A Security Framework for Mobile Agent Systems

Omer Mansoor Paracha

DISSERTATION.COM

Boca Raton

A Security Framework for Mobile Agent Systems

Dissertation.com
Boca Raton, Florida
USA • 2009

ISBN-10: 1-59942-724-9
ISBN-13: 978-1-59942-724-9

Abstract

Agent technology is a novel approach for the development of distributed systems. In particular, mobile agents can provide much greater flexibility and robustness than the traditional distributed system methodologies since they provide mobility from platform to platform. Thus, they form a vast area of research. One key problem faced by the mobile agent systems is security. A migrating agent can face many threats while migrating to a host/ agent platform. Similarly the platform can be maliciously affected by an agent. A number of different approaches have been suggested in the literature to deal with security of mobile agents. In this thesis, we present an overview of such threats and present an "agent threat model" for mobile agent systems. Based on this model we survey and evaluate the techniques that provide countermeasures to the mobile agent systems. Based on the techniques surveyed, a state-of-the-art is evaluated and the security of certain mobile agent systems is discussed. The thesis presents a proposed framework to provide mobile agent system security from both malicious mobile agents and platform. The idea is to provide a solution to the requirement of a security framework that provides security as a combination of components based on techniques for mobile agent system security and protection. The proposed framework is comprised of various components that are studied in the light of operation scenarios. An implementation of the system is discussed and the evaluation of the proposed framework as well as a comparison with the state-of-the-art mobile agent systems is provided to highlight the strengths and weaknesses.

Acknowledgements

The completion of a long and tough journey in the form of my Master's thesis would not have been possible without the remarkable support and supervision of Dr. M. Jaffar-ur-Rehman whose memory and guidance lives long with me. Hoping that my thesis and my research work has met his expectations; this thesis is dedicated to him.

I also thank Mr. Aamer Nadeem for his great advice during the course of my thesis, especially during the end of it. I thank him for his time, his comments and those helpful sessions discussing my work, without which this thesis would never have been completed.

I thank the members of the Centre for Software Dependability (CSD), their help and their massive inputs that constructed and gave life to the work in this thesis and being like a family to me. I would specially like to thank Mr. Masud Khokhar for introducing me to the topic and advising me immensely in drawing out my proposed framework. Thanks to Mr. Uzair Khan, Mr. Shaukat Ali, Mrs. Zille Huma and Mr. Zouhaib Zafar for sharing their thesis-writing experiences.

I thank the faculty, the students and the staff of Mohammad Ali Jinnah University for helping me achieves my goals. The faculty has always been available for a lot of help and guidance. I especially thank Prof. Zafar I. Malik for his immense support throughout the course of my thesis. His advice and his heart-lifting comments are duly appreciated. The staff is cordially appreciated, especially for the CSD lab and its facilities that let the research process flourish.

I would also like to thank all my friends for their moral support, especially my old batch mates from my undergrad (the BS-6). I specifically thank Mr. Shahid Ishtiaq, Mr. Waqas

Mahmood, Mr. Ifraseab Afzal, Mr. Waqas Javed, Mr. Ibraheem Zaman, Mr. Raja Asad and Mr. Waqas Raza for removing all the writer's blocks I faced. I also appreciate, Mr. Abeer-ur-Rehman for sending a very handy gift during my write-up. Also, I thank Mr. Wajahat Nosherwan for his comments on the proposed framework and the numerous discussions on the whiteboard in the CSD.

I thank my family especially my parents who believed in me and gave me strength to progress in my education, my father for his counseling on living life and my mother for her prayers. My brother and sister for staying up with me on my long nights and not letting me fall asleep. I am extremely grateful for their patience and their high-spirits that helped me focus through many difficult times during the course of my educational life. My family has been an astounding inspiration to my research work.

I thank Allah (SWT) for bestowing me with His uncountable blessings that are far too many to mention here.

