CATALOGUE DE PATRONS DE SÉCURITÉ, DE FIABILITÉ ET DE SÛRETÉ DANS LE CONTEXTE DES HABITATS INTELLIGENTS POUR PERSONNES AYANT DES TROUBLES COGNITIFS

par

Pierre Busnel

Thèse présentée au Département d'informatique
en vue de l'obtention du grade de philosophiæ doctor (Ph.D.)

FACULTÉ DES SCIENCES

UNIVERSITÉ DE SHERBROOKE

Sherbrooke, Québec, Canada, 4 avril 2014

Le 4 avril 2014

le jury a accepté la thèse de Monsieur Pierre Busnel
dans sa version finale.

Membres du jury

Professeur Sylvain Giroux
Directeur de recherche
Département d'Informatique
Université de Sherbrooke

Jean-Christophe Pazzaglia
Évaluateur externe
SAP Labs France

Professeur Gabriel Girard
Directeur de département
Département d'Informatique
Université de Sherbrooke

Luc Lavoie
Président rapporteur
Département d'Informatique
Université de Sherbrooke

Sommaire

D'après les derniers rapports de recensement, les pays occidentaux font face à une augmentation de la population vieillissante. Le vieillissement normal de la population entraîne une augmentation de maladies ou d'accidents. Ceci conduit à la perte d'autonomie et réduit la qualité de vie des personnes âgées notamment les personnes atteintes de la maladie d'Alzheimer. Cette dernière provoque principalement des pertes cognitives. Pour pallier à ce problème, un habitat rendu intelligent grâce à l'informatique diffuse permet d'interagir avec son occupant. Un tel habitat intelligent améliorera ou lui redonnera son autonomie et l'aidera à réaliser ses activités, voire interviendra pour éviter des situations à risque.

Le développement d'habitat intelligent amène de nouveaux défis en matière de sécurité, de fiabilité et de sûreté du patient. Il nécessite que les questions de sécurité, de fiabilité et de sûreté soient prises en compte dès le départ par les développeurs d'applications du domaine des habitats intelligents. Malheureusement, ces développeurs ne sont pas experts en sécurité, en fiabilité ou et en sûreté. Ces aspects sont souvent remis à plus tard, ce qui aboutit généralement à des applications fonctionnelles, mais peu sécuritaires. Les déficits cognitifs imposent aussi des contraintes supplémentaires ou nouvelles en ce qui a trait à la sécurité, la fiabilité et la sûreté.

Dans ce contexte, cette thèse propose de répondre aux problèmes de sécurité, de fiabilité et de sûreté des patients souffrant de troubles cognitifs lors de leur séjour dans un habitat intelligent. Pour cela, un catalogue de patrons de sécurité, de fiabilité et de sûreté est créé pour fournir un outil aux développeurs d'application de ce domaine. Dans un premier temps, une liste de besoins de sécurité, de fiabilité et de sûreté est identifiée à partir de scénarios illustrant la vie du patient et ses interactions avec les intervenants du service de santé, sa famille et son nouvel environnement. Ensuite

les solutions identifiées sont encapsulées sous forme de patrons et regroupées dans un catalogue mis à la disposition des développeurs. Les patrons de ce catalogue sont alors utilisés pour répondre aux besoins initialement formulés soient isolément, soient en combinaison avec d'autres patrons. La discussion finale permettra d'éclairer les avantages et limites de cette approche, et présentera des pistes à suivre pour étendre le catalogue de patrons.

Mots-clés: Catalogue ; Patrons ; Sécurité ; Sûreté ; Fiabilité ; Habitat Intelligent ; Troubles Cognitifs.

Remerciements

Je tiens à remercier Sylvain Giroux, Professeur à l'Université de Sherbrooke, qui m'a encadré tout au long de cette thèse. Un grand merci pour son soutien, ses recommandations et son aide précieuse.

Je remercie chaleureusement Hélène Pigot, Professeure à l'Université de Sherbrooke et Monsieur Sylvain Giroux à nouveau, pour m'avoir initié aux technologies au service de l'être humain et m'avoir fait découvrir un monde ou l'informatique joue un rôle humanisant.

Je souhaite également remercier Jean-Christophe Pazzaglia, Directeur de recherche à SAP Research ainsi que Luca Compagna, Keqin Li, Paul El Khoury et Azzedine Benameur dont je garde le souvenir d'une expérience très enrichissante lors de notre collaboration dans le cadre du projet européen SERENITY.

J'ai eu plaisir à travailler au sein d'une équipe dont la bonne ambiance a largement contribué à mon bien-être durant plusieurs années. J'adresse un très grand merci aux professionnels de recherche du laboratoire DOMUS de l'Université de Sherbrooke, aux étudiants et anciens étudiants avec que j'ai eu la chance de côtoyer durant cette belle aventure.

Plus particulièrement, je tiens à remercier Jean-Paul Viboud, Francis Bouchard et Nicolas Marcotte pour leurs conseils techniques précieux, Jérémy Bauchet pour avoir conçu Dominius, un "jouet" très appréciable lors des démonstrations.

Mes derniers remerciements vont à ma mère pour son soutien indéfectible et à Bruno Dufour pour m'avoir aidé à remettre la machine en marche.

Abréviations

AVQ Activité de la Vie Quotidienne

AVC Accident Vasculaire Cérébral

BPEL Business Process Execution Language

CSIU Centre de Supervision et d'Intervention d'Urgence

DME Dossier Médical Électronique

HI Habitat Intelligent

HIPAA Health Insurance Portability and Accountability Act

PIPEDA Personal Information Protection and Electronic Documents Act

RFID Radio-Frequency Identification

SOAP Simple Object Access Protocol

XACML eXtensible Access Control Markup Language

ICP Infrastructure à Clé Publique

IHM Interface Home-Machine

TC Troubles Cognitifs

PDP Policy Decision Point

PEP Policy Enforcement Point

PDA Personal Digital Assistant

Table des matières

Liste des figures

Liste des tableaux

Liste des programmes

Introduction

Les pays occidentaux font face à une augmentation de la population vieillissante, conjuguée à une baisse du taux de natalité. D'après une estimation du bureau de recensement américain, le nombre de personnes âgées de 65 ans et plus, était de 36 millions en 2003 et devrait atteindre 72 millions en 2030 et 86.7 millions en 2050 [42]. On retrouve des chiffres proportionnellement similaires dans l'ensemble des pays occidentaux. L'augmentation de la population âgée de 65 ans et plus entraîne une augmentation des maladies ou des accidents dus au vieillissement. Le vieillissement, qu'il soit normal ou marqué par des maladies ou des accidents, conduit à la perte d'autonomie et réduit la qualité de vie des personnes âgées.

La maladie d'Alzheimer est l'une des maladies les plus connues liées à l'âge. Selon [42], on estimait à 4,5 millions le nombre d'Américains atteints de la maladie d'Alzheimer en 2000. Ce nombre atteindrait 13,2 millions en 2050 [43].

La maladie d'Alzheimer est une maladie dégénérative qui provoque principalement des pertes cognitives [80]. Des déficits de mémoire, de planification et de jugement entraînent une perte d'autonomie. Dans les premiers temps de la maladie, les malades ressentent des difficultés lors de la réalisation de tâches inhabituelles ou complexes, mais restent toutefois capables de vivre dans un environnement familier et d'effectuer des tâches simples. Les risques d'isolement, de malnutrition, de brûlures, de dégâts des eaux et d'incendies augmentent au fur et à mesure de l'évolution de la maladie. Dans les derniers moments de la maladie, les malades nécessitent une assistance continue, qui entraîne fréquemment un transfert en milieu hospitalier.

Malgré ces handicaps, 92% des personnes âgées souhaitent rester chez elles et 40% préfèrent passer les derniers moments de leur vie dans leur maison [42]. Les personnes âgées dépendent de leur famille et d'aides-soignants pour les aider dans

leur vie quotidienne, ce qui devient rapidement très difficile pour les aidants naturels [80]. Afin d'alléger le fardeau des proches, un environnement intelligent pourrait compenser les pertes cognitives des personnes âgées en leur fournissant des indices environnementaux et des indications pour réaliser plus facilement leurs activités de la vie quotidienne (AVQ).

Un habitat intelligent interagit avec l'occupant pour améliorer ou lui redonner son autonomie grâce à l'informatique diffuse [46]. Un habitat intelligent est généralement équipé de différents types de capteurs connectés à un serveur qui emmagasine et analyse les données collectées grâce à des techniques d'intelligence artificielle. Un habitat intelligent peut ensuite intervenir pour réduire les situations à risque et pour aider l'occupant à terminer ses activités [81].

Bien que la téléassistance puisse être utilisée pour apporter au besoin une assistance humaine à distance, l'habitat intelligent délivre une assistance automatisée au moyen de son réseau de capteurs et d'effecteurs et d'intelligence artificielle.

L'assistance peut se diviser en deux parties : l'assistance physique et l'assistance cognitive. Dans la première, l'environnement vise à compenser le handicap physique en proposant des outils appropriés tels que des télécommandes, la reconnaissance vocale, un fauteuil roulant, etc. Dans le cas de l'assistance cognitive, l'environnement vise à compenser les pertes cognitives de l'individu en lui donnant des indices sur les AVQ à réaliser et en interagissant avec lui en fonction des besoins de la situation.

Au laboratoire Domus de l'Université de Sherbrooke, l'assistance cognitive s'oriente vers l'aide aux personnes souffrant de troubles cognitifs pour y développer des outils d'assistance cognitive [78].

Le laboratoire Domus comprend un appartement fonctionnel, équipé de différents capteurs : des capteurs électromagnétiques afin de détecter l'ouverture des portes, des détecteurs de mouvement, des tapis tactiles pour localiser l'occupant, etc. L'activité réalisée par l'occupant au sein de l'appartement est reconnue grâce à l'analyse des données issues des capteurs.

Par exemple, l'utilisation de capteurs permet de mieux connaître le contexte et d'offrir de l'assistance pour la réalisation d'AVQ auprès des personnes ayant des troubles cognitifs, tels que dans le projet Archipel [40], [14], [15]. Ce type d'assistance améliore leur autonomie dans l'environnement. Les habitats intelligents peuvent éga-

lement améliorer l'autonomie des personnes ayant des handicaps physiques en leur permettant de mieux interagir avec les objets de la vie courante [66].

La création de ces outils soulève des problèmes en matière d'informatique diffuse et sensible au contexte, d'intelligence ambiante, de réseautique et de conception d'interface homme-machine (IHM) [46].

Dans un registre autre que l'assistance aux activités de la vie quotidienne (AVQ), les personnes âgées sont aussi fréquemment les victimes de fraudes à leur domicile [2]. Les personnes souffrant de troubles cognitifs sont d'autant plus à risque. Un habitat intelligent pourrait aider les personnes souffrant de troubles cognitifs à prévenir et à éviter ce type de fraude en proposant de l'assistance lors de l'arrivée d'un visiteur ou lors de l'utilisation d'un moyen de paiement.

De même, l'utilisation d'un réseau de capteurs permet de connaître les habitudes de vie du résident. Une personne mal intentionnée peut utiliser ces données et détecter ses absences. Il devient alors essentiel de garantir le respect de la vie privée du patient en protégeant l'accès et la diffusion des informations le concernant.

L'utilisation d'habitats intelligents comme orthèse cognitive pour les personnes souffrant de trouble cognitif amène donc à prendre en compte la sûreté de ses occupants, la sécurité informatique des données qui y transitent et la fiabilité des services, que ce soit une utilisation d'ordre purement médical ou liée aux activités de vie quotidienne des patients.

D'une part les risques concernant la sûreté du patient sont à la fois inhérents à l'âge du patient, à une situation d'isolement et de plus grande vulnérabilité et que l'on retrouve dans le contexte d'un vieillissement normal de la population (protection des menaces extérieures, fraudes, accidents domestiques ...). La diminution ou la perte des ressources cognitives aggravent ces risques et doivent être prises en considération pour utiliser des solutions adaptées aux troubles du patient.

D'autre part, l'infrastructure particulière d'un habitat intelligent nécessite une attention particulière ; le réseau de capteurs qu'il comporte est capable de détecter une multitude d'actions réalisées en son sein et de les transcrire en données informatiques. La génération et le transit de ces données nécessitent un regard particulier sur la manière d'y accéder, de les transférer et de les stocker.

Certaines solutions répondant à ces problèmes de sûreté et de sécurité informatique

existent déjà [90], [89] mais elles nécessitent d'être adaptées au contexte des habitats intelligents et aux troubles cognitifs de ses occupants. D'autres doivent être créées et l'infrastructure particulière de l'habitat peut être utilisée pour en faciliter la mise en place.

Pour caractériser ces solutions de sécurité, de fiabilité et de sûreté de manière uniforme, tout en laissant la liberté aux développeurs d'application et concepteurs d'habitat intelligent de les adapter aux différentes variations d'infrastructures et aux troubles cognitifs des patients, leur description sous la forme de patrons de sécurité est privilégiée. Ces patrons peuvent ensuite être regroupés dans un catalogue de patrons de sécurité, de fiabilité et de sûreté dédiés aux habitats intelligents et aux troubles cognitifs de leurs occupants.

L'objectif de cette thèse est de créer un premier catalogue de patrons de sécurité, de fiabilité et de sûreté pour les développeurs d'application des habitats intelligents.

À cette fin, cette thèse propose d'étudier dans le Chapitre 1, la problématique de la sûreté des futurs occupants d'habitat intelligent soit en raison de leur âge, soit en raison de leur trouble cognitif, et la problématique de la sécurité informatique due à l'infrastructure particulière des habitats intelligents et au caractère sensible des données qui y transitent. Pour illustrer et identifier les besoins en sécurité, fiabilité et sûreté, des scènes de la vie quotidienne dans lesquelles la sécurité des données et la sûreté des occupants peuvent être à risque sont décrites sous forme de scénarios dans le Chapitre 2. Nos objectifs et notre méthodologie sont présentés dans le Chapitre 3. Les résultats sont présentés en deux chapitres ; le Chapitre 4 est le catalogue de patrons de sécurité, de fiabilité et de sûreté, le Chapitre 5 illustre l'application des patrons pour répondre aux besoins des scénarios. Enfin, le Chapitre 6 ouvre la discussion sur les avantages et les limites de cette approche, et présente des pistes à suivre pour étendre le catalogue de patrons.

Chapitre 1

sécurité

La démocratisation des habitats intelligents permettra d'augmenter l'autonomie des personnes dépendantes et souffrant de troubles cognitifs grâce à l'informatique diffuse et à une intelligence artificielle capable de comprendre les besoins de son occupant et d'agir selon le contexte. Pour autant, l'âge des occupants, leurs troubles cognitifs ainsi que l'infrastructure spécifique de ce type d'habitat sont à prendre en considération afin de garantir la sûreté et le respect de la vie privée de ses occupants. Des solutions existent pour la plupart de ces problèmes, mais ne sont pas pour autant adaptées à la double spécificité du contexte soit les troubles cognitifs des occupants et l'infrastructure de ces résidences.

Ce chapitre introduit les défis à relever afin de proposer des solutions adéquates auprès des développeurs et des autres acteurs évoluant dans le contexte des habitats intelligents pour des personnes ayant des déficits cognitifs. Notre problématique est découpée selon trois perspectives :

— La sûreté et les risques encourus par les personnes âgées vivant seules et fait le parallèle avec les résidents des habitats intelligents souffrant de troubles cognitifs (section 1.1).

— La vie privée et les réglementations qui la protègent et leurs répercussions dans le contexte des habitats intelligents (section 1.2).

— Les principaux problèmes de sécurité tels que l'authentification et la confiden-

tialité. Comme ces problèmes sont récurrents en informatique, nous passerons aussi brièvement en revue certaines des nombreuses variantes des solutions développées pour un contexte général. Puis nous verrons leurs limites dans le contexte des habitats intelligents pour les personnes ayant des troubles cognitifs (section 1.3).

Devant la complexité des besoins dégagés dans les trois précédentes sections, nous verrons comment l'emploi de patrons de sécurité est abordé pour faciliter la compréhension et l'intégration de solutions de sécurité et fournir un catalogue de références aux développeurs d'applications pour prendre en charge ce manque (section 1.4). Cette approche constitue un pont entre les experts de sécurité et les développeurs. Finalement nous établirons les limitations actuelles auxquelles fait face le développement d'habitats intelligents pour les personnes ayant des troubles cognitifs.

1.1 La sûreté

La sûreté est la qualité d'une personne, d'un endroit ou d'une chose qui offre des garanties ou une protection qui le rend sûr. Dans le contexte des habitats intelligents, la sûreté signifie assurer l'intégrité physique et morale du résident et l'intégrité de son habitat. Il existe une multitude de facteurs pouvant remettre en cause l'intégrité du résident et de son habitat. Il n'est pas possible de les couvrir de manière exhaustive. Aussi nous en avons choisi deux qui mettent en relief deux niveaux différents : les fraudes et les risques domestiques.

Les fraudes mettent l'accent sur les facteurs intentionnels provenant de l'action d'une tierce personne. Les personnes âgées et les personnes ayant des troubles cognitifs en sont régulièrement victimes. Il existe des moyens de les éviter. Les accidents domestiques mettent en relief les interactions entre le résident et son habitat.

1.1.1 Les fraudes les plus courantes auprès des personnes âgées

Chaque année, des milliers de personnes âgées sont victimes d'escroquerie depuis leur domicile. Avec beaucoup d'aisance, les fraudeurs parviennent à s'introduire dans

le domicile de nos aînés et à les convaincre d'acheter un produit dont ils n'ont pas forcément besoin, d'effectuer des travaux dispendieux d'entretien ou de leur verser de l'argent en se faisant passer pour quelqu'un d'autre, et ce avant même que leurs proches ne puissent intervenir.

En gagnant leur confiance, les fraudeurs en tirent avantage pour leur emprunter de l'argent, pour récupérer les numéros de leurs cartes de crédit, voire pour les convaincre de modifier leur testament. Les fraudes aux États-Unis sont estimées en milliards. Les escroqueries par télémarketing rapportent environ 40 milliards chaque année à leurs auteurs [41].

