Security Issues in Mobile Agents

Priyanka Dadhich
Research Scholar
Department of CSE
NIT, Hamirpur (INDIA)

Dr.Kamlesh Dutta
Associate Professor
Department of CSE
NIT, Hamirpur (INDIA)

Prof. (Dr.) M.C.Govil
Professor
Department of CE
MNIT, Jaipur (INDIA)

ABSTRACT
Software security to protect mobile agent consists of lots of aspects like cryptography, access control and trust management, intrusion detection and tamper resistance, authentication and privacy, signature schemes, e-commerce, security analysis, mobile computing security etc. So, to design and develop security mechanisms for mobile agents against malicious hosts this paper identifies different kinds of attacks and relationships between them. Security objectives and requirements are analyzed with security measures taken to protect mobile code, state and data.

Keywords
Cryptography, access control, trust management, intrusion detection, authentication, privacy, signature schemes, e-commerce.

1. INTRODUCTION
The mobile agent paradigm is a further extension to distributed computing paradigms. A mobile agent is a software program with mobility which can be sent out from a computer into a network and roam among the computer nodes in the network[28]. It can be executed on those computers to finish its task on behalf of its owner. The transferring of a mobile agent state facilitates it in working automatically to travel between one or more remote computer. The key characteristic of the mobile agent paradigm is that any host in the network is allowed a high degree of flexibility to possess any mixture of know-how, resources and processors. Its processing capabilities can be combined with local resources [4]. Know- how (in the form of mobile agent) is available throughout the network. Since, the mobile agent has many salient merits, so it has attracted tremendous attention in last few years and become a promising direction in distributed computing and processing as well as high performance network area. In mobile agents, the mobile code generated by one party transfers and execute in an environment controlled by another party so several security issues arise in various mobile agent computing. These issues include authentication, authorization (or access control), intrusion detection etc. Because of mobility of mobile agent, the security problems becomes more complicated and have become a bottleneck for development and maintenance of mobile agent technology especially in security sensitive applications such as e-commerce, military applications, scientific applications etc[35]. Security issues are becoming more significant in this age of pervasive mobile network computing where we have different types of information being used by mobile and fixed large scale distributed applications interacting over wireless and wired network to deliver useful services to enterprises and users , fixed and mobile. So, the research on security issues of mobile agent differs in its aim, emphasis, base and technique. Section two explains various security objectives. Section three discusses various communication threats/ attacks on mobile agents. Section four puts forward various security issues in mobile agent followed by security requirements to protect mobile agents. Section five emphases on security mechanisms for mobile code protection. Section six lays security measures to protect agent's data. Section seven concludes the overall approaches for protection of mobile agents against malicious hosts. Section seven presents some open research directions. References are marked where appropriate and necessary.

2. SECURITY OBJECTIVES
2.1 Generally a secure software system should meet the following security objectives.
2.1.1 Accountability (Responsibility)
This objective requires that users and administrators will be held accountable for behavior that impacts the security of information. Accountability is often an organizational policy requirements that directly supports non-repudiation, deterrence, fault-isolation, intrusion detection and prevention and after- action recovery and legal action[31]. For example in an electronic business both the user and the online store from where the user (customer) buy products are accountable for their communications and behaviors.

2.1.2 Assurance
Assurance grounds for confidence that other security goals(including integrity, availability, confidentiality, and accountability) are adequately met by specific implementation[26]. These include 1. functionality that performs correctly. 2. sufficient protection against unintentional errors(by users or software) 3. sufficient resistance to intentional penetration or by-pass.

2.1.3 Authentication
This requires verifying the identity of a user, process or device before allowing access to resources in a system. Authentication requires that the identity of an entity or the originator of the data can be verified and assured to prevent it from faking or masquerading[29].

2.1.4 Authorization (or access control)
This means to grant or to deny access rights to a user, program or process. This objective requires that only legitimate users have rights to use certain services or to access certain resources keeping unauthorized users out. Here, apart from password

access, digital signatures are also required to decide whether or not to grant a request to an entity[44].

2.1.5 Availability

This objective requires that data and system can be accessed by legitimate users within an appropriate period of time[15]. Some attacks like Denial of Service (DoS) or instability of the system can cause loss of availability.

2.1.6 Confidentiality

This objective requires that data should be protected from any unauthorized disclosure i.e. data can only be read by persons or machines for which it is intended[17]. A loss of confidentiality hurts data privacy.

2.1.7 Integrity

It is divided into two aspects: data integrity and system integrity. Data integrity is the objective that data should not be altered or destroyed in an unauthorized manner to maintain consistency. System integrity is the objective that a system should be free from unauthorized manipulation.

2.1.8 Non-Repudiation

This objective requires that either side of a communication cannot deny the communication later. To achieve this, important communication exchanges should be logged so as to prevent denials by any party of a transaction. It relies on authentication to record the identities of entities[22].

2.2 Relationship among five main security objectives

To increase the availability level, a system compromises its confidentiality or integrity levels. Both confidentiality and integrity can effect and also be effected by each other. Based on them, availability and accountability is achieved .Hence rather than individual security objectives, an overall security policy is often preferred.

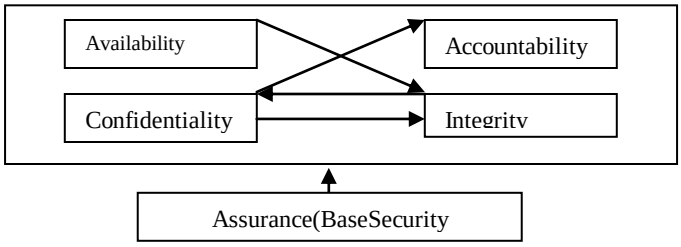
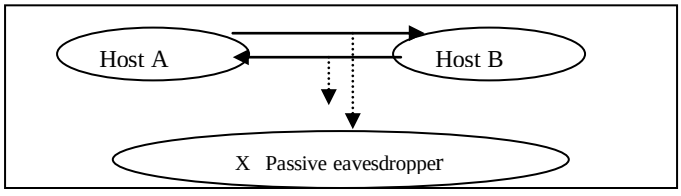


Fig. 1

3. TYPES OF ATTACKS

3.1 Passive Attack

This type of attack collects information but does not actively manipulate the mobile agent.



Here X monitors the communication between host A and host B

Fig. 2

3.2 Active attacks

In this attack an unauthorized attacker is able to insert his own data into the data stream, data replay from another connection or the same connection or can delete the data[24][25].

3.3 Attack against availability

Such attacks attempt to overload available resources or make a particular facility unavailable at a certain time. Attacks in this category are :

DoS(Denial of Service) or DDos(Distributed Denial of Service) attack: this attack is characterized by an explicit attempt by attackers to prevent legitimate users from using system services or cause delaying of time-critical operations[24]. DoS attacks can result in:

- Unavailability of a network service or temporary loss of all network connectivity and services.
- Can destroy programming and files in a computer system.
- Sending more traffic to a network so the functionality of that network node gets disabled.

Following three basic models of attack that comes in Dos attacks are:

- Consumption of scarce, limited or non-renewable resources.
- Destruction or alteration of configuration information.
- Physical destruction or alteration of network components.

Though DoS occur intentionally and maliciously but sometimes happen accidentally. They do not result in the theft of information or seriously loss but cost the target system significant time and money.

3.4 Attacks against Confidentiality

These attacks attempt to reveal the contents of communication or leak sensitive information of the system. It has following attacks:

3.4.1 Eavesdrop Attack

It is an attack where communication is monitored to reveal the secret. It occurs when some wiretap devices are plugged into the computer networks and eavesdrop on the network traffic[24]. Since network wiretap programs also comes with a feature called "protocol analysis" that allows them to decode the computer traffic and make sense of it.

3.4.2 Data Aggregation Attacks

This attack allows an attacker to deduce classified information from unclassified information. Here password or encryption key sniffing can do harm to system confidentiality[19]. Here attacker gain unauthorized access to system and steals legitimate user's password and masquerading as legitimate user or inspect encrypted files or communication messages by taking encryption keys illegally. This attack takes advantage of broadcast technology used in most networks.

3.5 Attacks against Integrity

This attack attempts to modify communication contents or data in a system. Various form of attacks here are:

3.5.1 Man-In –The- Middle (MITM) Attack

Here an attacker is able to read and modify messages between two parties without letting either entity to know that they have been attacked. Here attacker sniffs(detects) packets from network , modifies them and insert them back into the network[35]. Such attacks mostly happens in public-key based systems where introduction of signed keys by trusted third parties(TTP) can help with designing a mechanism for copying such attacks.

