Nom et Prénom : BERGUIG YOUSRA
Date de soutenance : 17/12/2020
Directeur de Thèse : J.LAASSIRI

Sujet de Thèse :

Analyse de la sécurité des Agents Mobiles dans les systèmes distribués : Proposition et validation des algorithmes et protocoles cryptographiques

Résumé :

Agent Mobile est une technologie émergente qui facilite considérablement la conception, l'implémentation et la maintenance de systèmes distribués. Nous constatons que l'agent mobile réduit le trafic réseau, fournit un moyen efficace de surmonter la latence du réseau, il aide à donner plus de robustesse et tolérance aux pannes et permet de recueillir des informations et accomplir des tâches de manière optimale. Les serveurs d'agents qui fournissent un environnement d'exécution pour les agents à exécuter peuvent être attaques par des agents malveillants. De même, les agents pourraient transmettre des informations sensibles à leurs propriétaires et devraient être protégés contre toute manipulation par des hôtes malveillants. De plus, les données collectées par l'agent d'un hôte doivent être protégées contre toute manipulation par un autre hôte dans l'itinéraire. Objectif principale de cette thèse est de garantir la sécurité des systèmes distribués d'agents mobiles , en préservant les performances et en garantissant une meilleure qualité de service. A cet effet, nous proposons, dans un premier temps notre approche basé sur la sérialisation binaire et la cryptographie hybride, afin d'assurer une mobilité persistante de l'agent ainsi qu'une communication sécurisée avec les plates-formes d'accueil. Notre deuxième approche a pour but d'assurer une authentification mutuelle et protéger l'agent et le système contre différentes attaques, on se basant sur la cryptographie à courbes elliptique. Par ailleurs, pour renforcer le niveau de sécurité du système d'agent mobile tout en conservant son efficacité, nous présentons une troisième approche, qui développe un nouvel algorithme basé sur la cryptographie légère. A ce niveau, nous avons trouvé fructueux de mettre en évidence l'utilité de l'agent mobile dans préservation de sécurité des autres technologies, telles que le réseau véhiculaire. Nous proposons dans une quatrième approche un système de détection d'intrusion intelligent. Qui permet de détecter les attaques DoS, en faisant appel à l'apprentissage automatique et les agents mobiles sécurisé et intélligents.

Abstract :

Mobile agents is an emerging technology with several advantages, it allows an easy design, implementation and maintenance of distributed systems. Also, they reduce network trac and provide an ecient way to overcome network latency. Furthermore they are robust and able to operate asynchronously and autonomously. Despite the di
erent benets of this computing paradigm. It raises many new security issues, which are very dierent from those of traditional client/server systems. Mobile agent servers can be attacked by malicious agents or malicious hosts. Likewise, mobile agents can be manipulated by malicious hosts or agents. In addition, the data collected by mobile agents must be protected against any manipulation they may face during their road trip. The main objective of this thesis is to guarantee the security of mobile agents distributed systems, while preserving the performances and assuring a better quality of service. For this purpose, we propose a rst approach based on binary serialization and hybrid cryptography, in order to ensure persistent agent mobility as well as a secure communication with reception platforms. Our second approach is based on elliptical curve cryptography and aims to ensure mutual authentication and protect the agent and the system

against dierent attacks. In addition, to strengthen the security level of the mobile agent system while maintaining its eciency, we present a third approach, which develops a new algorithm based on lightweight cryptography.
At this level, we have found it fruitful to highlight the usefulness of the mobile agent in preserving the security of other technologies, such as vehicular networks. We propose in a fourth approach an intelligent intrusion detection system, that helps to detect DoS attacks, using machine learning and secure and intelligent mobile agents.
Keywords: Mobile Agent, Security, Hybrid Cryptography, Elliptical Curve Cryptography (ECC), Lightweight Cryptography, Binary Serialization, Mutual Authentication, Anonymity, Multi Agent, DoS Attack.