Intrusion Detection with Mobile Agents

Noria Foukia, Jarle G. Hulaas and Jürgen Harms {foukia, hulaas, harms}@cui.unige.ch
Centre Universitaire d'Informatique
University of Geneva
24, rue du Général Dufour CH-1211 Genève 4,
Switzerland
Teleinformatics and Operating Systems Group

*abstract*

*During the last ten years, the Internet has grown considerably. More interconnected people yields increased information security problems. Indeed, the continuous increase in computer interconnectivity and interoperability in a fully open way enhances the intruder's ability to attempt malicious behaviour against computers and networks and furthermore allows intruders to make these attempts extremely efficient. Detecting an intruder in a network environment is hard for a human and even if the amount of circulating information is collected by computers there is still too much information to analyse in real-time.*
*Intrusion Detection Systems' (IDSs) goal is to detect attacks against information systems. Notably it is difficult to guarantee a completely and provably secure information system and to be sure to always maintain it in a secure state during its utilization. This is why IDSs have to monitor the usage of such systems to detect eventual insecure states. For this task, new approaches and designs on IDSs are required which avoid, for example, centralised control and analysis of data to determine if an intruder entered the network. With this perspective and in the scope of a Swiss National Project (ADAMA II-2000-054014.98), we are investigating the use of Mobile Agents (MAs) research to address Intrusion Detection (ID) in an Intranet. After the general description of the different goals of the project, we expose our first stage ID model using MAs based on immune system principles.*

***Keywords****: intrusion detection, mobile agent, immune system*

## 1. Introduction

MA technology has been a very proficient research topic for some years now. Use of MAs in sophisticated applications offers an enriching advantage for constructing flexible and adaptable distributed wide-area systems. Indeed, as they can be retracted, dispatched, cloned or put in stand-by, MAs have the ability to sense network conditions, and to load dynamically new functionalities into a remote node.
In parallel, IDSs have become even more relevant in the context of large scale network infrastructures, where traditional security mechanisms demonstrate se-vere weaknesses [5].
The effective deployment of MA technology has unfortunately been hindered by security considerations: the use of code mobility requires issues like execution privacy and integrity to be solved. In spite of this, we believe that the mobility and network awareness of MAs can also significantly contribute to detect and to respond to intrusions. The security issues raised by the use of mobile code have resulted in intense world-wide research efforts, and we take the optimistic point of view that satisfactory solutions will eventually be available. Therefore we propose to apply MA technology as support for intrusion detection in computer networks, which is a relatively unexplored terrain. We concentrate on aspects of intrusion detection where the mo-

bility and autonomy of agents are of particular benefit. In the remaining sections of the paper we first describe the objectives and goals of our research project. Then, we propose a new model based on immune system which uses MAs for ID. For that, we explain briefly how the immune system works and we describe our MA model for ID using immune system principles. Finally, we draw our conclusion in the last section.

## 2. Project objectives and general approach

MAs have many characteristics that can help enhancing ID technology. We investigate our approach focusing on the four following aspects: detection mechanisms, response mechanisms, scalability and dependability of the IDS.

### 2.1 Detection mechanisms

We design general methods to allow agents to discover the network topology, and to take into account the apparition and disappearance of hosts and connection links. Such techniques are inspired from our previous work [6] and are designed to enable loosely coupled cooperative structures. Based on the discovered network topology, agents select and migrate to the hosts for auditing local activity using a strategic deployment scheme. They move and communicate through dynamically chosen routes, avoiding suspected zones by exploiting possible redundancies in the network structure.
To complete the detection arsenal, we also need to define methods for locating the origin of a detected intrusion. By systematically scanning the network segments we will distinguish the different sources of the incident: either inside or outside the protected system.

### 2.2 Response mechanisms

In practice, most IDSs are restricted to detecting attacks. We are however exploring ways in which MAs could respond to an attack: “how to filter incoming packets in case of attack from the outside: MAs could automatically travel through the network and disallow malicious packets from traversing the networks routers and firewalls. This low-level activity implies that our agent system provide active networking [7] capabilities. “how to quench the intrusion with a counter-attack in case of inside attacks; MAs could move towards the suspected place, and exploit their ability to isolate, slow down or shut down the damaged host. “ideally the IDS should also suppress the origin of the incident and restore system safety; we might here take advantage of MAs to deploy fresh code and to replace or re-program infected components.

