www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 1 Jan 2013 Page No. 322-329

Optimize Security solution for mobile agent security: A Review

Sachin Upadhye[1] P.G.Khot[2]

Asst. Prof, Ramdeobaba College of Engg. And Management , Nagpur
Email : sachupadhye@gmail.com
Professor, Post Graduation Teaching Department of Statistics, R.T.M. Nagpur
Email: pgkhot@gmail.com

Abstract

The field of agents has many diverse researchers, approaches and ideas, which has helped to create one of the more dynamic research areas in recent years. Mobile agents are enjoying a lot of popularity and are destined to influence research in distributed systems for the years to come. Thus far, technology has been instrumental in disseminating new design paradigms where application components are not permanently bound to the hosts where they execute. Mobile agents are gaining in complexity as they evolve and are now widely used in e-commerce. All phases of a business transaction, such as negotiating and signing contracts can be done using mobile agents. In this paper, we provided a brief introduction to the recent researches & developments associated with the field of mobile agents, highlighting various security threats, also touching the weakest hot-spots of the field which need to be nurtured.

This paper also focuses on the optimization of computation cost for agent platform, which appears due to complex security operations. Traditionally, a security manager is integrated within an agent platform, which performs these operations for every mobile agent visiting the platform. To reduce the security costs at the agent platform, a detached security manager is used, which performs complex security operations on behalf of multiple agent platforms.

The paper is structured as follows. Section 1 Introduction to multi agent system and security. Section 2 briefly describes the characteristics of agents and Security Services. In section 3 we will discuss some security threats and countermeasures and in last section describes some recent research aimed at enhancing the security of mobile agent systems.

Keywords

Intelligent agent, Mobility, Security, Security Threats, Multi agent security, mobile agent security.

Introduction

The agent paradigm is currently attracting much research. A mobile agent is a particular type of agent with the ability to migrate from one host to another where it can resume its execution. Mobile agents moving around the network are not safe because the remote hosts that accommodate the agents can initiate all kinds of attacks and can attempt to analyze the agents' decision logic and their state and behavior, due to this mobile agent is one of the most challenging problems. Agents are an interesting topic of study because of their

utility in diverse disciplines of computer science including personal information management, artificial intelligence, electronic commerce, interface design, computer games, distributed processing, distributed algorithms, and many more[1, 2]. There are various differences among the existing mobile agent systems in the context that what they are allowed to move, and how it is actually moved. One of the distinctions can be drawn on the basis of execution state. The systems supporting strong mobility [6] allow the migration of both the code and the execution state along with the executing unit to a different computation environment. On the other hand, the systems supporting weak mobility [6], allows the code migration only. The code contains only some initialization data and execution state is not migrated. These security concerns can be classified in two broad Categories, according to whether the agent's or the Platform's security is at stake. On the one hand, host platforms receiving and executing mobile agents must be protected against malicious code. Common mechanisms addressing this issue include cryptographic authentication and integrity checks, code signing and encryption, etc. on the other hand, mobile agents must protect themselves against hosts trying to tamper maliciously with either the code or the data carried by incoming agents. Mobile agents are autonomous software agents that travel in a computer network to execute and perform tasks on different hosts on behalf of their owners. Autonomous mobile agents bring advantages such as task delegation, network communication, and cost reduction for distributed tasks [2].

Characteristics Of Agents

The invasion of various approaches under the banner of "agents" caused a need to classify and define this term. However that everyone had their own definition [7] due in part to the historical relationship with the AI community and the vague notion of intelligence. Numerous definitions and characteristics for the agents have been proposed, following are the characteristics of agents.