Les fraudes les plus souvent rencontrées sont celles liées au porte-à-porte, au télémarketing, au courrier [6] ou au courriel. Parmi les plus importantes, mentionnons :

Les faux travaux d'entretien : Le fraudeur frappe à la porte et propose une offre alléchante pour réparer le toit. Mais après avoir donné de l'argent, les réparations sont superficielles, voire inexistantes. Dans la majorité des cas, ces réparations n'étaient pas nécessaires et le travail du fraudeur empire l'état du toit.

Les faux dons à des œuvres caritatives : Les escrocs se font passer pour un représentant d'une organisation caritative et convainquent facilement la victime de faire une donation en ne présentant aucune attestation officielle d'appartenance à cet organisme ou en faisant usage de faux.

Les prix gratuits : Les victimes reçoivent un appel ou un courrier leur annonçant qu'elles ont gagné un prix ou une forte somme d'argent. Cependant avant de le recevoir, elles doivent acquitter les taxes, les frais de manutention et d'envoi. Certaines victimes vont jusqu'à utiliser leur fonds de pension pour couvrir ces frais qui atteignent en moyenne 2000 $ [6].

Ces exemples ne sont qu'une infime partie des fraudes réalisées chaque année auprès des personnes âgées.

1.1.2 La facilité de frauder

Les personnes âgées sont des cibles de prédilection pour les fraudeurs, ce qui s'explique en partie par le fait qu'elles font plus facilement confiance aux gens, qu'elles

sont généralement disponibles et chez elles durant la journée, qu'elles ne peuvent pas ou n'osent pas contacter rapidement un proche pour obtenir leur avis [2].

Les fraudeurs profitent de l'isolement et de la solitude de leurs victimes pour solliciter leur sympathie. Pour les victimes, contentes d'avoir de l'attention et de la compagnie, leur vulnérabilité est d'autant plus grande et profite aux fraudeurs.

Les raisons d'une grande proportion de personnes âgées parmi les victimes de fraudes [2] sont les suivantes :

1. Les personnes âgées ont de l'argent liquide chez elles.
2. Les personnes âgées d'aujourd'hui ont été élevées avec des principes de politesse et de confiance en l'autre. Ces traits de caractère s'avèrent un avantage pour l'éventuel fraudeur qui sait en tirer parti en sachant que ces personnes ont du mal à dire « non », à fermer la porte ou à raccrocher le téléphone.
3. Les personnes âgées osent rarement porter plainte ou ne savent pas à qui s'adresser. Elles ont parfois honte de s'être fait escroquer ou ne s'en rendent pas compte. Certaines études montrent que la victime a peur suite à une escroquerie d'être considérée par sa famille comme inapte à gérer sa vie financière de manière autonome [71], [96].
4. Les victimes de ces crimes ne sont souvent pas de bons témoins et l'effet de l'âge sur leur mémoire les gêne pour fournir aux enquêteurs suffisamment d'informations pour constituer un dossier de plainte solide, des informations telles que la description du fraudeur, le nombre de visites ou d'appels, à quel moment de la journée la visite a eu lieu, les sommes d'argent versées et le type de versement.
5. Avec les progrès réalisés ces dernières années en technologie ou en sciences, certains produits frauduleux pour améliorer les fonctions cognitives, la condition physique ou l'état de santé peuvent paraître crédibles. Les victimes peuvent facilement être amenées à croire que le produit qu'on leur vend sera utile.

Les fraudeurs savent exploiter les faiblesses de leurs victimes et les personnes âgées sont souvent des cibles de prédilections pour eux. Cependant, il existe des moyens pour les éviter.

1.1.3 Les moyens actuels de se protéger des fraudeurs

De nombreux organismes de soutien aux victimes de fraudes donnent des conseils pour prévenir les personnes âgées et leur famille de ces crimes. Ces conseils sont simples et permettent d'éviter d'entrer dans le jeu des fraudeurs. La liste ci-dessous contient une partie de ces conseils :

1. Les fraudeurs essayent de convaincre leurs victimes d'agir rapidement, que l'offre n'est valable qu'aujourd'hui ou qu'il est important de garder cette offre confidentielle. Lorsqu'une telle situation se produit, il est important dès le départ de refouler le fraudeur en disant « non merci » et en raccrochant le téléphone ou en fermant la porte.
2. Lorsqu'une personne représente un organisme ou une institution, elle doit être en mesure de le prouver et doit avoir en sa possession des papiers.
3. Se retirer de l'annuaire téléphonique.
4. Ne jamais donner son numéro de compte bancaire, de carte de crédit à une tierce personne.

C'est souvent le facteur de solitude et d'isolement qui profite aux fraudeurs. Les personnes âgées vivant dans un immeuble avec un gardien ou résidant dans une maison de retraite sont plus à l'abri grâce aux employés qui filtrent les visiteurs. Il n'existe malheureusement pas de filtre équivalent pour les personnes seules.

1.1.4 Les personnes atteintes de troubles cognitifs

Les personnes atteintes de la maladie d'Alzheimer sont des personnes âgées et ne font pas exceptions aux fraudes vues précédemment. Elles sont d'autant plus sensibles à ces fraudes que leur capacité à exécuter des tâches financières décline également. Parmi ces tâches, on peut distinguer la capacité à détecter des appels ou des lettres frauduleuses [10].

Dans le livre « Alzheimer's Disease and Related Disorders », Marson et Briggs tentent d'évaluer les compétences requises par les patients atteints de la maladie d'Alzheimer pour gérer leurs finances [60], [58], [33]. La capacité financière requiert de bonnes facultés de jugement et du pragmatisme pour pouvoir être autonome. Cette

capacité est considérée comme une AVQ avancée. Une AVQ avancée est régie par des fonctions cognitives plus importantes et se distingue des AVQ d'entretien (telles que préparer un repas ou faire ses courses) ou des AVQ de base (telles que s'habiller ou se laver) [60], [58].

La perte de cette capacité engendre de nombreuses conséquences sur la vie du patient et sur sa famille. Le patient peut éprouver de la difficulté à payer ses factures, à déceler une fraude et à utiliser ses moyens de paiement adéquatement.

Dans de nombreux cas, un membre de la famille ou un tuteur encadre le patient dans son budget hebdomadaire. Le patient devient alors responsable d'un budget limité pour ses dépenses essentielles et personnelles.

1.1.5 Les accidents domestiques

Pour garantir la sûreté d'un patient dans le contexte des habitats intelligents, d'autres aspects doivent être pris en compte tels que les accidents domestiques. Ces accidents peuvent être liés simplement à l'âge du patient ou encore découler de déficits cognitifs. Par exemple, le risque de chute et ses conséquences augmentent avec l'âge. Il arrive parfois qu'une personne âgée chute chez elle et que plusieurs jours s'écoulent avant qu'elle ne soit retrouvée et secourue. Des solutions commerciales ou expérimentales existent en matière de détection de chute ou d'alerte tels les bracelets électroniques, la reconnaissance d'images ou des dispositifs portés comprenant un accéléromètre.

Les pertes de mémoire et les troubles cognitifs augmentent également les risques d'accidents domestiques tels les cas de brûlure ou d'intoxication. Des cuisinières intelligentes ou des orthèses cognitives pour assister les patients dans leur tâche de cuisine pourraient y remédier dans un futur proche.

1.2 Protection de la vie privée

Cette section introduit la notion de vie privée et propose un aperçu des lois qui en garantissent la protection dans la vie de tous les jours, mais également dans le domaine de la santé. Enfin, un rapport de cause à effet est fait entre l'utilisation d'un

réseau de capteurs dans les habitats intelligents et la protection de la vie privée de ses occupants.

1.2.1 Qu'est-ce que la vie privée ?

La notion de vie privée pouvait autrefois se résumer au droit de vivre en paix. Aujourd'hui, avec l'explosion des systèmes d'information, cette notion couvre plusieurs aspects dans l'esprit des gens. Elle implique le droit d'avoir un espace personnel et privé, d'être libre de partager et d'échanger des informations de manière confidentielle et d'être libre de surveillance.

Le principe de vie privée implique la distinction entre espace privé et public, entre vie privée et vie publique et suppose des droits pour chaque individu tels qu'exprimés dans l'article 12 de la déclaration universelle des droits de l'homme de 1948 : « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. »

Ce principe de vie privée est protégé par des lois dans la plupart des pays.

1.2.2 La protection de la vie privée

Au Canada, deux lois fédérales protègent la vie privée : le Privacy Act de 1983, complété en 2001 par le Personal Information Protection and Electronic Documents Act (PIPEDA).

Le Privacy Act impose aux divers départements et agences du gouvernement de respecter le droit à la vie privée en limitant la collecte, l'usage et la divulgation d'informations personnelles. Il donne également le droit aux individus d'accéder à leurs informations personnelles et d'en demander la rectification. Le PIPEDA est similaire au Privacy Act, mais concerne la protection des individus par rapport au secteur privé.

Des lois protègent les individus de façon similaire en Europe telles que la directive européenne relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (directive 95/46/CE) de 1995 [1] ou aux États-Unis avec le Privacy Act de 1974.

1.2.3 La protection de la vie privée dans le domaine de la santé

Au Canada, la collecte, l'usage et la divulgation de données personnelles médicales sont régis par le PIPEDA. Dans le cas d'une province disposant d'une loi spécifique, cette dernière prévaut.

L'Alberta, le Manitoba, l'Ontario et la Saskatchewan disposent de législation spécifique en matière de données personnelles médicales gérées par les secteurs public et privé.

Aux États-Unis, le HIPAA (Health Insurance Portability and Accountability Act) adopté en 1996 régule l'utilisation des données personnelles médicales pour protéger le droit à la vie privée des individus dans le domaine médical. Il requiert notamment l'établissement de standards nationaux pour encadrer les transactions électroniques en matière de santé et assurer l'identification des professionnels de santé.

Ces lois contiennent des dispositions pour limiter l'accès et l'usage des données personnelles médicales au sein de l'organisme dépositaire des données et interdit tout autre usage auquel le patient n'a pas explicitement consenti.

1.2.4 La vie privée dans un habitat intelligent

Les capteurs répartis dans l'habitat détectent les actions réalisées dans l'appartement et engendrent des évènements qui sont relayés aux applications concernées. Ces applications peuvent les enregistrer pour les analyser ultérieurement. L'usage et la consultation de ces données peuvent être effectués par une application ou par un membre du personnel soignant afin de garantir une prise en charge adéquate du patient. Pour autant, ils doivent se faire en respect de la législation en vigueur et de la vie privée du patient. Par exemple, un membre du personnel médical peut avoir besoin d'accéder à des informations provenant du réseau de capteurs pour savoir si le patient prend bien ses médicaments. Si aucun contrôle n'est effectué, le réseau de capteurs est accessible par tous laissant à quiconque la possibilité d'espionner son occupant dans les moindres détails de sa vie privée et intime. À partir des informations recueillies par les capteurs, une personne mal intentionnée pourrait suivre les habitudes du patient et profiter de son absence pour entrer par effraction chez lui. Dans une telle situation,

il est important de permettre, d'une part, l'accès aux informations concernant le patient aux membres du personnel responsables de sa réadaptation, d'autre part, d'en limiter l'accès à ces personnes seulement et ce uniquement pour l'information dont ils ont besoin.

La vie privée des résidents des habitats intelligents est importante. Toutefois ces habitats posent des problèmes qui leur sont spécifiques tels la distribution des services, le chiffrement de données et les sauvegardes réparties dans le système pour n'en citer que quelques un.

1.3 Les principes de base de la sécurité informatique

Cette section énonce quelques-uns des principes de sécurité les plus fréquemment rencontrés dans les systèmes distribués [17] et les environnements intelligents [65] : l'authentification, le contrôle d'accès, la confidentialité, l'intégrité des données, la disponibilité, la fiabilité et la protection de la vie privée.

1.3.1 L'authentification

L'authentification est le moyen mis en œuvre pour garantir que la personne qui s'identifie comme telle est bien celle qu'elle prétend être. C'est l'un des éléments les plus importants en matière de sécurité avant d'autoriser une personne à accéder à une ressource ou à exécuter une tâche dans un système d'information. Pour s'authentifier, un individu doit interagir avec le système en fournissant une information qu'il soit seul en mesure de connaître (par exemple, un mot de passe), ou à pouvoir fournir (par exemple un badge d'identification) ou une caractéristique humaine qu'il est le seul à posséder (par exemple, une empreinte digitale).

1.3.2 L'autorisation et le contrôle d'accès

Le gestionnaire d'un système d'information peut donner différents niveaux d'accès aux ressources disponibles ou aux processus exécutés par le système. Ce procédé s'ap-

pelle l'autorisation et permet le contrôle d'accès. Après avoir authentifié une entité, l'autorisation sert à définir ce que l'entité peut faire ou ne pas faire. Il existe différentes techniques de contrôle d'accès, parmi lesquelles on retrouve le contrôle d'accès discrétionnaire, le contrôle d'accès obligatoire, le contrôle d'accès basé sur les treillis et le contrôle d'accès basé sur des rôles.

Le contrôle d'accès discrétionnaire

Le contrôle d'accès discrétionnaire est défini comme un moyen de limiter l'accès aux objets en se basant sur l'identité des individus ou des groupes auxquels ils appartiennent. Dans les politiques de contrôle d'accès discrétionnaire, chaque objet a un propriétaire. Qui peut accorder des droits d'accès tels que le droit d'écriture, de lecture ou d'exécution à un autre sujet.

Ce type de contrôle se retrouve par exemple dans la gestion des droits d'accès des fichiers dans le système Unix. Le propriétaire d'un fichier peut choisir les droits de lecture, d'écriture et d'exécution d'un fichier pour lui-même, un groupe et les autres utilisateurs non membres du groupe.

Le contrôle d'accès obligatoire

Dans le contrôle d'accès obligatoire, un niveau de sécurité est associé d'une part aux entités qui demandent l'accès et aux ressources d'autre part. Pour obtenir l'accès à une ressource ou exécuter une tâche sur le système, le niveau de sécurité de l'entité doit être égal ou supérieur au niveau de sécurité nécessaire pour accéder à la ressource ou exécuter la tâche. Cette technique de sécurité est assez simple à mettre en œuvre, car seule la hiérarchie des niveaux de contrôle d'accès doit être maintenue, mais elle présente de nombreux problèmes lorsqu'il s'agit d'affiner les politiques d'accès à une ressource. Les utilisateurs n'ont, de plus, pas la possibilité de modifier l'attribution des droits d'accès. Par exemple, on peut donner l'accès au réseau de capteurs aux médecins, mais non aux infirmiers, en attribuant un niveau de sécurité au réseau de capteurs égal à celui des médecins. Ce type de contrôle manque cependant de flexibilité. Un médecin ne peut donner l'accès que ce soit ponctuel ou permanent à l'infirmier responsable du patient.

Le contrôle d'accès basé sur les treillis

Dans ce type de contrôle d'accès, des niveaux de sécurités sont donnés aux ressources et aux sujets. Pour accéder à une ressource, un utilisateur doit posséder un niveau de sécurité supérieur ou égal à celui de la ressource. Défini pour la première fois par Dorothy E. Denning [31], ce type de contrôle d'accès avait pour but de gérer l'accès aux documents confidentiels d'un système informatique militaire. Ce contrôle d'accès fonctionne également par association des niveaux de sécurité des sujets ou des ressources. Par exemple, si deux sujets A et B désirent accéder à une ressource R, l'association des niveaux de sécurité de A et B doit être égale ou supérieure à celui de R pour y parvenir.

Il existe différents modèles, dont le modèle de Bell-La Padula développé par David E. Bell et Leonard J. La Padula en 1973 pour formaliser la politique de sécurité multi niveaux du Département de la Défense des États-Unis et le modèle d'intégrité de Biba. Ravi Sandhu les présente dans un article et en identifie les limitations [84]. Tandis que le modèle de Bell LaPadula met l'accent sur la confidentialité des données en attribuant des règles de classification des ressources et des niveaux de confidentialité, le modèle d'intégrité Biba a pour but de garantir l'intégrité des données.

Le contrôle d'accès basé sur les rôles

Le contrôle d'accès basé sur les rôles ou "Role-Based Access Control" (RBAC), a été introduit en 1992 par D. Ferraiolo et R. Kuhn [37], également repris par R. Sandhu [86], il est devenu un modèle de contrôle d'accès prédominant grâce à une simplification des descriptions de politiques de contrôle d'accès avancés et de leur maintenance. Avant RBAC, les organisations devaient maintenir des listes de contrôle d'accès ou "Access Control Lists" (ACL) pour autoriser l'accès à chacune de leurs ressources ou de leurs applications. L'ajout ou le retrait d'un utilisateur entraînaient la modification de chacune des listes de contrôle associées aux ressources ou aux applications autorisées ce qui devenait très difficile à effectuer pour les administrateurs des systèmes d'information. RBAC permet de faciliter cette gestion en attribuant des rôles aux utilisateurs et en définissant des permissions d'accès ou d'action pour ces rôles. Le principe de RBAC est le suivant :

— Un ou plusieurs rôles sont attribués à un utilisateur,
— Les autorisations sont associées à des rôles,
— Un utilisateur qui se voit attribuer un rôle possède les autorisations associées à ce rôle.

En 2000, à la demande du NIST, Sandhu, Ferraiolo et Kuhn intègrent leur travail et proposent un modèle unifié de RBAC [87] appelé "NCIST RBAC model" qui sera par la suite adopté comme standard par le "InterNational Committee for Information Technology Standards" (INCITS) en 2004. Selon un rapport effectué en 2010 [70] pour le compte du National Institute of Standards and Technology (NIST), ce type de contrôle d'accès est fortement utilisé dans les organisations de plus de 500 employés pour restreindre l'accès à certaines ressources ou fonctionnalités d'un système informatique aux seuls utilisateurs autorisés. On retrouve des implémentations de RBAC dans de nombreux produits informatiques tels que Microsoft Active Directory, Microsoft SQL Server, SELinux, FreeBSD, Solaris, Oracle DBMS. RBAC est suffisamment flexible pour simuler les contrôles d'accès obligatoire, discrétionnaire [73] et basé sur les treillis [85]. Le contrôle d'accès basé sur des rôles est aujourd'hui très répandu notamment dans les domaines bancaires, de la santé et des télécommunications grâce à son faible coût de mise en œuvre et à sa facilité d'utilisation.

