

ISSUES IN A MOBILE AGENT-BASED MULTIMEDIA RETRIEVAL SCENARIO

D.R.A. de Groot ^a M.L. Boonk ^b F.M.T. Brazier ^a A. Oskamp ^b

^a *Intelligent Interactive Distributed Systems Group, Department of Computer
Science, Vrije Universiteit Amsterdam
{dra.de.groot, fmt.brazier}@few.vu.nl*
^b *Computer and Law Institute, Vrije Universiteit Amsterdam
{a.oskamp, m.boonk}@rechten.vu.nl*

Abstract

Full version of this paper has been published in the proceedings of the 4th International Workshop on the Law of Electronic Agents 2005 (available at www.lea-online.net).

Mobile agents traverse the Internet, often on behalf of their users, moving to different sites with different characteristics. Mobile intelligent search agents access information in heterogeneous, often dynamic, environments. The legal and technical implications of the use of agents in such situations are not fully understood. Identity management, integrity, traceability and availability are major issues in this context. A scenario, in which mobile search agents search a multimedia database on behalf of their users, is used to illustrate the importance of the issues in a specific context and to identify technological requirements.

In our scenario, users interact with a personal search application designed to help them find snippets of movies. Mobile intelligent search agents are used to access information across the Internet: movies stored in a remote multimedia database. An example search task could be to find a snippet of a movie picturing a scene of a dog riding a bike.

In such situations, migration of agents has several advantages. First of all, a continuous, reliable high-bandwidth connection with the multimedia database service provider is not needed. Secondly, it provides service providers the option to exercise control over data returned to the users of mobile agents, e.g. to prevent misuse of the data. As in our scenario, with multimedia files in a remote database, there is a high risk of copyright infringement.

Once the search task has been completed, this scenario assumes that the agent contacts a guardian agent provided by the hosting location (cf. Noordende [2]). The guardian agent notifies the user and provides low-quality streams of the video snippets for pre-view purposes. The user is given the opportunity to accept one or more of the results, or to provide its agent with feedback on the results. Once the user has found the movie snippets he/she was looking for, a high quality download or shipment can be arranged along with payment options. The issue is that an agent first needs to negotiate an agreement with the agent platform that offers access to the multimedia database service before an agent can start its search. An agreement is needed in which both the facilities provided by the platform (both resources and services) and the procedures on the platform (e.g. whether the agent can communicate with its user while the agent is on the platform and whether the agents process is terminated after it has finished its search) are defined. In addition to the above agreement, an agent may want guarantees on the level of performance offered by an agent platform. If this is the case, a Service Level Agreement (SLA) can be agreed upon.

Identity management becomes an issue when agents request access to the hosts of a service provider. A service provider may want to know who the agent and its user are and ask proof of their identities. Thus, agents and user identities need to be managed. Technical solutions entail the introduction

of local names and global agent identities. Local names can function as a pseudonym for a specific agent in a specific environment. When needed, a mapping of an agents local name can be made to the global agent identifier, e.g. for access control, to reveal a users identity or show links between local names. It is not evident what and how much information on the identities of agents and users is needed in which situations; these issues need further research.

But what if an agent has legitimate access to the system and (maybe not intentionally) misbehaves and causes damage? Logging of communication and actions is necessary, for example because administrators need logs to be able to track which agent caused havoc, where it came from and to whom it belongs. For logging, tracing and identification, agents need to have unique identifiers. To determine responsibility and liability, logs are important to reconstruct the situation afterwards. Maintaining system-wide logs may be complicated due to the distributed nature of the system, however, mechanisms and policies are needed to prevent loss of information, i.e. logs should be robust and information should not disappear because of a failing node. Note that EU privacy regulations impose requirements on information maintained in identity administration and logs. User privacy needs to be respected in accordance with privacy regulations. Also, unauthorized access to the logs and administrative data should be prevented. What degrees of privacy protection (for example, anonymisation, traceable anonymity or pseudonymity) can be used in which situation needs further research.

To ensure proper functioning, guarantees on integrity of the system are needed, which can be subdivided into protection of entities (e.g. agents, hosts, services), data (e.g. content data, administration, logs) and transmissions (e.g. messages send by agents). Logs can be used for maintaining integrity of the system, for example, to determine where and when an agent has been tampered with. Integrity is partly regulated by law and needs to be enforced by technological measures.

The last, but not the least issue is availability of the system. To maintain its reputation as a reliable service, a service provider tries to limit interruption or disruption of its service (a user may have subscribed to a specific service with a predefined quality of service, at a given cost). As a result, service and system availability needs to be guaranteed.

The AgentScape platform provides a number of mechanisms which can be used to design systems and meet these requirements: the use of global and local agent identities, leasing of resources, sandboxing of agents, signing agents code and its state, mechanisms for logging, and secure communication. Policies are a current focus of research. Other foci are: 1) Logging in distributed mobile agent environments; 2) Identity management of agents and users in mobile agent systems; 3) Mobile agent systems and security issues, e.g. agents carrying and communicating confidential information.

Acknowledgements This multi-disciplinary research is a continuation of the ALIAS project [1], in which legal implications of the use of agent systems from both a legal and technological perspective are investigated. The authors thank the Vrije Universiteit and Stichting NLnet (<http://www.nlnet.nl>) for their support.

References

- [1] F.M.T. Brazier, A. Oskamp, J.E.J. Prins, M.H.M. Schellekens, E. Schreuders, N.J.E. Wijngaards, M. Apistola, M.B. Voulon, and O. Kubbe. Alias: Analysing legal implications and agent information systems. Technical Report IR-CS-004, 2003. Technical Report.
- [2] G. van 't Noordende, F.M.T. Brazier, and A.S. Tanenbaum. Security in a mobile agent system. 2004.