### 2.3 Scalability

The overall architecture must exploit MAs to allow computational load and diagnostic responsibilities to be dynamically distributed throughout the network. As the number of computing elements in the network increase, agents can be cloned and dispatched to new machines in the network. To reduce its vulnerability, the IDS may be composed of several specialized structures, each one covering a specific aspect of intrusion detection as well as a specific network area. These structures will develop dynamically, while avoiding that overlap of essential functions arise between them.

### 2.4 Dependability of the IDS

Regarding the proposed IDSs level of dependability, the basic assumption is that it has to be conceived as a survivable system: all its constituents can be efficiently replicated, sacrificed and replaced thanks to mobility - this implies a second assumption, the availability of a safe agent execution platform (a Java Virtual Machine, or JVM). In fact, we consider each node of the IDS as an atomic entity running with a safe platform; damages inside the agent platform itself might be detected with watchdogs executing on auxiliary tamper-proof hardware as described in [4]. At a finer level of granularity, MAs might in some situations replace the platform's services with fresh code to sustain the attack a bit longer.

## 3. Concrete Approach

This section explains some important choices regarding the IDS model we propose and describes our approach based on immune system model. As initial hypothesis, we focus on a state-based, network-based IDS which analyses the local nodes periodically. Our approach is targeted at corporate intranets, which corresponds to a logical security domain and to the privileges a successfully infiltrated attacker would have. We want to avoid having a monolithic IDS on every host of the network because of its cost; instead, MAs are to be dispatched dynamically visiting and monitoring randomly or statistically different hosts: in this scheme the most compute-intensive tasks are thus performed periodically. Every node will host a dedicated JVM. Our concrete choice is the J-Seal platform [2], which currently is one of the most efficient and secure MA platforms.

Natural immune system provides a source of inspiration for today computer security notably in building IDS because the immune system evolves many interesting mechanisms to defend the human body against external attacks and aggressions.

The first anomaly detection system based upon principles derived from the immune system was previously introduced in [8]. From this work, a lot of similarities between the problem faced by computer security and immune systems has been pointed out in [9]: among all, like the human body, computers systems have to protect themselves because they are often placed in an unsafe and uncontrolled environment such as the open Internet.

### 3.1 Immune system-an overview

In the human body, the immune system could be seen as a complex network of specialized cells and organs that has evolved to defend the body against diseases and infections by "foreign" invaders such as bacteria, viruses, fungi, parasites, and debris.

In a first step the immune system attempts to prevent or stop the entry of these external organisms before they enter the body. In a second step it seeks their presence in the body in order to destroy them. For that, it distinguishes between molecules and cells of the body called "self" from foreign ones called "nonself". The body's immune defences normally coexist peacefully with cells that carry distinctive "self" marker molecules. But when immune defenders encounter "nonselfs" they have to eliminate them quickly.

Any substance which is capable of triggering an immune response or alert is called an antigen. This can be:

- a germ such as a virus, or even a part of a virus,
- a tissue or cells from another person (except an identical twin),
- a nourishing proteins unless they are first broken down by the digestive system,
- in abnormal situations, the immune system can wrongly identify self as nonself and can attack it: This is the so-called auto immune disease.

An antigen is recognized by means of markers called epitopes, which protrude from its surface. Most antigens, even the simplest microbes, carry several different kinds of epitopes on their surface.
The structure of the immune system is multi layered with defences provided at many levels, from the skin which is the outermost barrier of protection to the adaptive immune system which can be viewed as a distributed detection system in the body. The organs of the adaptive immune system called Lymphoid organs are positioned throughout the body and lodge the lymphocytes, small white blood cells that are the key players in the immune system. Lymphocytes T or T cells are one of the many kinds of specialized lymphocytes in the immune system. They mature in the thymus and travel throughout the body, using either the blood vessels or their own system of lymphatic vessels. Their surface are covered by randomly generated receptors that can map specific antigen's epitopes: each lymphocyte has one kind of receptor which binds a specific related epitope. As most of the self proteins circulate through the thymus, T cells that match self proteins are destroyed. Released in the rest of the body, they operate a so called negative selection because they detect nonself and ignore self.

### 3.2 The model

In this section we explain our choice regarding the use of MAs for ID. As we already mentioned, our approach is targeted at corporate intranet which corresponds to a logical security domain. We subdivide this intranet in several smaller local domains constituted by a set of hosts or machines. We want to avoid having a monolithic IDS on every host because of its cost; instead, we propose to dispatch MAs, dynamically visiting and monitoring randomly different local domains. These MAs detect local attacks using a model which matches very closely the immune system model.
Since the MAs we present here perform anomaly detection, we need two stages in the proposed model. In the first stage, we build for each domain, a profile of normal behaviour. The second stage is the anomaly detection itself.

