International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 04 | April - 2021 ISSN: 2582-3930

Systematic survey of mobile agent security system

Jyoti Singh

Model College Dombivili East

ABSTRACT:-

A pivotal cause for the boom of Mobile Agent paradigm relies on the competence to ward off security attacks. this survey hands over a key to researchers who primarily target the security concerns of the mobile agent-based applications. Mobile agent technology is emanating as a new paradigm in the area of distributed and mobile computing, and has been engaged in many areas from network management tasks to information management.

In the recent years, mobile agent paradigm has emerged as a viable approach for the evolution of autonomic systems in the healthcare domain.Agent code represents the program written in a suitable language that defines the agent‘s behavior. Many people consider that security is one of the complexes problems for practical use of mobile agents that move around the networks and do their tasks.

The aim is to provide trusted mobile agent systems that can be easily deployed and widely adopted. here paper also identifies security objectives, and measures for countering the identified threats and fulfilling those security objectives. The security area still needs more efforts to protect the mobile agent system. A mobile agent has three ingredients: agent code, agent state and agent attributes.

Keyword:- Mobile agent, Security system, Security system, adaptive security, Mobile Cryptography.

INTRODUCTION:-

It has the unique ability to transport itself from one system in a network to another. Mobile agents reduce network traffic, overcome network latency, encapsulate protocols, execute asynchronously and autonomously, adapt dynamically, naturally heterogeneous and are robust and fault-tolerant. It has been engaged in many sectors, from network management errands to information management. It affords an infrastructure not only for executing autonomous agents but also for dispatching them between different computers. A mobile agent is a software object that is not bound to the system where it begins its execution. Over the years computer

systems have evolved from centralized monolithic computing devices supporting static applications, into client-server environments that allow complex forms of distributed computing. A new phase of evolution is now under way that goes one step further, allowing complete mobility of cooperating applications among supporting platforms to form a large-scale, loosely-coupled distributed system.

1. Mobile Agent Applications and Security Scenarios:-

Mobile agent technology is beginning to make its way out of research labs and is finding its way into many commercial applications areas. The following section takes a look at these application areas and discusses relevant security issues for typical scenarios.

1.1 Network Management:-

Network management refers to the processes, tools and applications used to administer, operate and maintain a network infrastructure. Performance management and fault analysis are also included in network management. To put it simply, network management is the process of keeping your network healthy, which keeps your business healthy. Network management is the process of administering and managing computer networks. Services provided by this discipline include fault analysis, performance management, provisioning of networks and maintaining quality of service. Software that enables network administrators to perform their functions is called network management software. Network management software is software that is used to provision, discover, monitor and maintain computer networks. Network management security policies are unlikely to allow code from outside the organization onto the network. These policies are more likely to allow only in-house code or code signed by a trusted vendor onto the network. Mobile agents are also well suited for network management applications such as remote network management, software distribution, and adaptive response to network events. Most of the current network management software is based on the Simple Network Management Protocol (SNMP). Mobile agents can also provide adaptive responses to network events. Without mobile agents, all of the software required to support and respond to all possible scenarios must be kept loaded and available on a device at all times. Agent developers and administrators could also benefit from better resource control mechanisms in mobile agent platforms.

1.2 Electronic Commerce:-

Mobile agents representing bidders may meet on an auction house's platform to engage in blind, straight, or Dutch auctions, each employing different strategies and

having different financial constraints. A mobile agent's tasks could be divided between static and mobile agents so that the more security the transaction required, the less mobile the agent would be. For example, a "window shopping" mobile agent could visit vendor sites searching for the price and availability of goods and services. When the mobile agent finds the goods and services that meet its criteria, a static agent at the home platform or at a trusted platform could complete the sale and sign the receipt with its private key. The level of security required for the application and the sensitivity of the mobile agent's

code and data directly influences the degree of mobility of a mobile agent. Mobile agent-based electronic commerce applications have been proposed and are being developed for a number of diverse business areas, including contract negotiations, service brokering, auctions, and stock trading [1, 4, 27, 41].