1.3.3 La confidentialité

La confidentialité est un principe qui se définit comme le fait d'assurer que les informations soient accessibles uniquement aux personnes autorisées et qu'elles ne puissent être divulguées à une tierce personne. C'est l'un des plus importants principes que l'on retrouve communément dans le domaine informatique, médical, légal et éthique, pour ne citer que cela.

On retrouve également ce principe dans le terme "besoin d'en connaître" ou "need to know" en anglais, utilisé dans les organisations ou l'armée pour décrire le caractère très sensible d'informations dont l'accès doit être limité uniquement à ceux qui en ont besoin spécifiquement.

En informatique, le contrôle d'accès et les techniques de cryptographie sont utilisés pour garantir la confidentialité des données.

1.3.4 L'intégrité des données

Le principe de l'intégrité des données est de garantir la non-altération, l'authenticité et la préservation des données. On le retrouve essentiellement dans la gestion des bases de données et dans le domaine de la cryptographie.

Dans le contexte des bases de données, l'intégrité des données correspond à garantir la cohérence du contenu de la base de données. Par exemple, dans un logiciel de gestion de livres, s'assurer que l'auteur existe avant d'ajouter un livre ou empêcher le retrait de la base de données d'un auteur si des livres qu'il a écrits y sont encore.

En cryptographie, l'intégrité des données consiste à garantir que les données ne subissent aucune altération, destruction accidentelle ou volontaire. La cryptographie permet également de vérifier l'authenticité (la non-fabrication) des données. Ces altérations peuvent être provoquées par l'interception du message original, sa modification, puis son émission sous une forme modifiée, ou peut-être non volontaire en cas de problème de transmission via le réseau.

Les fonctions de hachage ou un code d'authentification de message ou "Message Authentication Code" (MAC) peuvent être utilisés afin de comparer l'empreinte du message original avec l'empreinte du message reçu.

1.3.5 La disponibilité

Dans le cadre des systèmes informatiques, la disponibilité correspond à la capacité d'un système d'assurer ses fonctions sans interruption, délai ou dégradation, au moment même où la sollicitation en est faite.

La disponibilité peut être une exigence de sécurité prévue lors de la conception du système afin de garantir l'accès aux ressources au besoin. On parle de "haute disponibilité" lorsque l'on spécifie que le système aura un taux d'indisponibilité maximal spécifique. Par exemple, sur une année de mise en service, un taux de disponibilité de 99,99 % correspond à moins de 53 minutes d'indisponibilité par an.

Ce principe peut être remis en cause par des bris de matériel, des problèmes de réseau ou lors d'attaques informatiques dites de déni de service. Pour prévenir les périodes d'indisponibilité, les administrateurs de système disposent de plusieurs recours, dont la redondance des matériels, le remplacement de matériel ou les mises

à jour à chaud (sans avoir à éteindre le système).

1.3.6 La fiabilité

Alors que la disponibilité fait référence à la capacité de réponse d'un système, la fiabilité a trait à sa capacité à se comporter normalement, c'est-à-dire en conformité avec le cahier des charges à un moment donné. Dans ce cas, le système est dit fiable.

La fiabilité est une des composantes de la sûreté de fonctionnement et doit être prise en compte dès les premières étapes du cycle de développement. Notamment en suivant les recommandations de génie logiciel en termes de sûreté de fonctionnement des systèmes informatiques, elle participe à la disponibilité d'un système.

La fiabilité absolue n'existe pas, mais spécifier dans le cahier des charges le niveau de fiabilité d'un système permet de garantir un niveau acceptable de fiabilité.

1.3.7 La protection de la vie privée

Là où la confidentialité ne couvre que le caractère privé d'une information lors de sa transmission, la protection de la vie privée garantit à l'individu le droit de garder privées les informations le concernant. Plus précisément, il s'agit de la relation entre la collecte et la divulgation des données relatives à un individu, les attentes de l'individu en matière de protection de la vie privée et la législation qui les encadre.

1.4 Les patrons de sécurité

Cette section définit le concept de patron, sa motivation et son utilisation dans de nombreux domaines, puis introduit et illustre le concept de patron de sécurité. Les applications de la notion de patrons dans le domaine informatique et au sein de projets sont également abordées.

1.4.1 La définition d'un patron

Un patron peut être perçu comme un modèle ou un guide à suivre pour la réalisation d'un objet et est utilisable pour la copie ou l'imitation d'un original. Ce

peut être par exemple un support découpé utilisé pour peindre une forme identique à maintes reprises, le patron de conception d'une robe, les modèles des différentes pièces d'une chaussure (d'où le nom de patronnier donné aux ouvriers responsables de leur confection), une recette de cuisine ou les plans d'un bâtiment.

Les avantages des patrons sont nombreux, de la réduction des coûts à la facilité d'apprentissage grâce à la mise en exergue des points clés. En architecture, lorsque le plan d'un bâtiment a fait ses preuves, il peut être réutilisé et faire économiser le coût et le temps d'une nouvelle conception de plan. En musique, la connaissance des gammes musicales aide les musiciens à la compréhension de différentes musiques, à l'improvisation et à la création.

Tous domaines confondus, on retrouve généralement le concept de la redondance ou de la réutilisation d'un modèle dans le but de le copier ou de l'adapter dans une situation similaire.

1.4.2 Les patrons de conception

L'approche par patrons a déjà été adoptée dans le domaine de l'ingénierie logicielle comme un moyen de décrire et de réutiliser des concepts récurrents de programmation par objet. L'ouvrage le plus célèbre à ce sujet est celui d'Erich Gamma, Richard Helm, Ralph Johnson et John Vlissides [39], paru en 1994. Souvent surnommé comme le livre de la bande des quatre ("book by the gang of four" ou le "GoF book"), car écrits par quatre auteurs, ce livre s'inspire du travail de Christopher Alexander [7], architecte ayant travaillé dans les années 70 sur un langage de patrons dans le domaine de l'architecture. Selon Alexander, "chaque patron décrit un problème qui se manifeste constamment dans notre environnement, et donc décrit le cœur de la solution à ce problème, d'une façon telle que l'on puisse réutiliser cette solution des millions de fois, sans jamais le faire deux fois de la même manière [7]."

Selon Gamma et al. [39], les patrons de conception décrivent des solutions pour répondre à des problèmes récurrents d'architecture (informatique) et de conception des logiciels. Les solutions proposées se veulent indépendantes du langage de programmation, décrivent des procédés de conception généraux et intègrent l'expérience appliquée à la conception logicielle. Leur ouvrage regroupe 23 patrons de conception

classés en trois catégories, patrons de comportement (communication entre objets), patrons de création (d'objets ou de classes) et patrons structurels (composition d'objets et de classes).

Les patrons sont décrits en langage naturel et à l'aide de diagrammes. Ils sont composés en moyenne de 12 sections :

- Nom du patron : Le nom du patron doit être à la fois simple et significatif pour illustrer le problème et la solution qu'il propose.
- Intention : Brève description de l'objectif du patron de conception et du problème auquel il répond.
- Autres noms connus : Liste des autres noms couramment utilisés pour ce patron.
- Motivation : Description du problème de conception à l'aide d'un scénario et de la manière dont la structure des objets et classes du patron participe à sa résolution.
- Domaine d'application : Explication des situations pour lesquelles ce patron peut être appliqué et indications pour les reconnaître.
- Structure : Représentation graphique en UML des classes du patron à l'aide de diagramme de classes et de diagramme d'interaction pour illustrer la collaboration entre les différents participants du patron.
- Participants : Classes et objets qui participent à la solution du patron et leur responsabilité.
- Collaboration : Manière de collaborer des participants pour mener à bien leur responsabilité.
- Conséquences : Résultat de l'application du patron, comment les objectifs sont atteints et quelles sont les conséquences ou les inconvénients de son utilisation.
- Implémentation : Conseils et techniques pour une bonne implémentation du patron, conseils liés aux spécificités du langage utilisé.
- Exemple de code : Des portions de code (en C++ ou Smalltalk dans le livre) pour illustrer une implémentation possible du patron.
- Usages connus : Exemples connus d'applications du patron dans des situations réelles.
- Patrons liés : Patrons liés par leur imbrication ou leur opposition au patron

courant.

1.4.3 Les patrons de sécurité

Bien qu'un développeur d'applications puisse s'avérer excellent dans un langage de programmation et dans sa capacité à coder de manière efficiente, il n'est pas pour autant nécessairement un expert en sécurité. La sécurité est souvent remise à plus tard, car dans l'esprit des développeurs, il est courant de penser d'abord en termes de fonctionnalités du programme avant de sécuriser l'application elle-même. Les patrons de sécurité permettent d'y remédier en proposant des solutions de sécurité réutilisables correspondant aux exigences de sécurité demandées. Un patron de sécurité décrit un problème de sécurité particulier et récurrent et présente une solution de sécurité générique pour y remédier. Il s'agit pour cela de capturer l'expertise de sécurité et de la rendre disponible pour tous.

Yoder et Barcalow proposent des patrons architecturaux afin d'introduire des concepts de sécurité dans une application [99]. Fernandez et Pan décrivent différents patrons pour la plupart des modèles de sécurité tels que l'autorisation et le contrôle d'accès basé sur des rôles [36].

En suivant le même principe qu'en ingénierie logicielle, Markus Schumacher [90], [89] applique le concept de patron à des problèmes de sécurité en proposant une série de patrons de sécurité applicables dans le cycle de développement. Bien qu'il existe déjà une multitude de langages de description de patron [20], Schumacher et al. décident de reprendre le même format disponible dans l'ouvrage de Franck Buschmann [21] intitulé "Pattern-Oriented Software Architecture : a system of patterns". Ce format décrit un patron ainsi :

— Nom : Nom et brève description du patron.
— Autres noms connus : Liste des autres noms couramment rencontrés pour ce patron.
— Exemple : Exemple tiré du monde réel pour illustrer l'existence du problème et le besoin du patron.
— Contexte : Contexte d'applicabilité du patron.
— Problème : Problème auquel s'adresse le patron et raison qui motive l'utilisa-

tion du patron.

- Solution : Principe fondamental de la solution proposée par ce patron.
- Structure : Spécification détaillée de la structure du patron.
- Dynamiques : Description du comportement du patron entre ses différents composants lors de son utilisation.
- Implémentation : Conseils pour aider à l'implémentation et à l'adaptation du patron selon les besoins, parfois à l'aide de diagramme de classes.
- Exemples résolus : Exemples et aspects importants à mentionner pour la résolution de l'exemple donné, qui ne sont pas déjà indiqués dans les sections "structure", "dynamiques" et "implémentation".
- Variantes : Brèves descriptions de variantes ou de spécialisations du patron.
- Usages connus : Exemples d'utilisation du patron dans des systèmes concrets.
- Conséquences : Conséquences résultantes de l'application du patron et leurs implications positives ou négatives.
- Voir aussi : Références à d'autres patrons à utiliser en combinaison ou en guise d'alternative.

Toutes les sections ne sont pas obligatoires. Certains patrons n'ont pas forcément d'autres noms connus ou de variantes. Dans certains cas, la solution peut-être suffisamment explicite pour ne pas nécessiter d'information supplémentaire dans les sections "structure" ou "dynamiques", mais ces sections donnent une bonne manière de décrire et de présenter un patron.

Il n'existe donc pas un unique format à suivre pour décrire un patron. Cette situation offre à la fois une grande flexibilité aux auteurs de patrons et une grande difficulté lorsqu'il s'agit de saisir l'essence même d'une solution à un problème pour la présenter dans les différentes sections d'un patron. Écrire un patron est difficile et peut nécessiter plusieurs cycles de révision, d'autant plus qu'avant d'être décrite dans un patron, la solution doit avoir été éprouvée dans différentes situations réelles.

1.4.4 Quelques projets informatiques relatifs aux patrons de sécurité

En terme de patrons de conceptions, des logiciels existent pour assister les développeurs à intégrer des patrons dans leur application. C'est le cas du "Design Pattern Framework" publié par "Data & Object Factory" qui offre un logiciel disponible pour plusieurs langages de programmation.

Cependant, bien que plus fournis en code source qu'un simple ouvrage dédié aux patrons, ces logiciels ne remplacent pas les développeurs et ne font que les aider à comprendre le but d'un patron de conception et comment l'adapter dans leur code.

Dans le domaine des patrons de sécurité, on trouvera des composants ou des API qui sont souvent des implémentations de patrons de sécurité et qui peuvent s'intégrer dans une application pour appliquer des solutions de sécurité éprouvées et approuvées.

La section suivante présente un cadre d'applications plus ambitieux puisqu'il propose d'automatiser la sélection et l'intégration de patrons de sécurité dans une application et de suivre son bon fonctionnement.

1.4.5 Le projet SERENITY

Dans certains cas plus complexes, les descriptions en langage naturel laissent place à différentes interprétations de la solution fournie et de la manière d'appliquer le patron de sécurité. Le manque d'outils de validation peut poser des problèmes comme l'a démontré Alessandro Armando et al. [11].

Le projet SERENITY [3] est un projet européen qui s'est déroulé de 2006 à 2009 avec la participation d'une quinzaine d'organisations, d'institutions et d'entreprises pour développer des spécifications, des méthodes et des outils pour garantir la sûreté de fonctionnement et la sécurité informatique dans le contexte des environnements ubiquitaires [26], [27].

La motivation du projet part du principe que les systèmes et les applications telles que nous les connaissons aujourd'hui vont disparaître. Les architectures statiques avec des composants informatiques, des logiciels et des canaux de communication précis sont limitées et tendent à être remplacées par des architectures flexibles capables de s'adapter au contexte et de répondre aux besoins des utilisateurs tout en prenant en

compte leurs habitudes.

Des problèmes de sécurité et de fiabilité de fonctionnement se poseront de par la complexité, le caractère diffus et la faible capacité de calcul des éléments d'un environnement ubiquitaire. De plus, l'avènement de nouvelles habitudes sociétales nécessite de résoudre de nouveaux problèmes de respect de la vie privée, de moyens d'identification et d'authentification, de gestion de droits pour lesquels une recherche approfondie dans le domaine de la sécurité est requise.

Pour y remédier, SERENITY [3] propose la marche à suivre suivante :

— Rendre disponibles des solutions de sécurité validées dans les environnements ubiquitaires et en garantir le suivi.

— Promouvoir la définition des exigences de sécurité qui surviennent dans des situations d'ordre privé, d'affaires ou légales pour permettre la sélection, basée sur ces exigences, de mécanismes appropriés de sécurité.

— Fournir des mécanismes de suivi de sécurité lors de l'exécution et réagir dynamiquement aux menaces, aux brèches de sécurité ou changements de contexte.

— Intégrer les solutions de sécurité, la définition des exigences et la sélection de solutions, les mécanismes de suivi dans un cadre d'applications commun.

L'approche SERENITY

SERENITY propose de mettre à la disposition des développeurs un cadre d'applications pour consulter une bibliothèque de patrons pour sélectionner le patron correspondant aux exigences de sécurité à combler et pour le déployer dans une application (Figure 1.1). Le développeur d'applications adresse une liste d'exigences de sécurité (1) au cadre d'applications SERENITY. Celui-ci consulte son catalogue de patrons de sécurité (2) et propose une série de candidats susceptibles de convenir au développeur (3). Ce dernier peut sélectionner le patron qui lui correspond le mieux et déployer automatiquement l'implémentation qui lui correspond dans son application (4).

Le cadre d'applications propose également pour certains patrons de suivre en temps réel le bon fonctionnement des mécanismes de sécurité au sein de leur application en cas de changement de contexte (5).

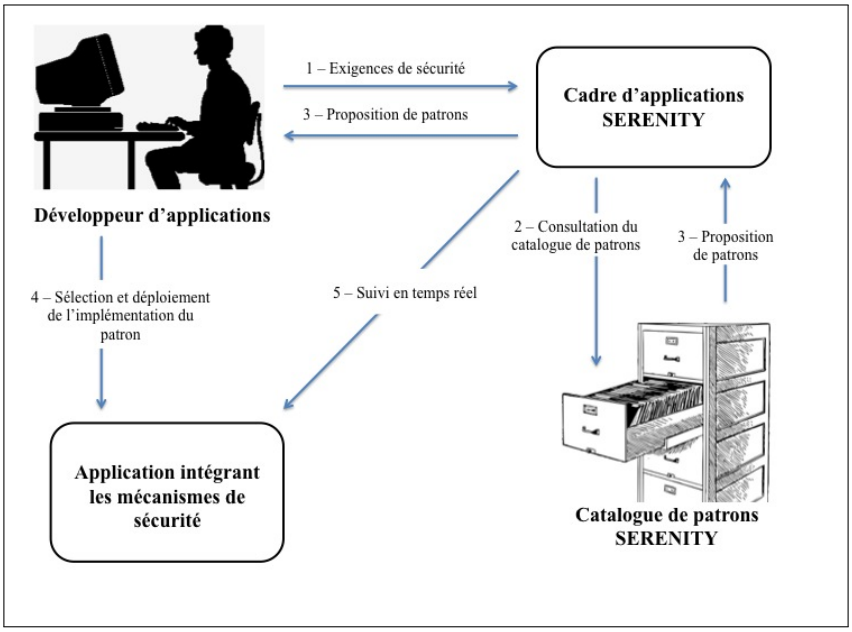

figure 1.1 – L'approche SERENITY.

L'organisation des patrons de sécurité dans le projet SERENITY

Pour faciliter la sélection, l'adaptabilité, l'utilisation et le suivi lors de le l'exécution de manière automatique, SERENITY propose de capturer les mécanismes et les techniques de sécurité au sein d'artefact de sécurité. Ces artefacts sont de trois types [83] : classe, patron et implémentation conceptuellement reliés (Figure 1.2).

— Une **classe Sécurité et Fiabilité** constitue une abstraction d'une série de patrons de sécurité partageant les mêmes exigences de sécurité, par exemple, l'intégrité et la confidentialité d'un message SOAP [4] entre deux acteurs légitimes à travers le réseau.

— Un **patron Sécurité et Fiabilité** représente une solution de sécurité préalablement validée et abstraite qui satisfait les exigences de sécurité de la **classe Sécurité et Fiabilité**, par exemple, coder et signer numériquement les données contenues dans un message SOAP.