- ***Autonomous*** - An agent should be able to execute without the need for human interaction, although intermittent interaction may be required.
- ***Social / Communicative*** - An agent should have a high level of communication with other agents. The most common protocol for agent communication is the Knowledge Query and Manipulation Language (KQML) [10].
- ***Reactive / Responsive*** - An agent should be able to perceive its environment and react to changes in it.
- ***Proactive*** - Proactive agents do not just react to their environment but can take active steps to change that environment according to their own desires.
- ***Adaptive*** - Adaptive agents have the ability to adjust their behavior over time in response to internal knowledge or changes in the environment around them.
- ***Goal-oriented / Intentions*** - These agents have an explicit internal plan of action to accomplish a goal or set of objectives.

- ***Persistence / Continuous*** - Persistent agents have an internal state that remains consistent over time.
- ***Mobility*** - Mobile agents can proactively decide to migrate to a different machine or network while maintaining persistence.
- ***Emotion*** - Agents with the ability to express human-like emotion or mood such agents might also have some.

Security Services

Security services are important for the protection of your agents and server from the attacks. The following is the list of commonly available services for securing agent system [11].

• ***Authentication:*** before accepting an incoming agent, you want to know who its sender is. In this case, you need authenticate the agent. This process includes the verification of the developer who created the agent or before sending the agent to some host you may wish to know who the host is and what its credentials are.

- *Authentication of user:* the user needs to authenticate himself to a given server. Public key encryption or a password can be used for this purpose.
- *Authentication of host:* before a server starts to communicate with another server or client, it needs to know with whom it is communicating.
- *Authentication of code:* before executing an incoming agent, the host needs to know who created the agent. Digital signatures are typically used for this purpose.
- Authentication of agent: before executing an incoming agent, the server needs to know who is responsible for this agent or who its owner is.

• ***Integrity:*** to trust an agent, you need to make sure that no one has tempered with its code and data. Checking the integrity of the agent is the technique we use to make sure that no manipulation is done with its code and data. Confidentiality: an agent may carry confidential information that should be readable only by intended server or agent. Such information should be kept secret form other servers and agents.

• ***Authorization:*** authorization or access control is the way to specify and enforce an agent's capability to access information or to use services provided by a server.

• ***Nonrepudiation:*** an agent or sever cannot deny that a given communication exchange or transaction has taken place.

• ***Auditing:*** auditing service records security-related activities of an agent for later inspection.

Security Threats & Countermeasures

Mobile agents can travel to other system in a network and can execute there by consuming remote host resources, this is the basic property of Mobile agents and because of this property the Mobile agents are open to several attacks and abuses. Mobile agents amplify the threats of abuse and misuse due to their mobility and execution on different platform. This chapter discusses about the threats that can be encountered by mobile agents. Firstly we will discuss the classification of all the threats and then we discuss these threats in detail and finally the countermeasures taken to prevent or avoid these attacks.

Security Threats

Threats to security generally fall into three main classes: disclosure of information, denial of service, and corruption of information. There are a variety of ways to examine these classes of threats in greater detail as they apply to agent systems. A number of models exist for describing agent systems [12, 13, 14]; however, for discussing security issues it is sufficient to use a very simple one, consisting of only two main components: the agent and the agent platform. Here, an agent is comprised of the code and state information needed to carry out some computation. Mobility allows an agent to move, or hop, among agent platforms. The agent platform provides the computational environment in which an agent operates. The platform from which an agent originates is referred to as the home platform, and normally is the most trusted environment for an agent. One or more hosts may comprise an agent platform, and an agent platform may support multiple computational environments, or meeting places, where agents can interact Four threat categories are identified:

Security Thread Categories

1) Agent to Platform
   - Masquerading
   - Denial of Service
   - Unauthorized Access
2) Platform to Agent
   - Masquerade
   - Denial of Service
   - Eavesdropping
   - Alteration
3) Agent to Agent
   - Masquerade
   - Repudiation
   - Unauthorized Access
4) Other Entities-to-Agent
   - Masquerade
   - Unauthorized Access
   - Denial of Service
   - Copy and Replay

COUNTERMEASURES

Most agent systems rely on a common set of baseline assumptions regarding security. The first is that an agent trusts the home platform where it is instantiated and begins execution. The second is that the home platform and other equally trusted platforms are implemented securely, with no flaws or trapdoors that can be exploited, and behave non-maliciously. The third is that public key cryptography, primarily in the form of digital signature, is utilized through certificates and revocation lists managed through a public key infrastructure.

Protecting the Agent Platform

More recently developed techniques aimed at mobile code and mobile agent security have for the most part evolved along these traditional lines. Techniques devised for protecting the agent platform include the following:

- Software-Based Fault Isolation,
- Safe Code Interpretation,
- Signed Code,
- Authorization and Attribute Certificates,
- State Appraisal,
- Path Histories, and
- Proof Carrying Code.

Protecting Agents

The Jumping Beans [15] agent system addresses some security issues by implementing a client server architecture, whereby an agent always returns to a secure central host first before moving onto any other platform. Some more general-purpose techniques for protecting an agent include the following:

- Partial Result Encapsulation,
- Mutual Itinerary Recording,
- Itinerary Recording with Replication and Voting,
- Execution Tracing,

- Environmental Key Generation,
- Computing with Encrypted Functions, and
- Obfuscated Code (Time Limited Blackbox).

Literature Survey

Picco in [6] explored the related research fields by showing evidence of the benefits mobile agents can potentially achieve, illustrated the foundations of architectures and technologies for mobile agents, and discussed some of the open issues still hampering a wider acceptance of this paradigm. Paper also presented the rationale for using mobile agents, hints at why and when mobile agents are preferable over other solutions, reviewed the basic architectural paradigms for code mobility, including mobile agents and lastly presented reflections on the present status and the future scope of the research area. This work studied two case studies, one is mobile agents for database access and secondly, mobile agents for network management were discussed to research in this field. Advantages of agents have also been highlighted. A distinction is also drawn based on whether the execution state is migrated along with the execution unit or not. Strong mobility & weak mobility has been supported by the systems in response to this distinction.

Knoll, Suri, & Bradshaw in [17] introduced a path-based security for mobile agents. The path-based security provided a mechanism that extended the security of the NOMADS mobile agent system in a multiple-hops scenario. NOMADS supported strong mobility and safe agent execution. Strong mobility allowed the execution state of an agent to be captured and moved with the agent from one host to another [6].

Gavalas, Tsekouras, & Anagnostopoulos in [16] proposed a mobile agent technology for the management of networks and distributed systems as an answer to the scalability problems of the centralized paradigm. The authors considered the design and implementation of a complete MAP research prototype that sufficiently addressed the issues such as security mechanism, fault tolerance.

Xiaorong, Su, & Mingxuan in [18] introduced the mobile agent technology based on quantitative hierarchical network security situational assessment model. Network security situational assessment quantitative model is a Hierarchical network consisting of Quantification of security situational index. This index has further different levels: Service-level security situational index, Host-level security situational index, Network system-level security situational index. The security model proposed by Xiaorong is distinct and refined method as compared to other models since most works are based on local area network and single host, which hardly meet the demand of large-scale network security assessment. But the technical realization of the quantitative model for further prediction had not been discussed which degrades the quality aspects of the model.

Moussa & Agha in [22] presented the design of "Bosthan", a multi-agent-based simulation tool that managed resources consumption in multi-inhabitants smart spaces. Bosthan had been built on the top of

Actor Net mobile agent platform to simulate different smart space topologies with varying numbers of residents. Bosthan had been used to study how proposed solution affects the performance and efficiency of smart computing environments without revealing their identity. Bosthan has been designed as a tool for agent-based discrete event simulations that would enable the analysis of different smart space scenarios, ranging from small environments such as smart rooms, to large smart spaces such as smart homes, smart offices or even smart buildings.

Rizvi, Sultana, Sun & Islam in [20] provided a solution for securing mobile agent in an ad hoc network. The paper provided a solution for securing mobile agent in an adhoc network. The authors used Threshold Cryptography in their model, because it provides solution to the problem of central certificate authority (CA) and trusted third party in PKI, by distributing trust among several network nodes. The model provides prime security services like confidentiality, integrity and authenticity. But mobile agent is not free from threats.

Singh, Juneja & Sharma in [21] explained about the working of agent community that it works on the core idea of cooperation and delegation of tasks, which in turn should be prevented from any malicious usage. In order to avoid this malicious usage, an instrument for ensuring proficient and secure communication among these collaborating agents is trust. The authors proposed an elliptical curve cryptography based security engine which extends a novel architecture namely CNTEP which successfully established trust among agents. Encryption of mobile agents and communicated messages is one of the solutions for ensuring security. However traditional encryption algorithm such as DH,DSA [23] and RSA [24], employ key sizes which are very large resulting in high time and space complexity. In contrast to this Elliptical Curve Cryptography (ECC) technique [25, 26] is a public key cryptosystem that besides using much smaller key sizes is able to provide a competitive security edge as that of other strong encryption algorithms.

Roth & Jalali-Sohi in [27] presented a mobile agent structure which supports authentication, security management and access control for mobile agents. They presented a flexible and extensible structure for the representation of mobile agents which supports hierarchical access control, and proposed an initial interpretation of this structure with respect to the roles in a general mobile agent model.

Karnouskos in [28] considered the concept of active networks. Active Networks (AN) are a rapid evolving area of research and in parallel an area of great industry interest. However, for this technology to make the step out of the labs and penetrate the market, the security problems have to be tackled effectively. This paper demonstrated why and how agent technology research, can and should be applied to active networks, in order to fulfill the new security challenges this infrastructure poses.

Conclusion

Agent technology has been used in many critical applications such as personal information management, electronic commerce, business process management, artificial intelligence, interface design, distributed processing and distributed algorithms. Besides its bright side, the technology has encountered many security threats. These problems are faced during the itinerary period of an agent traversing from platform to platform in the network. In this paper, we have surveyed various recent developments, researches and proposals related to the field of agents and have thrown some light on the delicate areas that needs to be paid more attention to promote growth in optimistic direction.

Reference

[1] N. Jennings and M. Wooldridge, "Software Agents", IEE Review, January 1996, pp. 17-20. [2] O.A. Ojesanmi and A. Crowther, "Security Issues in Mobile Agents", International Journal of Agent Technologies and Systems, 2(4), pp. 39-55, October-December 2010, University, Nigeria.

[3] D. C. Smith, A. Cypher and J. Spohrer (1994) "Programming Agents without a programming language" Communications of the ACM 37 (7) pp 55-67.

[4] P. C. Janca (1995) "Pragmatic Application of Information Agents: BIS Strategic Decisions. [5] T. Selker (1994) "A Teaching Agent that learns" Communications of the ACM 37 (7) pp 92-99. D. C.

[6] G.P. Picco, "Mobile agents: an introduction", Microprocessors and Microsystems 25(2001) pp. 65-74, Dipartimento di Elettronica e Informazione, Politecnico di Milano, Milan, Italy.

[7] H.S. Nwana, "Software Agents: An Overview", Knowledge Engineering Review, 11(3):1- 40, 1996.

[8] M. Woodridge and N. Jennings, "Intelligent Agents: Theory and Practice", The Knowledge Engineering Review, 10(2):114-152, June 1995.

[9] S. Franklin, A. Graesser, "Is it an Agent, or just a Program?: A Taxonomy for Autonomous Agents", University of Memphis, Proceedings of the Third International Workshop on Agent Theories, Architectures, and Languages, Springer-Verlag,1996.

[10]T. Finin, Y. Labrou & J. Mayfield, "KQML as an Agent Communication Language", J. Bradshaw (Eds), MIT Press, 291-316, 1997.

