IMTCI2004, International Workshop on Intelligent Media Technology for Communicative Intelligence, Warsaw 2004, pp.189-192

Mobile agents: preserving privacy and anonymity

Aneta Zwierko[1] and Zbigniew Kotulski[2]

[1] Warsaw University of Technology, Faculty of Electronics and Information Technology, Institute of Telecommunications, azwierko@tele.pw.edu.pl
[2] Polish Academy of Sciences, Institute of Fundamental Technological Research, zkotulsk@ippt.gov.pl

Abstract. The paper presents two new methods for providing mobile agents with privacy and anynomity. The proposed schemes are based on different cryptographic primitives: a secret-sharing scheme and a zero-konwledge proof.

1 Introduction

A software agent is a program that can exercise an individual's or organization's authority, work autonomously toward a goal, and meet and interact with other agents. Agents can interact with each other to negotiate contracts and services, participate in auctions or barter. Agents are commonly divides into the two types

– stationary
– mobile.

The stationary agent reside at a single platform, mobile can move among different platforms at different times.

Agents systems are used for intrusion detection, combined with metalearning agents create even more powerful tools for detecting security threats in network environment ([6]). Other field where agent systems are widely used are managment systems for telecommunication networks. The most popular telecomunication managment protocol, SNMP (Simple Network Managment Protocol), existing for over 20 years, is based on an idea of an agent and a manager. Many similar systems have been proposed in the past and still exists. Mobile agents are also well suited for software distribution and can provide adaptive responses to network events. Other practical application field for agents systems is the e-commerce where mobile agent-based applications have been proposed and are being developed for a number of diverse business areas like contract negotiations, service brokering, auctions, and stock trading ([3]). Mobile agents representing bidders may meet on an auction house's platform to engage in blind, straight, or Dutch auctions, each employing different strategies and having different financial constraints.

One of the new directions for the development of the agents' systems is a communicative intelligence. The future agents' systems are not only supposed to be communicating or/and interacting with each other but also with real people. They should have the same capabilities as people: to hide their identity when convenient and show their credentials when needed. Preserving privacy and anonymity, so easy in a human enviroment, is one of the current most significant problems in the agents' systems.

2 Security

Providing security is complex and tough for most existing services. It is even more problematic in distributed environment, such as agents' systems. Most important securiy requirements are ([5]):

- confidentiality: any private data stored on a platform or carried by an agent must remain confidential. Mobile agents also need to keep their present location and route confidential.
- integrity: the agent platform must protect agents from unauthorized modification of their code, state, and data and ensure that only authorized agents or processes carry out any modification of shared data.
- accountability: each agent on a given platform must be held accountable for their actions: must be uniquely identified, authenticated, and audited.
- availbility: every agent (local, remote) should be able to access data and services on an agent platform, which responsible to provide them.
- anonymity: agents' actions and data should be anonymous for hosts and other agents, still accountability should be enabled.

Threats to security generally fall into three main classes: disclosure of information, denial of service, and corruption of information ([5]).

3 Anonymity

The anonymity is very complex and tough to provide in classical services, like browsing web. It's even more complex to provide anonymous agents. Many services require the anonymity to function as in real world e.g some e-commerce transactions. If someone is observing actions of an agents, this can be itself a source of a very useful knowledge, even without eavesdropping on agents data. In many situations privacy and anonymity should be preserved ([2]).

Agents should be able to reveal (or not) their presence to other agents or hosts. For example an agent shopping for goods and services may wish to do so in privacy. Also during auctions or an initial phase of negotiations agents may want to remain anonymous. In some situations the knowledge that a particular agent is interested in some kind of services can be an adventage for a vendor over its opponents. In addition, an agent may not want to disclose which hosts it has visited before current. It may need to keep not only its present location but also route secret. However, the anonymity is not always an adventage in agents systems. Every agent has to authenticate itself to other agents or hosts to be able to performe needed actions e.g. when a financial transaction is to be carried out the platform may require some form of authentication. Also the authentication mechanisms provide accountability for user actions. An agent's anonymity is also connected with some security risk. In some cases the security policy of hosts does not accept anonymous agents, or offers different levels of priviligies with different anonymity levels. The level of sensitivity of the transaction or data for which agents request access may require the agent to offer different degrees of authentication ([1]). Also sometimes host may not be willing to accept agents that have been on certain platforms, e.g., outside the authority of certain approved security domains. In agent societies where reputation is valued and used as a means to establish trust, an agent's reputation can be harmed by other agents through masquerade. It should be protected by an agent platform.

In this paper we propose two mechanisms of agents authorization preserving its anonymity at a certain level.