#### 3.2.1 The learning stage

To detect local attacks each MA responsible for a local domain has to be able to discriminate between normal and abnormal activity. In the immune system it is doing by distinguishing "self" from "nonself". For more simplicity we choose to examine the good running of different programs and their deviation compared to a normal activity. For that, we collect short sequences of system calls when the program runs in safe conditions and environment, as it was done in [11]. In each local domain we run a different program and build a database specific to the program (Figure 1). This avoids having too big databases needed for data collection. This is a well known problem in anomaly detection system. This also avoids having too big corresponding management. This presupposes that, at the beginning of the second stage, the MAs placed in

each domain will be specialized in one program, in the sense that they will have to detect deviation of system calls specific to this program.

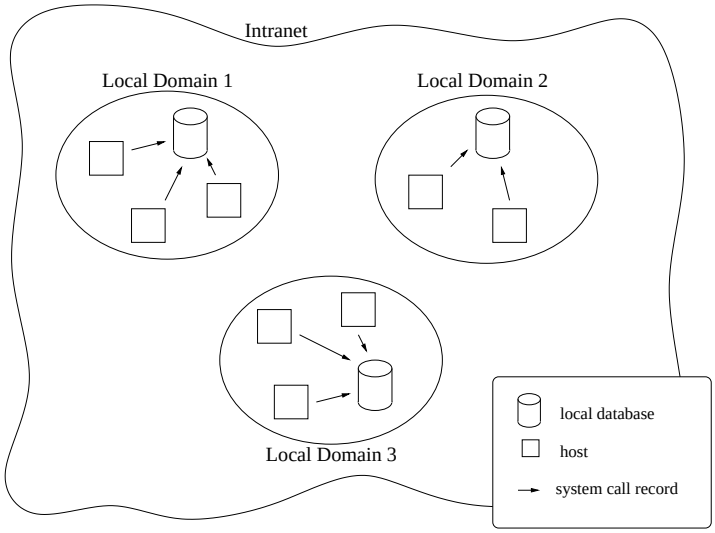


Figure 1: The learning stage

### 3.2.2 The anomaly detection stage

After the first learning step, MAs play their role in the detection step.
In each domain, MAs specific to a program are able to memorise a set of system call sequences obtained from the normal profile database. We propose that each program specific MA selects a set randomly (or selects one after the other, a block of n sequences) and examines locally, in each domain it is located, the deviation of the coming system call sequences from the selected set (Figure 2). If the deviation is too high the MA launches an alert. Otherwise, under a certain level of deviation the sequence is accepted. Each MA can be considered as short lived because it continually selects and memorises new system call sequences from its database. As we already mentioned, each local domain contains a database specific to the program we decided to inspect. In order to detect anomaly emerging locally from other programs or to allow a MA specific to a program to detect an anomaly in all the intranet we subdivided, we propose to use the mobility. Indeed each program specific agent will continuously circulate and visit randomly the neighbour domains where it performs anomaly detection before returning in its home domain to do the next sequences random selection. A-priori, as the number of MAs per domain is limited, we envisage to clone a MA before moving to the next domain, only if the level of suspicion for an anomaly becomes to high in the current domain, because the level of suspicion augments with the frequency of alerts for this anomaly.

