLORIDA – July 12-16, 1998

A Mobile Agent-based Security Architecture for Intranets

N.Agoulmine
PRISM Laboratory
University of Versailles-Saint Quentin en Yvelines
45 Avenue des Etats-Unis
78030, Versailles Cedex
France
Email : naz@prism.uvsq.fr

K.Boudaoud
EURECOM Institute
Corporate Communications Department
2229 Route des cretes. B.P 193
06904 Sophia Antipolis Cedex
France
Email : boudaoud@eurecom.fr

B.Bhushan
GMD Fokus
Research Institute for Open Communication Systems
Kaiserin-Augusta-Allee 31
D-10589 Berlin
Germany
Email : bhushan@fokus.gmd.de

Abstract: Huge popularity and demand of the Internet and Intranets has come at the prize of weakening data and network security, which cannot be overlooked. Data and networks are distributed, making them even more vulnerable to attacks. The security technologies must coexist with and take maximum advantages of recent technologies of autonomous distributed computing. One such technology, which is gaining ground, is Mobile Agent technology. This paper takes a look at the aptness of Mobile Agent technology for security management and applies it to the management of the Internet and Intranets.

Keywords: Security Management, System Architecture, Mobile Agents, Security Policies.

1. Introduction

Vast developments of telecommunications market are intensifying the complexity in the management of networks, services and users. Three main factors to which the complexity in the management can be attributed are:

- the achievements in networking technologies;
- increasing capacity of infrastructures;
- development of new services; and
- users' demand and awareness of the newly emerging services.

Therefore, the explosion in use of Internet is an indication of the scale of this revolution. One of the biggest problems introduced by the development of network is the security of the networks and services. The needs of remote access from customers, users and service provider to a particular environment requires that the precautions must taken in order to make a balance between the security demands and the access flexibility.

The existing security solutions are very complex and costly. What needed is a flexible, adaptable and affordable security solution, which provides greater autonomy. Therefore, it is necessary to review the way security system architectures are designed. The emerging distributed systems technologies such as CORBA (Common Object Request Broker Architecture) and Internet technologies (Web and JAVA) should be analysed in order to identify new approaches.

In this context it must be noted that the concept of Mobile Agent (MA) is attracting much interest. The agent technology has already been used in many different application areas, supporting different functionality. However, it is the emergence of distributed systems and the Internet technologies that has made the realisation of Mobile Agent technically possible. MAs represent transportable and even active objects. With this, MAs can realise global tasks, which are carried out autonomously and co-operatively.

In this paper, we, first investigate the MA concept from the Security Architecture point of view. Then, we propose an MA-based Security Architecture, which supports security in the Internet in a cost-effective manner. The driving force behind the MA-based Security Architecture is to determine:

- The impact of this concept in the global design of the system.
- The gains of using such a technology in term of flexibility, adaptability etc.

MA-based Security Architecture will also help in the definition and dynamic deployment of security policy directly into the network, based on specific user requirements. In fact, security aspects will not be the same for all users and service providers, so categorisation of security threats is an important requirement for this work, especially when the architecture is to be applied to the Internet and intranets.

2. Security Management

Security management is a task of maintaining the integrity, confidentiality and availability of systems and services. The reality of the present time is that increasing number of people, organisations, and enterprise are installing and subscribing to the Internet, consequently raising the concerns of security. Thus, the security management is an issue of paramount importance.

First of all, it is necessary to identify the risks by identifying the attacks that the networks are exposed to. Applying security management is a two-fold activity. Firstly, the security architecture is to be deployed to protect networks against the attacks by detecting attacks. Secondly, when attacks are detected the security architecture is to respond to attacks and to take security measures, preferably in real time.

2.1. Attacks

On the 5th of March 1997, NASA's home page was hacked and the content modified by a new page criticising the American institutions. This is an example of various others attacks to which the enterprise expose themselves.

