Intelligent agent technology within information warfare

Busuttil, T. B. and Warren, Matthew. 2001, Intelligent agent technology within information warfare*, Journal of information warfare*, vol. 1, no. 2, pp. 52-61.

©2001

Reproduced with permission.

Online copyright Mindsystems Pty Ltd
www.mindsystems.com.au
www.jinfowar.com

Downloaded from DRO:
http://hdl.handle.net/10536/DRO/DU:30001243

DRO
Deakin Research Online,
Deakin University's Research Repository
Deakin University CRICOS Provider Code: 00113B

Intelligent Agent Technology Within Information Warfare

T. B. Busuttil, and M. J. Warren

School of Computing and Mathematics
Deakin University, Australia
E-mail: tbb@deakin.edu.au

Abstract

Research into Intelligent Agent (IA) technology and how it can assist computer systems in the autonomous completion of common office and home computing tasks is extremely widespread. The use of IA's is becoming more feasible as the functionality moves into line with what users require for their everyday computing needs. However, this does not mean that IA technology cannot be exploited or developed for use in a malicious manner, such as within an Information Warfare (IW) scenario, where systems may be attacked autonomously by agent system implementations. This paper will discuss the current state of malicious use of IA's as well as focusing on attack techniques, the difficulties brought about by such attacks as well as security methods, both proactive and reactive, that could be instated within compromised or sensitive systems.

Introduction

The growing need of information technology users to complete more tasks in less time has been the driving force behind the development of agent technology. Agents are entities that act on our behalf. Software Agents perform tasks for us, learn about our wants and needs and let us carry on with our everyday tasks whilst they complete some of our tasks autonomously (Vitek & Castagna, 1999). Due to the immense amount of information, both formatted and unformatted, which resides across the Internet, Agents have a seemingly boundless workplace where tasks such as collection, matching, choosing and sorting of information and data are being started or completed constantly (Sharpe, 1997). Information Warfare attacks have also continued to increase in both frequency and effectiveness as new technology and IT methodologies surface (Black, 1996). Just as agent technology can be very helpful in the completion of tasks it can also be used or programmed to act in a malicious manner (Goldschlag et al, 1998, Hunter, 1999). Agents may be developed from the beginning of the lifecycle to behave in a damaging manner on certain systems (Washington, 1995).

Few agent systems have been blatantly attacked and exploited (Wilder & Dalton, 1997), however vulnerabilities are apparent within existing systems and the exploitation methods required to cause damage or disruption within agents and agent systems are being reviewed and researched currently (Hohl, 1998).

Taxonomies of Agent Technology

Agents can be deployed in a number of different schemas so as to complete a required task to the best possible level of effectiveness and efficiency. There are a number of predominate taxonomies that are in existence in the field of agents. These are:

- Single Static Intelligent Agents;
- Single Mobile Intelligent Agents;
- Collaborative Mobile Intelligent Agents and
- Multiple-Intelligent Agent Systems.

Single Static Intelligent Agents

A single agent employed to complete a task for a user on a commercial system that it is installed on is schematically described as being a Single Static Agent. This is a simple taxonomy wherein a user provides input, the agent completes its designated task and some output is produced. Security is an issue but in this case the agent tends to be isolated from networks and therefore less prone to IW-based attacks.

The most prevalent use of the single static agent in a commercial environment is within a database as a search agent shown in Figure 1. The user would input a query, the agent then seeks information regarding the query, and outputs information based on the query search.

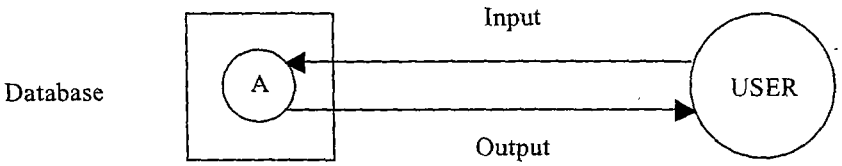

Figure 1: Single Static Intelligent Agent

Single Mobile Intelligent Agents

Mobile agents are useful at finding things that are stored across distributed systems such as the Internet. A single mobile agent can be deployed with the agenda of searching for information distributed across web servers and other such systems. As the agent is mobile it is capable of transporting itself from one networked system to the next completing any allocated tasks. Security in this case is a far greater problem than with static agents as the mobile agent may interact with many hosts on many systems (Tschudin, 1999) possibly leading to some sort of malicious attack toward or from the mobile agent.

