

POM - A Mobile Agent Security Model against Malicious Hosts

Xudong Guan, Yiling Yang, Jinyuan You

Dept. of Computer Sci. & Eng., Shanghai Jiaotong University, 200030, China

{guan-xd, yang-yl, you-jy}@cs.sjtu.edu.cn

Abstract

Security, especially the attacks performed by hosts to the visiting mobile agents (the malicious hosts problem), is a major obstacle that prevents mobile agent technology from being widely adopted. Being the running environment for mobile agents, the host has full control over them and could easily perform many kinds of attacks against them. This problem has not been fully solved yet. After the analysis of mobile agent security requirements, this paper first gives some design issues of a practical security model of malicious hosts problem. Based on this, POM (Police Office Model), a mobile agent security model, is presented. By setting up special hosts called police offices within regions, POM can prevent most attacks performed by malicious hosts through the separation of the safety-critical parts of mobile agents from the malicious hosts.

1. Introduction

While mobile agent paradigm expresses many advantages over the traditional network computing models [1], the code mobility of the mobile agents brings some severe security problems. One of the problems lies in the attacks performed by the malicious agents against their execution environments, the *hosts*. Another security problem, often called as the *malicious hosts problem*, is the attacks by the host to the visiting mobile agents. The Police Office Model (POM) proposed here is a security model trying to solve the second problem.

2. The malicious hosts problem

In the mobile agent paradigm, the hosts have full control over the mobile agents running in them, which no longer works for them like that in the traditional computer system. Here we briefly conclude some of the attacks that could be performed by malicious hosts to the mobile agents, which are totally controlled by them.

a). *Spying*

Spying focuses on understanding the code, data, and network communication of the mobile agents. We call an spying attack *fast-spying* if the environment has no knowledge of whether the agent has been spied. Otherwise, we call it *tardy-spying*.

b). *Thieving and pirating*

Based on successful spying, the host could either steal data (thieving) or pirate code (pirating) from the agent.

c). *Manipulation*

Based on successful fast-spying, the host could modify the code, data, and network communication of a mobile agent or return wrong system call result without being known by the agent's environment.

d). *Other attacks*

Apart from the above attacks, there exist some others, for example, *killing, denial of service, flooding*, etc.

More detailed discussions can be found in [3] and [5].

3. Design issues

To solve the malicious hosts problem, some design issues are listed below, which should all be addressed by a practical security model.

a). *Spying attacks must be prevented first.*

In Section 2, most of the attacks are based on spying. By the prevention of spying, the agents could not be understood by the malicious host, so that the following attack chains might be cut off.

b). *Tardy-spying should not be neglected.*

Manipulation attacks could not be based on tardy-spying, yet thieving/pirating attacks can. A practical security model should also provide ways to prevent tardy-spying.

c). *Killing attacks should be considered.*

While preventing spying attacks, the security model should also pay attention to killing attacks. A simple way is to set up agent location tracing mechanism, which records the current location of every agent by introducing special-purpose tracing servers [6].

d). *Security model should either integrate with or be able to cooperate with other mobile agent facilities.*

Mobile agent system is a complicated distributed environment with many common services. A practical

malicious hosts security model should be facilitated by other existing/upcoming services to reduce overheads.

4. POM - Police Office Model

Analogy to the police office system in the real world, we introduce a special host called Police Office (PO) in each predefined region to carry out our security model, POM. Every visiting agent to a special region should first register at the region's PO before entering its destination. By this, the PO can discover the killing attacks and take some actions.

Before presenting POM in detail, we first give some basic concepts and assumptions.

Region: is made up of a special group of hosts, which have relatively high connection speed to each other and low connection speed to the hosts outside the region. Regions can not be overlapped.