An intrusion [1] can be defined as any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource. The following are some examples of attack:

- *IP spoofing:* is the action to send packets to a host with other source IP address than the original one, thus making the user believe that packets were originated from another host, preferably a host which is allowed to establish connections with the attacked host, if the real sender (attacker) itself is not allowed.

- *TCP SYN flooding:* the purpose of this attack is to constantly fill the backlog queue of a host, where incoming connections requests are kept, by sending a bulk of SYN requests. The attacking host must spoof the IP address of an unreachable host for the server so the SYN/ACK answers will never be received and ACK messages never generated. The consequences of TCP SYN flooding is that all further requests to this TCP port will be ignored. In some cases, the attacked host may even exhaust memory and crash.

- *ICMP flooding:* ICMP packets (usually ping requests but other type of requests are also possible) can be used to flood a network and bring it down. Requests must be sent at a high rate to many host destinations. Concurrent answers generate many collisions on local area networks and fill routers queues.

- *Doorknob rattling:* repetitive attempts to log in to several hosts with any user-id/password combination in order to obtain an access to an account.

- *Traffic Analysis:* information is leaked to unauthorised entities, through observation of communications traffic patterns

- *Web attack*: An organisation's pages on its web site are modified in order to give the reader wrong information.

2.2. Network Intrusion Detection

Securing a network involves protecting it against all possible attacks. But, in practice it is not possible to have a completely secure network. So, it is important to detect security violations right on the moment when they happen.

Intrusion Detection is a practical approach for enhancing the security of computer and network systems. The goal of Intrusion Detection Systems (IDS) is to detect attacks in real time. There are systems based on host-audit-trail, other systems analyse network traffic to detect suspicious activity. These systems use one or both of the two approaches of intrusion detection. The first approach is the behaviour-based intrusion detection, which discovers intrusive activity by comparing the user or system behaviour with a normal behaviour profile. The second approach is a knowledge-based intrusion detection approach, which detects intrusions upon a comparison of parameters of the user’s session to a database of techniques that are used by attackers to penetrate the system. The behaviour-based intrusion detection approach allows to detect unknowns intrusions and the knowledge-based intrusion detection approach detect well-known intrusions.

In this part, we deal with network-based intrusion detection systems. These systems monitor multiple hosts and bases their analyse on:

- monitoring the network traffic; and
- information transferred from multiple monitored hosts to a central site for processing.

A short list of intrusion detection systems is given below:

a) Traffic Analysis

- **NSM** (Network Security Monitor) has been developed at the University of California, Davis.
- **DIDS** (Distributed Intrusion Detection System) is a joint project by UC Davis, Lawrence Livermore National Laboratory, Haystack Laboratory and the US Air Force. It uses a statistical method and an expert system. It is also a distributed host-based intrusion detection system.

b) Operating System’s Audit Trail Analysis

- **NADIR** (Network Anomaly Detection and Intrusion Reporter) was designed at Los Alamos National Laboratory. It works in real time and uses an expert system as well as a statistical method.
- **NIDES** (Next Generation Intrusion Detection Expert System) was developed at SRI International. It uses a statistical approach and an expert system.

- **ISOA** (Information Security Officer's Assistant) is a distributed host-based intrusion detection and real-time security monitor.
- **CSM** (Co-operating Security Managers)

NADIR was designed for the Integrated Computing Network (ICN) established at Los Alamos National Laboratory. This network is divided into four partitions; each dedicated to a specific level of processing. Special nodes called *service nodes* enforce this partitioning and are the point at which monitoring and analysis of network activity is implemented [2]. The network protocols used at Los Alamos are non-standard, and the service nodes are arranged in a unique way to the dedicated workstations, which constitute NADIR. These features present an important disadvantage because the system would not be ported easily to an internet-worked environment with many heterogeneous systems.

NSM presents some deficiencies, e.g., the NSM cannot monitor an attacker who enters a system via a dial-up line and hence may not generate any network activity. Hence, the NSM can be spoofed via encrypted traffic [3]. It also requires special hardware on each Ethernet segment.

