

Nom et Prénom : HANAOUI SANAE

Date de soutenance : 01/07/2022

Directeur de Thèse : LAASSIRI JALAL

Sujet de Thèse :

**TOWARDS A SECURE MULTI AGENT SYSTEM USING TRENDING CRYPTOSYSTEM SOLUTIONS
UNDER AVISPA AUTOMATED TOOL VALIDATION**

Abstract:

Nowadays various types of interactions are based on digitization, Moreover, everything is connected to the network and everyone is using multiple interconnected applications by different and heterogeneous devices starting with social applications to Markets and bank applications, etc, and with the covid-19 crisis arising, many old businesses had to upgrade following their consumers moving toward public services, and supermarkets. As an outcome, the speedup of digital technologies adoption. Hence, the consistent need of the network users for efficiency and fast responses combined with artificial intelligence makes it hard for the client-server system where the applications to answer the new upgraded digital world aspiration. However, the existence of mobile agent technology with innovative potentials makes it easier to design implement, as well as maintain the distributed system. Owing to, its serval features. Despite the various benefits of this computing paradigm. It raises many new security issues, which are different from those of traditional client/server systems. Mobile agent servers can be attacked by malicious agents or malicious hosts.

This thesis main objective is the protection of mobile agent from sustainable threats by assuring both its security and the remote or local hosting platform. By taking into consideration the different threats that face both the agent and the platform executing the agent. Therefore, the primary idea of our work is to design a secure model that respects the security mechanism aspects which maintain the agent system security and meet security requirements without compromising their flexibility, autonomy, or their mobility features.

Keywords: Mobile Agent, Cyber Security, Hybrid Cryptography, Elliptical Curve Cryptography (ECC), Lightweight Cryptography, Identity Signature, Authentication, JADE, AVISPA, Multi Agent System, E-commerce Solution, Schnoor, batch verification.

Résumé:

A De nos jours, divers types d'interactions sont basés sur la numérisation, De plus, tout est connecté au réseau et tout le monde utilise de multiples applications interconnectées par des appareils différents et hétérogènes à commencer par les applications sociales aux marchés et les applications bancaires, etc., Et avec la crise du covid-19 qui survient, de nombreuses anciennes entreprises ont dû se moderniser suite à l'évolution de leurs consommateurs vers les services publics et les supermarchés. En conséquence, l'accélération de l'adoption des technologies numériques. Par conséquent, le besoin constant des utilisateurs du réseau d'efficacité et de réponses rapides combiné à l'intelligence artificielle rend difficile pour le système client-serveur où les applications répondent à la nouvelle aspiration du monde numérique amélioré. Cependant, l'existence de la technologie des agents mobiles avec des potentiels innovants facilite la conception, la mise en œuvre et la maintenance du système distribué. En raison de ses caractéristiques de service. Malgré les divers avantages de ce paradigme informatique. Elle soulève de nombreux nouveaux problèmes de sécurité, différents de ceux des systèmes client/serveur traditionnels. Les serveurs d'agents mobiles peuvent être attaqués par des agents malveillants ou des hôtes malveillants.

L'objectif principal de cette thèse est la protection de l'agent mobile contre les menaces durables en assurant à la fois sa sécurité et la plateforme d'hébergement distante ou locale. En prenant en considération les différentes menaces auxquelles sont confrontés à la fois l'agent et la plate-forme exécutant l'agent. Par conséquent, l'idée principale de notre travail est de concevoir un modèle sécurisé qui respecte les aspects du mécanisme de sécurité qui maintiennent la sécurité du système agent et répondent aux exigences de sécurité sans compromettre leur flexibilité, leur autonomie ou leurs fonctionnalités de mobilité.

Mots clés : Agent Mobile, Sécurité, Cryptographie Hybride, Cryptographie à Courbe Elliptique (ECC), Cryptographie Légère, Signature, Authentification, JADE, AVISPA, Système Multi Agent, Solution E-commerce, Schnoor, vérification batch