1.3 Personal Digital Assistants (PDA):-

A personal digital assistant (PDA), also known as a handheld PC,[1][2] is a variety mobile device which functions as a personal information manager. A PDA has an electronic visual display, letting it include a web browser. The term is more commonly used for software that identifies a user's voice to reply to the queries. Most PDAs can access the Internet, intranets or extranets via Wi-Fi or Wireless WANs. Agent developers often cite the example of a user launching an agent to make travel, hotel, and dinner reservations by negotiating with other agents, as an illustrative scenario for mobile agent technology [1,4, 27]. A number of conventional security mechanisms are being applied to mobile agent systems. Manufacturers of cell phones, personal organizers, car radios, and other consumer electronic devices are introducing more and more functionality into their products and are becoming the focus of agent developers. A number of conventional security mechanisms are being applied to mobile agent systems. These institutions would be responsible for the safety of the agent systems, and in return could differentiate themselves from their competitors and generate new sources of income from these new agent-based services.

2. Security Requirements:-

The users of networked computer systems have four main security requirements: confidentiality, integrity, availability, and accountabihty. The users of agent and mobile agent frameworks also have these same security requirements. This section provides a brief overview of these security requirements and how they apply to agent frameworks.

2.1. Confidentiality:-

Confidentiality is the keeping of another person or entity's information private. Certain professionals are required by law to keep information shared by a client or patient private, without disclosing the

information, even to law enforcement, except under certain specific circumstances.

2.2. Integrity:-

Integrity is the practice of being honest and showing a consistent and uncompromising adherence to strong moral and ethical principles and values. In ethics, integrity is regarded as the honesty and truthfulness or accuracy of one's actions.

2.3. Accountability:-

Audit logs are also necessary and valuable when the platform must recover from a security breach, or a software or hardware failure. Full recovery fi"om a faulty or compromised system requires not only restoring the system to a safe state and performing some sort of fault diagnosis, but also sorting out which agents belonging to which organizations were affected. Audit logs are also necessary in cases of agents falsely repudiating their actions and for potential liability issues that are unique to agent societies.

3. Security, Design, and Performance Issues:-

A number of advantages of using mobile code and mobile agent computing paradigms have been proposed [4, 36, 42]. These advantages include: overcoming network latency, reducing network load, executing asynchronously and autonomously, adapting dynamically, operating in heterogeneous environments, and having robust and fault-tolerant behavior. The following subsections briefly discuss the impact of various security issues on the design and performance of mobile agent systems.

3.1. Adapting Dynamically:-

the DAP involves the four phases of the EPIS implementation conceptual model (Exploration, Preparation, Implementation, and Sustainment) [13] that, while generally sequential, allow for feedback to earlier phases. This process is continuously iterative, in that ongoing experience can inform continued adaptation as needed. The ability of a computing system to autonomously modify its behavior during its execution. The addition, removal or replacement of software elements (e.g. components) at runtime i.e. while the system is performing its core operations. Communicating, negotiating, and managing mobile agent security policies also introduces new security administration costs for the mobile agent platform.

3.2 Robust and Fault-Tolerant Behavior:-

Based on the fault diagnosis result, a robust fault-tolerant controller is designed by the virtual actuator approach, which aims to construct a reconfiguration block to force the output of the reconfigured faulty plant approximated the behavior of a nominal system. Simulation results demonstrate the effectiveness of the proposed method. A number of surveys are discussed various

aspects of fault-tolerant control. The most common approach in coping with such a problem is to separate the overall design in two distinct phases. The first phase concerns "Fault Detection and Isolation" (FDI) problem, which consists in designing filters (dynamical systems) able to detect the presence of faults and to isolate them from other. The ability of mobile agents to react djaiamically to unfavorable situations and events makes it easier to build robust and fault-tolerant distributed systems. The ability of the mobile agents to move from one platform to another in a heterogeneous environment has been made possible by the use of virtual machines and interpreters.