DIDS is an outgrowth of the NSM System and was designed to guard against some of NSM s deficiencies. It operates on a local area network (LAN) and its architecture combines distributed monitoring and data reduction with centralised data analysis. A DIDS director, a LAN monitor, and a series of host monitor [3] constitute it. The LAN monitor reports to the DIDS director unauthorised or suspicious activities on the network. The host monitors collect audit data for the individual host and perform some simple analysis on the data. The relevant information is then transmitted to the DIDS director. This director is responsible for analysing all these data and detecting possible attacks. A shortcoming of DIDS is that the centralised nature of DIDS will limit its usefulness in WANs where communication with a central director from all hosts may swamp portions of the network [2]. An approach to applying DIDS to an internetworked environment has been proposed, but it relies on a hierarchical structure, which does not exist in many networks [4].

CSM was designed to perform intrusion detection in a distributed environment. A CSM must be run on each computer connected to a network to facilitate the co-operative detection of network intrusions [2]. It consist of following parts:

- a local intrusion detection component (IDS)
- a security manager (SECMGR)
- an intruder handling component (IH)
- a graphical user interface (GUI)
- a command monitor (CMNDMON)
- a TCP communication (TCPCOM)

The IDS performs intrusion detection for the local host and is responsible for proactive detection of attacks on other host. The SECMGR co-ordinates the distributed detection intrusion between CSMs. The role of the IH is to take actions when an intruder is detected. The security administrators can communicate with individual CSMs to monitor the security status of the computer system through the GUI. When a user executes commands, the CMNDMON intercept these commands and send them to the IDS for analysis. And finally, the TCPCOM permits TCP communications between CSMs.

CSM take an approach that uses no established centralised director but each of the individual managers assumes this role for its own users when that manager suspects suspicious activity. The most important feature of CSM is that the co-operation among CSMs permits them to handle certain type attacks in a proactive manner (e.g. doorknob rattling attack). In a heterogeneous environment, two CSMs can communicate because communication takes place via messages that relay information that need not be system-specific. However CSM cannot simply be ported from one computer system to another because the action-based intrusion detection module is heavily system-specific [2].

Looking at these approaches undertaken to counter security attacks, some features of these approaches can be derived as main requirements:

Distribution of activities: This aspect is found mainly in all the approaches. It is very important to distribute the control of security management among a number of entities that can monitor the network access at different points.
Autonomy: The CSM and DIDS approach have shown the necessity to have a certain level of autonomy in the various entities that constitute the system. They differ in the sense that the final in the DIDS system decision is taken by a centralised manager, whereas in the CSM some decision can be directly taken in the entity.
Co-operation: The CSM has shown also the necessity of security manager co-operation in order to detect security attacks that can not be detected by individual manager.
Migration: This aspect is related to the overall systems. In fact, all systems need to install individual software or hardware on various points of the network. This approach can be complex and costly. Although, if the network consists of hundred of equipment, it is necessary to install this entities at the various point, even if it is exactly the same entity. This approach make the system inflexible, difficult to enhance and costly in term of maintenance. Thus, migration of security process among various systems is a main requirement.

3. Mobile Agent Concept

Having highlighted the main requirements for security architecture, the Mobile Agent concept seems to be a candidate approach to fulfil these requirements. What is the Mobile Agent concept [5][6][7][8][9]? The term Agent is a concept used in different area and having different meaning depending on the context [10][11]. Nevertheless, different types of agents reflect a set of properties, which common among them and are described below [12]:

- Encapsulation: An Agent is a piece of software that is able to perform a set of functionality's that defines its behaviour. The way these functions are performed is completely hidden to the Agent environment. This is similar to Object-Oriented encapsulation concept.
- Autonomy: An Agent behaves in an autonomous way. It decided itself when and under which condition it will perform the actions. The autonomy is linked to a reactive or a pro-active behaviour. The reactive behaviour means that the Agent reacts to an event that occurs. The pro-active behaviour means that the Agent is capable of acting independently from any changes in the environment.
- Co-operation: An Agent is co-operative and is able to have a social ability. This sociability allows an Agent to interact with other Agents for the purpose of performing tasks that are beyond the capability of a particular agent. This capability goes from delegation (distribution of sub-tasks) to peer-to-peer inter-working.
- Intelligence: The term “Intelligence” means that the agent is able to exhibit a certain level of intelligence priority, ranging from predefined actions (planning) up to self learning (define new actions).
- Mobility: An Agent is mobile. It is capable of moving from one localisation to another in order to perform a particular task or to react to a particular event

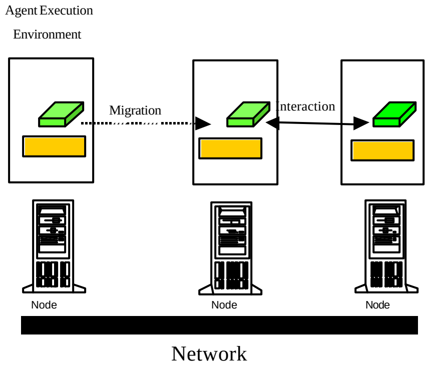

Figure 1: Mobile Agent Environment

Having studied the properties of the MA and the aspects and requirements of a security management, it can be concluded that MA provides a more coherent and flexible approach of security management. The security management architecture based on the concept of MA can be conceived as if it were made of the autonomous MAs co-operating with each other to achieve Global Security Policy. The MAs of the security architecture also possess intelligence. The next section describes the security management architecture.

4. Architecture

The key characteristics of the security architecture are flexibility, adaptability, and distribution of security mechanisms.

4.1. Physical Architecture

The MS-based Security Management Architecture consists of four main components as described in the following figure:

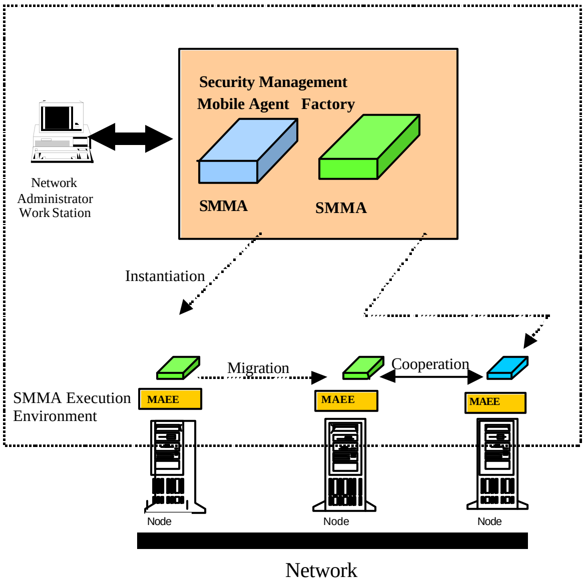

Figure 2: Mobile Agent Security Management Architecture

-The Management Agent Factory (**MAF**) is an environment, in which security management mobile agents are created, initiated, resumed, and controlled. The environment also serves as an access point for network security administrator.

-The security management mobile agent (**SMMA**) is an intelligent process that is able to migrate from and to different point of the network and the system to collect, filter management information and to perform management activities [10]. The management activities are defined by the administrator and reflect the Security Policy. Thus, network environment is populated by a set of mobile management agents that co-operate with each other in order to perform global security management activities (described in the following figure).

- The Mobile Agent Execution Environment (**MAEE**) is a set of components necessary for the execution and the migration of MAs.

- Network Administrator Workstation (**NAWS**) is an interface with which a security administrator (a person) interacts with the architecture. A security administrator must specify the security policy to apply and to create, instantiated, control the Mobile Agents. For these operations, the security administrator needs to access the Mobile Agent Factory, and NAWS facilitate security administrator with an access to the Mobile Agent Factory.