Table of Contents

TABLE OF CONTENTS VI
LIST OF FIGURES IX
LIST OF TABLES X

CHAPTER 1 INTRODUCTION 1

CHAPTER 2 MOBILE AGENT SYSTEMS SECURITY: A BACKGROUND 4

2.1 REMOTE CODE EXECUTION 4
2.2 SOFTWARE AGENTS 5
2.3 MOBILE AGENTS 6
2.4 MOBILE AGENT BENEFITS 7
2.4.1 Mobile Agent Applications 9
2.5 MOBILE AGENTS LIMITATIONS 10
2.5.1 Mobile agent security 12

CHAPTER 3 MOBILE AGENT SYSTEMS SECURITY - THREAT MODEL 13

3.1 OVERVIEW OF MAS SECURITY THREATS 13
3.1.1 Malicious Platform 14
3.1.2 Malicious Agent 15
3.1.3 Malicious Network 15
3.2 THE MAS THREAT MODEL 15
3.2.1. Masquerading 16
3.2.2. Denial- of-Service 17
3.2.3. Unauthorized Access 18
3.2.4. Repudiation 19
3.2.5. Eavesdropping 20
3.2.6. Alteration 20
3.2.7. Copy and Replay 21

CHAPTER 4 SURVEY OF COUNTERMEASURES FOR PROTECTION OF MOBILE AGENT SYSTEMS 23

4.1 COUNTERMEASURES OVERVIEW 23
4.2 AGENT PROTECTION 24
4.2.1 Partial Result Encapsulation 25
4.2.2 Environmental Key Generation 26
4.2.3 Code Obfuscation 27
4.2.4 Cryptographic Functions 28
4.2.5 Execution Traces 31
4.2.6 Itinerary Protection 33
4.2.7 Time Techniques 35
4.3 PLATFORM PROTECTION 36
4.3.1 Agent Authentication 36
4.3.2 Path Histories 39
4.3.3 State Appraisal 41
4.3.4 Resource Protection 42
4.3.5 Fault Isolation or Sandboxing 43
4.3.6 Safe Interpretation and Padded Cells 45
4.3.7 Proof Carrying Codes 46
4.3.8 Payment-based Techniques 47
4.4 NETWORK PROTECTION 48
4.4.1 Secure Sockets 48
4.4.2 Firewalling 49
4.4.3 Tamper-Resistant Hardware 50
4.5 EVALUATION 50

CHAPTER 5 MOBILE AGENTS SYSTEMS AND THEIR SECURITY: STATE-OF-THE-ART . 53

5.1 MOBILE AGENT SYSTEMS OVERVIEW 53
5.2 TELESCRIPT 54
5.2.1 General Architecture 55
5.2.2 Security in Telescript 57
5.2.3 Comments on the Telescript Security Model 62
5.3 AGENTTCL AND D'AGENTS 63
5.3.1 General Architecture 63
5.3.2 Security in Agent Tcl and D'Agents 65
5.3.3 Comments on the Security of Agent Tcl and D'Agents 69
5.4 ARA 71
5.4.1 General Architecture 71
5.4.2 Security in Ara 73
5.4.3 Comments on the Security of Ara 75
5.5 TACOMA 76
5.5.1 General Architecture 77
5.5.2 Security in Tacoma 78
5.5.3 Comments on the Security of Tacoma 79
5.6. AJANTA 81
5.6.1 General Architecture 81
5.6.2 Security in Ajanta 84
5.6.3 Comments on the Security of Ajanta 88
5.7 AGLETS 89
5.7.1 General Architecture 89
5.7.2 Security in Aglets 91
5.7.3 Comments on the Security of Aglets 93
5.8 CONCORDIA 93
5.8.1 General Architecture 94
5.8.2 Security in Concordia 96
5.8.3 Comments on the security of Concordia 97
5.9 GRASSHOPPER 98
5.9.1 General Architecture 98
5.9.2 Security in Grasshopper 100
5.9.3 Comments on the Security of Grasshopper 101
5.10 MOLE 101
5.10.1 General Architecture 102
5.10.2 Security in Mole 103
5.10.3 Comments on the Security of Mole 104
5.11 MAS SECURITY EVALUATION 105

CHAPTER 6 MOBILE AGENT SECURITY FRAMEWORK 107

6.1 FRAMEWORK OVERVIEW 107
6.2 FRAMEWORK ASSUMPTIONS 109
6.3 THE HOST 110
6.3.1 Agent Creator 111
6.3.2 Agent Dock 112
6.4 MOBILE AGENT 112
6.4.1 Code and Data 113
6.4.2 Itinerary 114
6.4.3 Credentials 115
6.4.4 Certificate Vector 115
6.4.5 Hash List 115
6.4.6 Encryption Function 116
6.5 CERTIFICATION AUTHORITY 117
6.5.1 Certificate Authorizer 117
6.5.2 Certificate Verifier 118

6.5.3 Key Distribution Centre *118*
6.6 AGENT PLATFORM 118
6.6.1 Authenticator *120*
6.6.2 Cryptographic Component *121*
6.6.3 Padded Cell *122*
6.6.4 Policy Engine *123*
6.6.5 Resource Registry *124*
6.6.6 Domain Database *124*
6.6.7 Resources, Their Access and Proxies *125*
6.6.8 Proxy Manager *126*
6.6.9 Agent Transferer *126*

CHAPTER 7 MOBILE AGENTS SECURITY FRAMEWORK – OPERATION SECURITY SCENARIOS 128

7.1 SCENARIO 1: SPAWNING AGENTS AT THE HOST 128
7.2 SCENARIO 2: AUTHENTICATING THE AGENT 129
7.3 SCENARIO 3: ACCESSING THE MOBILE AGENT BY THE PLATFORM 131
7.4 SCENARIO 4: AUTHORIZATING THE MOBILE AGENT 132
7.5 SCENARIO 5: CHECKING THE MOBILE AGENT'S FUNCTIONALITY BY THE PLATFORM 134
7.6 SCENARIO 6: ACCESSING AND ALLOCATING RESOURCES 135
7.7 SCENARIO 7: ACCESSING ONLY THROUGH THE ENVIRONMENT 136
7.8 SCENARIO 8: TRANSFERRING AGENTS 136
7.9 SCENARIO 9: ASSIGNING AND USING AGENT ID 137
7.10 SCENARIO 10: PROTECTING AGENT COMMUNICATION 138
7.11 SCENARIO 11: TRACING EXECUTION 138
7.12 SCENARIO 12: SIGNING COMPUTED CODE HASHES 139
7.13 SCENARIO 13: PROTECTING THE ITINERARY 139
7.14 SCENARIO 14: RECEIVING AGENTS AT THE HOST 140

CHAPTER 8 IMPLEMENTATION 142

8.1 IMPLEMENTATION OVERVIEW 142
8.2 MOBILE AGENTS 143
8.3 HOST 147
8.4 AGENT PLATFORM 148

CHAPTER 9 EVALUATION OF THE PROPOSED FRAMEWORK 153

9.1 FRAMEWORK EVALUATION 153
9.2 SECURITY COMPARISON WITH STATE-OF-THE-ART MAS 156
9.3 STRENGTHS AND WEAKNESSES OF THE PROPOSED SECURITY FRAMEWORK 158
9.3.1 Strengths *158*
9.3.2 Limitations *159*

