

Migrating agents: Do sysadmins have a license to kill?

M. Apistola², F.M.T. Brazier¹, O. Kubbe¹, A.Oskamp², J.E.J. Prins³, M.H.M. Schellekens³, M.B. Voulon²
(in alphabetical order)

¹ Intelligent Interactive Distributed Systems
Faculty of Sciences, Vrije Universiteit Amsterdam

² Computer and Law Institute
Faculty of Law, Vrije Universiteit Amsterdam

³ The Center for Law, Public Administration and Informatization
Faculty of Law, Tilburg University

Email: {frances, kubbe}@cs.vu.nl, {a.oskamp, m.b.voulon, m.apistola}@rechten.vu.nl;
{m.h.m.schellekens, j.e.j.prins}@kub.nl

Introduction

A mobile agent is a process that can autonomously decide to move from one machine to another across the Internet. Migrating entails serialising code, data and state into an agent image, acquiring permission to move, "shipping" its image to another machine, and requesting activation on the new host. Each local network may have a specific policy with respect to the agents it is willing to accept and activate, and under which conditions. This paper is based on results of the ALIAS research project¹ in which legal experts, computer scientists and AI experts aim to increase the understanding of the legal and technical implications of the use of mobile software agents. A number of legal and technical issues concerning the implications of hosting mobile, possibly hostile agents are addressed.

Legal considerations

The legal problem in this paper is whether sysadmins are allowed to shut down mobile agents that run on their computer system. Examples of mobile agent systems are Tacoma [1, 2] and d'Agents [3, 4]. When analysing the problem from a legal point of view, three rules of thumb can be distinguished. First of all, the sysadmin (or, rather: the service provider for who s/he works) is involved in a contractual relation with clients. The clients are users of a certain service. A sysadmin (or rather, again, a service provider) can contractually be obliged to guarantee provision of a service to a client, including the necessary resources to host mobile agents. Peak usage (between 6 pm and 8 pm, for example) may cause problems. Depending on the exact circumstances of a case, this may involve a breach of contract on behalf of the service provider. To reduce the risk of not being able to provide the necessary resources a sysadmin may need to decide to refuse to host agents other than those owned by his own clients onto his machines when needed. The second "rule" that can be distinguished is that a service provider may have the right to block specific mobile agents from entering his computer system because of his own interest in keeping system resources available for his own core business. The third rule entails the general duty to protect computer systems and data. This duty arises from criminal law, which sanctions negligence in case of the destruction or alteration of computer data. Therefore, if a sysadmin could have known that certain mobile agents cause damage, but still allows the agent to enter his system, the sysadmin might be criminally liable.

The case of eBay vs. Bidder's Edge,² decided in the United States, is relevant. This case can be seen as an application of the second rule. Furthermore, arguments used in the case can be applied by analogy regarding the other two rules. The case is as follows. Bidder's Edge maintains a so-called "portal-website." Via this site websurfers could access all kinds of online auctions. Bidder's Edge maintained a database of the products that were offered via online auctions. This database was updated using software robots: computer programs which operate across the Internet to perform searching, copying and retrieving functions on the websites of others. In this case, Bidder's Edge used software robots (also known as spiders or crawlers) to search the database of eBay. In the end, the court decided that the use of these robots by Bidder's Edge constituted *trespass to chattels*. Trespass to chattel arises out of unauthorized dispossession, use or interference with the tangible property of another. Historically this required some form of physical contact with the chattel. Recently, courts have argued that electronic signals are sufficiently tangible to support a trespass action. Furthermore, trespass requires some form of diminishing of the condition, quality of value of personal property. According to the court, the sending of 80,000 to

¹ The website of the ALIAS Research group can be found at: <http://www.iids.org/alias>

² 100 F. Supp. 2d 1058 (N.D. Cal. 2000)

100,000 requests per day to eBay's computer systems, can diminish the value of these computer systems "by using valuable bandwidth and capacity, and necessarily compromising eBay's ability to use that capacity for its own purposes".

Technical considerations

In order to deal with and prevent cases such as this, sysadmins may need to consider several technical issues related to identifying agents, identifying and assigning permissions, and dealing with suspicious agents.

Identify agents: A systems administrator could require information on the identify of an agent before deciding to host an agent. Agents can be identified by a unique number, or name (e.g. of the owner), or a certain specific characteristic. In case of updating the Bidder's Edge database software robots were used to search, amongst others, eBay's database. eBay's sysadmin could identify agents such as the Bidder's Edge agents. Their agents could, for example, be identified by names such as 'Bidder's_Edge_Agent_001'.

Identify permissions: once agents have been identified, the systems administrator needs to determine and assign access rights. Examples are permissions to access the system, read, write, store, delete and change content. In case of eBay for example, it was *technically* possible to, extensively, access their system by Bidder's Edge agents.

Dealing with suspicious agents: Although many technical security solutions exist, such as firewalls and encryption tools, absolute security remains impossible. One cannot absolutely prevent damaging agents from entering a system. If a suspicious agent is identified, the system administrator has several options. In the eBay case he could consider isolating the suspicious Bidder's Edge agents in such a way that is not harmful to eBay's system. He could also consider isolating the suspicious Bidder's Edge agents and storing enough data in order to allow the agents to resume on another system. A more drastic option which eBay's sysadmin could consider is killing Bidder's Edge agents. In all cases the sysadmin could consider notifying the owner of the agents (Bidder's Edge) of their illegal presence and their potential termination.

About the authors

Martin Apistola and Marten Voulon are PhD-students at the Computer and Law Institute at the Vrije Universiteit Amsterdam. Onno Kubbe is adjunct researcher within the IIDS group at the Vrije Universiteit Amsterdam. Maurice Schellekens is a post-doc researcher at the Center for Law, Public Administration and Informatization of the University of Tilburg.

Frances Brazier is a full professor in the Intelligent Interactive Distributed Systems (IIDS) group at the Vrije Universiteit in Amsterdam. Anja Oskamp is a full professor within the Computer and Law Institute at the Vrije Universiteit Amsterdam and also a full professor at the University of Nijmegen. Corien Prins is a full professor at the Center for Law, Public Administration and Informatization of the University of Tilburg.

This collaborative project would not have been possible without the Stichting NLnet's financial support.

References

- [1] Gray R.S. (1995) Agent Tcl: A transportable agent system. In Proceedings of the CIKM Workshop on Intelligent Information Agents, Fourth International Conference on Information and Knowledge Management (CIKM 95), Baltimore, Maryland, December, 1995.
- [2] Johansen D., Renesse R. van, Schneider F.B. (1998) Operating system support for mobile agents. Mobility, Mobile Agents and Process Migration - An edited Collection", Dejan Milojicic, Frederick Douglass, and Richard Wheeler eds., Addison Wesley Publishing Company, 1998.
- [3] Johansen, D. Schneider, F.B. Renesse, R. van. (1998) What TACOMA taught us. In, "Mobility, Mobile Agents and Process Migration - An edited Collection", Dejan Milojicic, Frederick Douglass, and Richard Wheeler eds., Addison Wesley Publishing Company, 1998.
- [4] Lauvset K. J., Johansen D., Marzullo K. (2000) TOS: A Kernel of a Distributed Systems Management System