3.3. Overcoming Network Latency:-

Reducing the physical distance between the data source and its eventual destination is the best strategy for how to reduce latency. For markets and industries that rely on the fastest possible access to information, such as IoT devices or financial services, that difference can save companies millions of dollars. Mobile agent solutions have been proposed for critical systems that need to respond to changes in their environments in real time. Mobile agents have been offered as a solution, since they can be dispatched from a central controller to act locally and directly execute the controller's instructions. These distributed manufacturing processes may allow different companies to use their special-purpose machining tools and run proprietary data-analysis algorithms. Developers and researchers have made increasing virtual machine and interpreter performance a top priority, and faster hardware is continuously being introduced to the market, but the quest for better performance will always remain.

3.4. Reducing Network Load:-

A mobile agent-based search and data analysis approach can help decrease network traffic resulting from the transfer of large amounts of data across a network for local processing. A mobile agent-based search and data analysis approach can help decrease network traffic resulting from the transfer of large amounts of data across a network for local processing. Instead of transferring the data across the network, mobile agents can be dispatched to the machine on which the data resides, essentially moving the computation to the data, instead of moving the data to the computation, thus reducing the network load for such a scenario. Clearly, transferring an agent that is smaller in size than the data to be transferred reduces the network load. These benefits hold when the comparison is made between encrypted lightweight mobile agents and the relatively larger data to be transferred. This is possible because the parameters of the query are well defined and understood by the server, and the query poses a low risk to a secure computing environment or to the information provider's business operations.

3.5 Operating in Heterogeneous Environments:-

Since mobile agents are generally computer- and transport-layer-independent, and dependent only on their execution environment, they offer an attractive approach for heterogeneous system integration. Mobile agents' ability to operate in heterogeneous computing environments is made possible by virtual machines or interpreters on the host platform. The benefits of heterogeneity, however, introduce several new security concerns. The current implementations of virtual machines or interpreters that make heterogeneous computing environments possible, however, do not provide adequate support for resource control. For example, Java currently provides no way for the host to limit the processor and memory resources allocated to a given object or thread and is, therefore, susceptible to denial of service attacks. A related issue is the ability of the agent to allocate resources external to the program, for example, by opening files and sockets, and creating windows. In addition, the current Java VM offers no protection from references to an object's public methods.

4. Areas for Future Research:-

The area of mobile agent security is still in a somewhat immature state. The traditional host orientation toward security persists, and the focus of protection mechanisms with in the mobile agent paradigm remains on protecting the agent platform. From the threats and countermeasures reviewed earlier and in the ensuing discussion, there appears to be an opportunity for research along the following lines:

• Agent Security Framework,

• Security Design Tools

4.1. Agent Security Framework:-

describes a distributed security infrastructure for mobile agents. The first property of the infrastructure is believability ; this means that mechanisms are provided for authenticating information furnished by an agent. A second security property is survivability . This means that an agent computation can be programmed to survive attacks by malicious hosts on individual agents; this is achieved through encryption as well as agent replication and voting. In the past, as teams of individuals have developed agent systems, pragmatics prevailed and emphasis was placed on functionality over security.

4.2. Security Design Tools:-

Mobile agent application developers currently face a number of obstacles before they can efficiently design and develop large-scale mobile agent systems. The limitations of agent and agent platform security mechanisms must also be overcome before agent developers can realize the full benefits of mobile agent technology. Mobile agent security design tools can help agent system developers determine the effects of employing various security mechanisms and

make better decisions about functionality and performance tradeoffs.

CONCLUSION :-

In this paper we have shown the implementationg of two different security approaches to protect the mobile agents against the malicious hosts, in IBM Aglets. We have also presented our implementation that checks the integrity of the aglets. In these security approaches the computation is done on the encrypted data itself without decrypting, thus providing security. A wide variety of techniques for implementing security in agent systems is available. Not all are compatible with one another, nor are they all suitable for most applications. Many of these techniques must be implemented within the framework of the agent system, while a number of them can be applied independently within the context of the application. Clearly, this is a period where establishing such a baseline requires more experimentation and experience with alternative design choices, including those involving tradeoffs in performance, scalability, and compatibility.