4 Proposals

Assume, we have an agent system that contains n_1 agents and n_2 hosts. Each agent has to authorize itself to the host to be able to perform any action (e.g., buy anything, start negotiations, ask for an offer, etc.). Agents should be anonymous: malicious hosts, even working together, should not be able, basing on an authorization data, to identify actions performed by each agent. Still, this system should have some management capabilities and auditability: any authorized entity (e.g. manager) should be able to identify actions performed by each agent with each host. So, each pair agent-host should use a different authorization data, which will be unique, but should not enable host to differentiate between agents. One of possible solutions for such a system can be based on a secret-sharing scheme. The secret authentication-message is divided into n-parts: *t-1* parts are for host, the rest of them is distributed to agents. The treshold for the secret is t. When an agent comes to some host it is authorized to perform its actions because it has t'th part of secret and he can reconstruct it with the host. The agent is still anonymous because the host does not know which of *n-t-1* agents it is. We can assume that agents can be rented; meaning agents with shares of the same secret and performing the same kind of actions (e.g., biding during auctions, buying content) can be rented.

In our proposal the Asmuth and Bloom secure secret sharing scheme ([4]) is used. Every participant of this scheme is assigned a public modulus: p_i ($i = 1, \ldots, n$, $p_0 < p_i < \ldots < p_n$), where p_i can be prime or co-prime. The delear selects at random an iteger s, such as $0 < s < \prod_{i=1}^{t} p_i$. He computes the secret (denoted as k): $k \equiv s \pmod{p_0}$ and shares: $s_i \equiv s \pmod{p_i}$. The shares are distributed to participants via secure channel. There have to be at least t participants to recreate the secret. The combiner takes their shares and solves following system of equations:

$$s_{i_1} \equiv s \pmod{p_{i_1}} \ldots s_{i_t} \equiv s \pmod{p_{i_t}}.$$

This system has one unique solution according to Chinese Reminder Theorem.

In our system one such scheme is generated for each host: the host has a different secret k_j and $t-1$ shares. This enables the host to recreate the secret with at least one agent. To improve the anonymity we modify the scheme giving each agent several shares of the same secret: this way the host cannot follow the repeating visits of the agent if every time it uses different shares to authorize. The recreated secret can be used as a secret key in other schema or to authorize for different actions. Each host can have a few different sets of shares that will, e.g., enable authorized agents to gain different priviliges.

Other possibility for providing authorization to such agents is zero-knowledge proof (ZKP). Each agent has one and "‘prove"’ itself to host, without leaving any additional information. An ZKP-based anonymous authorization system will be presented during the conference and in the extended version of the paper.

5 Conclusions

Preserving anonymity and providing security is a main issue in many agents' systems. In this paper we propose a new authorization systems, enabling agents to stay anonymous. The presented systems are based on a certain secure secret-sharing scheme and, alternatively, on some zero-knowledge proof. These systems are effective way for providing the security and the anonymity for mobile agents. The proposed solution is easy to implement in many existing agents' systems, making possible a secure and anonymous communication between agents and other parts.

References

1. Reiter M. K., Rubin A. D.: Crowds: Anonymity for Web Transactions, ACM Transactions on Information and System Security, Vol. 1, No. 1, November 1998, pp. 66-92.
2. Kulesza K., Kotulski Z., Kulesza K.: On Mobile Agents Anonymity; Formulating Traffic Analysis Problems, in: Advanced Computer Systems, Proceedings of the 10th International Conference, ACS'2003, Miedzyzdroje, October 22th-24th 2003, pp. 15-21.
3. Kulesza K., Kotulski Z.: Decision Systems in Distributed Environments: Mobile Agents and Their Role in Modern E-Commerce, in: A.apinska, [ed.] Information in 21st Century Society, University of Warmia and Mazury Edition, Olsztyn 2003, pp. 271-282. ISBN 83-89112-60-4.
4. Pieprzyk J., Hardjono T., Seberry J.: Fundamentals of Computer Security, Springer-Verlag, Berlin 2003
5. Jansen W., Karygiannis T.: NIST Special Publication 800-19 - Mobile Agents Security
6. Chan P.K., Fan D.W., Lee W., Prodromidis A.L., Stolfo S.J., Tselepis S.: Jam: Java agents for meta-learning over distributed databases. In *Proceedings of the 3rd International Conference on Knowledge Discovery and Data Mining*, 1997.
7. Reyes A., Sanchez E., Barba A.: Routing Management Application Based on Mobile Agents on the INTERNET2. EUNICE 2000, Holland.