Web spiders or Web indexing agents are the most popular uses for single mobile agents. These agents tend to hop from networked system to networked system searching and returning indexes ofthe documents store on servers as shown in Figure 2.

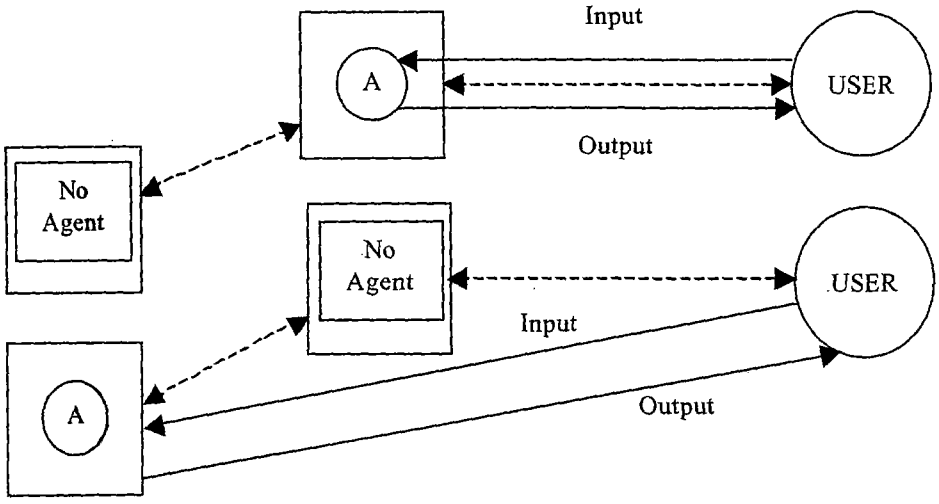

Figure 2 – Cycle of a Single Mobile Intelligent Agent

Collaborative Mobile Intelligent Agents

Singular mobile agents have many uses, however, when mobile agents are used in groups to complete more complex tasks such as Internet shopping the abilities of agent technology are truly seen. The ability of agents to share information and also learn from new information means that the decision making process that agents follow can be refined autonomously. This information exchange and sharing can also lead to security problems within the commercial environment due to the possibility of agent sabotage or host sabotage by hosts, agents or outside sources.

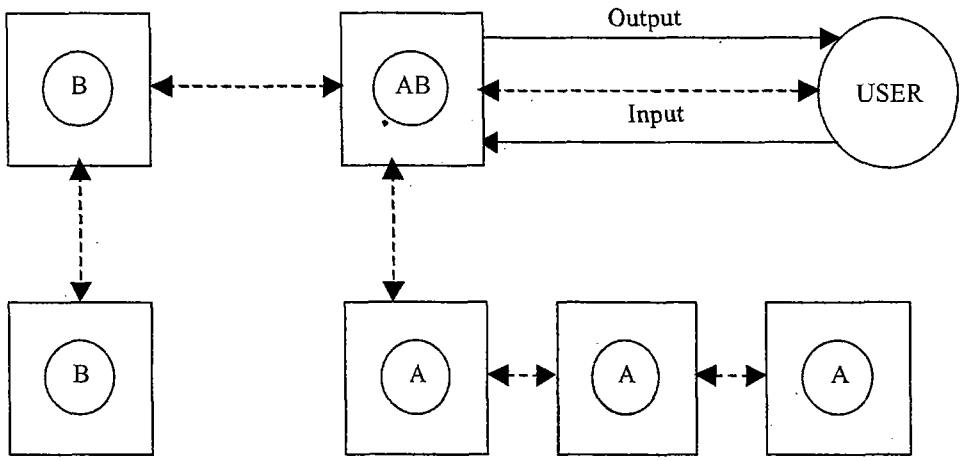

Figure 3 – Cycle of Collaborative Mobile Agent System

Multiple Intelligent Agent Systems

Multi-Agent Systems are similar in schematics to a collaborative agent system, however, in this case the system tends to be in a more logically and physically secure arrangement where network hosts and agents are all either trusted entities or are at least authenticated and certified as being trustworthy. Despite the increased security of this agent taxonomy there are still risks involved with the use of multi-agent systems (Wooldridge & Jennings, 1998).