— Une **implémentation Sécurité et Fiabilité** est la solution à intégrer dans l'application pour garantir les exigences de la **classe Sécurité et Fiabilité**. Une même implémentation peut correspondre à un ou plusieurs **patrons Sé-**

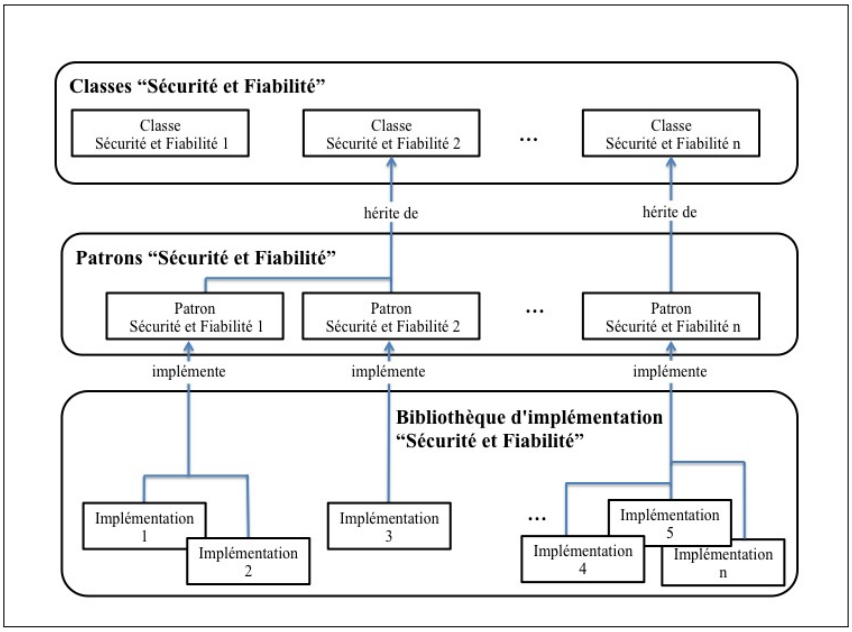

figure 1.2 – Patron de sécurité dans le projet SERENITY

curité et Fiabilité.

La description des artefacts (classe, patron et implémentation) de SERENITY est très spécifique et est propre aux outils du cadre d'applications SERENITY. Ainsi, un patron de sécurité doit être transposé dans le langage de description de classes, de patrons et d'implémentations pour être correctement interprété par le cadre d'applications. Un langage de description des artefacts a été développé en conséquence pour le projet SERENITY [56].

1.5 Conclusion

Ce chapitre a traité des aspects de la sûreté des personnes et de leur vulnérabilité grandissante en raison de leur âge ou de leurs troubles cognitifs (Section 1.1), de la vie privée, des lois qui la protège et des inquiétudes pour la préserver dans un habitat intelligent (Section 1.2), des principes de sécurité couramment rencontrés (Section 1.3) et finalement des patrons de sécurité (Section 1.4).

De ces quatre sections, il est important de retenir les points suivants :

1.5. Conclusion

— Les habitats intelligents et les personnes ayant des troubles cognitifs amènent des problématiques nouvelles en terme de sécurité, de fiabilité et de sûreté.
— Trois perspectives sont à prendre en compte dans le maintien de personnes ayant des troubles cognitifs ; le résident et la spécificité des ces troubles cognitifs, la protection de la vie privée dans un habitat intelligent et les particularités de son infrastructure informatique.
— Les patrons permettent de décrire des solutions de sécurité, de fiabilité et de sûreté prenant en compte ces perspectives.
— Il n'existe pas de catalogue pour habitats intelligents pour personnes ayant des troubles cognitifs.

Chapitre 2

Illustrations des besoins en sécurité, en fiabilité et en sûreté

Pour illustrer les problèmes de sécurité informatique et de sûreté des patients lors du maintien à domicile, ce chapitre présente des mises en situation sous forme de scénario et dresse pour chacune d'elles, la liste des besoins de sécurité et de sûreté à combler.

2.1 Cinq scénarios

Le but de ces scénarios est de représenter une mise en situation aussi réaliste que possible de ce que sera la vie d'un patient dans un habitat intelligent. Dans ce contexte particulier, le patient sera suivi médicalement et des intervenants passeront au domicile du patient régulièrement pour lui prodiguer des soins. Il pourra recevoir de la visite des membres de sa famille, d'un conjoint et d'amis. Selon le degré de supervision auquel il est soumis, il pourra effectuer une partie de ses propres achats et bien d'autres activités.

La vie du patient ne sera pas sans danger et les scénarios ont été choisis pour montrer des situations dans lesquelles le patient pourrait se montrer en état de vulnérabilité pour mettre en évidence les besoins de sûreté. De même, l'environnement des scénarios et les interactions entre les différents acteurs mettent en évidence les

besoins de sécurité informatique.

Ces scénarios sont les suivants :

— Scénario 1 : Assistance médicale à domicile.

— Scénario 2 : Intervention d'urgence.

— Scénario 3 : Visite à domicile des intervenants.

— Scénario 4 : Accès à l'appartement.

— Scénario 5 : Utilisation des moyens de paiement.

Ces mises en situation ne sont pas suffisantes pour dresser la liste exhaustive de toutes les situations à risques, cependant elles reprennent des épisodes de la vie quotidienne ayant trait à l'assistance médicale de nature urgente ou ordinaire, à la gestion de l'argent, au respect de l'intégrité physique et au respect de la vie privée du patient.

2.2 Motivations

Dans le cadre des habitats intelligents, les besoins en sécurité sont multiples. Une multitude d'appareils sont utilisés pour obtenir des informations et interagir avec les occupants. Ces appareils donnent des informations sur eux-mêmes ou sur les différents objets avec lesquels ils sont associés. Ils peuvent aussi transmettre ces informations à d'autres appareils. Par exemple, un capteur mesure la température de la pièce et la transmet au serveur d'événements de l'habitat intelligent. Cet ensemble d'appareils constitue un réseau dynamique, hétérogène et flexible qui sera notre réseau de capteurs.

Bien que ce type de réseau offre des possibilités immenses en termes d'utilisation et d'applications tous domaines confondus, ces réseaux sont également sujets à un grand nombre d'attaques. La transmission d'informations confidentielles, la transmission de fausses données, l'usurpation d'identité et l'accès non autorisé pour accéder à ces informations doivent être considérés sérieusement. Le respect de la vie privée du patient et le caractère confidentiel des informations générées et transitant par l'habitat intelligent doivent être considérés dès le départ.

En plus de la sécurité à garantir au niveau du réseau, certains de ces capteurs fournissent aux applications des données critiques en temps réel. Ceci oblige les déve-

loppeurs à répondre à davantage d'exigences de sécurité pour garantir que les informations critiques, mais aussi les services web et les réseaux qui relaient ces informations soient toujours disponibles.

Les techniques de sécurité usuelles telles que les infrastructures à clés publiques (ICP) ou la cryptographie, appliquées dans des réseaux traditionnels risquent de ne pas répondre à toutes les exigences des réseaux de capteurs où certains composants sont susceptibles de bouger souvent et ont des capacités de communication et d'exécution limitées et qui peuvent varier dans le temps. Le changement de contexte ne doit pas altérer le fonctionnement du service, mais les solutions de sécurité devront s'adapter à ce changement de contexte. Par exemple, un service d'assistance peut être disponible à l'intérieur de l'habitat par le biais de matériel informatique et du réseau local. Lorsque le patient quitte l'habitat, ce service peut être porté sur son téléphone intelligent. Les communications transiteront alors par le réseau de téléphonie sans-fil.

Les scénarios qui suivent traitent du suivi médical du patient à domicile et de l'accès partagé à certaines ressources critiques de l'appartement. Ils incluent de nombreux acteurs tels que le patient, la famille, les membres du personnel médical, d'autres personnes et de nombreux composants tels que les terminaux e-Santé du patient et de l'équipe médicale, les serveurs de l'hôpital et de l'habitat intelligent et les services web.

Ils requièrent également l'intégration d'appareils médicaux (par exemple, un oxymètre ou un électrocardiogramme), des données de l'environnement (par exemple, les données du réseau de capteurs de l'habitat), ainsi que des données du patient stockées dans l'habitat ou dans le dossier médical électronique.

Dans ce type d'applications, la qualité de vie du patient et le caractère privé des informations récoltées à son sujet doivent être respectés tout en permettant l'accès et l'échange de ces informations avec l'équipe médicale et la famille. La supervision du patient doit donc se faire de la manière la plus transparente possible tout en répondant aux besoins des différents acteurs et en satisfaisant les exigences de sécurité.

Le but de ces scénarios est de montrer des exemples concrets d'applications de l'habitat intelligent dans le contexte de la réhabilitation et du suivi médical à domicile du patient d'une part, et d'exposer les risques de sécurité et les solutions existantes ou à combler, d'autre part.

Les situations présentées dans ces scénarios ne sont pas exhaustives, mais ensemble elles reprennent les thématiques essentielles de la vie des personnes ayant des troubles cognitifs dans un habitat intelligent : la santé du patient, son suivi médical régulier et en cas d'urgence, la sûreté du patient et la protection de son intégrité physique et de sa vie privée, l'assistance lors de l'utilisation de moyens de paiement.

Ils servent de point de départ à l'illustration du quotidien d'un patient atteint de troubles cognitifs et de problèmes cardiaques dans un tel environnement et les risques de sûreté et de sécurité qui en découlent.

2.3 Les acteurs impliqués dans les scénarios

Cette section présente les différents acteurs impliqués durant le séjour du patient dans un habitat intelligent. Sans être exhaustive, la liste des acteurs comprend le patient lui-même, les membres de sa famille, les intervenants responsables de son suivi médical, les techniciens responsables du maintien en état de l'habitat. Leurs rôles et leurs caractéristiques sont détaillés ci-dessous :

— Le *patient* est le résident de l'habitat intelligent et a souscrit à un programme d'assistance pour être suivi médicalement et aidé dans la réalisation de ses activités de la vie quotidienne (AVQ). Il ou elle souffre de troubles cognitifs.
Plusieurs profils de patients sont à distinguer. D'une part, les cérébraux-lésés ont perdu une partie de leurs facultés cognitives suite à un traumatisme crânien. Ils sont de tous les âges. Leur suivi consiste à les réadapter progressivement à la vie quotidienne après leur accident pour leur rendre leur autonomie dès que possible. Ils sont donc sur la voie de la récupération d'une partie de leurs facultés cognitives. D'autre part, les personnes atteintes de la maladie d'Alzheimer sont en général des personnes situées à un âge avancé et leurs facultés cognitives décroissent progressivement. Leur suivi consiste à prolonger autant que possible leur autonomie.
À ces profils, s'ajoute celui des personnes en réadaptation suite à un Accident Vasculaire Cérébral (AVC). Ces personnes sont généralement à un âge avancé. Leur suivi consiste à les réadapter à la vie quotidienne. Ils souffrent également d'autres pathologies fréquemment rencontrées en raison de leur âge, par

exemple la maladie d'Alzheimer. En raison de leur problème cardiaque, elles portent un capteur en permanence dans le but d'enregistrer et de transmettre leur rythme cardiaque en continu à un centre de supervision et d'intervention d'urgence (CSIU).

Dans l'ensemble de ces profils, ces personnes peuvent vivre seules ou être en couple, avoir de la famille autour d'elles ou non, et doivent être suivies médicalement.

— Le *CSIU* s'apparente à un centre de réadaptation couplé à des services supplémentaires tels que la prise en charge d'urgence, la localisation du patient et la gestion de l'habitat intelligent. Il reçoit et gère les requêtes et les alertes déclenchées par le patient (assistance médicale et demandes d'intervention d'urgence). Il coordonne également les activités des différents acteurs incluant le médecin traitant et les différents intervenants. Il est responsable de l'entretien de l'habitat. Il se charge de prévenir les secours le cas échéant.

— Le *dossier médical électronique (DME)* représente le dossier médical du patient sous forme électronique. Il est utilisé par le CSIU pour coordonner la réhabilitation du patient et est composé de diverses informations telles que ses prescriptions, les notes écrites par les médecins et les différents intervenants, les données enregistrées par les capteurs médicaux et par les capteurs de l'habitat intelligent.

— Les *aidants professionnels* sont les personnes impliquées dans le suivi médical et la réadaptation du patient. Sans être exhaustive, la liste des intervenants inclu le gestionnaire de cas soit le coordinateur du suivi du patient, des médecins et des infirmiers, des psychologues, des physiothérapeutes et des préposés aux bénéficiaires. Ils peuvent être amenés à pratiquer leur soin au domicile du patient et ont besoin d'accéder au DME et de le mettre à jour.

— Les *techniciens* sont responsables du maintien en état de l'habitat intelligent. Cela consiste en l'entretien de la structure de l'habitat, du réseau informatique ou du réseau de capteurs. Il peut arriver qu'un technicien passe au domicile du patient pour mettre à jour de l'équipement, le réparer ou changer les piles des capteurs sans-fil.

— Les *aidants naturels* (la famille, le conjoint ou les amis du patient) sont parfois

présents autour du patient. Ils peuvent vivre lui dans le cas du conjoint, lui rendre visite régulièrement et l'aider à faire ses achats par exemple. Un aidant naturel peut avoir accès à l'appartement et agir comme le curateur du patient.

— Le *terminal e-santé* est le téléphone intelligent que porte sur lui le patient. Il est connecté aux capteurs que le patient porte et envoie les données récoltées au CSIU.

— L'*habitat intelligent (HI)* est le domicile du patient. Il est équipé de capteurs et d'effecteurs pour reconnaître l'activité réalisée par le patient et l'assister au besoin. Ceci est davantage expliqué dans la section 2.4.

2.4 L'environnement des mises en situation

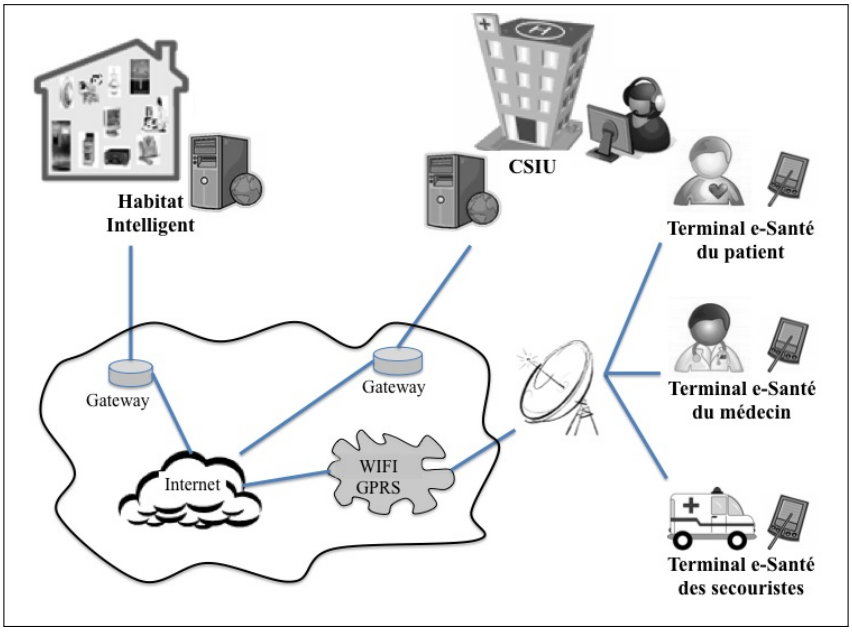

figure 2.1 – Environnement des mises en situation

L'environnement des mises en situation est l'habitat intelligent du patient. L'habitat intelligent est géré par un centre de réadaptation (CRE). Il consiste en un appartement conventionnel équipé de capteurs et d'effecteurs pour suivre et assister le patient dans ses activités de la vie quotidienne (AVQ) [40], [14], [15]. Des tapis tac-

tiles, des capteurs électromagnétiques, des détecteurs infrarouges et des débitmètres sont répartis dans l'habitat pour reconnaître l'activité réalisée par le patient et l'assister au besoin. Des microphones, des haut-parleurs et des caméras sont disponibles pour faciliter la communication entre le patient, le personnel médical et la famille. Un lecteur de cartes RFID est utilisé à l'entrée de l'habitat pour identifier les différents acteurs lors des visites à domicile.

L'habitat dispose d'une interface pour communiquer avec le CSIU en cas de demande d'assistance ou d'urgence. Une application tourne en tâche de fond pour envoyer régulièrement les données récoltées par les capteurs médicaux au CSIU. Le personnel médical peut également utiliser cette interface pour consulter le DME du patient lors des visites à domicile. La figure 2.1 présente l'infrastructure utilisée pour les communications entre l'habitat, le CSIU et les différents acteurs.

À l'intérieur de l'habitat, la communication s'effectue grâce à divers types de réseaux : sans-fil, Ethernet, Bluetooth, X-10 (courant porteur) et ZigBee.

2.5 Le scénario 1 – Assistance médicale à distance

Ce scénario aborde le sujet de l'assistance médicale à distance lorsque le patient ne se sent pas bien et envoie une requête d'assistance médicale auprès du CSIU. Il prend en compte l'acheminement de la requête auprès du médecin traitant ou d'un autre médecin disponible et la prise en charge du patient, l'accès aux dernières données médicales jusqu'à l'émission d'un rapport d'intervention.