3.5.2 Web Site Defacing and Hijacking Attacks

This type of attack modifies, destroys or replaces some web pages of certain instructions[30][15]. Visitors of these instructions are given altered information or hijacked to other site without knowing the fact. Attackers can then request and collect certain information or gain benefits from the client. Weaknesses of web servers are always the base for this of attacks.

3.5.3 Replay Attacks

It is an attack in which the attacker records data or communication contents and replays it later to deceive the recipient[15].

3.6 Attacks against miscellaneous security objectives

3.6.1 Viruses

These are self propagating entities that move across the nodes of the internet. There are six stages in the life cycle of virus:Creation, Replication, Activation, Discovery, Assimilation and Eradication. A virus with damage routine can be activated when certain conditions are met on certain day or when the infected user performs a particular action. A virus without damage routine does not activate it only cause damage by stealing storage space. If virus do not cause a damage routine, it can still degrade the overall performance of system to its legitimate users by consuming storage space and memory that hurts system availability. Virus replicates by using their damage routine delivers virus payload to destroy files, reformat hard drive and other damages. Assimilation is a process by which software developers modify their software to detect and kill new viruses.

3.6.2 Unauthorized access attacks

These attacks include unauthorized use of resources and illicit access of data. A "backdoor" in a computer system is a method of bypassing normal authentication or obtaining remote access to a computer. Backdoor can be in form of an installed program or modification to a legitimate program. This attack can hurt system as well as user confidentiality and integrity.

3.6.3 Code exploit attacks

These attacks exploits software flaws to gain control of a computer or to cause it to operate in an unexpected manner. These attacks are in form of "Trojan Horses". These attacks do harm to system confidentiality, integrity and availability.

4. SECURITY ISSUES IN MOBILE AGENTS

4.1 Attacks on Mobile Agents by Mobile Agent Platforms

In case of strong mobility of mobile agent all its code, data and state are exposed to the mobile agent platform in which it migrates for execution of operation. Because of this mobile agent faces more severe security risks. Following are possible attacks by malicious platforms[29]:

4.1.1 Leak out/ modify mobile agent's code

Since the mobile agent's code has to be readied by a guest platform, so this malicious platform can read and remember instructions going to be executed to infer rest of the program based on that knowledge .By this process, platform knows the strategy and purpose of mobile agents[15]. If mobile agents are generated from standard building libraries , the malicious platform knows a complete picture of mobile agent's behavior and it finds out the physical address and can access its code memory to modify its code either directly or by insertion of virus. It can even change code temporarily , execute it and finally resuming original code before the mobile agent leaves.

4.1.2 Leak out/ modify mobile agent's data

There are many data which are very security sensitive like security keys, electronic cash, social security number that cause leak of privacy or loss of money. If the malicious platform get to know the original location of data it can modify the data in accordance with the semantics of data[24]. Above tasks can lead to severe consequences. Even if data is not sensitive, malicious platform can attack on normal data like traveling data of person and leaking it to somebody.

4.1.3 Leak out/ modify mobile agent's execution flow

By knowing the mobile agents physical location of program counter, mobile agent's code and data the malicious platform can predict what will be set of instructions to be executed next and deduce the state of that mobile agent. By help of this process, it can change the execution flow according to its will to achieve its goal[30]. It can even modify mobile agent's execution to deliberately execute agent's code in wrong way.

4.1.4 Denial of Service(DoS)

This attack causes mobile agent to miss some good chances if agent can finish its execution on that platform in time and travel to some other platform. DoS causes not to execute the mobile agent migration and put it in waiting list carrying delays.

4.1.5 Masquerading

Here malicious platform pretends as if it is the platform on which mobile agent has to migrate and finally becomes home platform where mobile agent returns. By this mechanism, it can get secrets of mobile agents by masquerading and even hurts the reputation of the original platform[35]. For example: malicious platform pretends an original airline company and give mobile agent a fake ticket and after receiving money, mobile agent founds the fakeness of the received ticket which in turn leads to dispute with real airline company later on.

4.1.6 Leak out/ Modify the interaction between a mobile agent and other parties

Here malicious platform eavesdrop on the interaction between a mobile agent and other parties like another agent or another platforms. This leads to extraction of secret information about mobile agent and third party. It can even alternate the contents of interaction and expose itself as part of interaction and direct the interaction to another unexpected third party. By this way, it can perform attacks to both mobile agent and third party.

4.2 Security Requirements to protect Mobile Agents

4.2.1 Authentication and Authorization

Authentication of a entity is the process of verifying the identity or other relevant information about the entity. The outcome of the authentication processes is that the user/agent knows the identity of the server/agent execution environment and the server/agent execution environment knows the identity of the user/agent. The process of deciding whether or not to grant a request after confirmation about the authentication of the principal is called authorization or access control[8]. To achieve those security properties, digital signatures are required in addition to password access.

4.2.2 Privacy and Confidentiality

Privacy requirement includes problems of confidentiality of exchanges and interactions in a mobile agent system. Since platforms are responsible for entire state of a mobile agent so mechanisms are needed that allow privacy of the information being accumulated and carried by agents to other platforms.

4.2.3 Non-Repudiation

This problem of repudiation arise when party involved in communication or activity denies its involvement. For this we should log important communication exchanges to prevent later denials. This is very important when mobile agent and mobile agent platforms commit to a digital agreement, contract, sale or any other such transactions.

4.2.4 Accountability

Since every user, agent or process on a platform is responsible for its action so we need to record not only unique identification and authentication but also an audit log of security relevant events to which both agent or process responsible for those events. All security related activities must be recorded for auditing and tracing purposes. Also, audit logs must be protected from unauthorized access and modifications.

4.2.5 Availability

This requirement ensures availability of both data and services of a mobile agent to local agents and incoming mobile agent. This mobile agent platform should ensure availability of controlled concurrency, support for simultaneous access, deadlock management and exclusive access when required[40]. Agent platform should able to detect and recover from software and hardware failures. It should have the ability to deal with and avoid Dos attacks as well.

4.2.6 Anonymity

The security policies of agent platform and their auditing requirements should be carefully balanced with agent privacy expectations. Here platform should keep agent's identity secret from other agents and maintains anonymity so as to determine agent's identity when necessary and legal.

4.2.7 Fairness

Fairness requirement means that no party can give advantage over other parties. So, in mobile agent system, mechanisms are necessary to ensure fair agent platform interaction in electronic exchange.

4.3 Security Mechanisms for Mobile Code Protection:

Security mechanisms provide assurance that remote hosts will adhere to policies for Mobile Code programs. Mechanisms are classified according to whether they aim to detect or prevent policy violations against a mobile code program[23][12].

Detection of Agent Tampering: this includes solutions to detect unauthorized modifications of code, state or execution flow of a mobile agent[16]. These detection mechanisms are further subdivided depending on whether they:

- D1: detect manipulation automatically or require a suspicion.
- D2: detect manipulation during execution of a mobile agent or after it has terminated.
- D3: detect all possible manipulations of mobile agent or only some of them.

4.3.1 Detection mechanisms

These mechanisms enable a mobile agent's owner to identify that an attack has occurred on the mobile code program. This helps in analyzing validity of results that program has accumulated but only when attack has done its work[31]. These mechanisms helps to find actual identity of remote host and tries to partially or fully repairmen of tampered results.

4.3.2 Range Checkers

Detects illicit mobile code manipulation that verify values of variables in the mobile code program or timing computations.

4.3.3 Embedding Function

These functions are called in normal program execution and assures that mobile code program executed correctly.

4.3.4 Detection of tampering using Traces

Here the mobile code program's owner detects tampering by comparing the mobile agent's expected execution trace against its actual execution history. A protocol given by Vigna detects mobile agent tampering by cryptographically signing in execution trace when mobile code program moves from one remote host to another.

4.3.5 Protocols using Cryptographic hash functions and Message authentication Codes (MAC)

Yee and Karjoth and colleagues proposed detection mechanisms for protecting the forward integrity of results collected by mobile code programs [34].

4.4 Prevention Mechanisms

The mechanisms here try to make it impossible or very difficult to access or modify code, state or execution flow of a mobile agent[11]. These are further subdivided into:

- P1: prevent attacks on the entire agent or only parts of it
- P2: rely on some trusted functionality or no trust at all.
- P3:prevent attacks permanently or only temporarily.

