Sécurité cryptographique appliquée aux agents mobiles

IDRISSI HIND : hind.idr@gmail.com
Grade doctorante en 1ére année - Sujet : Sécurité des agents mobiles
Laboratoire MIA (Rabat - Maroc) : Pr E.M.SOUIDI (emsouidi@yahoo.com)
Laboratoire L3I (La Rochelle - France) : Pr A.REVEL (arnaud.revel@univ-lr.fr)

Un système multi-agents (SMA) selon Ferber [J.F,95] [1] est un système dans lequel ont fait coopérer un ensemble d'entités autonomes qu'on nomme des "agents" dotées d'un comportement intelligent, et qui ont la puissance de coordonner leurs buts et leurs plans d'actions pour résoudre un problème ou atteindre un objectif. Ils sont largement appliqués dans les télécommunications et le e-commerce dans lequel on a introduit des agents collecteurs d'informations et assistants aux consomateurs qui réduisent le temps de recherche, ainsi que des agents négociateurs de produits entre utilisateurs, le meilleur exemple sont les sites pour les ventes aux enchères.

Du point de vue informatique, les programmes sont considérés comme des entités individualisées capables de simuler le comportement humain, et les systèmes multi-agents sont une nouvelle discipline visant à approcher les capacités cognitives de l'être humain.

Les agents mobiles sont alors une catégorie particulière d'agents logiciels dont la caractéristique prédominante est leur capacité de se transporter entre les noeuds d'un ou plusieurs réseaux. Or, cette mobilité d'agents pose évidemment des problèmes de sécurité. En effet, lorsqu'un agent se déplace, il est crucial de s'assurer que l'agent sera exécuté correctement et en toute sécurité sur le nouveau système visité. De même, il est crucial de rassurer le système d'accueil qu'il n'y aura aucun risque d'héberger un nouvel agent qui pourrait être malveillant.
On en déduit alors qu'il y a un point de confiance manquant, puisque l'hôte visité et sur lequel l'agent s'exécute a la possibilité de manipuler l'agent ou même de le détruire, aussi l'hôte donne un accès total à l'agent qui pourrait l'exploiter et par suite mener tout type d'attaques sur lui .

Après une étude menée sur les interactions entre agent et hôte, et les contraintes qu'elles posent, on a pensé à une approche de sécurité regroupant une diversité de mécanismes se basant sur la cryptographie et gérant les sensibilités de l'authentification , la confidentialité, l'intégrité et la disponibilité.

Notre plate-forme de test est JADE (Java Agent DEvelopment Framework) [2] , une plate-forme qui respecte la norme FIPA spécifiée pour les agents, et qui utilise le langage Java étant le plus répandu et qui offre plus de services pour l'interopérabilité facilitant la mobilité des agents.

Notre solution consiste, en premier lieu, à créer un secret commun entre les plate-formes interagissantes pour gérer l'authentification, et ce par l'algorithme de Diffie Hellman qu'on a associé au DSA (Digital Signature Algoritm) pour vérifier l'identité et aussi assurer l'intégrité des échanges.
Pour la confidentialité, il n'y a certainement pas mieux que le chiffrement afin de protéger les données et le code de l'agent, on a choisit alors des systèmes dotés de rapidité en calcul qui sont les systèmes de chiffrement à clé secréte, notamment la clé qu'on a obtenue en phase d'authentification.
Pour remédier au problèmes à la fois de mobilité et disponibilité , on a pensé de travailler en mode non-connecté et on a introduit la sérialisation XML pour construire un format persistant transportable d'agent, tout en faisant aussi recours au principe de URLClassLoader pour charger des classes de l'agent dans les cas où le site d'accueil ne les reconnaissait pas.

1. J.FERBER. Les systèmes multi-agents : vers une intelligence collective, InterEdition
2. Site officiel de JADE : http ://jade.tilab.com/