2.5.1 Mise en situation de l'assistance médicale à distance

Dans ce contexte, le patient se trouve dans son appartement et a pris ses médicaments dans la matinée. Il ne se sent pourtant pas très bien et décide de demander de l'assistance à un médecin (1) (Figure 2.2). À partir de son terminal e-Santé, il envoie une requête d'assistance au CSIU qui s'assure de contacter son médecin traitant (2), un médecin de garde ou les secours en l'absence de réponse. Le médecin traitant est disponible et répond favorablement à sa demande d'assistance. Il utilise son terminal e-Santé pour confirmer sa prise en charge du patient et pour accéder

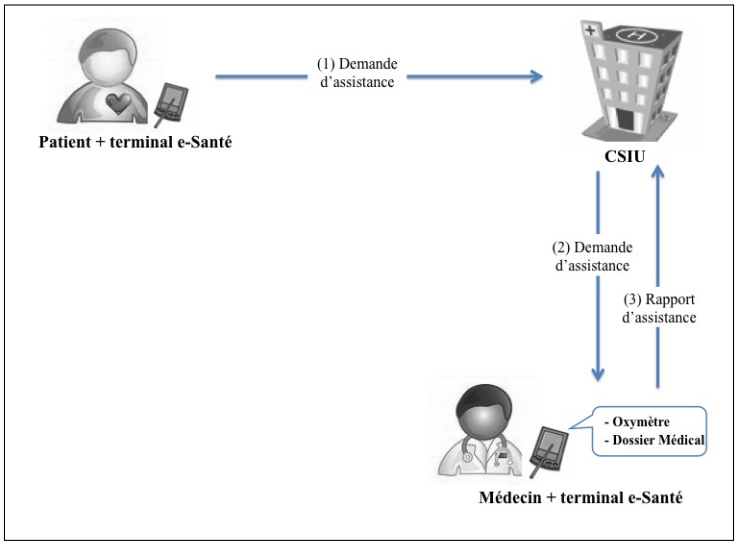

figure 2.2 – Scénario 1 - Assistance médicale à distance

aux dernières données collectées par les capteurs médicaux portés par le patient. Il appelle le patient à son appartement et le rassure en lui disant que les médicaments prennent normalement un certain temps à faire effet. Il lui propose de passer le voir le lendemain. Il ajoute l'événement à son calendrier et à celui du patient, puis clôt le processus d'assistance (3).

2.5.2 Problématique et besoins de sécurité, de fiabilité et de sûreté lors de l'assistance médicale à distance

Comme l'illustre la figure 2.2, le scénario porte sur la communication entre le patient et le médecin via le CSIU. Il nécessite de répondre à une multitude de problèmes de sécurité informatique tels que la non-répudiation, la disponibilité de service, le contrôle d'accès, l'intégrité et la confidentialité ainsi qu'à des problèmes de sûreté, par exemple la prise en charge automatique du processus métier de l'assistance. Ces besoins sont détaillés dans le tableau 2.1.

	Besoins
B 1	Les services du CSIU doivent être disponibles en tout temps.
B 2	L'intervenant qui accepte la prise en charge en assume la responsabilité et ne peut répudier la prise en charge par la suite.
B 3	Respecter le caractère privé des transmissions de données sensibles et en garantir la confidentialité, l'authenticité et l'intégrité.
B 4	Les intervenants qui participent à la prise en charge doivent être authentifiés.
B 5	Prévenir l'accès au DME aux personnes non autorisées.
B 6	Le patient doit porter les capteurs et son terminal e-Santé à l'extérieur.
B 7	Respecter un temps de réponse court même lorsqu'aucun médecin n'est disponible.
B 8	Le bon déroulement des différentes étapes de la prise en charge doit être garanti par le CSIU.

tableau 2.1 – Besoins de sécurité et de sûreté du scénario d'assistance médicale à distance.

2.6 Le scénario 2 – Intervention d'urgence

Ce scénario montre la prise en charge médicale du patient lors d'une situation où le patient requiert une assistance immédiate. Il prend en compte la notification auprès du CSIU que le patient soit conscient ou non, la recherche de sa localisation, la communication entre le CSIU et le service de secours et l'accès à ses dernières données médicales.

2.6.1 Mise en situation de l'intervention d'urgence

Le patient se trouve dans la cuisine lorsqu'il commence à se sentir mal. Il utilise son terminal e-Santé pour envoyer une requête d'urgence au CSIU (1) avant de s'évanouir dans le fauteuil (Figure 2.3). Les données médicales collectées par les capteurs que porte le patient sont transmises automatiquement par son terminal au CSIU. La requête d'urgence est acheminée au CSIU qui s'assure dans un premier temps que le patient est bien à son domicile en consultant les données des capteurs de l'habitat (2).

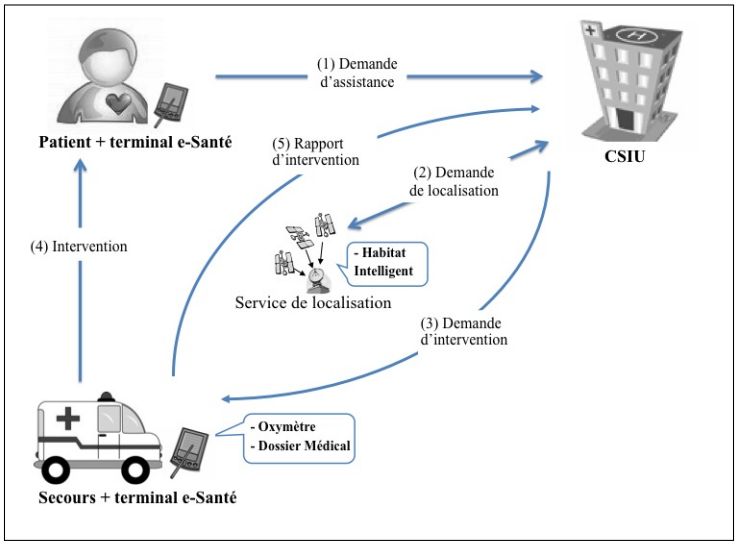

figure 2.3 – Scénario 2 - Intervention d'urgence

Le CSIU prévient ensuite les secours et leur envoie les coordonnées du patient (3). Les secouristes accusent réception de la requête par l'intermédiaire de leur terminal. En chemin, ils accèdent au DME du patient qui contient les dernières données médicales collectées par les capteurs qu'il porte sur lui. La lecture de ces données indique qu'il s'agit d'une crise cardiaque. Les secouristes se déplacent jusqu'au domicile du patient (4), parviennent jusqu'à lui et tentent de le réanimer. Sur la route de retour vers l'hôpital, ils préviennent l'hôpital de leur arrivée imminente. Lorsque le patient est pris en charge à l'hôpital, son DME est mis à jour (5) et le médecin traitant en est notifié. Le processus d'urgence prend fin.

L'origine de la requête d'assistance d'urgence peut varier, ce peut être le patient lui-même qui envoie la requête depuis son terminal, l'application de suivi médical de l'habitat intelligent ou le terminal porté qui détecte un problème cardiaque puis envoie la requête. Le médecin peut également déclencher la situation d'urgence suite à une demande d'assistance médicale (voir Scénario 1).

Si la requête d'urgence est envoyée par le patient depuis son domicile, le CSIU connaît déjà sa localisation et relaie directement les coordonnées du patient aux secouristes. Autrement la localisation du patient s'effectue depuis le CSIU en accédant au serveur de l'habitat intelligent qui fournit une liste des dernières activations de cap-

teurs ou les dernières coordonnées GPS du patient si celui-ci accepte d'être localisé en extérieur également.

Pour les patients atteints de schizophrénie, les fluctuations du rythme cardiaque peuvent indiquer une crise de panique. Dans ce cas, une intervention rapide est nécessaire, mais ne nécessite pas l'assistance de personnel médical. La requête peut-être redirigée vers un aidant naturel tel un membre de la famille ou un voisin.

2.6.2 Problématique et besoins de sécurité, de fiabilité et de sûreté lors d'interventions d'urgence

L'intervention d'urgence s'appuie sur le bon déroulement du processus de prise en charge du patient et de coordination des différents acteurs du scénario. Pour cela, il est nécessaire de mettre en place un système d'orchestration des services utilisés lors du processus. De plus, ce scénario nécessite de répondre à des besoins de sécurité informatique pour garantir le respect de la confidentialité, l'identité des intervenants et l'accès au DME par les personnes autorisées seulement. Ces besoins sont présentés dans le tableau 2.2.

2.7 Le scénario 3 – Visite à domicile des intervenants

Ce scénario décrit la visite d'un intervenant au domicile du patient pour le suivi médical et met en avant l'accès à distance au DME du patient et l'accès au réseau de capteurs, ainsi que le contrôle d'accès à ces ressources et le respect de la confidentialité.

2.7.1 Mise en situation des visites à domicile

Une visite d'un intervenant pour le suivi médical du patient est prévue depuis quelques jours au domicile du patient. Cet événement est inscrit au calendrier du patient par l'intermédiaire du CSIU et doit être confirmé par le patient. La description de l'évènement identifie le membre du personnel qui fera la visite ainsi que sa raison.

	Besoins
B 1	Les services du CSIU doivent être disponibles en tout temps.
B 2	L'intervenant qui accepte la prise en charge en assume la responsabilité et ne peut répudier la prise en charge par la suite.
B 3	Respecter le caractère privé des transmissions de données sensibles et en garantir la confidentialité, l'authenticité et l'intégrité.
B 4	Les intervenants qui participent à la prise en charge doivent être authentifiés.
B 5	Prévenir l'accès au DME aux personnes non autorisées.
B 6	Le patient doit porter les capteurs et son terminal e-Santé à l'extérieur.
B 7	Respecter un temps de réponse court même lorsqu'aucun médecin n'est disponible.
B 8	Le bon déroulement des différentes étapes de la prise en charge doit être garanti par le CSIU.
B 9	Le patient doit être localisé avant d'envoyer les secours.
B 10	Prévenir l'accès à la localisation du patient aux personnes non autorisées.

tableau 2.2 – Besoins de sécurité et de sûreté du scénario d'intervention d'urgence.

Cette mise en situation implique l'arrivée de l'intervenant au domicile du patient. L'intervenant peut avoir l'accès à l'appartement automatiquement. Cependant par respect pour la vie privée du patient et pour que le patient se sente chez lui, le visiteur sonne à la porte et attend de se faire inviter à l'intérieur.

Lors de l'examen médical, l'intervenant peut nécessiter de consulter le DME et le mettre à jour, et accéder aux dernières données capteurs (Figure 2.4).

2.7.2 Problématique et besoins de sécurité, de fiabilité et de sûreté lors de visites à domicile

Plusieurs problèmes de sécurité, de fiabilité et de sûreté peuvent survenir dans ce scénario. Les troubles cognitifs du patient peuvent engendrer des pertes de mémoire. Le patient peut oublier la visite ou ne pas reconnaître l'intervenant qui sonne à la porte, ce qui peut créer des situations de confusion entre le patient et l'intervenant.

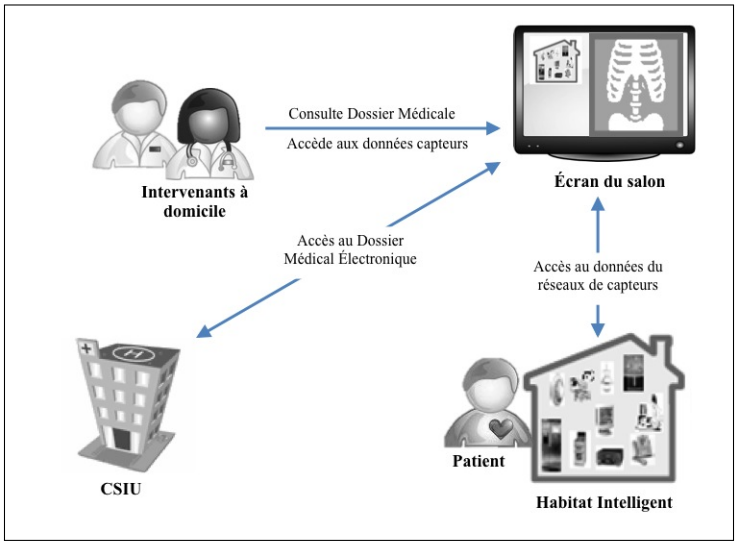

figure 2.4 – Scénario 3 - Visite à domicile des intervenants

Il se peut également que la personne à la porte ait de mauvaises intentions vis-à-vis du patient (démarcheur, fraudeurs ...). Un moyen de reconnaissance des personnes connues du CSIU est nécessaire pour éviter les situations de confusion d'une part, et les situations à risques pour le patient d'autre part. Dans certains cas, il peut arriver des cas exceptionnels dans lesquels un membre du personnel soignant requiert l'accès au réseau de capteurs pour des raisons médicales, mais n'est pas autorisé à y accéder. Un compromis entre le contrôle d'accès strict et l'autorisation exceptionnelle pourrait être mis en place.

Ce scénario implique de répondre à des besoins de sécurité et de sûreté pour garantir le maintien du patient à domicile dans de bonnes conditions. Le tableau 2.3 détaille les principaux besoins identifiés et met en évidence les aspects suivants : la non-répudiation, la disponibilité de service, le contrôle d'accès, l'intégrité, la confidentialité, le respect de la vie privée et la fiabilité.

2.8 Le scénario 4 – Accès à l'appartement

Ce scénario montre la gestion de la porte d'entrée à distance par un préposé aux bénéficiaires en cas d'urgence, d'oubli de la carte d'identité du personnel ou en cas

	Besoins
B 1	Les services du CSIU doivent être disponibles en tout temps.
B 2	L'intervenant qui accepte la prise en charge en assume la responsabilité et ne peut répudier la prise en charge par la suite.
B 3	Respecter le caractère privé des transmissions de données sensibles et en garantir la confidentialité, l'authenticité et l'intégrité.
B 4	Les intervenants qui participent à la prise en charge doivent être authentifiés.
B 11	L'affichage du DME au domicile du patient, seuls le patient et le médecin doivent être dans la pièce utilisée pour la consultation.
B 12	L'identité de l'intervenant et le but de sa visite doivent être connus pour rappel au patient.
B 13	Un intervenant disposant d'un accès limité aux réseaux de capteurs, peut avoir une nécessité ponctuelle et limitée dans le temps d'avoir accès à plus d'information.

tableau 2.3 – Besoins de sécurité et de sûreté du scénario de visite à domicile des intervenants

de suspicion de la part du patient.

2.8.1 Mise en situation des accès à l'appartement

Le patient se trouve dans son appartement lorsque la sonnerie de la porte d'entrée retentit. L'image de la personne à l'extérieur s'affiche à l'écran du salon, mais aucune information concernant l'identification du visiteur ou concernant une éventuelle visite prévue aujourd'hui n'apparaît à l'écran.

Le patient a la possibilité de communiquer avec son visiteur qui lui indique qu'il doit vérifier l'état du réseau de capteurs de son domicile. Ne se sentant pas très à l'aise avec cette visite imprévue, le patient appuie sur le bouton d'assistance disponible sur l'écran du salon. Une alerte arrive au standard du CSIU indiquant que le patient est chez lui et qu'un visiteur attend à la porte. Le préposé du CSIU appelle le patient pour lui confirmer l'information puis communique avec l'éventuel technicien qui attend toujours à la porte.

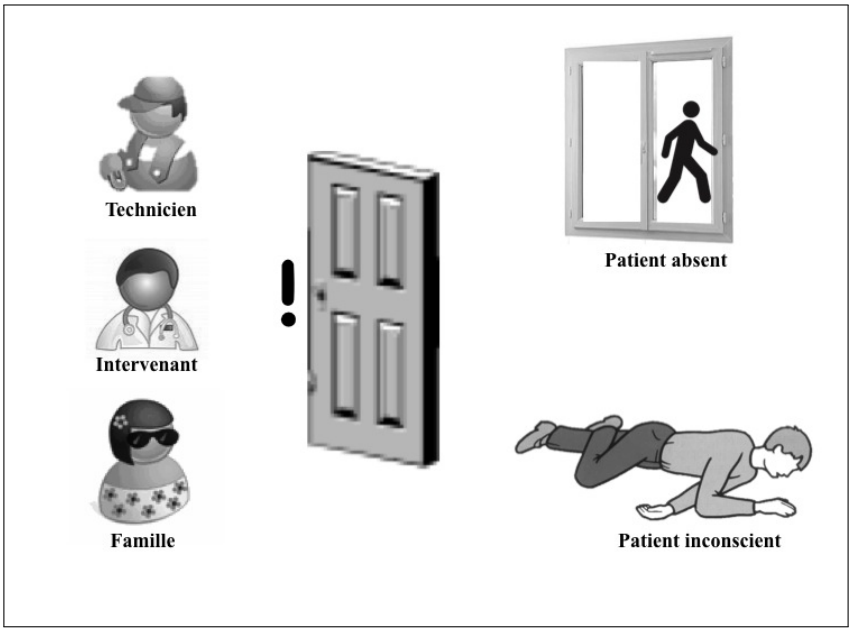

figure 2.5 – Scénario 4 - Accès à l'appartement

Après vérification de la part du CSIU, il s'avère que cette visite avait été approuvée par le CSIU quelques jours plus tôt, mais que l'événement n'avait pas été ajouté au calendrier pour une quelconque raison. Le préposé communique à nouveau avec le patient pour lui expliquer la situation et lui demande d'ouvrir la porte. Le patient accepte et ouvre la porte au technicien.

2.8.2 Extensions du scénario 4

Le déroulement normal du scénario implique la présence du patient pour ouvrir la porte au membre du personnel du CSIU. Il faut toutefois prendre en compte quelques alternatives :

— Si une visite est prévue lors de l'absence du patient, mais que ce dernier a donné préalablement son autorisation, le technicien peut soit utiliser un badge pour s'identifier à la porte, soit demander l'accès à l'appartement auprès du CSIU une fois sur place.

— Dans le cas d'une situation d'urgence durant laquelle le patient est présent dans l'appartement, mais peut être inconscient, les secours peuvent alors demander

directement l'accès de l'appartement auprès du CSIU.

2.8.3 Problématique et besoins de sécurité, de fiabilité et de sûreté liés à l'accès à l'appartement

Le tableau 2.4 présente une liste non exhaustive d'exigences de sécurité liée au scénario 4 et met en évidence les aspects suivants : la non-répudiation, la disponibilité de service, le contrôle d'accès, l'intégrité, la confidentialité, le respect de la vie privée et la fiabilité.

	Besoins
B 14	L'accès à l'appartement doit se faire sans clé.
B 15	Restreindre l'accès à l'appartement aux personnes autorisées seulement.
B 16	Autoriser un intervenant ou un groupe spécifique d'intervenant à accéder à l'appartement dans une situation d'urgence.
B 17	Garder une liste des personnes qui entrent dans l'appartement.
B 18	Prévenir la présence ou la fréquence de visite de certains visiteurs.

tableau 2.4 – Besoins de sécurité et de sûreté du scénario d'accès à l'appartement

2.9 Le scénario 5 – Utilisation des moyens de paiement

Ce scénario présente la situation relative à l'usage de l'argent et la problématique qui en résulte dans le quotidien des personnes ayant des troubles cognitifs.

