Résumé

Les environnements connectés promettent de nous apporter de nouveaux services: meilleure gestion de l'énergie, optimisation des transports, ciblage de l'information diffusée, etc. La grande valeur ajoutée de ces architectures à base d'objets connectés (IoT) est la donnée dont la collecte et le traitement impliquent un très grand nombre de systèmes informatiques opérés par des acteurs différents. Chaque acteur pouvant avoir ses propres objectifs, contraintes et enjeux, un des défis en terme de sécurité est de garder la maîtrise des informations échangées afin d'assurer ce que l'on appelle l'autodétermination informationnelle. Cette notion signifie par exemple que chaque acteur peut contrôler qui utilise ses données, où et pour quelle finalité.

Cette thèse décrit notre approche pour la gestion du partage des données dans les environnements connectés. L'exploitation des données générées par les ressources de l'internet des objets soulève des risques de sécurité en raison du manque de transparence entre les différents acteurs de l'environnement. Ainsi, nous proposons tout d'abord une ontologie de gestion du partage des données IoT qui prend en considération les contextes, appelée IdSM-O, afin d'établir un vocabulaire de sécurité partagé et de gérer l'interopérabilité des environnements IoT. Ensuite, nous introduisons un gestionnaire de règles sémantiques automatique à trois niveaux, qui recueille les exigences des politiques de sécurité des fournisseurs de données et les traduit automatiquement en règles sémantiques prêtes pour le processus du raisonnement. Ces contributions constituent la base d'IdSM, un framework de sécurité de bout en bout pour la gestion du partage des données, qui répondent aux exigences de sécurité de l'information et au respect des obligations entre les différentes parties. Enfin, nous développons un prototype de la proposition afin de prouver sa faisabilité et d'analyser ses performances.

Mots clés : Sécurité, Internet des objets (IoT), web sémantique, politique de contrôle d'usage, provenance des données