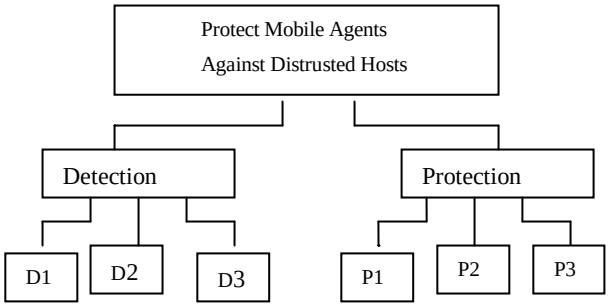


Fig. 3

4.4.1 Trusted Environments through Secure Coprocessors (SC)

This is a very attractive approach to both detection and prevention mechanisms for mobile code programs. Just like smart cards to cards installed in dedicated slots in host machines secure coprocessors provide a tamper-resistant, trustworthy hardware computing base at each remote host[12]. Mobile code program performs cryptographic operations at a remote host where crypto keys are hidden from the host.

The secure coprocessors can encrypt and digitally sign program code, execution state and partial results at each remote host before transmitting to a subsequent host[12]. Also, secure coprocessors securely provide critical algorithms to a mobile code program in hardware form that guarantees that algorithm will not be inspected or modified.

Limitation of SC: SC extend the hardware trust computing base (TCB) to each remote host in a way that limits the mobile code's ability to migrate at will. Hence they are helpful in applications where secure coprocessors are deployed throughout or controlled network such as closed corporate system or secure military network. To provide solution to above problem is to implicitly provide each mobile code program with its own trusted computing base for both internal computations and those with the remote host[10].

4.4.2 Encrypted Functions(EF)

EF provides execution privacy by transforming functions into encrypted forms that become part of the mobile code program and hence no information is revealed about its original function. The EF's migrate to remote hosts, where they operate on unencrypted input provided by the host[31]. The output produced by EF is itself encrypted and remains until the mobile code returns to its original host. This encrypted output not leaks information about the actual output of the original function that we applied to the input. Once the mobile code program completes its itinerary , it decrypts the encrypted output to provide values that would have been generated if original function would have applied to the input.

4.4.3 Secure –Function Evaluation(SFE)

SFE algorithm's work on any function represented as Boolean circuit , but this flexibility comes at a cost. This method restricts the mobility of mobile code programs because it requires the programs to communicate with the origin in order to evaluate the encrypted functions.

4.4.4 Homomorphism Encryption Computing(HEC)

This is given by Sander and Tschudin. This method encrypts a polynomial functions coefficients [13][31].

Advantage: This method do not require complex communication with the mobile code program's origin to evaluate the encrypted function.

5. CONCLUSION

For mobile code computing and to realize its full potential as the software infrastructure of truly distributed computing, we must understand and develop security mechanisms that both detect and prevent malicious attacks against mobile code program[27]. All security mechanisms discussed are effective to some degree and the use of them should be retained. But most of the security measures are not adequate because they are not geared towards software i.e. mobile, works cooperatively, interacts with its own environment and reacts unpredictly to unexpected events like software flaws, human errors etc.

6. FUTURE CHALLENGES

Some profitable directions for further development of mobile agent system security are:

- Tracking Mobile Agent locations while mobile agent is running.
- Inter-Mobile Agent –system communication and collaborations.
- Harmful pattern monitoring and identification
- Mutual authentication between mobile agent and its host.
- Monitoring the flow of information and execution of a running mobile agent.
- Real-Time detection of attacks on mobile agents.

7. REFERENCES

[1] "Designing Autonomous Agents,pgs 49-70,The MIT Press:Cambridge,MA,!990.P.Maes:Situated agents can have goals.

[2] A.S.Rao and M.P.Georgeff. a model-theoretic approach to the verification of situated reasoning systems. In proceedings of thirteeth International Conference on AI(IJCAI-93)pg 318-324,Chambery,France,1993.

[3] SHOHAM.Y.:'Agent-oriented programming',Artificial Intelligence 1993,60(1)pp,51-92.

[4] S.Franklin and A.Graesser. Is it a agent or just a program? In J.P.Muller,M.Wooldridge and N.R. Jennings,editors,Intelligent Agents III(LNAI Volume 1193).Springer-Verlag:Berlin,Germany,1997,pp.21-36.