2.9.1 Mise en situation lors de l'utilisation des moyens de paiement

Les troubles causés par la maladie d'Alzheimer ou par un traumatisme crânien ont des conséquences directes sur la manière dont les personnes qui en sont atteintes gèrent leur argent. Les premières sont principalement victimes de leurs pertes de mémoire. Elles peuvent oublier de payer leurs factures ou les payer plusieurs fois, dépenser de fortes sommes d'argent, puis en oublier les raisons. Elles sont aussi facilement les victimes d'escroquerie. Les secondes sont également victimes de leur impulsivité découlant de leur traumatisme. Elles dépensent sous le coup de leurs émotions pour des achats dont elles n'ont pas l'utilité, et dont le prix peut être au-delà de leur capacité financière.

Une assistance dans la gestion des paiements est donc nécessaire pour assurer le maintien à domicile du patient. Les techniques actuelles consistent bien souvent en la mise sous tutelle du patient. Ses moyens de paiement et les sommes dépensées sont alors supervisés par un curateur. Dépendamment de sa capacité à gérer ses finances, le patient disposera de ses cartes de crédit et de ses chéquiers avec la nécessité d'obtenir la co-signature du curateur au-delà d'une somme spécifiée. Dans d'autres cas, une somme d'argent lui est remise en espèces à intervalles réguliers.

2.9.2 Problématique et besoins de sécurité, de fiabilité et de sûreté liés aux moyens de paiement

Un patient pourrait avoir à payer pour la livraison de ses médicaments, pour un fournisseur de service reconnu ou non par le CSIU ou se retrouver face à un démarcheur sans scrupule (Figure 2.6). Pour le protéger contre les escroqueries et le prémunir contre un mauvais usage de son argent, une assistance plus avancée est nécessaire lors de l'utilisation de ses moyens de paiement. Cette assistance devra apporter une réponse aux besoins de sécurité et de sûreté énumérés dans le tableau 2.5.

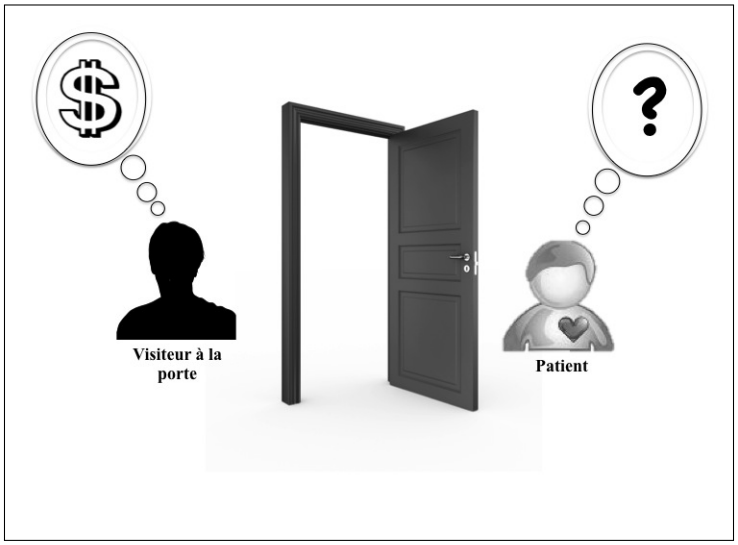

figure 2.6 – Mise en situation 5 - Utilisation des moyens de paiement

2.10 Conclusion

Ce chapitre présente cinq scénarios qui illustrent des situations de la vie quotidienne d'un patient dans un habitat intelligent. Ils abordent la problématique du maintien à domicile d'un patient et prennent en compte les dimensions du domaine de la santé, des troubles cognitifs du patient, et les spécificités des habitats intelligents. L'environnement et les acteurs impliqués sont également décrits.

Ces scénarios servent à identifier les besoins de sécurité, de fiabilité et de sûreté auxquels les développeurs devront répondre dans leurs applications dédiées aux habitats intelligents. Ces besoins détermineront quelles solutions devront être trouvées et décrites sous forme de patrons pour créer un catalogue de patrons de sécurité, de fiabilité et de sûreté dédié aux habitats intelligents pour personnes ayant des troubles cognitifs.

	Besoins
B 4	Les intervenants qui participent à la prise en charge doivent être authentifiés.
B 12	L'identité de l'intervenant et le but de sa visite doivent être connus pour rappel au patient.
B 19	Savoir quand un moyen de paiement est utilisé.
B 20	Prévenir toute dépense au-delà d'un certain montant.
B 21	Prévenir le gestionnaire de cas ou le tuteur lors de l'utilisation de moyens de paiement en présence de personnes inconnues ou en présence de personnes spécifiques.

tableau 2.5 – Besoins de sécurité et de sûreté lors de l'utilisation des moyens de paiement.

Chapitre 3

Les objectifs et la méthodologie

Le Chapitre 1 soulève les problèmes de sécurité informatique et de sûreté des patients dans le contexte des habitats intelligents, puis le Chapitre 2 illustre des situations ou l'habitat intelligent (HI) peut soit remédier à ces problèmes, soit en amener de nouveaux.

Pour démocratiser les HI, il faut rendre possible le bon déroulement des scénarios du Chapitre 2 en abordant ces problèmes bien réels et complexes qui mêlent les particularités de l'architecture des HI, des troubles cognitifs de leurs occupants et du caractère médical des données et des interactions interpersonnelles.

Des solutions techniques ou des stratégies d'implémentation doivent être mise en place pour cela, et être à la disposition des concepteurs d'HI et des développeurs d'applications pour en faciliter l'usage. Mais dans ce cas, il faut présenter ces solutions de sorte que leur concept soit bien compris et que leur déploiement puisse être adapté aux diverses conceptions des HI.

Une approche par catalogue de patrons de sécurité est proposée ici pour offrir cette boite à outils de solutions. Cette approche a été présentée lors de la conférence ICOST 2010 dans l'article *Security, Privacy, and Dependability in Smart Homes : A Pattern Catalog Approach* [25] (voir Annexe A).

Ce chapitre propose une marche à suivre jusqu'à la création de ce catalogue (Figure 3.1). La section 3.1 présente les objectifs de la thèse en se basant sur les constats

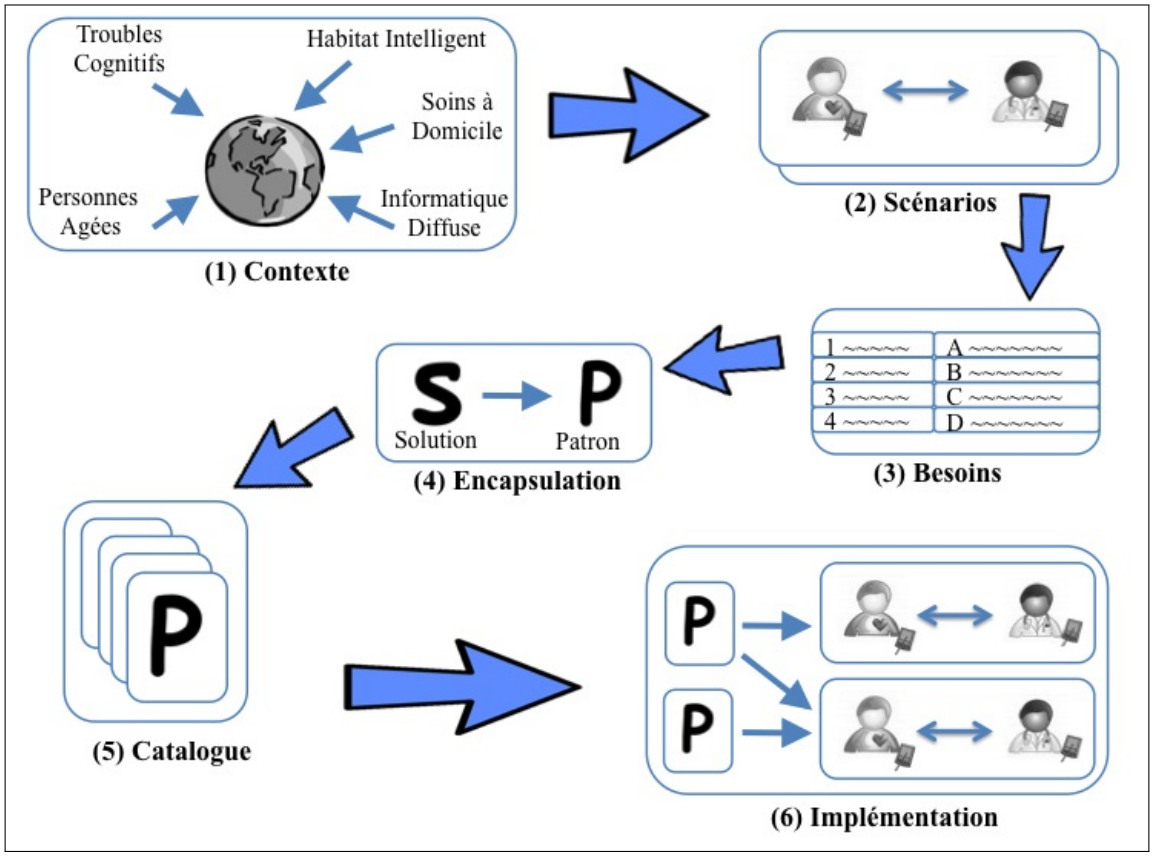

figure 3.1 – Méthodologie de l'approche par catalogue

des chapitres précédents et la liste des livrables pour les atteindre. Les sections suivantes présentent la méthodologie pour chacun de ces objectifs, soit la rédaction des spécifications à partir des scénarios et des caractéristiques des HI, des patients et de leurs troubles cognitifs (Section 3.2), la création des patrons et du catalogue (Section 3.3) et finalement l'implantation de certains patrons pour en valider le concept (Section 3.4).

3.1 Les objectifs

Pour assurer la sûreté des occupants et la sécurité informatique au sein d'un habitat intelligent, il est nécessaire d'analyser les spécificités de ce contexte et d'en extraire une meilleure vision des besoins pour apporter des solutions adéquates. Quels

sont les problèmes de sécurité et de sûreté qui surviennent lors du maintien à domicile d'une personne souffrant de troubles cognitifs ? Comment respecter la vie privée d'une personne lorsque celle-ci est entourée de capteurs qui détectent et enregistrent chacune de ses actions ? En quoi l'informatique diffuse peut-elle améliorer le travail de coordination du personnel médical et améliorer la sûreté de ses occupants tout en se conformant au respect des règles de sécurité informatique en vigueur ?

Certaines de ces solutions de sûreté, de fiabilité et de sécurité sont à définir et à raffiner à partir des solutions déjà existantes, et peuvent être réutilisées telles quelles ou adaptées à notre contexte. D'autres devront être inventées et implémentées entièrement en tirant profit de l'architecture particulière des HI et de l'omniprésence des actuateurs, des capteurs et des écrans répartis dans l'appartement.

Enfin, ces solutions doivent être distribuées sous une forme claire, compréhensible, et de sorte à être réutilisées et adaptées facilement dans d'autres HI et par l'ensemble des développeurs dans un catalogue.

Les objectifs de cette thèse se composent des trois points suivants :

1. *Identifier les besoins* : Identifier les besoins spécifiques à notre contexte au plan médical, légal, des troubles cognitifs et de l'informatique diffuse : En partant des scénarios du Chapitre 2, il est possible de caractériser chacun des acteurs qui composent le contexte d'étude ; l'habitat intelligent, les personnes qui y vivent ou y travaillent et les problèmes inhérents à l'univers qu'ils composent. Puis, à partir de ces informations, identifier dans un tableau les besoins auxquels il faut répondre pour soutenir le bon déroulement du scénario et organiser les futures entrées du catalogue. Cet objectif est détaillé dans la section 3.2 et correspond à l'étape 3 de la figure 3.1.
2. *Créer le catalogue* : Trouver ou composer les solutions adéquates aux scénarios du Chapitre 2, et les rendre accessibles et réutilisables : Des solutions existent déjà et peuvent être adaptées ou utilisées telle quel parfois. Sinon, il faut en implémenter de nouvelles. Par exemple, les solutions pour assurer la confidentialité des données seront semblables à celles appliquées dans d'autres domaines, mais dans le cas de l'utilisation d'appareils mobiles aux ressources limitées, elles doivent parfois être adaptées. Par la suite, ces solutions doivent être encapsulées pour être regroupées dans un catalogue. Cet objectif est détaillé dans la section

3.3 et correspond aux étapes 4 et 5 de la figure 3.1.

3. *Implanter des patrons* : Implanter une sélection de patrons pour les valider. Développer, implémenter et intégrer une partie des patrons dans le milieu réel. Cet objectif est détaillé dans la section 3.4 et correspond à l'étape 6 de la figure 3.1.

3.2 L'identification des besoins

La rédaction des spécifications passe par la connaissance des besoins des patients et de leur trouble cognitif, des aidants et des développeurs, et par la compréhension de ce que l'HI peut apporter comme avantages et inconvénients au bon déroulement des scénarios.

L'identification des problèmes de sécurité dans le contexte des habitats intelligents peut s'effectuer en couvrant les trois dimensions suivants : les besoins des développeurs d'applications destinées aux habitats intelligents, aux résidents et aux aidants, les problèmes de sécurité qu'engendre l'infrastructure de ce type d'habitat, et les besoins spécifiques de sécurité liés aux troubles cognitifs.

3.2.1 Les besoins des développeurs

Sécuriser les applications destinées aux habitats intelligents nécessite d'être à l'écoute des développeurs et de leurs besoins en matière de sécurité. Il est fréquent de devoir identifier ou authentifier un utilisateur avant de le laisser évoluer dans l'application ou de devoir chiffrer les messages échangés entre les différents intervenants. Pour autant, ces aspects sont souvent mis de côté ou remis à plus tard par les développeurs, car jugés non primordiaux pour le bon fonctionnement de leur application. Certaines fonctions essentielles sont alors vite comblées pour les besoins de l'application sans toutefois garantir fiabilité et sécurité dans une utilisation concrète. La connaissance des besoins permettrait d'identifier les premiers problèmes de sécurité à résoudre.

3.2.2 Les besoins liés à l'infrastructure des habitats intelligents

L'infrastructure d'un HI oblige également à penser autrement en matière de sécurité. L'omniprésence de capteurs et la génération d'évènements impliquent le transit, le partage et l'accès d'une multitude de données entre diverses applications et divers acteurs. Ces données doivent être protégées à des fins de confidentialité, de respect de la vie privée et de sûreté. L'assistance du patient en extérieur nécessite également le même niveau de protection. Enfin, cette infrastructure soulèverait des problèmes d'éthique si des garde-fous n'étaient pas mis en place pour préserver l'accès aux données uniquement aux personnes autorisées. L'infrastructure doit donc être prise en considération quant aux problèmes de sécurité qu'elle engendre.

3.2.3 Les besoins liés aux troubles cognitifs

Le dernier axe à suivre concerne les troubles cognitifs de l'occupant. Augmenter l'autonomie d'un patient souffrant de troubles cognitifs nécessite de remplacer des procédés trop gourmands en ressources cognitives (tel que la mémorisation d'un mot de passe par exemple) par des procédés mieux adaptés aux troubles dont souffre l'occupant. De plus, même temporaire, l'absence d'aidant livre le patient à lui-même dans des situations de colportage ou d'escroquerie au porte-à-porte. La prise en compte des troubles cognitifs est donc à considérer lors de l'étape d'identification des problèmes de sécurité.

3.3 La création d'un catalogue de patrons de sécurité, de fiabilité et de sûreté

Un catalogue de patrons de sécurité est une collection de patrons de sécurité accompagnés de directives d'implémentation, de combinaison de patrons et d'utilisation de ces patrons. Un catalogue permet à la fois aux auteurs de patrons d'organiser leurs solutions de sécurité et aux développeurs de les consulter et de choisir le patron adéquat. Bien que des catalogues de patrons existent déjà (en matière de design [39],

d'architecture et de sécurité [90], [89], [51]), aucun catalogue ne prend en compte les dimensions des habitats intelligents et des troubles cognitifs.

Un catalogue aide les développeurs à choisir les solutions de sécurité en correspondance avec leurs besoins et le contexte d'utilisation. Beaucoup d'éléments reviennent régulièrement dans notre contexte tels que le réseau de capteurs, l'usage de téléphones intelligents et les troubles cognitifs ; ce qui a un impact majeur dans l'application de certaines solutions de sécurité. Un catalogue tenant compte de ces différences apporterait une grande aide aux développeurs du milieu des habitats intelligents.

Un catalogue destiné aux développeurs d'applications pour les habitats intelligents et pour personnes souffrant de troubles cognitifs reste donc à créer pour qu'ils puissent disposer d'un ouvrage prenant en compte leur contexte dés le départ.

3.4 L'implantation de patrons pour les valider

Le dernier objectif de notre thèse consiste à valider la réalisation des objectifs précédents en intégrant certains patrons dans l'infrastructure et les applications principales du laboratoire DOMUS. À mesure que l'identification des besoins et la création de patrons progressent, il deviendra possible de valider notre travail en testant l'utilisation des patrons et du catalogue.

Dans un premier temps, les patrons créés seront proposés aux développeurs pour qu'ils les intègrent à leur application. Cette étape permettra de tester la compréhension du patron et sa facilité d'implémentation par les développeurs et sera l'occasion de bénéficier d'une rétroaction de leur part.

De la même manière, l'utilisation du catalogue sera mise à l'épreuve pour tester l'organisation et l'aide apportée aux développeurs dans leur choix de patrons. Cette étape sera importante lors de l'étude de la combinaison de patrons.

3.5 Conclusion

Ce chapitre présente les objectifs fixés dans le cadre de notre thèse. La création d'un catalogue de sécurité, de fiabilité et de sûreté passe par l'identification des besoins de sécurité, de fiabilité et de sûreté. Cette identification des besoins s'appuiera sur les

cinq scénarios du Chapitre 2 et devront prendre en compte plusieurs dimensions telles que celles relatives aux troubles cognitifs du patient et celles relatives à l'infrastructure particulière des habitats intelligents.

À partir de ces besoins, des solutions seront créées ou adaptées à partir de solutions couramment rencontrées dans d'autres domaines. Ces solutions seront décrites sous forme de patrons et regroupées dans un catalogue (Chapitre 4).