An example of a multi-agent system is a financial investment package. This system searches trusted exchanges and brokerages to find investments for clients, which coincide with customer spending limits and preferred investment type within a secure trade circle as depicted in Figure 4.

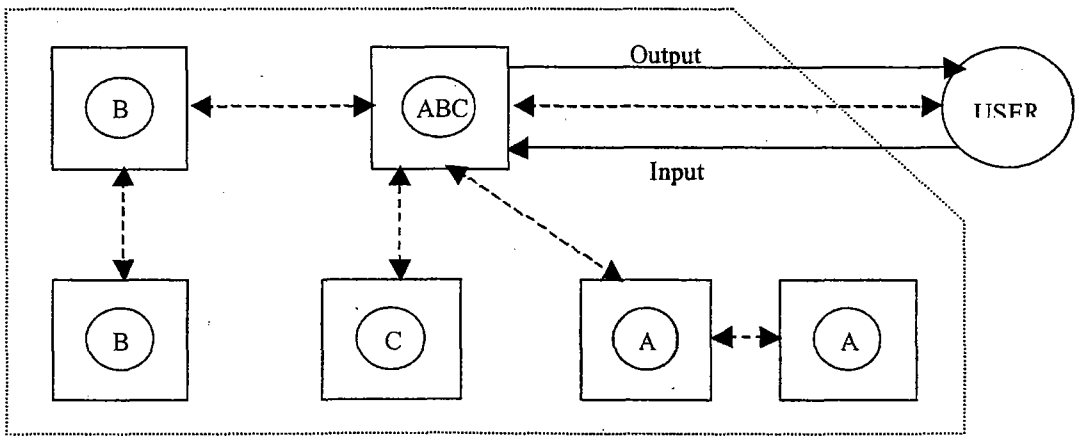

Figure 4 – Cycle of Multi-Agent System

Attack Targets of Intelligent Agents

Attacks can occur based on when processing is taking place or where processing is taking place. The paper will look at the physical stages within an agent scheme where an attack may occur.

Information Action Stages

The information systems-IW taxonomy as drafted by Cramer (Cramer, 1998) is made up of the following six categories:

- Information Acquisition;
- Information Protection;
- Information Processing;
- Information Transport;
- Information Management and;
- Information Denial.

These events are tightly coupled to actual occurrences within an agent system and attacks related to agent system-IW would tend to fall into these six categories (Cramer, 1998):

Information Acquisition Attack

An attack that occurs during the information acquisition stage involves disrupting or sabotaging the agent system during the transfer of information from one agent/host to another agent/host. One example of this technique of attack would be the addition of a malicious host into an agent system for the prime purpose of deleting, changing or transferring misleading or incorrect information to an insecure agent within the system.

Information Protection Attack

The protection of information at the host is important to the value of the system. If information can be tainted in any way then the reliability of any data provided by the system is compromised. An attack using a host or agent that renders a system component subject to security vulnerabilities is an information protection attack. This type of attack would normally be associated with the inclusion of remotely accessible, malicious code, which attacks a system entity causing system security failure.

Information Processing Attack

An attack during the information-processing phase within an agent system would tend to be aimed at a host target or the user system where the agent was originally deployed. If a host is attacked the information being processed on the host may be compromised perhaps by a malicious function of an agent. These sorts of attacks could also stem from an outside entity presenting malicious code to either the host or user systems that is then executed, causing processing sabotage or failure. The use of agents to actually process data on other hosts as they traverse a system can also cause problems as each host must be stable during processing or data will be lost.

Information Transport Attack

The information transport attack can happen at any stage of an agents travel across networks or at a malicious host or user. This type of attack is aimed at causing data or agents to be sabotaged or destroyed whilst in transit. The main technique involved in this type of attack is for a host to insert code into an insecure agent so as to cause the agent to fail whilst moving

about the network. Other techniques exist also such as the commandeering of a mobile agent so that attacks can be mounted against hosts that are visited by the malicious agent.

Information Management Attack

The management of information is an extremely important process within an information system. An information management attack focuses on creating problems within the databases and other information management software and hardware involved with the storage, organisation and use of information within an organisation. This method of attack can cause many difficulties for organisations as the entire staff may depend on the one system to be reliable and if that system fails working hours, sensitive information and company reputation may be lost. The period for information recovery may be extremely lengthy and costly and in the worst case may never be possible due to the extent of the attack..