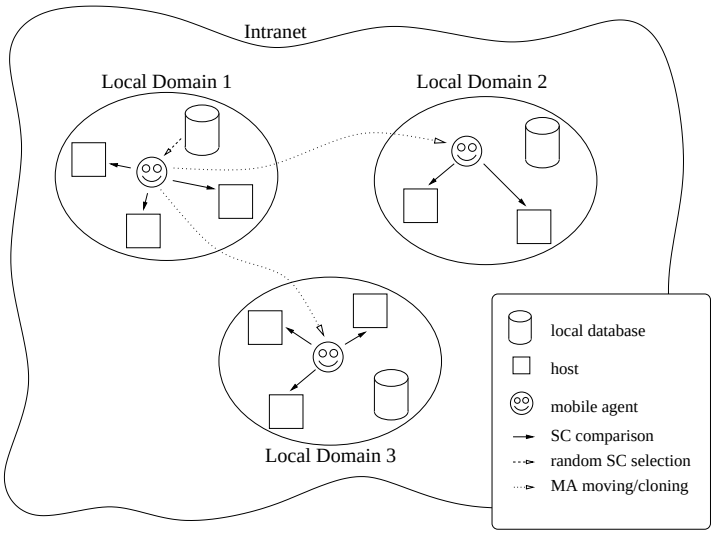


Figure 2: The anomaly detection stage

We are also investigating how to integrate our MA infrastructure with an existing IDS based on static intelligent agents (IAs), namely the MANSMA (Multi-Agents system-based Network Security Management Architecture) [1] [10]. In this architecture the Java-based IAs will be acting as providers of the high-level ID functionalities. The idea is to keep the global logic structure of MANSMA, notably for its intelligent and learning part, to allow more correlation between local domains. This will result in a collection of light-weight and heavy-weight MAs that together will reduce the amount of data transfer, provide more structural flexibility and enable load-balancing of the different functionalities between available network resources.

## 4. Conclusion

We propose to use MA technology for intrusion detection and response. Recently other researchers have started looking at the benefits drawn from mobility to enhance conventional IDSs [3][5], and there is hardly any aspect of our approach that hasn't already been described abstractly.The originality of our proposal lies in the way we apply MAs. We propose a structure with different levels of functionalities: mobile IAs with high-level ID functions, and lower-level MAs to enhance the flexibility and agility of the IDS. Above all, there is a trade-off between the quick detection of an attack and the rational use of network and computing resources by the IDS. One alternative is to transfer the computation to the local data sources using code mobility. Moreover, as specialized agents cover specific aspects of intrusion detection as well as specific network areas, we propose to incorporate network-aware MAs to implement efficient response mechanisms.

We also propose a new model for anomaly detection using MAs and we draw strongly our inspiration from the immune system model. Among all, the common key points our model borrows from the immune system are the following:

- the specificity because each MA is specialized in one kind of anomaly and memorises new sequences specific to this anomaly,
- the dynamicity because each MA continuously circulates through the different domains, which increases the global coverage provided by all the MAs over time,
- the autonomy because each MA can decide to clone itself only if the level of suspicion becomes too high in a domain,

- the distribution of databases among the different domains, which avoids a central point of failure and which allows a distribution of the different points of alerts in the intranet.

## 5. References

[1] K. Boudaoud, H. Labiod, Z. Guessoum and R. Boutaba, Network Security Management with Intelligent Agents, In proceeding of 2000 IEEE/IFIP Network Operations and Management Symposium (NOMS'2000), 10-14 April 2000, Nonolulu, Hawaii.
[2] Walter Binder, J-SEAL2 - A Secure High-Performance Mobile Agent System, in proceedings of the IAT99 Workshop on Agents in Electronic Commerce, at the 1st Asia-Pacific Conference on Intelligent Agent Technology (IAT 99), Hong-Kong, December 14, 1999.
[3] W. Jansen, P. Mell, T. Karygiannis, D. Marks, Mobile Agents in Intrusion detection and Response, in Proceedings of the 12th Canadian Information Technology Security Symposium, Ottawa, Canada, June 2000, to appear.
[4] S. Loureiro, R. Molva, Mobile Code Protection with Smartcards, accepted for publication at the ECOOP 2000 Workshop on "Mobile Objects: Operating System Support, Security and Programming Languages", Cannes, France, June 13, 2000, to appear.
[5] S. Martino, A Mobile Agent Approach to Intrusion detection, Joint Research Centre, Institute for Systems, Informatics and Safety, Italy, June 1999.
[6] M. Muhugusa, Distributed Services in a Messenger Environment: The Case of Distributed Shared-Memory, Ph.D. Thesis no 2903, University of Geneva, 1997.
[7] D. Tennenhouse et al., A Survey of Active Networks Research, IEEE Communications Magazine, Vol. 35, No. 1, pp. 80-86, January 1997.
best regards,
Noria Foukia.
[8] S. Forrest, A. S. Perelson, L. Allen and R. Cherukuri, "Self-nonself discrimination in a computer", In proceedings of the 1994 IEEE Symposium of Research in Security and Privacy, Los Alamitos, CA: IEEE Computer Society Press, 1994.
[9] S. Forrest, S. A. Hofmeyr, A. Somayaji, "Computer Immunology", Communications of the ACM, 40(10):88-96, 1997.
[10] K. Boudaoud, "Intrusion Detection: A new approach using multi-agents system", PhD thesis, EPFL, Switzerland 2001.
[11] S. Forrest, S. A. Hofmeyr, A. Somayaji, "Intrusion Detection using sequences of System Calls", Department of Computer Science, University of Mexico Albuquerque, NM 87131-1386.