Finalement, des patrons du catalogue seront implantés pour les valider (Chapitre 5).

Chapitre 4

Catalogue

Ce chapitre présente le catalogue de patrons de sécurité, de fiabilité et de sûreté dédié aux habitats intelligents (HI), soit la première partie des résultats. La seconde partie traitant de l'application des patrons dans les scénarios est présentée dans le Chapitre 5.

Dans le Chapitre 2, des scénarios illustrent les interactions entre le patient, le personnel soignant ou de maintenance, les proches du patient, l'HI et ce qui le compose. Ces scénarios sont la source des besoins de sécurité, de fiabilité et de sûreté dans le domaine des HI. Les patrons de ce catalogue décrivent des solutions pour répondre à ces besoins.

Ce chapitre est organisé ainsi : la section 4.1 présente le but du catalogue et explique à qui il s'adresse. La section 4.2 présente la structure d'un patron, la section 4.3 présente l'organisation du catalogue. Finalement la section 4.4 présente la liste des patrons. Les patrons suivent directement cette section.

4.1 Le but du catalogue

L'objectif de ce catalogue est de fournir aux développeurs des HI des solutions de sécurité, de fiabilité et de sûreté qui correspondent aux besoins du domaine des HI et qui prennent en compte les dimensions du domaine de la santé et des troubles

cognitifs des patients. Après avoir exprimé ses besoins, le développeur peut parcourir le catalogue pour y trouver le patron ou l'ensemble de patrons qui y répond.

Le catalogue s'adresse principalement à des développeurs du domaine des HI. Avoir des connaissances en informatique est très utile pour le lire, mais pas systématiquement nécessaire. Par exemple, les patrons de sécurité et de fiabilité nécessitent plus de connaissances en informatique que ceux de sûreté. Ces derniers nécessitent plus de connaissance dans les spécificités du maintien dans un HI de personnes ayant des troubles cognitifs.

Il n'est cependant pas nécessaire d'avoir des connaissances en sécurité, en fiabilité ou en sûreté pour le lire. Les éléments essentiels à la compréhension du problème et de sa solution sont présentés de sorte à englober tout le savoir de sécurité, de fiabilité ou de sûreté nécessaire à sa compréhension.

Avoir des connaissances dans les domaines des HI est utile, car certaines solutions requièrent que le développeur connecte son application aux serveurs, capteurs et effecteurs de l'environnement ubiquitaire.

4.2 La composition d'un patron

Cette section présente les éléments qui composent un patron de sécurité, de fiabilité ou de sûreté. Ces éléments sont les suivants :

- **Nom :** Le nom du patron décrit le patron de la manière la plus concise et représentative possible.
- **Alias :** Les autres noms rencontrés pour ce patron.
- **Résumé :** Le résumé du patron décrit brièvement le problème et la solution,
- **Problème :** Cet élément décrit le contexte et le problème spécifique auquel la solution apporte une réponse.
- **Particularités contextuelles :** Cet élément met en avant les spécificités du contexte des troubles cognitifs (TC), du domaine de la santé et de l'habitat intelligent (HI).
- **Solution :** La solution décrit en quoi le patron résout le problème précédemment soulevé. Elle peut également contenir les contremesures qui doivent être appliquées pour limiter le risque et les choses à ne pas faire pour appliquer

correctement la solution. Lorsqu'un problème peut avoir plusieurs solutions, cette section explique en quoi cette solution est à choisir parmi d'autres.

— **Conséquences :** Cet élément liste les conséquences de l'utilisation de ce patron. Cela peut concerner l'utilisabilité de l'application, la réduction des performances, etc.

— **Patrons en lien :** Les patrons qui ont rapport avec le patron courant. Ce sont généralement les patrons qui vont de pair ensemble.

— **Références :** Les références d'autres recherches et études sur lesquelles s'appuie la solution ou qui expliquent d'avantage la problématique.

4.3 L'organisation du catalogue

Cette section présente l'organisation des patrons du catalogue. Les patrons correspondent à une ou plusieurs catégories : la catégorie sûreté, la catégorie fiabilité et la catégorie sécurité.

— La sûreté concerne tout ce qui touche à l'intégrité physique du patient ou à celle de ses biens. Par exemple, la protection de ses moyens de paiement ou la vérification de l'identité de ses visiteurs.

— La fiabilité concerne tout ce qui rend l'infrastructure informatique fiable, par exemple, assurer la disponibilité des services critiques.

— La sécurité concerne tout ce qui touche à la sécurité informatique du système d'information, par exemple, le respect de la confidentialité ou la restriction de l'accès au système aux seules personnes autorisées.

Chacun des patrons contient un élément nommé "Particularités contextuelles". Cet élément du patron est la section qui traite des spécificités des trois domaines suivants : le domaine de la santé, celui des habitats intelligents (HI) et celui des troubles cognitifs (TC). Dans cette section, les particularités contextuelles entre ces trois domaines et le patron courant sont mises en avant.

— Santé : Le domaine de la santé englobe une structure particulière, un système d'information qui lui est propre, du personnel soignant dans différentes spécialités médicales, etc.

— HI : L'habitat intelligent possède une multitude de capteurs et d'effecteurs qui

sont parfois à prendre en compte dans la problématique et la solution proposée dans le patron.

— TC : La problématique provient souvent des troubles cognitifs du patient notamment pour les patrons de sécurité. Les TC ont également un impact sur le choix des solutions présentées.

4.4 Les patrons

Le tableau 4.1 liste les 18 patrons de sécurité, de fiabilité et de sûreté du catalogue. Les patrons sont présentés dans l'ordre de la liste à partir de la page suivante.

Les relations entre les patrons sont représentées dans la figure 4.1. Un patron est en relation avec un autre lorsqu'il s'appuie sur celui-ci ou est souvent utilisé avec, comme l'authentification (Patte Blanche) et le contrôle d'accès par exemple (Cerbère). Ils sont souvent utilisés ensemble mais peuvent être utilisés individuellement.

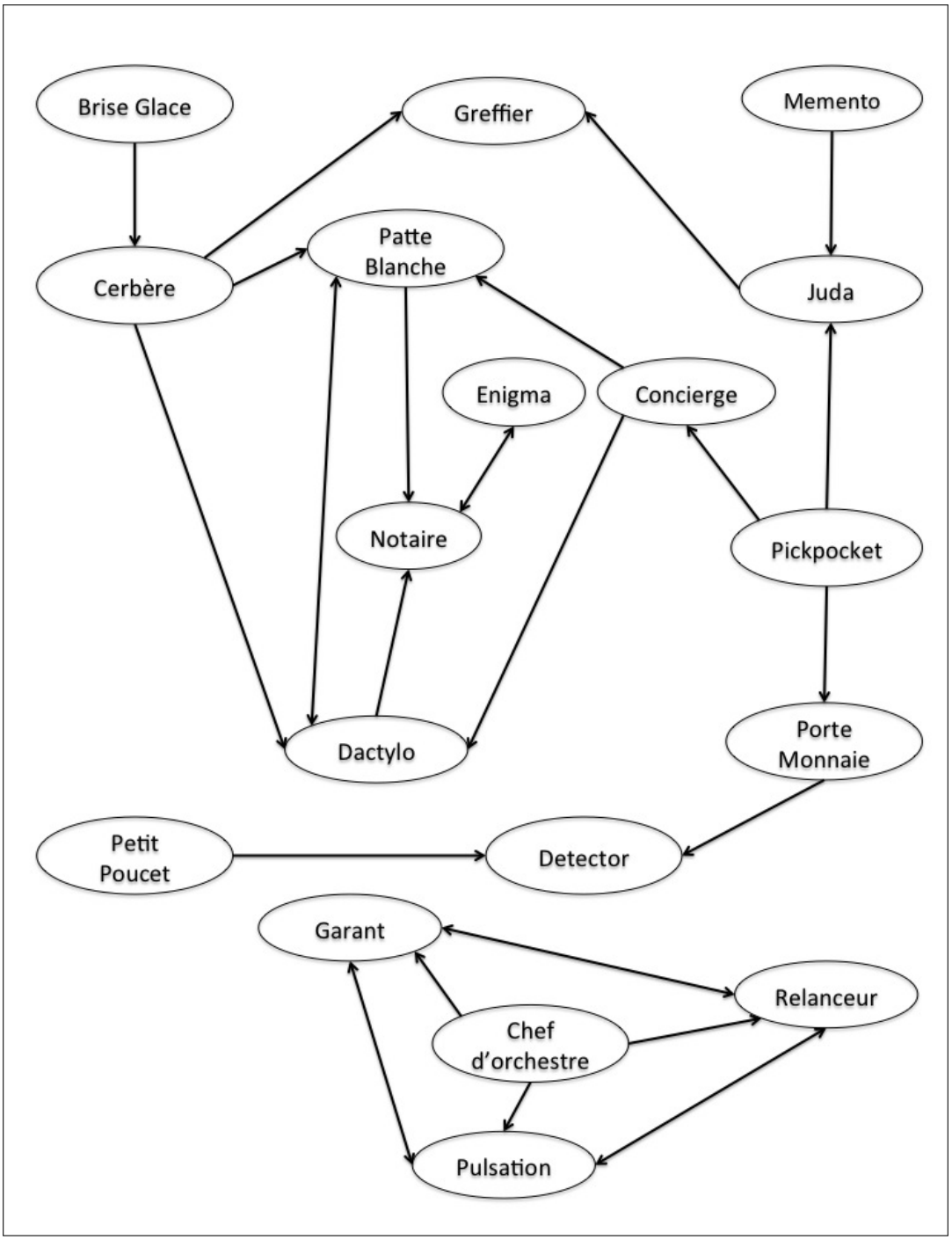

figure 4.1 – Relations entre patrons

	Noms	**Description**	**Type**	**Liens**
1	Chef d'orchestre	Orchestration de service web	Fiabilité, Sûreté	Santé, HI
2	Concierge	Suivi des présences	Sûreté	HI, TC
3	Petit Poucet	Localisation du patient	Sûreté	Santé, HI, TC
4	Memento	Rappel du contexte d'une visite	Sûreté	Santé, HI, TC
5	Detector	Détection d'objet	Sûreté	HI, TC
6	Porte-monnaie	Suivi des dépenses	Sûreté	HI, TC
7	Pickpocket	Contextualisation des paiements	Sûreté	HI, TC
8	Juda	Photographie des visiteurs	Sûreté	HI, TC
9	Relanceur	Mise en mémoire tampon des requêtes d'assistance	Fiabilité, Sûreté	Santé, HI, TC
10	Cerbère	Contrôle d'accès basé sur les rôles	Sécurité, Sûreté	Santé, HI
11	Brise-glace	Outrepasser temporairement ses droits d'accès	Sécurité, Sûreté	Santé, HI, TC
12	Greffier	Journal des évènements	Sécurité, Sûreté	Santé, HI, TC
13	Patte blanche	Authentification des intervenants	Sécurité, Sûreté	Santé, HI, TC
14	Dactylo	Reconnaissance des empreintes digitales	Sécurité, Sûreté	Santé, HI, TC
15	Enigma	Chiffrement des communications	Sécurité, Sûreté	Santé, HI
16	Notaire	Signature électronique	Sécurité, Sûreté	Santé
17	Garant	Disponibilité des services web	Fiabilité, Sûreté	Santé, TC
18	Pulsation	Détection de l'indisponibilité des services web	Fiabilité, Sûreté	Santé, TC

tableau 4.1 – Liste des patrons de sécurité, de fiabilité et de sûreté

Chef d'orchestre

Alias : Orchestration de services web, flux de travail, flux de travaux, automatisation de processus métier, workflow.

Type : Fiabilité et sûreté.

Résumé

Ce patron aborde l'automatisation des flux de travail pour réaliser des séquences d'opérations automatiques incluant des services web et des opérations réalisées par des personnes.

Lorsque programmé de façon ad hoc, il devient difficile de suivre le déroulement d'un flux de travail et de savoir s'il se termine correctement. À cela s'ajoute le problème de la détection d'erreur. Dans le contexte de prise en charge urgente d'un patient, cela amène des problèmes de fiabilité et de sûreté du flux de travail.

L'utilisation d'un moteur d'orchestration de service web permet de remédier à cela.

Problème

Le domaine de la santé s'appuie largement sur une architecture orientée services car elle facilite l'accès et l'échange d'information aussi bien entre les équipes et leurs départements en interne qu'entre les organisations externes.

La prise en charge d'un patient à domicile nécessite l'utilisation d'une série de services web dont les appels successifs et les informations spécifiques à une prise en charge représentent un processus qui requiert une certaine organisation [18].

Chef d'orchestre

Pour mettre un flux de travail en place dans une architecture orientée services, les points suivants doivent être pris en compte :

— L'organisation des acteurs : Il y a une multitude de services en liens, ceux-ci doivent être appelés dans le bon ordre et en leur fournissant les bonnes informations.

— La prise de décisions : Selon la valeur d'un paramètre, le flux empruntera un chemin ou un autre.

— Les interruptions et reprises de processus : Il arrive qu'un flux soit mis en suspend puis repris comme lors d'une intervention humaine. Dans ce cas, l'interruption donne le contrôle à une personne pour effectuer une tâche. Une fois terminé, le flux reprend.

— Le transit d'information contextuelle : L'information contextuelle, soit les informations relatives au flux de travail en cours sont communiquées d'un service à l'autre.

Il est possible de coordonner les services ensembles de manière ad hoc, mais cela :

— ne prend pas en compte la détection d'erreur dans une instance d'un processus,

— ne prend pas systématiquement la reprise d'une instance d'un processus,

— engendre plus de maintenance lors de la modification d'un service web,

— complique le suivi des processus en cours.

Particularités contextuelles

Santé : Le domaine de la santé comprend un très grand nombre de flux de travail. Par exemple, la prise en charge d'un patient inclut un enchaînement de services entre l'admission, les consultations, les interventions médicales et sa sortie de l'établissement. Un flux de travail impliquant des services web permet d'automatiser les processus complexes du domaine de la santé, d'avoir un suivi du début à la fin d'une prise en charge, de voir les prises en charge en cours et leur statut, et d'y avoir accès depuis l'extérieur.

HI : Les flux de travail peuvent être mis en place dans un HI, par exemple pour suivre le déroulement d'activités comportant plusieurs services. Un flux de travail

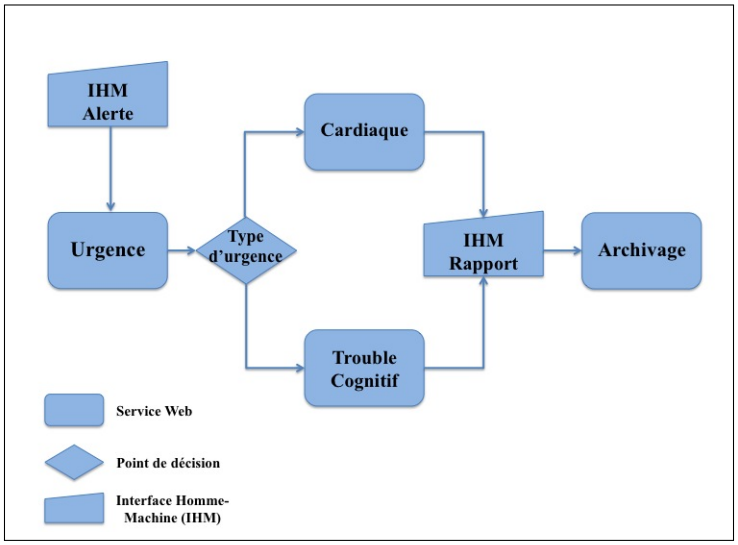

figure 4.2 – Exemple de processus automatisé par orchestration

déployé dans un hôpital ou un centre de réhabilitation peut faire appel à des services déployés dans un HI.

TC : Pas de lien en particulier.

Solution

Un flux de travail est une séquence d'étapes interconnectées, c'est une représentation d'une séquence d'opérations organisées dans le temps et réalisées par divers acteurs telles que des personnes, des applications ou des services. Dans le domaine de l'informatique, on parle également de processus métier. Cela consiste à décrire :

- le circuit de validation ou de traitement d'un processus,
- les tâches à accomplir entre les différents acteurs d'un processus,
- les délais à respecter,
- les modes de validation (ce qui détermine qu'un processus se termine correctement).

Il fournit en outre, à chacun des acteurs, les informations nécessaires pour la réalisation de sa tâche.

Chef d'orchestre

Appliqué dans une architecture orientée services, un flux de travail consiste en l'orchestration de services web, soit la formalisation des interactions entre les services web, des points de décision et des interventions humaines à l'aide d'un langage approprié.

Le langage BPEL (« Business Process Execution Language » pour langage d'exécution de processus métier) est un langage de description de flux de travail. C'est un standard OASIS qui définit les règles d'interaction entre les services web. BPEL est un langage dérivé de XML. Il est issu des langages WSFL (Web Services Flow Language) et XLANG. Un fichier BPEL contient les informations relatives à l'orchestration de services web, soient la logique des actions qui seront exécutées par le moteur d'exécution BPEL, les liens vers les services web. Sa structure est similaire au flux de travail dont il représente le code source.

Le moteur d'exécution est lui-même un service web qui agit comme le client des services web qu'il orchestre.

La figure 4.2 représente un flux de travail comprenant trois services web. Le premier est le service "Urgence" qui est appelé par une interface personne-machine (IHM) avec un paramètre "<Type d'urgence"> qui peut soit prendre la valeur "Cardiaque" s'il s'agit d'une urgence liée à une anomalie cardiaque, ou "Trouble Cognitif" s'il s'agit d'une urgence causée par les troubles cognitifs du patient. Dépendamment de la valeur du type d'urgence, le service web "Cardiaque" ou "Trouble Cognitif" sera appelé. La décision d'appeler l'un ou l'autre est prise par le moteur d'exécution qui teste la valeur "Type d'urgence". Lorsqu'ils sont appelés, ces services web ont pour but de trouver le meilleur intervenant disponible pour aider le patient. Une fois celui-ci trouvé, le processus est interrompu jusqu'à ce que l'intervenant utilise une IHM pour envoyer son rapport. Lors de l'envoi du rapport, le flux reprend en appelant le service "Archivage", ce qui termine le flux de travail.