Information Denial Attack

This form of attack in a most basic form involves stopping users of a system from accessing a particular piece of information that is required for completing a certain task. The denial of information can be brought about using a number of different attack techniques including use of viruses and other malicious code based attacks. The denial of information can be a very inhibitive form of IW due to the fact that many systems and people are often waiting for access to the same files and data, such as during a login procedure with a single encrypted password file. This type of attack could leave organisations without any option but to shutdown as the information within an organisation is often the only asset, especially in some e-business models.

Agent System Attack Scenarios

Within agent systems there are three major concerns when looking at security issues. The first is obviously attacks targeting or being waged from outside the system. The other two possibilities are that the host and/or agent could be solicited as either a target or and attacker. The scenarios that can occur in IW situations involving agents are (Jansen, 1999):

Agent-to-Agent

An agent-to-agent attack consists of one or more agent within a particular system attack another agent from the local system. This does not mean there is a limit on the size of the agent system, however, the locality of the system is implied by the agent's relation to the current system. This type of attack can be directly via agent communication or through use of a host as a method of attacking the target agent.

Agent-to-Host

An agent-to-host attack relies on a host's vulnerability so as to be successful. A scenario for this type of attack is an agent that visits a vulnerable host and in some way executes code that damage or disrupts the services that can be delivered by the host. The vulnerability of the host is extremely important as hosts may have proactive or reactive security strategies in place, which could lead a path to the origin of the offending mobile agent. The agent may also be destroyed if it does not interact in the predetermined correct fashion with a protected host.

Host-to-Host

Hosts within an agent system will tend to communicate mainly via the agents that are involved within the system. A host may receive directives to place some code within a

vulnerable agent which inturn could pass this code to a vulnerable host. The vulnerable host could then be attacked by some payload, which may also travel across communications channels with the vulnerable agent. Another scenario could exist wherein a vulnerable agent may place some sort of triggered code fragment on the vulnerable host so as to perhaps collect information or deny services at a later though still designated date.

Host-to-Agent

A Host-to-agent attack will on most occasions require the agent to have at some stage interacted with at least one host. The host that attacks the agent does not necessarily have to be malicious. The host could perhaps have been infected with some virus which inturn attacks subsequent visiting agents. Use of hosts to attack agents is possibly the easiest form of attack due to the fact that the vulnerable agent actually resides on the system and can therefore be controlled either manually by a user or autonomously by a system.

Outside System-to-Agent System

The use of agents has come about due mainly to the fact that users want to interact with other systems without needing to know they are interacting so as to make these operations more user-friendly. This autonomous interaction between many systems may mean that at some stage an agent system may be compromised by an attack on a vulnerability that a particular agent has. A security hole within an agent may not be detected until the agent has returned to a host system. By that time detection may be useless, as the compromised agent may have also attacked many systems that it has dealt with. This form of attack is difficult to defend against due to the autonomous nature of agent technologies and also the inability to keep track of some agent dealings.

Problems Caused by Attacks on Intelligent Agents

The actual damage or disruption caused when agents are used in a commercial IW scenario can vary greatly depending on:

- The size and importance of the agent system being attacked (Gray, 1996);
- The amount of disruption and/or damage the attacker wants to cause (Etzioni & Weld, 1995) and;
- The security involved with the system being targeted (Tschudin, 1999).

Examples include:

Information and Data Manipulation

As information within agent systems is transferred, updated, deleted and stored, perhaps many times per agent execution, the changing of information to some non-preferred value is an attack method that can be used effectively and without extreme risk of apprehension to the perpetrator. The changing of information in the commercial IW sense could lead to incorrect business decisions, such as poor investment, as well as possible loss of privacy depending on the vulnerability being targeted by the attack.

Information and Data Destroying

This case involves the same parties and problems as per the issue of information change attacks discussed. In this case rather than the information being changed to reflect another value, the information is just deleted or totally obscured so that the user of the data is unable

to take away any opinion from analysis of the data. Despite the fact that this attack sounds far more dangerous to an organisation than an Information change attack, it is often the information change attack that can be more damaging as wrong decisions are more likely to be made based on complete data rather than incomplete data (Meadows, 1997).

