Chapter XI

Intelligent Software Agents:
Security Issues
of a New Technology

Stefan Kirn and Mathias Petsch
Technical University of Ilmenau, Germany

Brian Lees
University of Paisley, Scotland

INTRODUCTION

To obtain maximum benefit from the increasingly widespread use of the Internet in today's information-oriented society, powerful tools are required for gathering and preparation of information. Intelligent agents, which have emerged in recent years, provide a successful technological approach to information handling. Intelligent agents are becoming increasingly important because of their flexibility and power for cooperative working in solving complex tasks. Usually such an approach requires agents which have the capability for extensive cooperation and communication among themselves. This raises the question of security. But, up to now, little work has been done which addresses the security issues associated with intelligent agents.

For a new technology, such as that offered by intelligent agents, to be successful and widely accepted, it is necessary for systems, based on that technology, to be capable of maintaining security and consistency of operation when integrated into the existing infrastructure of an organisation. This paper explores some of the security issues relating to application of intelligent agents and the integration of such systems into existing organisations.

First, existing information security issues for enterprises are considered. Then, a short introduction to the new technology of agents and agent systems is given. Following this, the special security problems of the new technology of software agents and the emerging risks for software and enterprises are discussed. Finally, a new security architecture for multi-agent systems is proposed, together with an explanation of how this multilevel architecture
can help to improve the security of agent systems.

Security Issues in Information Technology Systems

Because of the increasing importance of timely reaction by an enterprise in an ever-changing, competitive market environment, convenient access to and use of up-to-date information is becoming a key factor for economic survival. Indeed, the continuing existence of an enterprise may be heavily dependent on the support provided by well-designed and secure information systems made possible through the application of state-of-the-art information technology (IT). Secure and robust information systems are necessary to protect enterprises from bankruptcy after a possible collapse of the IT infrastructure.

The last few years have seen a steep rise in the globalization of markets. As a result, commercial enterprises are forced to enter the global competitive arena and to adopt a strategy directed towards inter-organizational cooperation. The result is the deployment of increasingly more complex software systems, leading to extended communication requirements between the different IT systems, and hence to the need for an inter-organizational standard for IT infrastructure.

To avoid, or at least minimize, the risks resulting from the introduction of new complex IT systems and their coordination among existing IT systems, it is necessary to identify the problems, risks, or threats in the overall IT infrastructure and to develop strategies to guarantee security in these systems.

In considering security issues we can distinguish between security and safety. The word security describes the ability of software to fend attacks against the system. But, safety means the robustness of information systems versus emerging problems and exceptions. This chapter mainly treats security issues in connection with safety; security problems resulting from the robustness of the system are more the object of software engineering research.

According to Rannenberg et al. (1997) security is considered to mean the enforcement of protective goals against intelligent attackers. They identify four security threats with their associated protective goals, which those threats aim to attack (Table 1).

The above-mentioned classification of threats can be very helpful in the identification of possible risks. Many opportunities may exist for malevolent persons to create threats. It is possible to gain unauthorised access to information through eavesdropping on communication channels. Unauthorised modification of information may be achieved through either active modification of messages (possible when the attacker has, for example, access to a router) or when the message is held and is transmitted later in an other context (which is also possible when the attacker has access to a router).

The availability of information may be under threat either when the attacker can

<table>
<thead>
<tr>
<th>Threat</th>
<th>Protective Goal</th>
</tr>
</thead>
<tbody>
<tr>
<td>unauthorised information gain</td>
<td>confidentiality</td>
</tr>
<tr>
<td>unauthorised modification of information</td>
<td>integrity</td>
</tr>
<tr>
<td>unauthorised derogation of functionality</td>
<td>availability</td>
</tr>
<tr>
<td>inadmissible loss of bind</td>
<td>accountability</td>
</tr>
</tbody>
</table>
Related Content

A Method of Assessing Information System Security Controls
[www.irma-international.org/chapter/method-assessing-information-system-security/23352/](www.irma-international.org/chapter/method-assessing-information-system-security/23352/)

A New Meta-Heuristics for Intrusion Detection System Inspired from the Protection System of Social Bees

Dilemmas of Online Identity Theft
[www.irma-international.org/chapter/dilemmas-online-identity-theft/13465/](www.irma-international.org/chapter/dilemmas-online-identity-theft/13465/)

Social Responsibility and the Transition Toward a Knowledge-Based Society in Latin America
[www.irma-international.org/chapter/social-responsibility-transition-toward-knowledge/7392/](www.irma-international.org/chapter/social-responsibility-transition-toward-knowledge/7392/)

A Secure Hybrid Network Solution to Enhance the Resilience of the UK Government National Critical Infrastructure TETRA Deployment
[www.irma-international.org/article/secure-hybrid-network-solution-enhance/53012/](www.irma-international.org/article/secure-hybrid-network-solution-enhance/53012/)