Proposition de recherche doctorale

Les Protocoles de Sécurité Serverless Légers Pour l'Internet des Objets

Mots clés :

- **Directeur de thèse** : Maryline Laurent
- **Co-encadrant(s)** :
- **Unité de recherche** : Services répartis, Architectures, MOdélisation, Validation, Administration des Réseaux
- **Ecole doctorale** : École Doctorale Informatique, Télécommunications, Électronique de Paris
- **Domaine scientifique principal**: Divers

Résumé du projet de recherche (Langue 1)

Les avancées technologiques permettent d'intégrer des capteurs et des modules de communication dans les objets du quotidien pour les rendre intelligents et faciliter leur intégration sur l'Internet. L'Internet du futur sera sans nul doute celui des objets connectés. Les objets connectés génèrent, collectent, stockent et partagent des informations entre eux et aussi avec les serveurs d'authentification centralisés. La plupart des informations collectées doivent être protégées pendant le stockage et le transfert. Par le passé, divers protocoles assurant une sécurité robuste basés sur la cryptographie asymétrique et d'autres sur la cryptographie symétrique ont été proposés dans la littérature. Du fait que les objets connectés possèdent de faibles capacités de calcul, de mémoire et d'énergie, et que l'accès au medium radio est très consommateur en ressources, les protocoles cryptographiques traditionnels ne sont pas adaptés aux objets connectés. Il y a lieu donc d'adapter ou de concevoir des protocoles propres et conformes à leurs exigences. Dans cette thèse, nous abordons les défis de sécurité et de vie privée pertinents aux systèmes pervasifs avec des contraintes de ressources strictes. Nous regardons les protocoles d'authentification serverless, qui sont des mécanismes d'authentification qui ne nécessitent pas la présence du serveur central au cours de la phase d'authentification entre deux objets connectés. Tout d'abord, nous fournissons les caractéristiques et les besoins pour les protocoles serverless. Grâce à ces besoins et caractéristiques, nous avons fait des recherches, des analyses complètes et des comparaisons des protocoles serverless existants en termes de sécurité, de vie privée et de performances. Nous examinons leurs capacités à résister à diverses attaques et leurs aptitudes à minimiser l'usage des ressources. Après quoi, notre objectif est de proposer des protocoles de sécurité serverless permettant aux objets de s'authentifier tout en garantissant efficacité, passage à l'échelle et efficacité énergétique, l'énergie étant une ressource très critique qui a une influence directe sur la durée de vie d'un objet connecté. Trois nouvelles contributions sont proposées dans cette thèse. Notre première contribution est un protocole léger serverless d'authentification mutuelle pour les objets connectés hétérogènes. La première contribution fournit trois avantages par rapport aux protocoles existants. Cette contribution répond aux exigences des systèmes pervasifs. La validation de notre proposition a été faite en utilisant l'outil AVISPA et la validation informelle en utilisant sécurité et de vie privée des jeux. Notre deuxième contribution comprend deux protocoles complémentaires dans le domaine des technologies RFID. Le premier protocole vise à l'authentification de masse entre un lecteur RFID et un groupe d'étiquettes tandis que le deuxième protocole effectue une recherche sécurisée pour une étiquette cible parmi un groupe d'étiquettes dans le voisinage du lecteur. Les deux protocoles proposés tiennent compte des contraintes de ressources des étiquettes RFID. Après une étude approfondie des protocoles serverless, nous avons proposé une troisième contribution, un guide pour la conception des protocoles serverless sécurisé et efficaces pour les systèmes pervasifs. Le guide contient six principes et six meilleures pratiques en vue d'élaborer des protocoles serverless. Le guide est destiné à aider à la conception de protocoles serverless efficaces, sécurisés et simples en évitant des erreurs couramment faites dans les protocoles existants. --- {{Mots clés}} : {Sécurité, Protocoles de recherche sécurisés, Vie privée, Contrôle d'accès, Protocoles légers serverless, Faible empreinte énergétique, Authentification mutuelle,Confiance}