[5] S.Kraus,J.Wilkenfield and G.Zlotkin. Multiagent negotiation under time constraints.Artificial Intelligence.vol.75(2)pp.297-345,1995.

[6] GENESERETH,M.R. and KETCHPEL,'software agents ',commun,ACM,1994,(7),pp 48-53.

[7] S.Russell and P.Norvig. Artificial Intelligence:A Modern Approach,Prentice-Hall,1995.

[8] Joris Claessens, Bart Preneel, Joos Vandewalle , "(How) Can Mobile Agents Do Secure Electronic Transactions On Untrusted Hosts? A Survey Of The Security Issues and The Current Solutions", pp. 38-41, ACM Transactions on Internet Technology, Vol. 3, No. 1, February 2003.

[9] J. Vitek,M. Serrano and D.Thanols. "Security and Communication in Mobile Object Systems,"Mobile Object Systems: Toward the programmable Internet, J. Vitek and C.Tschudin, Eds ., Springer-Verlag, 1997.

[10] Sergi Robles, Mobile Agent system and Trust, a combined View toward Secure Sea-Data applications. July 2002. Http://www.tdx.cesca.es/TESIS_UAB/ AVAILABLE/TDX-1128102-173916//srmldel.pdf

[11] U. G. Wilhelm," A Technical Approach to Privacy based on mobile Agents Protected by Tamper-resistant Hardware", PhD Theses nr. 1961. Dept. of D'Informa-tique, Ecole polytechnique Federale de Lausanne,1999.URL: http:// lsewww.epfl.ch/~wilhelm/Papers/thesis.pdf.

[12] . B. Yee. Using Secure Coprocessors . Ph.D thesis , Carnegie Mellon University. 1994.

[13] Zachary ,John.2003. Protecting Mobile Code in the Wild . Internet Computing, IEEE,7(2).

[14] Wu, Xiaoping ; Shen, Zhidong; and Zhang, Huanguo.2006. The Mobile Agent Security Enhanced by Trusted Computed Technology, Proceedings of Int. Conf. ,pp. 1-4.

[15] Schelderup, K.olnes, J: Mobile agent security-Issues and Directions. In: Proceedings of the 6th Int. Conf. on intelligence and services in networks Barcelona, Spam, Apr 1999.

[16] Thmed S. Mohamed & D. Fakhry, Security in Mobile Agent Systems. In proceedings of the 2002 Symposium on Applications and the Internet, pgs 4-5, Washington, DC, USA,2002, IEEE Computer Society.

[17] Butscgje, L.; Paprzycki, M.; and Ren, M.2004. Mobile agent security-an overview, In E. Niedzielska et al (eds), Modern information Technologies in Management Wroclaw Univ. of Economics Press,pp.600-608.

[18] T. Sander and C. F. Tschudin, "*Protecting Mobile Agents Against Malicious Hosts*". G. Vigna, editor, Mobile Agents and Security, volume 1419 of LNCS, pp. 44–60. Springer-Verlag, June 1998.

[19] Ma ,L., and Tsai, J. J.P., "Attacks and countermeasures in software system security,"Handbook of Software Engineering and Knowledge Engineering, ".

[20] X. D. guan, Y.L. Yang and J. Y. You, "POM- A Security Model against Malicious hosts", DCTC Tech Report, Shanghai jiaotong Univ. Dec 1999

[21] J. Guttman and V. Swarup . Authentication for Mobile agent . In LNCS, pgs 114-136. Springer 1998.

[22] William M.Farmer, Joshua D. Guttman, and Vipin Swarup, "*Security for Mobile Agents: Authentication and State Appraisal*", pp. 5-11, pp. 118-130, 1996 European Symposium on Research in Computer Security (ESORICS).

[23] Ahmed S. Mohamed & D. Fakhry, Security in Mobile Agent Systems. In proceedings of the 2002 Symposium on Applications and the Internet, pgs 4-5, Washington, DC, USA,2002, IEEE Computer Society.

[24] C. Meadows. Detecting attacks on mobile agents. In proceedings of 1997 foundations for secure mobile code workshop, pgs 64-65, Monterey, CA, March 1997, position paper.

[25] Dan S. Wallach. A new approach to mobile code security. Ph.D thesis, dept. of CS, Univ. of Princeton, Jan 1999.

[26] N.Karnik, Security in Mobile Agent Systems. Ph.D thesis, dept. of CS&E Univ. of Minnesota.