CHAPTER 10 CONCLUSIONS & FUTURE WORK 161

REFERENCES 164

List of Figures

FIGURE 3.1: A SIMPLE MOBILE AGENT SYSTEM 16
FIGURE 5.1: TELESCRIPT PARTIAL ARCHITECTURE (ADAPTED FROM (BAUMER, BREUGST, CHOY & MAGEDANZ, 1999)) 57
FIGURE 5.2: D'AGENTS ARCHITECTURE (GRAY, CYBENKO, KOTZ & RUS, 2001) 64
FIGURE 5.3: AGENT TCL (MAGNIFIED) (ADAPTED FROM (GRAY, 1996)) 65
FIGURE 5.4: D'AGENTS SECURITY MODEL 69
FIGURE 5.5: ARA PLATFORM ARCHITECTURE 73
FIGURE 5.6: TACOMA ARCHITECTURE (JOHANSEN ET AL., 2001) 78
FIGURE 5.7: AJANTA ARCHITECTURE (TRIPATHI, KARNIK, VORA, AHMED & SINGH, 1999) 82
FIGURE 5.8: AGLETS ARCHITECTURE (KARJOTH, LANGE & OSHIMA, 1997) 90
FIGURE 5.9: CONCORDIA SYSTEM ARCHITECTURE (WONG ET AL., 1997) 95
FIGURE 5.10: THE GRASSHOPPER DISTRIBUTED AGENT ENVIRONMENT (BAUMER, BREUGST, CHOY & MAGEDANZ, 1999) 99
FIGURE 5.11: MOLE ARCHITECTURE (BAUMANN, HOHL, ROTHERMEL & STRABER, 1998) 102
FIGURE 6.1: MAS FRAMEWORK OVERVIEW 109
FIGURE 6.2: HOST 111
FIGURE 6.3: MOBILE AGENT AND ITS COMPONENTS 113
FIGURE 6.4: ITINERARY 114
FIGURE 6.5: CERTIFICATE VECTOR 115
FIGURE 6.6: HASH LIST 116
FIGURE 6.7: CERTIFICATION AUTHORITY 117
FIGURE 6.8: AGENT PLATFORM AND ITS COMPONENTS 119
FIGURE 6.9: AUTHENTICATOR 121
FIGURE 6.10: AGENT RIGHTS ALLOCATION PROCESS (POLICY APPLICATION) 123
FIGURE 6.11: RESOURCE BINDING VIA PROXIES 125
FIGURE 6.12: AGENT COMMUNICATION 126
FIGURE 7.1: AGENT CREATION PROCESS 129
FIGURE 7.2: AUTHENTICATION PROCESS 130
FIGURE 7.3: AGENT DECRYPTION – CRYPTOGRAPHIC COMPONENT PROCESS 132
FIGURE 7.4: AUTHORIZATION PROCESS – RIGHTS ALLOCATION 133
FIGURE 7.5: PROXY USAGE 136
FIGURE 7.6: AGENT TRANSMISSION PROCESS 137
FIGURE 7.7: AGENT INTERACTION 138
FIGURE 7.8: RECEIVE PROCESS AT HOST 141
FIGURE 8.1: MOBILE AGENT INTERFACE 144
FIGURE 8.2: MOBILE AGENT ACCESSOR INTERFACE 145
FIGURE 8.3: MOBILE AGENT CLASS 145
FIGURE 8.4: CREDENTIALS 145
FIGURE 8.5: HASH LIST 146
FIGURE 8.6: CERTIFICATE VECTOR 146
FIGURE 8.7: AGENT CREATOR 147
FIGURE 8.8: AUTHENTICATION 149
FIGURE 8.9: TESTING THE AGENT IN THE PADDED CELL 149
FIGURE 8.10: POLICY ENGINE POLICY RETRIEVAL 150
FIGURE 8.11: POLICY 150
FIGURE 8.12: ACCESS CONTROL LIST (ACL) 150
FIGURE 8.13: RESOURCE INTERFACE 151
FIGURE 8.14 RESOURCE IMPLEMENTATION 151
FIGURE 8.15 RESOURCE PROXY DELEGATION 151
FIGURE 8.16: AGENT TRANSFERER SEQUENCE 152

List of Tables

TABLE 4.1: PROTECTION OF THE MOBILE AGENTS 51
TABLE 4.2: PROTECTION OF THE AGENT PLATFORM 52
TABLE 4.3: PROTECTION OF THE MAS NETWORK 52
TABLE 5.1: MOBILE AGENT SYSTEM SECURITY EVALUATION – MOBILE AGENT PROTECTION 105
TABLE 5.2: MOBILE AGENT SYSTEM SECURITY – PROTECTION OF THE AGENT PLATFORM 106
TABLE 9.1: EVALUATION OF THE PROPOSED FRAMEWORK 154

Chapter 1

Introduction

Software systems have advanced immensely with the technology march with special regard to expansion of systems over a distributed concept. Various approaches for development of software systems especially distributed systems have come into existence. This advent of distributed system application and performance has lead to many research dimensions and topics. Since distributed systems require immense communication between its components or subsystems and the information that they share is considerably large in amount, approaches to access, search and access of this is vital. So, for this, various theories for communication and information retrieval exist.