Misuse or Overuse of Resources

Software agents are often used as a method of selecting, organising and using web-based services and resources. The autonomous nature of agents means that difficulties can arise if agents are exploited in a way which allows them to use too many or misuse some of the resources and services they must interact with. This attack technique can cause problems not only within a particular agent system but also to other systems that require interaction with the problematic agent system or other systems that in some way make contact with a vulnerable agent from the compromised systems.

Misinformation

A misinformation attack is a way of confusing an enemy user or system into believing or using some tainted data within a normal execution procedure. This information may be a skewed data set, an incorrect news report etc. The use of agents to maliciously misinform other systems that they interact with is a method that could be extremely destructive in current world situations where peace can be dependant on comments made by world-leaders. If contents of speeches were to be misreported, wrongly dated or tainted in some other way, this could lead to disruptive behaviour on the world stage (Black, 1996), which shows the importance of protection from this method of attack.

Disabling Agents

The disabling of an agent within a system can cause major disruptions or may go unnoticed. This form of attack is heavily dependent on the reliance an organisation has on the particular agent that is destroyed. In a system where there are many threads and many agents all completing similar tasks the bss of a single agent would cost very little in efficiency. In the case of a business being heavily reliant on a single agent-system the results of an attack of this nature could be catastrophic as information regarding business transaction and other sensitive data could be rendered lost and unrecoverable.

Disabling Hosts

The disabling of a host is more costly than the disabling of associated agents. The loss of a host often leads to a failure of the host system to send and receive data. This failure may cause full failure of the agent system but may also go unnoticed, although, this is far less likely in the case of disabled hosts. The loss of a host may also mean that agents are destroyed or discontinued, as they are unable to meet a particular system goal. The disabling of a host can be in two forms. The first loss could be from the agent system point-of-view only so that the host computer may still operate. The second and more severe host attack would leave the host computer totally unusable.

Agent-Based Attacks

Software Agents that damage other systems and software have been around for many years, however, they have commonly been referred to as viruses (Goldschlag et al, 1998). It has been evidenced since Cohen (1994) put forward early research on viruses, that the virus is basically an agent with varying degrees of intelligence and mobility. The major issue with viruses being regarded as agents is that viruses are, for the most part, created for malicious

and/or disruptive purposes. We have seen the Code Red/Code Red II worm cause disruption and damage to many systems as the polymorphic denial of service attack payload forwards itself to remote systems (CERT, 2001). "Viruses and worm programs carry out the bidding of their designer autonomously by creating duplicates of themselves among many computers" (Denning, 1990). The use of the words intelligent and mobile when discussing agent technologies does not imply that the agent is to be used for perceived good or bad they are only characteristics of said programs.

Aside from the issue of viruses there are also more complex agent systems that have been and are being developed currently (Cramer, 1998) which could be greatly compromised if security measures, both proactive and reactive, are not built into systems. Any of the aforementioned attacks are possible, as agents, by design are merely *computer programs* that are not only designed to work together, derive intelligent solutions to problems and be mobile but also to have the same vulnerabilities that can be found in most common programs.

Dealing with Intelligent Agent Based Attacks

Information Warfare threats can be dealt with in a number of ways. These methods tend to fall into two categories shown in Table 1:

Handling Method	Definition
Proactive Handling	Where agent technology is built to prevent attacks from occurring
Reactive Handling	Where agent technology is used and problems are dealt with as they arise

Table 1: Risk Handling Methods and Definitions

Agent-Based IW is no different to other IW techniques in the sense that proactive and reactive methods can still both be used for risk management (Pellissier, 2000).

Risk Management - Proactive or Reactive?

The major differences between proactive and reactive risk management strategies when dealing with agent-based IW are still those of cost in time, money and efficiency. The decision involved in this case is whether to prevent attacks from occurring or to detect them and then deal with them as they arise. Major questions exist as to whether or not mobile-agent systems can be made totally secure as a proactive measure and if so is it still more efficient to solve problems as they occur considering the youth of some of the newer agent technology advances.

Agent or Host as Platform for Security Features?

Another major decision to make is whether to develop security at the host or within the agent. The development of host security is seen as the more expensive and difficult project to uptake as one agent could visit many hosts (such as in the case of web crawlers) therefore meaning every host would need to be updated or developed with new security in mind. Developing agent security is seen as a more efficient method of building security into agents. The major problem with this approach is that excess agent code to deal with security may make the agent slow and costly to use on a large scale and therefore less efficient as an information collection solution. The current methods of security being developed or currently in use are shown in Table 2.