[11]Danny B.Lange and Mitsuru Oshima, "Programming and Developing Java Mobile Agents with Aglets". (Addison Wesley publication)

[12] A. Fuggetta, G.P. Picco, and G. Vigna, "Understanding Code Mobility," IEEE Transactions on Software Engineering, 24(5), May 1998. <URL: http://www.csucsbedu/~vigna/listpubhtml>

[13] "Agent Management," FIPA 1997 Specification, part 1, version 2.0, Foundation for Intelligent Physical Agents, October 1998. <URL: http://www.fipa.ord/spec/fipa97/fipa97.html>

[14] "Mobile Agent System Interoperability Facilities Specification," Object Management Group (OMG) Technical Committee (TC) Document orbos/97-10-05, November 1997.

[15] "Jumping Beans White Paper," Ad Astra Engineering Inc., Sunnyvale CA, December 1998.

[16] D. Gavalas, G.E. Tsekouras, C. Anagnostopoulos, "A mobile agent platform for distributed network and systems management", In Journal of Systems and Software 82 (2), 355-371, 2009.

[17] G. Knoll, N. Suri, and J.M. Bradshaw, "Path-based Security for Mobile Agents", Electronic Notes in Theoretical Computer Science, Vol. 58, No. 2 , pp. 16, (2002)

[18] C. Xiaorong, L. Su, L. Mingxuan, "Research of Network Security Situational Assessment Quantization Based on Mobile Agent", Volume 25, 2012, Pages 1701–1707, International Conference on Solid State Devices and Materials Science, April 1-2, 2012, Macao.

[19] S. M.. Moussa, G.A. Agha, "Integrating Encrypted Mobile Agents with Smart Spaces in a Multi-agent Simulator for Resource Management", Journal of Software, Vol 5, No 6 (2010), 630-636, Jun 2010.

[20] S.M.S.I. Rizvi, Z. Sultana, B. Sun, and Md. W. Islam, "Security of Mobile Agent in Ad hoc Network using Threshold Cryptography", World Academy of Science, Engineering and Technology 70- 2010.

[21] A. Singh, D. Juneja, and A.K. Sharma, "Elliptical Curve Cryptography Based Security Engine for Multiagent Systems Operating in Semantic Cyberspace", In International Journal of Research and Review in Computer Science (IJRRCS), Vol. 2, No. 2, April 2011.

[22] D.M. Chess, " Security issues in mobile code systems. In : mobile agents and security", Editor Vigna, vol. LNCS1419. Springer-Verlag 1998.

[23] K. Lauter, "The Advantages of Elliptic Curve Cryptography for Wireless Security", In IEEE

Wireless Communications, pp. 62-67. February 2004.
[24] R. Shanmugalakshmi and M. Prabu, "Research Issues on Elliptic Curve Cryptography and its applications", In International Journal of Computer Science and Network Security, Vol. 9, No.6, pp 19-22, June 2009.
[25] N. Koblitz, "Elliptic Curve Cryptosystems", Mathematics of Computation, Vol. 48, pp. 203-209, 1987.
[26] V.S. Miller, "Use of Elliptic Curves in Cryptography", Advances in Cryptology- CRYPT ‟85, LNCS, vol. 218, Springer-Verlag, pp. 417-426,1986.
[27] V. Roth & M. Jalali-Sohi, " Access Control and Key Management for Mobile Agents", Fraunhofer Institute for Computer Graphics, Rundeturmstr. 6, 64283 Darmstadt, Germany, 8 November, 2001.
[28] S. Karnouskos, "Security implications of implementing active network infrastructures using agent technology", Special Issue on Active Networks and Services, In Computer Networks Journal, ElsevierVol36Issue 1pp87-100June 2001
[29] A. Singh, D. Juneja, A.K. Sharma, "Introducing Trust Establishment Protocol in Contract Net Protocol". In Proceedings of IEEE International Conference on Advances in Computer Engineering (ACE‟2010), pp. 59-63, June, 2010.
[30] P. Dadhich, Dr. K. Dutta, and Prof.(Dr.) M.C. Govil, "Security Issues in Mobile Agents", International Journal of Computer Applications(0975-8887), Volume 11-No.4, December 2010.