Distributed systems came into existence so that a wider network could be used for information sharing and also for service access. A large number of applications were derived from this ability to scale a large area and distribute information and service. Distributed systems become vitally important due to their function. However, the function and capabilities are vast and the requirement from such systems becomes larger. Features of such systems make the system different in construction and operation. Performance issues include the issues of extensive reliability, like fault tolerance, safety and security. Of these, one important issue is the security of software. When software

goes distributed, it becomes potentially more prone to network insecurity and threats. Thus, it is very important to assess the threats and insecurities that the system might undergo during its lifetime and, that the system can somehow prevent the occurrence of attack.

Mobile agents are an innovative idea in the field of distributed system research (Kotz, Gray & Rus, 2002). They are basically autonomous units of code and state data that can migrate from host to host for remote processing. Their capabilities are immense in comparison to normal remote procedure calls and remote processing as they themselves carry the process and data but use the remote host's capability to carry out the execution. The uses of agents are many as their prime propose is in their name. They are actually representatives for cyber-users.

Mobile agents may be characterized as "good" agents that carry out tasks for us on our behalf remotely, for example an agent to purchase a book online. The agent looks for the book on different hosts and purchases the one that fits the criteria like its cost or its required stock. Also, there may be "bad" agents, like viruses and worms that can go online and travel to hosts to damage them or spy on them. As agents are composed of code and data it can use this for virus like activity.

Mobile agents and their activity may be malicious or it may be attacked by the host it is supposed to execute on, meaning that the host is malicious. Also, both agent and host may be "good" but the network may be comprised of hackers. This means that the network is insecure and liable to attacks in its route.

Our aim is to create a framework to insure secure agents and hosts (Jansen & Karygiannis, 1998). The framework that has been suggested deals with primarily the security. The prime aim in abstract is to allow "good" mobile agents and disallow "bad"

mobile agents on the host and to protect the mobile agent from the host's activity. The agent has to send its processed information back to the host from where it came from along with its execution log containing the entire trace of its execution on the host. Also, the use and access of resources has to be taken into consideration. The framework accommodates the protected resource use by the visiting mobile agent.

The thesis is arranged as follows: Chapter 2 covers the background to Mobile agents, their theories and to their applications as well as giving the concepts of security that is required in mobile agent systems. Chapter 3 presents the Threat Model that accommodates the various threats that occur in a mobile agent system i.e. to the agent and the agent platform. Chapter 4 surveys the countermeasures and techniques in the literature on mobile agent security and is evaluated to see what threats are protected by these measures using the threat model. Chapter 5 covers the various state-of-the-art mobile agent systems and describes their security architectures and evaluates these on the basis of the techniques that are used for security from Chapter 4. Chapter 6 details our proposed framework and describes its components and subcomponents. Chapter 7 describes the various operation scenarios to check their security of our proposed framework. Chapter 8 describes the implementation issues of our proposed system. Chapter 9 evaluates our system and lists down the benefits and limitations of the proposed system using the threat model and also a comparison with other state-of-the-art mobile agent systems. Chapter 10 concludes the thesis and provides some research directions.

Chapter 2

Mobile Agent Systems

Security: A Background

This chapter gives the background that is required for mobile agent system security. It covers the different theories that are available in the literature on mobile agents and mobile agent systems in general.

2.1 Remote Code Execution

Taking the generic client server model, a set of traditional approaches to remote processing can be discussed. The client server model generically contains a client that issues a request to be processed by the server on its behalf. The server then processes the request and responds as required. For this kind of communication model, approaches for remote code execution were developed (Aneiba & Rees, 2004; Picco, 2001). The approaches for remote code execution are Remote Procedure Calls and Remote Evaluation (Lange, 1998; Rothermel & Schwehm, 1998).