4.1 Security Policies :

The architecture relies on many intelligent MAs for assuring intrusions detection. The MAs operate autonomously but according to a predefined security policy. These policies can be defined at the initialisation of the Mobile Agent or dynamically according to the global business policy.

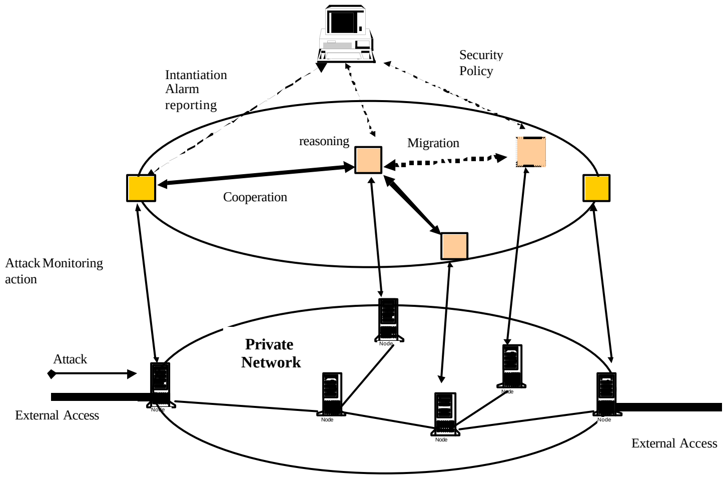

Figure 2: Security Mobile Agent Monitoring of Telecommunication Services

The first step to specify this security policy is to use access control rules. The access control rules provide a flexible means of specifying management policy as a relationship between initiator domain and target domain in terms of the operations client can perform on remote hosts. Constraints (contextual information) also make up a part of the access control rules and specified in the rules. Access control procedures (i.e. validation of Initiator-bound Access Control Information (ACI), identification of the Target etc.) are performed according to the established Security Policy, which is specified by access control rules.

The access control rules is the part of the ACI, which represents the permitted operations and the conditions upon their execution in a security domain. There are five classes of access control rules that are to be applied:

Globally deny rules: These deny access to all targets. If a global rule denies access, then no other rule shall apply. If a global rule does not deny access, then the item deny rules are imposed.

Item deny rules: These deny access to particular targets. If an item deny rule denies access, then no other rule shall apply. If an item deny rule does not deny access, then the global grant rules are applied.

Global grant rules: These grant access to all targets. If a global rule grants access, then no other rule shall apply. If a global rule does not grant access, then the item grant rules are imposed.

Item grant rules: These grant access to particular targets. If an item grant rule grants access, then no other rule shall apply. If an item grant rule does not grant access, then the default rules are applied.

Default rules: These rules are to be applied when no other rule has specifically granted or denied access. The default rules shall grant or deny access.

Authentication	**Key Management**	**Integrity/Confidentiality**	**Access Control**
AuthenticationFailure	keyExpired	InformationModificationDetected	unauthorizedAccessAttempt
AuthenticationSucc		DuplicateInformation	outOfService
			outOfHoursActivity
			keyExpired
		BreachOfConfidentiality	unspecifiedReason

Table 1: Security Events

The MAs should monitor the network in order to detect these events and then react according to the behaviour specified by the administrator. The MAs may also report the administrator

Workstation the events. In case of a special event, the MAs may also decide to migrate, if they have to move to another host to check information in order to have a more precise status on the special event. For example, if an agent detects an “unauthorizedAccessAttempt”, it can migrate from one host to others hosts to check whether or not “unauthorizedAccessAttempt” has been detected on other hosts too. In the case of the doorknob rattling, the MA may also migrate from one host to another host in order to detect multiple login attempts. The migrating agent can also cooperate with others agents to check if there are other login attempts on their hosts. An example of this functionality is given below.

