이동 에이전트 기술에서의 보안성 문제 분석

김정태
목원대학교

Analyses of Security Issues in Mobile Agent Technology

Jung-Tae Kim
Mokwon University
E-mail : jtkim3050@mokwon.ac.kr

요 약

As wireless communications and mobile multimedia services are booming nowadays, systematic research of the overall aspects of mobile security is crucial. This paper presents a frame model for guising the systematic investigation of mobile security. Based on the introduction of some background viewpoints of security targets from n novel perspective, the framework is described as a hierarchical model in which mobile security research is partitioned into three different layers.

I . Introduction

The mobile agent paradigm is an emerging technology for developing applications in open, distributed and heterogeneous environments, such as the Internet. Mobile agents(MA) are software entities that can block execution in their allocation node and resume it later in another network node. Agents are able to decide autonomously where to act after migrations. MA technology offers several advantages in many application areas, such electronic commerce, mobile, computing, network management and information retrieval. Mobile agents are designed to execute locally to the information they have to operate upon, thus reducing networks traffic and latency. In addition, the MA asynchronous interaction model can provide efficient solution in the case of unreliable and low bandwidth connections and in the support to mobile users that could disconnect while their agents roam in the network. Current research on agent-based systems generally does not exploit all the capabilities classified by these dimensions. For example, multi-agent systems based on distributed artificial intelligence try to execute a given task using a large number of possibly distributed but static agents that collaborate and cooperate in an intelligent manner. On the other hand, research on mobile agents usually emphasizes agent mobility and agent coordination, and mobile agents are typically assumed to only have very limited or even no intelligence. The development schema in the latter case is sometimes called a weak agent approach, which contrasts with the strong agent approach that involves artificial intelligence techniques.

II. Secure and Open Mobile Agent

SOMA offers a way to exploit the MA paradigm in several application areas, by providing a secure and open infrastructure for both execution sites and mobile agents. The SOMA support a hierarchy of abstraction localities suitable for modelling the internet scenario; against execute in places that represents physical nodes and can be grouped in domains abstraction that represent LANs possibly interconnected via gateway abstraction. In addition, SOMA supports a naming infrastructure capable of fiding mobile entities independently of their current allocation, a standard interface to exchange information with the CORBA dis tributed environment and a security framework.

III. SOMA Security Architecture

This section introduces the main building block of the SOMA security architecture in charge of supporting entity authentication, authorization, policy enforcement and credential management. The definition of different locality abstractions allows to enforce layered security policies in which actions are controlled at both domain and place level. The domain defines a global security policy that imposes general authorizations and prohibitions; each place can only apply restrictions to the domain-level set of permissions. The SOMA security infrastructure is composed of:

1) a policy server(PS) for managing domain policies; only SOMA administrators with the necessary privileges can use the policy editor to activate/de-activate the policies at the domain level;

2) a domain server(DS) in charge of maintaining consistent references to the resources visible in the domain;

3) a role server(RS) responsible for handling role management; a graphical role editor dynamically permits to associate principles with roles, to define new roles ad to update exiting ones;

4) a certification authority(CA) in charge of the issuing and the lifecycle management of certificates;

5) an authentication server(AS) for authenticating users, agents and execution sites;

6) an authorization server for permitting access to resources.

IV. A Mobile Agent System Design

Today's users demand ubiquitous network access independent of their physical location. This style of computation, often referred to as mobile computing, is enabled by rapid advances in wireless communication technology. The networking scenarios enabled by mobile computing range roughly between two extremes. At one end, the availability of a fixed network is assumed, and its facilities are exploited by the mobile infrastructure. We call this form of mobility logical mobility. At the other hand, the fixed network is absent and all network facilities must be implemented by relying only on the available mobility. Mobile agent technology is a new networking technology that deals with both forms of mobility. It offers a new computing paradigm in which a program, in the form of an intelligent software agent, can suspend its execution on a host computer, transfer itself to another agent-enabled host on the network, and resume execution on the new host, here, we define a host as either a stationary host or a mobile host that is situated in an ad hoc network.