Code can be accessed simply by calling the procedures like through RPC (Remote Procedure Calls) and through REV (Remote Evaluation). In RPC, the methods are invoked by the agent through method calls. Client is the caller whereas the server is the callee. The server responds by sending the results of the procedure execution back to the client. In REV, the method is downloaded to the client by the server and it executes there. Here, there are two further approaches; one is that the client may call the code for download and execution. The other is that the code may be sent by the server to be executed on the client according to the server. The first approach is remote execution where as the second is code-on-demand.

In contrast we have software agents that can be mobile, i.e. mobile agents that can carry out remote code execution and overcome the limitations that traditional approaches have (Rothermel and Schwehm, 1998).

2.2 Software Agents

To understand what software agents are, we have to understand what agents are. As defined in various papers, agents are best defined by Franklin and Graesser (Franklin & Graesser, 1996) that highlights the notion of what agents are according to various definitions that people defined. However, the best understanding was found in the definition that was derived in (Lange, 1998) that the definition of an agent is based on which perspective we are elucidating its nature. Generally, an agent is a representative for a user that has been delegated some work. As stated before the debate becomes rather immense (Franklin & Graesser, 1996) and the requirements of an agent and its actual meaning becomes too narrow. Thus, the definition needs to be broadened and the definition from (Lange, 1998) is rather complete by which we adapt our definition of an

agent; an agent is a delegate or a representative that can operate in an environment, is reactive, autonomous, goal-driven, continuous, communicative, mobile, learning and believable. Agents may possess all of these or some of these characteristics (Sundsted, 1998).

From this definition of an agent, we can define what a software agent is. A software agent is basically an object possesses all of the aforementioned characteristics. Rothermel and Schwehm in (Rothermel & Schwehm, 1998) classify software agents. From this classification and the classification done in (Franklin & Graesser, 1996) we understand that due to the features of a software agent, the agent can assume a number of forms. In this thesis, we take the mobile agent class of software agents.

2.3 Mobile Agents

After explaining software agents, the class of mobile agents does not require much of a formal definition. However, we do explain mobile agents and their context in the rest of this thesis. A mobile agent is an agent that can simply carry out our tasks for us as users remotely. By remotely, we can mean many other remote locations. A mobile agent is thus simply one that is created at one place, carries its code and state over to another place and resumes its execution. It does not require the remote code execution approaches for this; instead it propagates itself over the communication network to carry out its tasks (Lange, 1998).

To explain what a mobile agent is, we have to understand certain basic concepts. As explained by (White, 1998) and (Milojicic, LaForge & Chauhan, 1998) a mobile agent system has agents and places. A place is where the agent visits in its journey. At each of these places, there exists an agent environment to allow its execution. The environment

allows processing on the basis of a policy. Of course, the underlying features that define the agent and the place implementation differ in its state-of-the-art as various mobile agent systems implement the features differently.

(Marrow & Ghanea-Hercock, 2000) define the mobile agent computing approach and give the features of the actual setup and features that are required. Traced from what has been discussed and by (Marrow & Ghanea-Hercock, 2000) mobile agents have certain fundamental features. Taking a general idea that a mobile agent moves from place to place, a mobile agent requires the elements of mobility, communication and task association. A mobile agent is fundamentally mobile and can migrate from place to place as specified. Similarly, a mobile agent needs to communicate and co-ordinate with agents and the execution environment to execute. Lastly, an agent needs to be associated with a specialized task to perform on the behalf of the creator of the agent that it is representing.

2.4 Mobile Agent Benefits

Mobile agents along with their features can thus provide a number of benefits to distributed and component based systems and technology (Kotz & Gray, 1999). Their applications due to these benefits are thus numerous. As explained in a lot of papers, mobile agents have large potential. To assess this we highlight the benefits from mobile agents that are mentioned in the literature. As expressed by (Lange & Oshima, 1999), there are several good reasons for mobile agents. These are listed as follows:

1) Network load is reduced because multiple interactions are not required between the server and the client like in traditional approaches. Instead, a mobile agent carries the

complete set of interactions to the server. The agent executes the commands locally and thus reduces the set of instructions that had to be sent. Also, for a large amount of data, transmission over channels is rather expensive; hence the mobile agent using the data locally reduces the network load.