Suppose that an intruder came from an external network, in the night or in the weekend, obtained an access, and had an unauthorised activity. The agent that is monitoring all the incoming connections detects an “unknownAddress” and an “outOfHoursActivity” event. This agent can track the intruder by migrating to the host were the intruder is working. If the intruder “travel” from one host to another host, migrating agent can follows intruder’s activities by co-operating with the others agents, responsible for monitoring these hosts. If one of the co-operating agents detects, for instance an “unauthorizedAccessAttempt”, or an “suspiciousActivitiy”, the first agent can migrate to the host on the entry of the internal network and close the connection or to ask another agent to do it.

5. Conclusion

In this paper, we have highlighted the security requirements for enterprise intranets. We presented some existing security management systems and highlighted their limitations. Mainly, the flexibility, autonomy and adaptability were the principal features to be addressed in order to propose a security architecture that met the security requirements. Thus, we proposed an approach based on Mobile Agent technology to make security management more flexible, customisable and cost-effective. Mobile Agents address the security management problem in a different manner. In fact, by giving more autonomy to Mobile Agent in the control of the overall security, the task of administration becomes easier. Administrators do not have to concern about all the security problems. They interact with the agent from a high level using security policies. Security policies tell the Mobile Agents what behaviour they should exhibit when attacks occur. Moreover, by their capability to migrate from different points of the network, the configuration is of the managed system is made easier and consequently cost-effective. Hence, the migration permits the Mobile Agent to move around the network and the system in order to collect information. This information permits the agents to identify attacks that can not be detected if they are static. Giving more autonomy to the agent permits the system to react in “real time” to attacks and to take necessary actions that permit avoid severe consequences of the attack.

6. References

[1] R.Heady, G.Luger, A.Maccabe, M.Servilla. The architecture of a network level intrusion detection system. Technical Report, University of New Mexico, Department of Computer Sciance, August 1990.

[2] Maj.Gregory B. White, Eric A. Fisch, and Udo W. Pooch, "Cooperating Security Managers: A Peer-Based Intrusion Detection System", IEEE Network journal, January/February 1996, pp. 20-23.

[3] L.T. Heberlein, B.Mukherjee, and K.N.Levitt, "Network Intrusion Detection", IEEE Network journal, May/June 1994, pp. 26-41.

[4] L.T. Heberlein, B.Mukherjee, and K.N.Levitt, "Internetwork Security Monitor : An intrusion-Detection System for Large-Zscale Networks", Proc. 15th National Computer Security Conference, October 1992, pp. 262-71

[5] Y.Yemini and al :”Network Management by Delegation”, in Integrated Network Management II, Krishnan & Zimmer (Eds), pp 95-107, Elsevier Science Publishers, 1991.

[6]C.G. Harrison, D.M. Chess and A.Kershenbaum, Mobile Agents : Are they a good idea ?, IBM T.J.Watson Research Center, March 1995.

[7] T.Magedanz, K.Rothermel and S.Krause, “Intelligent Agents : an Emerging Technology for Next Generation Telecommunications ?”, In Proceedings of the IEEE INFOCOM ’96, San Francisco, USA, March 1996, pp464-472.

[8] J.P.Muller, The Design of Intelligent Agents – A Layered Approach. LNAI state-of-the-art

Survey, Springer, Berlin, Germany, 196.

[9] OMG (Object Management Group) Working Group. Mobile Agent Facility Specification. Technical repor, Crystaliz, Inc., General Magic, Inc., GMD Fokus, International Business Machine Corporation, Nov 1997, OMG TC Document arbos/97-10-05.

[10] M.Breugst, T.Magedanz, "On the usage of Mobile Agent Platforms in Telecommunication Environments", 5th IS&N Conference, Antwerpen, Belgium, 25-28 May 1998.

[11] S.Corley and al, "The Application of Intelligent Agent Technologies to Network and Service Management", 5th IS&N Conference, Antwerpen, Belgium, 25-28 May 1998.

[12] T.Magedanz, " Mobile Agents – An Overview", ACTS IS&N Conference – Cernobbio (Como), Italy, May 27-29, 1997.