Proposition de recherche doctorale

Sécurité robuste à faible empreinte énergétique dans un réseau de capteurs connectés à un système centralisé ou à des terminaux mobiles

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)

L'évolution technologique liée aux systèmes embarqués, à la sécurité des systèmes d'information, aux moyens de communications, à la miniaturisation des devices rend possible un meilleur suivi/traçage des objets, et donc une meilleure interaction entre leur représentation virtuelle et réelle. En particulier, cette évolution prend tout son sens dans le cadre d'une application logistique de transport de fret où des containers sont équipés d'un boitier appelé TRACKBOX qui permet de communiquer avec un serveur central PIC afin de l'informer de son état de progression et des éventuels problèmes de transport. Tous les échanges induits ont besoin d'être sécurisés, pour éviter des fuites d'informations, des possibilités de perturbation du système de suivi de marchandises… On s'intéressera tout particulièrement à la protection des échanges entre TRACKBOX et PIC. En outre, il est possible que la TRACKBOX soit directement interrogée par un terminal local (technologie sans fil – type NFC) pour qu'une personne puisse accéder à certaines informations de la TRACKBOX (listing de marchandises, alertes…). Le niveau d'informations fournies par la TRACKBOX doit dépendre de l'équipe en faisant la demande. Cette thèse de doctorat portera sur les différentes problématiques de sécurité mentionnées ci-dessous. Elle visera à adapter les outils cryptographiques élaborés à Télécom SudParis [EL12] pour élaborer un protocole de sécurité visant à répondre aux besoins de l'application ci-dessous : - Authentification mutuelle entre TRACKBOX et PIC ; - Etablissement d'une clé partagée entre TRACKBOX et PIC ; - Confidentialité et intégrité des échanges entre TRACKBOX et PIC ; - Authentification mutuelle entre TRACKBOX et terminal local ; - Confidentialité et intégrité des échanges entre TRACKBOX et terminal local ; - Contrôle d'accès dans la TRACKBOX. Les solutions élaborées prendront en compte : - Les problématiques d'administration et de maintenance de la sécurité pour déployer, initialiser et maintenir le niveau de sécurité de la solution ; - Les coûts induits par les opérations cryptographiques mais aussi les divers traitements (protocoles, transmission/réception…) en termes d'énergie, calculs, mémoire, bande-passante dans la TRACKBOX ; - Le passage à l'échelle (scalability) du côté PIC, l'idée étant qu'un PIC gère le plus grand nombre de TRACKBOX possible ; - La robustesse de la solution de sécurité vis-à-vis des attaques de sécurité sur le protocole et de la cryptanalyse. Une validation par prototypage mais aussi à l'aide d'outils formels (ex : [BL09], [AV]) sera effectuée. L'ensemble de ces travaux de recherche sera valorisé dans des conférences et journaux d'envergures nationale et internationale. Un travail de veille à la standardisation (ISO) et éventuellement de contribution sera effectué.

Résumé du projet de recherche (Langue 2)

concevoir une solution de sécurité qui allie passage à l'échelle, robustesse, minimum d'énergie consommée