**COMPUTER SCIENCE LITERATURE REVIEW REPORT**

This abridged model of a Computer science technical Literature review report has been adapted from a report by **Luther Krake**, DSTO, titled **Mobile Agent Security**.

| | |
|---|---|
| Overview<br><br>Purpose | **Abstract**<br><br>To function in open computing environments, mobile agents must access and make use of resources supplied by remote host platforms. The interaction between a mobile agent and its host immediately raises the issue of trust: can the agent trust that the host will not tamper with it and can the host trust that the agent will not act maliciously towards it? This paper surveys the various security threats that can arise in agent-based distributed systems and examines the techniques that can be employed to counter them. |
| Background definition of terms<br><br>Context<br><br>In-text citations (Vancouver<br><br>Location of the paper in the research literature<br><br>Purpose of report | **1. Introduction**<br>A mobile agent is 'an executing program that can migrate, at times of its own choosing, from machine to machine in a heterogeneous network' [1]. Like itinerant workers [2], mobile agents travel from place to place in order to work (i.e. achieve a goal or goals) and rely on the goodwill of strangers… (cont).<br><br>Many of the advantages that mobile agent paradigm has over traditional distributed programming paradigms are due to this ability to execute locally, close to the data to be analysed or near the system outputs to be processed.<br><br>Trust is clearly an important requirement for interactions between mobile agents and remote hosts. In closed environments, trust can usually be taken for granted because the agents & its remote host infrastructure will generally be working in the interests of a common user or group of users. However, in open computing environments like the Internet, mobile agents are likely to interact with arbitrary remote hosts…So there is potential for malicious behaviour. Chess et al [2] describe security as 'one of the cornerstone issues' in mobile agent computing…(cont.)<br><br>Not surprisingly, a lot research in recent years has been directed at solving the unique security problems raised by open agent- based distributed systems. Much of this work has focused on developing mechanisms to protect the remote host from attack by malicious agents. Consequently, a high level of host protection is now achievable [6]. However, the more difficult problem of protecting the security of the mobile agent remains an open research topic.<br><br>This paper surveys the various security threats that can arise in open agent-based distributed systems and examines the techniques that can be employed to counter them. Particular attention is paid to the problem of how to protect mobile agents from malicious hosts. |

Discussion – identifying the problems

## 2. Mobile Agent Security Threats (p2)

A variety of sinister-sounding security hazards can occur in agent-based distributed systems. For example, the mobile agent literature warns of 'subversion', 'hijacking', 'brainwashing' [3], and 'sabotage', 'implanting', and 'killing'.

To make sense of the various threats to mobile agent systems, it is instructive to apply some broad categorisations. First, threats can be grouped according to which entity is the source of the threat and which entity is the target. Four threat categories can be identified:

1. A malicious mobile agent can attack a host platform.
2. A malicious host platform can attack a visiting mobile agent.
3. A malicious mobile agent can attack another mobile agent.
4. Some other malicious third party can interfere with a host platform.

Sentences introducing bullet points

In the case of a malicious mobile agent attacking a host platform there are generally three forms that an attack can take:

Note bullet points to list areas covered

These are expanded on in the original.

- ***Masquerading*** (i.e. a mobile agent poses as an authorised agent to gain access to services and/or data to which it is not entitled...(cont.)
- ***Denial of service*** (i.e. a mobile host consumes excessive amounts of the host platform's computing resources…(cont.)
- ***Unauthorised access*** (i.e a mobile agent obtains access to services and resources on the host platform without permission to do so…(cont.)

Attacks by a malicious host platform against a visiting mobile agent typically take one of four forms:

- …..
- …..

An attack by a malicious mobile agent against another mobile agent will generally take one of four forms:

- ….
- ….

Indicates what is to come

The following section surveys the techniques that have been developed to counter these security threats.

Lit. survey discussion – finding solutions

## 3. Protection Mechanisms (p4)

Having outlined the various security threats in open mobile agent systems, it is clear that some can be handled using existing security approaches while others have unique requirements that demand new approaches….(cont.)

Note numbering systems for subheadings

### 3.1 Protecting the Mobile Agent

In an open agent-based distributed system, the mobile agent is most vulnerable to attack. This is because …… Indeed [2], [3], [6], and [12], all report that…. To this end a variety of techniques have been

| | |
|---|---|
| Critical analysis of solutions - expanded on in the original | proposed to tackle the unique security requirements of mobile agents.<br>• Tamper-proof hardware …<br>• Obfuscation…<br>• Undetachable Digital Signatures…<br>• Secure Function Evaluation…<br>• Nested Execution Environments. Bem [13] proposes an approach based on… |
| Note use of linking words | A major disadvantage of this approach is the extra bandwidth required to send three agents instead of just one. It is also likely that the indirect execution of the agent would adversely affect its speed of execution. Furthermore, a determined malicious host is likely to be able to reverse-engineer an agent's interpreter given sufficient time. New languages and interpreters could be generated to keep ahead of such developments; however, the associated development cost would probably be prohibitively expensive.<br>… |
| Logical use of sub headings | **3.2 Protecting the Agent Platform**<br>The host platform is also vulnerable to attack; however, the technology available to protect the host is more mature than it is for the converse problem of protecting of protecting the mobile agent. Consequently, a high level of host protection is now achievable [6], The following dot points describe some of the main host protection mechanisms:<br>• **Sandboxing**. Sandboxing is an …….<br>• **Code signing**. This approach requires that……<br>• **State appraisal**. Farmer et al [15] describe a state appraisal mechanism, which allows<br>… |
| Returns to the purpose of the report<br><br>Overviews what has been covered<br><br>Opens out to general issues again | **4. Conclusion**<br>In open computing environments, mobile agents and remote hosts are susceptible to a wide range of security threats. This paper has surveyed the sorts of security threat that can arise in such systems and has also examined the major protection mechanisms that have been developed to address these threats. Many different techniques have been proposed; however, not all are practical…. Nonetheless it is important that research continues since, unless the remaining security issues can be addressed satisfactorily, the mobile agent paradigm is unlikely to gain widespread acceptance and fulfil its potential. |
| | **5. References**<br>*See original report for list of references.* |