[27] Bennet S. Yee. A Sanctuary for Mobile Agents. In J. Vitek and C. Jensen, editors, Secure Internet Programming volume 1683 of LNCS, pgs 261-273, Springer- Verlag, Berlin Heidelberg New York, 1999.

[28] Colin G. Harrison, David M. Chess, and Aaron Kershenbaum, "*Mobile Agents: Are they a good idea*?", technical report, 1995, IBM Research Division.

[29] Mousa Alfalayleh and Lijiljana Brankovic, "*An Overview of Security Issues and Techniques in Mobile Agents*", The School of Electrical Engineering and Computer Science, The University of Newcastle, Newcastle, NSW 2308, Australia.

[30] W. Jansen and T. Karygiannis, "*Mobile Agent Security* ", Nist Special Publication 800-19 -, 2000. National Institute of Standards Technology

[31] J.Algesheimer et al.,"Cryptographic Security for Mobile Code,"Proc.2001 IEEE Symp. Security and Privacy, IEEE Press,2001

[32] P.Stone and M.Veoso.Multiagent systems:A survey from the machine learning perspective.IEEE transactins on knowledge and data engineering ,Forthcoming,1998.

[33] M.P.Georgeff .Communication and Interaction in Multi-Agent planning. In Proceedings of the Third

National conference on Artificial Intelligence(AAAI-83),Washington,D.C.,1983,pp 125-129.

[34] D.R.Kuokka and L.P.harada.Issues and extensions for information matchmaking protocols. International Journal of Cooperative Information Systems,vol5(2-3)pp. 251-274,1996.

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

[36] U. G. Wilhelm," A Technical Approach to Privacy based on mobile Agents Protected by Tamper-resistant Hardware", PhD Theses nr. 1961. Dept. of D'Informa-tique, Ecole polytechnique Federale de Lausanne,1999.URL

[37] T.R.Gruber. A translation approach to portable ontologies. Knowledge acquisition,vol.5(2) pp.199-220,1993.

[38] The Foundation for Intelligent Physical Agents.See http://drogo.cselt.it/fipa/.

[39] M.WOOLDRIDGE(1997)"Agent-Based software engineering"IEEE PROC. On Software Engineering,144(1)26-37.

[40] Ma ,L., and Tsai, J. J.P., "Attacks and countermeasures in software system security,"Handbook of Software Engineering and Knowledge Engineering

[41] A. Lingnau, O. Drobnik et al. An Infrastructure for Mobile Agents: Requirements and Architecture. 1995.

[42] K.P.Sycara.Resolving goal conflicts via negotiation. In Proceedings of Seventh National Conference on Artificial Intelligence(AAAI-88)St.Paul,MN,1988.

[43] Butscgje, L.; Paprzycki, M.; and Ren, M.2004. Mobile agent security-an overview, In E. Niedzielska et al (eds), Modern information Technologies in Management Wroclaw Univ. of Economics Press,pp.600-608.

[44] Borselius, N: Mobile agent security. Electron. Communication Engineering. IEEE London 14(5),211-218(2002)

[45] R.S. Gray. A flexible and secure mobile agent system. 4th Annual Tcl/Tk Workshop Proc,1996.

[46] G. Vigna. Crypograhic traces for mobile agents. In Giovanni Vigna, editor, mobile agents systems, vol.1419 of mobile agents and security, pgs 137-153, Springer-Verlag Berlin Heidelberg New York, 1998.

[47] WOOLDRIDGE.M. and JENNINGS. N.R.:'Intelligent agents: theory and practise'. Knowl.Eng.Rev., 1995, 10, 20,pp.115-152.

AUTHOR'S PROFILE

Priyanka Dadhich, was born in Jaipur, (India), in 1980.She received B.E. (Computer Engineering) Degree from the University of Rajsthan, in 2003 and M.Tech. (Computer Science) Degree from the JRN University, Udaipur, (India) in 2006.

She is at present working as Asstt. Professor in Deptt. of Computer Engineering in AIET, Jaipur. She has six years teaching experience.

Dr. Kamlesh Dutta, is working as Associate Professor in the Department of Computer Science & Engineering in National Institute of Technology,Hamirpur(India).

Prof (Dr.) M.C.Govil is working as Principal,Govt. Women Engineering College,Ajmer(India).