2) No delays are witnessed as the mobile agent executes at the point of execution. For example, in the traditional approaches, a large amount of wait had to be done for a command to be processed and responded to. In the case of mobile agents, an agent is actually sent there and the wait time is reduced.

3) Protocols do not need to be enhanced for mobile agents that are migrating and they can utilize the protocols at hand as for other mechanisms the protocols need to be upgrade according to the specification of the communication required.

4) Autonomous execution makes the mobile agent independent of the creator. This is favorable for the example of limited devices like mobile devices. The agent moves to the server, executes and the device collects the agent later.

5) Dynamism is enhanced as the mobile agents can be adapted according to the environment that is given to them.

6) Heterogeneity is provided because the underlying specification is independent to the mobile agent allowing better integration of heterogeneous systems and environments.

7) Robustness is achieved because dynamism allows agents to be configurable as the environment suggests, this also makes them fault-tolerant if required.

2.4.1 Mobile Agent Applications

Now we discuss the applications that are possible because of mobile agents.

2.4.1.1 Telecommunication

In the field of telecommunication, mobile agents can use their advantage in reduction of network bandwidth and can enhance these for several network services that future or next-generation telecommunication networks (Pham & Karamouch, 1998).

2.4.1.2 Network Management

Mobile agents can be used to evolve current client/ server based network management approaches to a more distributed approach (Pham & Karamouch, 1998).

2.4.1.3 Information Retrieval

Mobile agents can be used for retrieval of information over a network and the Internet. The mobile agents can carry queries and can retrieve particular information (Pham, 2001). This can be extended for cache management and searching as well.

2.4.1.4 Others

There is other work in progress in many dimensions as seen in the literature on them. Mobile agents can be used in Global Information Systems for tracking, in Grid Systems,

in Intrusion detection systems, for distribution of multimedia and so on. Also, agents have a broad research potential (Kotz, Gray & Rus, 2002).

2.5 Mobile Agents Limitations

Mobile agents have their immense applications and there are several benefits because of them but they still have their limitations. Their possibilities are hindered by several challenges (Schoder & Eymann, 2000). Some of these are limitations to the technology and some are because there are missing solutions to numerous issues that arise in mobile agent systems concepts and design (Rothermel, Hohl & Radounikilis, 1997; Kotz & Gray, 1997).

Various authors have written about the mobile agent dimension limiting and the reasons that cause the limitations to their adoption (Gray, 2004). Also, the reason has been highlighted as because of applying it in the wrong regard despite having a clear concept to their use (Johansen, 2004). For this the reasons listed in (Vigna, 2004) define the limitations and their reasons quite well. The listed reasons are:

1) Performance issues can be limiting. A generalization states that agents may reduce network bandwidth consumption and so on, but this is not true in every scenario.

2) There is a lack of a systematic approach to design a mobile agent, making it difficult to develop.

3) Implementing agents is also hard work as so many unpredictable interactions are present in its journey to so many places consisting of adverse environments.

4) The testing and debugging of such systems are extremely complex. This is due to the fact that the approaches become so unpredictable.

5) Authentication can be based on so many things the agent is associated with. For this the authentication mechanism may be weak.

6) Corruption of the agents is possible as the agent transfers over the various places it visits. This means an agent can lose its information or actually deviate from its goal.

7) Since information might be lost, the agent cannot be trusted with secret information either. The information can be leaked on its way.

8) A mobile agent requires a setup or an infrastructure to actually perform. A system that bases itself on mobile agents would require that all the places can execute the mobile agent.

9) Mobile agents in order to interact require a sort of mechanism, a means to interact and to collaborate; there is a lack of such an approach, such a language that supports this mechanism.

10) Mobile agents remotely execute at one place and go to the next; this is very much like a worm that actually can cause so much damage to the system if they are allowed to process.

