Ecole Doctorale STIC
Sciences & Technologies de l'Information et de la Communication

ED STIC - Proposition de Sujets de Thèse

pour la campagne d'Allocation de thèses 2011

Titre du sujet :	Gestion de la sécurité orientée utilisateurs dans les environnements ambiants
Mention de thèse :	Informatique
HDR Directeur de thèse inscrit à l'ED STIC :	Riveill Michel

Co-encadrant de thèse éventuel :

Nom :	Boudaoud
Prénom :	Karima
Email :	karima.boudaoud@unice.fr
Téléphone :	04 92 96 51 72

Email de contact pour ce sujet :	karima@polytech.unice.fr
Laboratoire d'accueil :	I3S

Description du sujet :

Mots-clés : environnements ambiants, programmation par composition, services mobiles, sécurité

Contexte et motivation

Le cadre de cette thèse est celui de la maison intelligente mais les résultats ont vocation à pouvoir être réutilisés dans les différents domaines d'application de l'informatique ambiante qui repose sur deux concepts clés :

•l'informatique ambiante (ou ubiquitaire) permet aux utilisateurs d'interagir de n'importe où et n'importe quand avec un environnement constitué d'objets communicants : objets du quotidien (lampe, réfrigérateur, etc.), capteurs (contrôle d'accès, température, etc.) et actionneurs (gâche électrique, interrupteur, etc.). L'interaction entre les utilisateurs et ce type d'objets ou entre les objets eux-mêmes est possible via des réseaux de différentes natures généralement sans fils.

•les interfaces utilisateurs multi-modales permettent à un utilisateur de contrôler et d'interagir

avec l'environnement ambiant de manière la plus naturelle possible grâce à la reconnaissance vocale et/ou gestuelle ou alors de manière personnalisée en fonction de préférences utilisateur et/ou du contexte d'usage.
L'environnement ambiant de la maison intelligente est composé d'appareils intelligents, de capteurs, d'infrastructures de communication hétérogènes dont l'objectif est d'améliorer la vie quotidienne des personnes vivant dans la maison. Un des domaines cible actuellement privilégié est l'aide à la personne en perte d'autonomie. La gestion de cet environnement est possible grâce à des applications logicielles qui interagissent aussi bien avec l'utilisateur qu'avec les différents objets intelligents déployés dans la maison. L'une des caractéristiques clés de ces applications est qu'elles doivent pouvoir s'adapter dynamiquement aux situations et contextes d'usage dépendant du comportement des personnes, objets, etc. pour selon les cas palier à des déficiences ou lever des alarmes lorsque la sécurité de la personne est en jeu.
D'un point de vue sécurité informatique, la maison intelligente peut être sujet à différents types d'attaques dues notamment à la vulnérabilité des différents réseaux et appareils constituant son environnement et à sa connexion à l'Internet. Ces attaques peuvent être 1) soit externes comme le vol et modification d'informations personnelles (ex: carte de crédit, liste des courses, etc.) ou 2) internes, dans le cas d'appareils utilisés pour attaquer d'autres objets intelligents ou systèmes (par exemple les serveurs distants qui gèrent le réseau de la maison intelligente). Par conséquent, la gestion de la sécurité de la maison intelligente est primordiale. Cependant, ce n'est pas une tâche facile à cause de l'hétérogénéité de l'environnement ambiant et de ses besoins en sécurité qui concernent non seulement chacun des objets intelligents et chacune des applications logicielles mais également l'ensemble des données qu'ils gèrent et s'échangent. Ces besoins en sécurité varient continuellement en fonction des situations, de la nature des informations gérées et échangées mais également des préférences de l'utilisateur qui pourrait souhaiter configurer lui-même la sécurité des applications déployées dans son environnement, modifier les contrôles d'accès ou contrôler ses données. Par conséquent, la sécurité mise en place pour sécuriser la maison intelligente doit pouvoir s'adapter dynamiquement au contexte d'usage ; autrement dit, il doit être possible de choisir « à la volée » les propriétés de sécurité (vie privée, intégrité, confidentialité, etc.) et donc les mécanismes de sécurité appropriés (de manière plus ou moins automatique ou avec l'aide de l'utilisateur). De plus, les propriétés de sécurité doivent être assurées de bout en bout et être conservées lorsqu'une application est adaptée.
Pour finir l'utilisateur final doit pouvoir avoir un retour sur la sécurité appliquée.

Objectif de la thèse
L'objectif de cette thèse est de définir un « Framework » de sécurité contrôlé par l'utilisateur de la maison intelligente afin qu'il puisse gérer non seulement la sécurité de ses données mais également des objets et services déployés dans son environnement. Plus précisément, ce Framework devra permettre de résoudre les problèmes suivants :
- permettre aux différents types d'utilisateurs (novices, novices mais intéressés par la sécurité et experts en sécurité) de contrôler la sécurité de leurs données et de gérer leur vie privée.
- Prouver à l'utilisateur que la sécurité déployée est celle qu'il a spécifié et qu'elle répond à sa demande et ses besoins (i.e. convaincre l'utilisateur qu'il n'y a pas de faille)
- garantir l'adaptation dynamique de la sécurité des applications ambiantes en fonction du

contexte et du niveau d'expertise en sécurité des utilisateurs.
- prouver qu'une propriété de sécurité est conservée même lorsqu'une application est adaptée.
- garantir une sécurité de bout en bout.

Méthodologie
Pour pouvoir mener à bien cette thèse, le travail sera décomposé en 5 phases : étude bibliographique, conception, prototypage, validation à grandeur réelle et étude de performances.
Dans la phase d'étude bibliographique, il s'agira de faire un état de l'art de l'existant, notamment :
• Identifier les problèmes et besoins en sécurité des environnements ambiants en se focalisant sur la maison intelligente.
• Étudier et analyser les modèles de sécurité existants pour la sécurité des données et réseaux dans le domaine des réseaux de capteurs, réseaux wi-fi, services Webs, services pour dispositifs ainsi que les solutions proposées pour les environnements ambiants.
Dans la phase de conception, il s'agira de définir le « framework » de sécurité adéquat en identifiant les mécanismes de sécurité qui permettraient de répondre aux besoins définis dans la phase d'analyse. En particulier, il s'agira de proposer un modèle de sécurité pour la nouvelle génération de services utilisés et/ou conçus pour les environnements ambiants et en particulier pour la maison intelligente .
Dans la phase de prototypage, le modèle proposé sera validé par la réalisation d'un prototype qui sera testé et déployé au sein de l'Ubiquarium Informatique de Polytech'Nice Sophia. Une réalisation d'expérimentations à grandeur réelle devra également être effectuée. Enfin des études de performances devront être menées pour évaluer la robustesse et l'efficacité du modèle proposé.

English version: