Abstract

Mobile agents are software which moves autonomously through a computer network with aim to perform some computation or gather information on behalf of its creator or an application. In the last several years, mobile agents have proved their numerous applications including e-commerce, telecommunication systems, information management, on-line auctions or service brokering. In most applications, the security of mobile agents is a burning issue. Indeed, the agent is vulnerable while it is executing on the host's execution platform. Its owner therefore requires some guarantees concerning the protection of the agent against malicious host threats. Thus, the mobile agent has to protect itself from any act aiming at the deterioration, the destruction or the handling of its code, its state or its data. So, mobile agents must be prepared to execute on different hosts with various environmental security conditions. There are plenty of techniques to protect mobile code. This paper presents a survey of existing techniques for achieving a self-protected mobile agent.

References

- I. Schaefer. Secure Mobile Multiagent Systems In Virtual Marketplaces: A Case Study

- Filiol E.: Strong Cryptography Armoured Computer Viruses Forbidding Code Analysis:
the Bradley virus. Proceedings of the 14th EICAR Conference, 2005
- Grandison T., Sloman M: A Survey of Trust in Internet Applications. IEEE
Communications Surveys and Tutorials, Fourth Quarter (2000)
- Castelfranchi C. , Falcone R. : Trust is much more than Subjective Probability: Mental Components and Sources of Trust. The 32nd Hawaii International Conference on System Sciences - Mini-Track on Software Agents, Maui, Hawaii (2000)

Index Terms

Computer Science Security

Keywords

Malicious Host Mobile agent protection Security Trust