2.5.1 Mobile agent security

Of all the above, security is one of the greatest weaknesses to a mobile agent. Security alone is a large reason for the lack of use of agents for providing the solutions they promise (Li, Zhang, Sun & Yin, 2004).

A huge amount of research material is available that has either raised the notion of security of mobile agents or has tried to solve it in one way or another. The notion of mobile agent security is because the mobile agents that are roaming a network can be used as malicious objects for accessing private or confidential information and resource, for causing corruption like viruses and worms and so on. Similarly, in this regard if an agent is supposed to be correct and non-malicious, we are never sure that the place it is visiting may be malicious to it or not and may also leech information from the agent, corrupt it or even use it for its malicious purpose.

The lack of security has been highlighted mainly because of a lack in approach to so many things that have to be secured about a mobile agent system. A mobile agent system thus lacks approaches because of a lack of a security providing framework that will fulfill the end to end security requirements of the agents and the places.

Chapter 3

Mobile Agent Systems Security - Threat Model

This chapter looks into various security threats and the aspects that may be malicious in a MAS. Also, a MAS threat model is presented that denotes the threats that an MAS may comprise.

3.1 Overview of MAS Security Threats

Threats to a mobile agent are an area of fond interest as they stand out to the acceptance of mobile agent systems for various applications. The vulnerabilities alone have cause immense interest in the field of security of distributed systems. Various goals have been highlighted to protect a system out of which some have a substantial solution and some do not (Abdalla, Cirne, Franklin & Tabbara, 1997). This chapter identifies the threats that occur in a mobile agent system so that a MAS can be evaluated according to the threat that they countermeasure.

The threat model has been derived from the various papers discussing the countermeasures to the threats. However, (McDonald, Yasinsac & Thompson, 2005) derived threats to the MAS. In this model, we generalize the threats to the MAS and create our own threat model. Also, the threat model includes threats from a malicious network not present in (McDonald, Yasinsac & Thompson, 2005).

The security of mobile agent systems encompasses protection of the mobile agent, the platform and the network (Greenberg, Byington & Harper, 1998). Thus, the work on security in mobile agents can be classified in to three broad categories (Gray, 1997; Brooks, 2004):

- Malicious Agent Platform and environment
- Malicious Agent
- Malicious Networks

3.1.1 Malicious Platform

Malicious platform security is necessary so as to defend the agent and the spawning host from any platform to which the agent is transferred to. This includes various security threats like spying on the agent and its data, masquerading or posing as a correct platform and also the corruption or misuse of the agent (Farmer, Guttman & Swarup, 1996b; Kun, Xin & Dayou, 1999).

Similar to this, other agents may harm the incoming agent(s) and so may the environment (Kun, Xin & Dayou, 1999).

3.1.2 Malicious Agent

The protection of the platform on which the agent is executing has to be protected as well (Farmer, Guttman & Swarup, 1996b). This is because the agent may act like a virus and may corrupt the platform or can act as a Trojan and can spy on the platform and its resources (Kun, Xin & Dayou, 1999).

3.1.3 Malicious Network

This security deals with the network on which the mobile agent is transferred to other platforms (Farmer, Guttman & Swarup, 1996b). The networks can be tampered and insecure channels may be created luring agents and corrupting them and may also allow the spying on the agents themselves (Kun, Xin & Dayou, 1999). The framework supposes that the network being considered is secure.

3.2 The MAS Threat Model

The different types of threats that the MAS would encounter according to 1) malicious platforms, 2) malicious agents and 3) malicious networks are as follows. Like (Jansen & Karygiannis, 1998; Jansen, 2001; Jansen & Karygiannis, 1998), we use simple mobile agent architecture to identify the threat model shown in Figure 3.1. The arrows indicate an underlying network that carries the mobile agent. The host O spawns a mobile agent A to an agent platform X for execution. The mobile agent A continues its execution to agent platform Y and so on. The three major security considerations can be expressed here, the malicious platform, malicious agent and the malicious network. This threat