Countermeasure	Technique	Security Platform
Signed Code	Reactive	Host
State Appraisal	Reactive	Host
Path Histories	Reactive	Host
Partial Result Encapsulation	Reactive	Agent
Mutual Itinerary Recording	Reactive	Agent
Itinerary Recording with Replication and Voting	Reactive	Agent
Execution Tracing	Reactive	Agent
Software-Based Fault Isolation	Proactive	Host
Safe Code Interpretation	Proactive	Host
Proof Carrying Code	Proactive	Host
Environmental Key Generation	Proactive	Agent
Computing with Encrypted Functions	Proactive	Agent
Obfuscated Code	Proactive	Agent

Table 2: Risk Countermeasure and Handling Table (Copied from Jansen, 1999)

Conclusions

This paper has highlighted the current state of agent technologies and how they can be exploited in terms of Information Warfare attacks. A number of conclusions were reached. Initially there was confirmation from review of literature that it is possible for IA technology to be exploited for use within an IW campaign. There are also a number of both proactive and reactive security methodologies either in use or being developed currently. The development of host-based security is more expensive but is also more secure. The use of proactive security methods is more expensive to initially develop but provides a more reliable agent system. Despite this fact moves toward proactive security are slow due to the fact that overheads involved with proactive security, especially built within agents, are extremely high and does remove functionality and efficiency from the system. There are a number of possible vulnerabilities and methods of attack associated with agent technology. This is due mainly to the novelty of the technology at present. The new security methods being developed do go a long way toward attempting to deny some of the existing attack methodologies and vulnerabilities within certain agent systems.

References

Black S. K. (1996) Information Warfare in the Post Cold-War World, *Ridgway Viewpoints 96-1*, USAF, USA.

CERT (2001) Continued Threat of the "Code Red" Worm, *CERT Advisory CA-2001-23*, USA.

Cohen F (1994). *It's alive! : the new breed of living computer programs,* New York : Wiley, USA.

Cramer M (1998) Intelligent Agents in Information Warfare, *InfowarCon '98*, Washington DC, USA.

Etzioni O and Weld D.S (1995) Intelligent Agents on the Internet, *Department of Computer Science and Engineering Technical Report,* University of Washington, USA.

Goldschlag D, Landwehr C and Reed M (1998) Agent Safety and Security, *Naval Research Laboratory Research Report,* Washington DC, USA.

Gray R. S (1996) Mobile-Agent Security, *Dartmouth College Technical Report*, New Hampshire, USA.

Hohl F (1998) A model of Attacks of Malicious Hosts Against Mobile Agents, *Institute of Parallel and Distributed High-Performance systems (IPVR) Research Report*, University of Stuttgart, Germany.

Hopwood D (1997) A comparison between Java and ActiveX Security, *Network Security,* UK

Hunter P (1999), Spies on Your Hard Drive, *Computer Weekly,* United Kingdom.

Jansen W (1999), Countermeasures for Mobile Agent Security, *National Institute of Standards (NIST),* USA.

Jennings N.R and Wooldridge M (1998), Applications of Intelligent Agents, *Queen Mary & Westfield College Technical Report,* University of London, United Kingdom.

C. Meadows, "Detecting Attacks on Mobile Agents", Center for High Assurance Computing Systems, Naval Research Laboratory, Washington DC, USA.

Pellissier S.V (2000), A Brief Overview of Software Agent Applications and Risks, *SANS Institute,* USA.

Sharpe R (1997), Interrogating the Software Agents, *Computer Weekly*, United Kingdom .

Tschudin C.F (1999), Mobile Agent Security, *Technical Report*, Department of Computer Systems, Uppsala University, Sweden.

Vitek J and Castagna G (1999) Mobile Computations and Hostile Hosts, *Journees Francophones des Langages Applicatifs,* February, France.

Washington, D.W (1995) Onward Cyber Soldiers, *Time Magazine,* Volume 146 - No.8, USA.

Wilder C and Dalton G (1997) The World Wide Web Watch – Using Web Agents, *Information Week*, Issue 652, CMP Media, USA.

Wooldridge M and Jennings N.R (1998) Pitfalls of Agent-Oriented Development, *Technical Report*, Department of Electronic Engineering, Queen Mary & Westfield College, University of London, United Kingdom.