Each node in a mobile as hoc network logically consists of a router with possibly IP addressable hosts and multiple wireless communications devices, or may be integrated into a single device such as a laptop or handheld computer. A set of nodes making up a Magnet area is essentially a "mobile routing infrastructure" and can operate in isolation or be connected to the greater Internet via exterior routing functionality. The nodes are equipped with wireless transmitters and receivers using antennas that can be omnidirectional, highly directional, steerable, or some combination thereof. At a given point in time, depending on the nodes positions, their transmitter and receive coverage patterns, transmission power levels, and co-channel interference levels, a wireless connectivity in the form of a dynamic, multi-hop graph or as hoc network exists between the nodes. Our approach to communication security in sensor network is based on a basic infrastructure, that says that data items must be protected to a degree consistent with their value. In the particular architecture, for which we are developing our communication security scheme, we differentiate between three types of data sent through the network

- Mobile code
- Locations of sensor nodes
- Application specific data

Following this categorization, we specify the main security threats and appropriate security mechanism:

- Fabricated and malicious mobile code injected into a network can change the behavior of the network in unpredictable ways.
- Acquiring locations of sensor nodes may help an adversary to discover locations of sensor nodes easier than using radio location techniques.
- Protection of application specific data depend on the security requirements of a particular application. In a target tracking application, which was a test case for the given security scheme, we treated the application specific data as the least sensitive type of data.

V. Agent Protection against Malicious hosts

As the mobile agents in the Mobile Grid Services will migrate to and execute on untrusted hosts, the code or the data of the mobile agents may possibly be modified by the hosts during the execution. Therefore, we should have some measures to protect the agents against malicious hosts which may attack their incoming agents. Unfortunately, this kind of agent protection is not provided in JADE or JADE-S. Among several current approaches for agent protection against malicious hosts(including execution tracing, computing with encrypted function, introducing a trusted hardware, and adding time limitation), execution tracing is the most suitable one because of the high feasibility, large scalability and relatively high accuracy. Execution tracing methods employ re-execution to detect malicious actions. For each mobile agent execution in a host, the initial state, inputs from the outer environment and the final state will be recorded in a trace. By using the details in the traces, the execution can be re-executed in another host. If any inc onsistent result is found in the re-execution, modification of data or code

of the mobile a gent by the malicious hosts can be detected. In the framework, we achieve this agent protection by combining the Random Execution Tracing into the Mobile Grid Services Frame work. To gain the protection, service developers are responsible to provide a checker (a gent carrying out the re-execution) for each Task Agent. Figure 2 shows the ste ps involved when the Random Execution Tracing is carried out in our framework. The steps are as follows:

1. The Agent Manager of a Mobile Grid Service at Node A sends its Task Agent to another host (Node B) for execution.
2. After execution on each host (Node B), the Task Agent will produce a trace (Trace B) for this host and forward it to the Agent Manager.
3. The Task Agent can then migrate to other hosts for other resources.
4. At the same time, a checker will be created in that host (Node B).
5. After the Task Agent has visited several hosts, the Agent Manager will randomly send each received trace to one of those checkers (except the one in the host producing that trace) for re-execution. In this example, Trace C is sent to the checker in Node B.
6. The checker compares its result and the recorded result after re-execution. If there is any inconsistency, there is an attack. Finally, the checker replies the result to the Agent Manager.

VI. Conclusion

Despite the advantages offered by MA systems, a wider diffusion of this technology is limited by the lack of a comprehnsive security framework suitable to address the protection of both agents and sites of execution without introducing significant performance constraint. A challenge is to build security mechanism that do not the features of mobile agents, such as autonomy and efficiency. These considerations have been taken into account in the development of the SOMA framework that supports the protections of both execution sites and agents as a distinctive feature. Efficiency and scalability have been key driving factors in the design of SOMA security solutions.

References

[1] V. Raghunathan, C. Schurgers, S. Park, "Energy-aware Wireless Microsensor Networks", IEEE Signal Processing Magazine, Vol. 19, N.2, IEE, March 2002, pp.40-150

[2] J. Kulik, "Negotiation-based protols for disseminating information in wireless sensor networks", Wireless Network, v.8, n.2, pp.169-185,2002

[3] W. Stallings, Network and Internetwork Security, IEEE Press, 2 edition, 1995

[4] W. Stallings, Network and Internetwork Security, IEEE Press, 2 edition, 1995

[5] A. Sinha and A. Chandrakasan, "Dynamic power management in wireless sensor networks," IEEE Design and Test of Computers, pp.62-74, 2001

[6] W. Fumy and P. Landrock,"Principles of key management," IEEE J. of Selected Areas in Communication, vol.11, pp.785-793, June 1993