REFERENCES:-

Tarig Mohamed Ahmed. 2009. Using secure-image mechanism to protect mobile agent against malicious hosts. Int. J. Com-put. Electr. Auto. Control Info. Eng. 3, 11 (2009), 439–444. Retrieved from: http://www.waset.org/.

Tarig Mohamed Ahmed. 2012. Generate sub-agent mechanism to protect mobile agent privacy. In Proceedings of the IEEE Symposium on Computers & Informatics (ICSI'12), IEEE, Penang, 86–91. DOI:http://dx.doi.org/10.1109/ISCI.2012.6222672

Raja Al-jaljouli and Jemal H. Abawajy. 2007. Secure Mobile Agent-based E-Negotiation for On-Line Trading. In Proceed-ings of the IEEE International Symposium on Signal Processing and Information Technology, IEEE, Giza, 610–615. DOI:http://dx.doi.org/10.1109/ISSPIT.2007.4458205

Hasan Omar Al-Sakran. 2015. Intelligent traffic information system based on integration of internet of things and agent technology. Int. J. Adv. Comput. Sci. Appl. 6, 2, (2015), 37–43. DOI:http://dx.doi.org/10.14569/IJACSA.2015.060206

Mousa Alfalayleh and Ljiljana Brankovic. 2005. An overview of security issues and techniques in mobile agents. In Proceedings of the 8th IFIP TC-6 TC-11 Conference on Communications and Multimedia Security. Springer U.S. 59–78. DOI:http://dx.doi.org/10.1007/0-387-24486-7_5

Joan Ametller, Sergi Robles, and Joan Borrell. 2003. Agent migration over FIPA ACL messages. In Lectures on Mobile Agents for Telecommunication Applications, Eric Horlait, Thomas Magedanz and Roch H. Glitho (Eds.). Lecture Notes in Com-puter Science. 2881. Springer, Berlin,

210–219.
DOI:http://dx.doi.org/10.1007/978-3-540-39646-8_20

Peng Yong, Zhao Wei, Xie Feng, Dai Zhong-Hua, Gao Yang, and Chen Dong-Qing. 2012. Secure cloud storage based on cryptographic techniques. J. China Univ. Posts Telecommun. 19, 2, (2012), 182-189. DOI:http://dx.doi.org/10.1016/S1005-8885(11)60424-X

Adam Young and Moti Yung. 1997. Sliding encryption: A cryptographic tool for mobile agents. In Lectures on Fast Software Encryption. Eli Biham (Ed.). Lecture Notes in Computer Science. 1267, Springer-Verlag, Berlin, 230–241. DOI:http://dx.doi.org/10.1007/BFb0052350

Nauman Zafar, Edin Arnautovic, Ali Diabat, and Davor Svetinovic. 2014. System security requirements analysis: A smart grid case study. Syst. Eng. 17, 1 (Jul. 2014), 77–88. DOI:http://dx.doi.org/10.1002/sys.21252

Y. Sakurai, M. Yokoo, and K. Kamei. An efficient approximate algorithm for winner determination in combinatorial auctions. In Proceedings of the Second ACM Conference on Electronic Commerce (EC-00), pages 30–37, 2000.

T. Sandholm. An algorithm for optimal winner determination in combinatorial auction. In Proceedings of the Sixteenth International Joint Conference on Artificial Intelligence (IJCAI-99), pages 542–547, 1999.

E. Rasmusen. Games and Information. Blackwell, 1994.

Makoto Yokoo, Koutarou Suzuki. Secure Multi-agent Dynamic programming based on Homomorphic Encryption and its Application to Combinatorial Auctions.