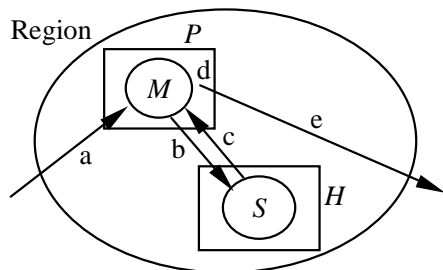
PO: is a special host belonging to each region, with the following characteristics:

- All hosts inside a region are supervised by the PO of that region.
- Given a host address, an agent can easily find the host's supervising PO.
- Every PO is assumed to be honest at any time, it never attacks any mobile agents.

MA: is a mobile agent, but now with some conceptual refinements. It is divided into the *master* part and the *slave* part. The master part is security-critical while the slave part is security-free. Moreover, the slave part is designed to be capable of only migrating between the host and PO.

Host: is the mobile agent running environment. It may perform all kinds of attacks to the visiting agent.

POM can be illustrated as figure 1.



Note: P - Police Office, H - Host
M - Master Part, S - Slave Part

Figure 1. Mobile agent migration model under POM

The steps of a mobile agent visiting a new host is described below:

- a). To visit host *H*, the mobile agent arrives at *H*'s supervising PO *P*.
- b). On *P*, *M*, the master part of the agent, become active. After some preparation, *M* sends the slave part *S* to *H* to perform some security-free actions such as data gathering.

c). *S* returns to *P* with its work result.

d). *M* performs some security-critical actions on *P* using the results returned by *S*. If there are more work to be done on *H*, *M* can send there another slave and back to step c), else it can choose the next destination to visit.

e). The mobile agent begins its next migration phase.

The two main obstacles in POM is region partitioning and MA code division. To get more details, the readers are encouraged to see [7].

5. Conclusions

While there are drawbacks in POM like the PO bottleneck and the add-on difficulties in agent programming, POM gives a new way towards a secure and general environment for the mobile agent computation. Moreover, it requires little computational overhead and can be integrated with other mobile agent facilities to improve the overall performance of the whole mobile agent environment.

The related work includes: mobile cryptography [2], time limited blackbox protection (TLBP) [3], cryptographic tracing [4], and tamper-resisted hardware [5]. A detailed analysis could be found in [7].

References

- [1] C. G. Harrison, D. M. Chess, and A. Kershenbaum, "Mobile agents: Are they a good idea?", IBM Research Report, March 1995. URL: <http://www.research.ibm.com/massdist/mobag.ps>
- [2] T. Sander and C. Tschudin, "Protecting Mobile Agents Against Malicious Hosts", G. Vigna (Ed.): *Mobile Agents and Security*, Springer-Verlag, 1998, pp. 44-60.
- [3] F. Hohl, "Time Limited Blackbox Security: Protecting Mobile Agents From Malicious Hosts", G. Vigna (Ed.): *Mobile Agents and Security*, Springer-Verlag, 1998, pp. 92-113.
- [4] G. Vigna, "Protecting Mobile Agents through Tracing", *Proc. of the Third ECOOP Workshop on Operating System Support for Mobile Object Systems*, 1997.
- [5] U. G. Wilhelm, "A Technical Approach to Privacy based on Mobile Agents Protected by Tamper-resistant Hardware", PhD Theses Nr. 1961. Departement D'Informa-tique, Ecole Polytechnique Federale de Lausanne, 1999. URL: <http://lsewww.epfl.ch/~wilhelm/Papers/thesis.pdf>
- [6] P. Zhu, "Research on Locating and Communication Services of Mobile Object System", Ph.D thesis, Shanghai Jiaotong Univ., 1999.
- [7] X. D. Guan, Y. L. Yang, and J. Y. You, "POM - A Security Model against Malicious Hosts", DCTC Tech Report, Shanghai Jiaotong Univ. Dec. 1999. URL: [http://gxd.home.chinaren.net/tr_dctc_pom\(1999_7_pages\).zip](http://gxd.home.chinaren.net/tr_dctc_pom(1999_7_pages).zip)