La solution consiste à :

— Décrire le processus à l'aide du langage BPEL,

— Lier le fichier BPEL avec les services web en utilisant les fichiers WSDL des services,

— Déployer le fichier BPEL dans un moteur d'exécution BPEL.

Conséquences

L'orchestration des services web est un outil puissant qui permet de gérer un flux de travail impliquant plusieurs services, et qui permet de :

— Formaliser les flux de travail de services web,
— Interrompre et reprendre un flux,
— Faire le lien entre des services web internes ou externes,
— Suivre les flux en cours,
— Disposer d'un historique des flux passés,
— Voir les flux qui comportent une erreur.

L'orchestration des services web offre une gestion plus fiable et plus sûre des flux de travail que des services web interconnectés de manière ad hoc.

Limitations

Ce patron permet de voir s'il y a une interruption ou une erreur dans le processus mais il ne protège pas contre l'indisponibilité d'un service web. Il ne peut garantir qu'un processus sera réalisé en un temps minimum (ceci est fait au niveau des services web du processus).

Patrons en lien

— **Garant** : Pour assurer la disponibilité d'un service web.
— **Pulsation** : Pour vérifier la disponibilité d'un service web.
— **Relanceur** : Pour relancer la requête une fois le service web disponible à nouveau.

Références

[18] - Morad Benyoucef, Craig Kuziemsky, Afrasiabi AmirRad et Ali Elsabbahi. « Modeling healthcare processes as service orchestrations and choreographies ». Business Process Management Journal, 17(4) :568–597, 2011.

[74] - J. Pasley. « How BPEL and SOA are changing Web services development ». Internet Computing, IEEE, 9(3) :60–67, 2005.

[9] - P. Amnuaykanjanasin et N. Nupairoj. « The BPEL orchestrating framework for secured grid services ». Dans Information Technology : Coding and Computing, 2005. ITCC 2005. In- ternational Conference on, volume 1, pages 348–353 Vol. 1, 2005.

[75] - C. Peltz. « Web services orchestration and choreography ». Computer, 36(10) :46–52, 2003.

Concierge

Alias : Suivi des présences.
Type : Sûreté.

Résumé

Ce patron propose une solution de suivi des présences dans une pièce ou un ensemble de pièces. Une base de connaissances des présences est alimentée par les informations récoltées par les capteurs de l'appartement et des moyens d'authentification qui s'y trouvent. La consulter permet d'obtenir la localisation et la description des personnes présentes dans l'HI dont la précision dépend du nombre de capteurs disponibles.

Problème

L'HI est le lieu de vie du patient. C'est également un lieu visité par ses proches, le personnel soignant et les techniciens chargés de la maintenance. Pour des raisons de sûreté, pratiques ou légales, un moyen de connaître la liste des personnes présentes dans l'HI est nécessaire. Ce moyen doit permettre de :

— Savoir qu'un visiteur particulier est présent, connaître les dates de ses dernières visites quand on estime qu'une grande fréquence des visites peut avoir un impact sur le patient
— Connaître l'identité des visiteurs et les authentifier,
— Connaître le nombre de personnes sur place,
— Vérifier le respect de la confidentialité d'une visite médicale à domicile,

Concierge

— Garder un historique des visites, leur date et leur durée,
— Localiser un membre du personnel, lui adresser un message, valider sa présence lors d'une visite à domicile,
— Réaliser un audit des visites,
— Superviser la visite de personnes spécifiques, par exemple un membre de la famille en cas de conflit.

Particularités contextuelles

Santé : Les intervenants doivent s'authentifier à leur arrivée.

TC : Certains visiteurs doivent quitter au-delà d'une certaine durée ou disposent d'un nombre limité de visites hebdomadaires, leur présence pouvant nuire à la longue au bien-être du patient. Dans des situations conflictuelles avec des membres de la famille, il arrive que la présence d'un visiteur requière celle d'un superviseur.

HI : Le HI dispose de points d'authentification (hall d'entrée, écrans, lecteurs biométriques) et de capteurs dont le déclenchement permet de suivre les déplacements de personnes. Il est conseillé aux proches du patient qui lui rendent régulièrement visite de s'identifier à l'entrée.

Solution

Un service web de suivi des présences tel qu'illustré par la figure 4.3 peut répondre à la problématique en réalisant les tâches suivantes :

1. Alimenter une base de connaissances : Une base de connaissances des personnes présentes représente la mémoire vive du service et est mise à jour chaque fois qu'une nouvelle information est connue. Par exemple, trois personnes entrent dans l'appartement, une seule s'authentifie en entrant. La base contient alors :
   — Personne authentifiée 1
   — Visiteur inconnu 1

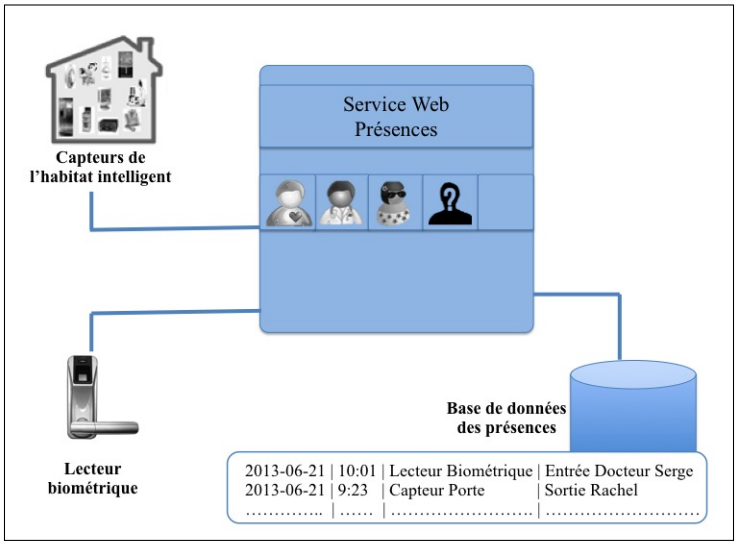

figure 4.3 – Service de suivi des présences

— Visiteur inconnu 2

Lorsque le visiteur inconnu 2 s'authentifie auprès d'un des postes de l'HI, la base devient alors :

— Personne authentifiée 1
— Visiteur inconnu 1
— Visiteur authentifié 2

2. Alimenter une base de données ou un journal des entrées et des sorties : Consigner la date et l'heure de l'entrée et de la sortie d'un visiteur permet de calculer la durée de la visite, de retrouver le nombre de visites dans un laps de temps donné ou la date de la dernière visite. Pour chaque entrée, il faut ajouter le nom du visiteur s'il est connu, ou lorsqu'il devient connu.
3. Suivi des trajets des visiteurs : En utilisant le réseau de capteurs, il devient possible de déterminer le trajet d'une personne ou du moins sa position actuelle. Cette information peut être utilisée comme donnée contextuelle dès qu'une personne approche d'une pièce spécifique ou pour savoir quelles pièces ont été visitées.

L'utilisation d'une base de connaissances permet d'obtenir une représentation actuelle des personnes présentes dans l'HI. En se basant sur toutes les informations

disponibles et détectables par les capteurs de l'HI, on peut détecter une présence, identifier quelqu'un et suivre ses trajets dans l'habitat.

Pour identifier, et pour détecter les entrées et les sorties, on dispose par exemple de :

— Lecteurs RFID à l'entrée, dans l'HI,
— Lecteurs d'empreintes digitales à la porte d'entrée et à l'intérieur de l'HI,
— Reconnaissance vocale et faciale si disponible.

Pour suivre les déplacements dans l'HI, on dispose de l'ensemble des capteurs. Le nombre de capteurs influe sur la qualité de suivi des déplacements. Lorsqu'un grand nombre de personnes sont présentes, il devient plus difficile voir impossible de distinguer les déplacements d'une personne à l'autre.

Conséquences

En appliquant ce patron, l'HI dispose d'un service qui :

— Donne accès à la liste des personnes présentes
— Historique des entrées et des sorties des visiteurs, leur identité lorsqu'elle est connue, le moment et la durée de leur visite.
— Permet de détecter l'approche d'un visiteur vers une zone spécifique de l'appartement

En terme de sûreté, ce patron offre un moyen de protection du patient en suivant les entrées et sorties des visiteurs. Cependant, il donne accès à des informations confidentielles sur le patient et ses habitudes de vie et doit être sécurisé et utilisé seulement en cas de nécessité. Dépendamment des pays, un encadrement légal peut s'avérer nécessaire.

Limitations

Ce patron ne permet que le suivi des présences à l'intérieur des pièces équipées de capteurs, et dans les limites de détection et du suivi individuel des personnes du réseau de capteurs. Ce patron dépend de la bonne utilisation des procédés d'authentification ou d'identification des personnes entrant dans l'habitat intelligent.

Concierge

Patrons en lien

— **Patte Blanche** : Pour l'authentification des intervenants.
— **Dactylo** : Pour l'authentification à partir des empreintes digitales.

Références

[100] - Steven H. Zarit, Karen E. Reever et Julie Bach-Peterson. « Relatives of the Impaired Elderly : Correlates of Feelings of Burden ». The Gerontologist, 20(6) :649–655, 1980.

Petit Poucet

Alias : Localisation extérieure, géolocalisation, localisation par GPS.
Type : Sûreté.

Résumé

Ce patron propose une solution pour localiser un individu à l'extérieur grâce à l'utilisation d'un téléphone intelligent muni d'un système de géolocalisation et d'un service web.

Problème

Un appartement intelligent dispose de nombreux capteurs qui permettent d'induire la présence de son occupant lorsque l'un d'eux est activé. Cela donne un moyen de connaître la localisation de l'occupant lorsqu'il est chez lui. Dès qu'il sort, par contre, cette possibilité est perdue.

L'occupant d'un HI effectue parfois des trajets hebdomadaires en dehors de chez lui. Il dispose autant que possible d'une assistance cognitive pour ses trajets.

Cependant, en raison de ses troubles cognitifs, le patient peut se perdre et ne plus être en mesure de retrouver son chemin et demander une assistance pour le retrouver. Il arrive également que le patient ne soit pas en mesure de communiquer du tout.

Un système de localisation pour le localiser et pour aller jusqu'à lui devient nécessaire.

Particularités contextuelles

Santé : Dans le cas d'une urgence médicale, localiser le patient même en dehors de l'HI doit être fait rapidement pour lui porter secours.

TC : En raison de ses troubles, le patient a des problèmes d'orientation et de gestion du temps. Il peut ne plus trouver son chemin et demander de l'assistance, ou ne plus reconnaître le chemin sur lequel il se trouve. Le patient peut également ne pas se présenter à un rendez-vous planifié avec un intervenant à l'extérieur. Le localiser permet de voir s'il a divergé de son itinéraire. Les secours, le tuteur/curateur, le gestionnaire de cas peuvent avoir à connaître la position de leur patient aussi rapidement que possible.

HI : L'HI peut rappeler au patient d'emmener son téléphone avec lui en partant et prendre le relais à son retour.

Solution

La plupart des téléphones intelligents disposent d'un système de géolocalisation. En fournissant ce type d'appareil à l'individu à localiser, celui-ci peut être programmé pour transmettre les coordonnées de géolocalisation à un service web.

La consultation directe auprès du téléphone est techniquement possible en programmant le téléphone pour répondre à certaines requêtes spécifiques. Cependant, ce procédé fonctionne uniquement si le téléphone est joignable au moment de faire la demande de localisation. Si le téléphone est éteint ou dans un immeuble ayant une faible réception du réseau de téléphonie mobile, la demande ne pourra aboutir.

En programmant une application sur le téléphone, celle-ci peut envoyer les coordonnées de géolocalisation vers un service web à intervalle régulier.

L'utilisation d'un service web tel qu'illustré sur la figure 4.4 permet de récupérer les coordonnées de géolocalisation transmises par le téléphone et de les enregistrer dans une base de données pour consultation ultérieure. Ainsi, même si le téléphone devient inaccessible, le service web sera en mesure de fournir les dernières coordonnées

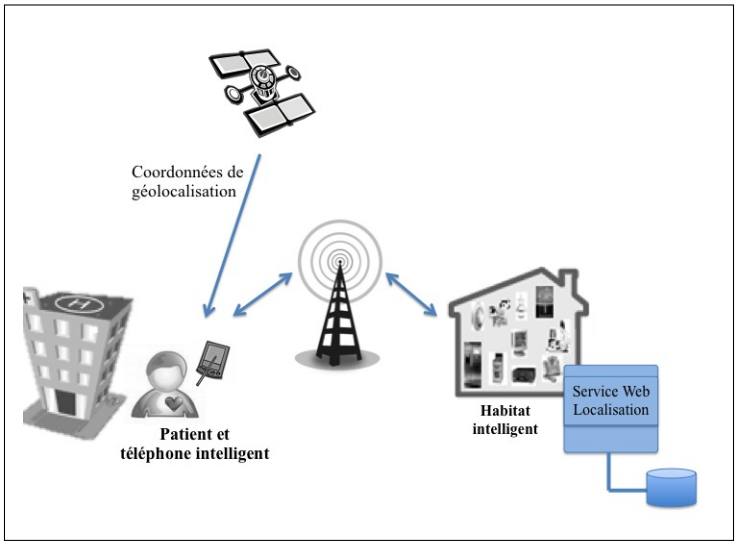

figure 4.4 – Localisation extérieure d'un individu

et d'indiquer à quel moment elles ont été récoltées.

Le service web doit retenir les informations suivantes :

1. Date et heure de l'enregistrement, en donnant la préférence à celles données par le téléphone plutôt que celles données par le serveur web,
2. Longitude et latitude de la localisation, l'édifice ou le patient se trouve, etc.

Le délai maximum de stockage des données devra éventuellement être pris en considération. Il peut varier en fonction de réglementations légales, d'un comité d'éthique, voire en fonction de la capacité de stockage disponible et des la quantité de données que le procédé génère.

Conséquences

En appliquant ce patron, le patient peut être localisé en dehors de chez lui tant qu'il porte le téléphone sur lui. En cas de possibilité d'oubli de porter le téléphone, l'utilisation du patron Detector est conseillé.

La géolocalisation consomme de la batterie et entraîne une réduction du temps d'utilisation du téléphone.

La réception du signal téléphonique peut être nulle dans certains bâtiments ou dans le métro.

Utiliser un service de localisation d'une personne nécessite l'accord préalable de la personne concernée et de son tuteur légal.

Limitations

Ce patron dépend de la bonne utilisation du GPS, de sa batterie et du fait que le patient sorte de chez lui avec son GPS. L'utilisation du GPS est également limitée par la réception du signal satellite qui diminue ou devient nul dans certains bâtiments. Par exemple, le signal se perd dans un souterrain. Si l'utilisateur utilise le souterrain pour se rendre d'un bâtiment à un autre, la dernière position connue sera celle de l'entrée dans le premier bâtiment.

Patrons en lien

— **Detector** : Pour détecter le terminal e-Santé du patient (et lui rappeler de le prendre lorsqu'il l'oublie en sortant).

Références

[91] - K. Shimizu, K. Kawamura et Katsuyuki Yamamoto. « Location system for dementia wandering ». Dans Engineering in Medicine and Biology Society, 2000. Proceedings of the 22nd Annual International Conference of the IEEE, volume 2, pages 1556–1559 vol.2, 2000.

[16] - Bruno Stanislas Beauvais, Vincent Rialle et Juliette Sablier. « MyVigi : An Android Application to Detect Fall and Wandering ». Dans The Sixth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, pages 156–160, 2012.

Memento

Alias : aucun.
Type : Sûreté.

Résumé

Ce patron propose une solution de contextualisation des visites dans l'HI. Lorsqu'un visiteur sonne à la porte, le patient est informé de l'identité du visiteur lorsque celui-ci s'identifie à la porte et du contexte de la visite si celle-ci a été ajoutée au calendrier du patient.

Problème

Un visiteur sonne à la porte de l'habitat d'une personne souffrant de TC.

Les personnes âgées qui se sentent seules sont plus à même de faire entrer des inconnus chez elles. Les personnes souffrant de la maladie d'Alzheimer ne reconnaissent pas systématiquement leurs proches et le personnel soignant qui leur rend visite régulièrement.

Dépendamment de l'étendue des TC, il peut s'avérer préférable que le patient n'ouvre uniquement la porte qu'aux personnes dont on connaît l'identité et le lien avec le patient.

Le problème est de connaître l'identité du visiteur et de la communiquer au patient avant d'ouvrir la porte pour lui donner la possibilité de ne pas ouvrir si le visiteur n'est ni un proche, ni un membre du personnel soignant.

Particularités contextuelles

Santé : Les membres du personnel disposent de badge ou utilisent leurs empreintes digitales comme moyen d'authentification.

TC : Le patient ne reconnaît pas toujours les membres de sa famille ou ses amis et s'en retrouver gêné. Lui rappeler l'identité et son lien avec le visiteur procure un moyen de le rassurer avant d'ouvrir la porte.

HI : L'HI dispose de moyen d'authentification à la porte (lecteur de badge RFID ou d'empreinte digitale par exemple) et d'écrans tactiles répartis dans l'appartement. Une application calendrier contient les rendez-vous du patient pour lui rappeler à l'avance la visite du personnel soignant ou de maintenance.

Solution

La solution implique de demander aux proches du patient et aux membres du personnel de s'authentifier à leur arrivée. Lorsqu'ils sonnent à la porte, ils utilisent leur badge ou passent leur doigt au lecteur d'empreintes digitales de la porte.

Le profil des proches doit au préalable être ajouté dans le système par le gestionnaire de cas. Les membres du personnel sont déjà dans le système du CSIU, mais le développeur doit faire le lien avec l'annuaire des membres du personnel pour accéder aux informations nécessaires.

Le profil doit contenir les informations d'identification suivantes :

— Le nom et prénom,
— Son affiliation (par exemple, ami, fils, médecin, technicien de maintenance etc.),
— Sa photo prise lors de la saisie initiale des informations.

Comme le montrent les figures 4.5 et 4.6, une IHM est nécessaire. Celle-ci s'affiche lorsqu'une personne sonne ou s'authentifie à la porte d'entrée. Une fois le visiteur authentifié, les informations relatives à l'identité du visiteur sont affichées sur l'IHM.

Si le visiteur est un membre du personnel soignant ou de maintenance, la date, l'heure, son identité et le but de sa visite sont enregistrés dans son calendrier. Ces

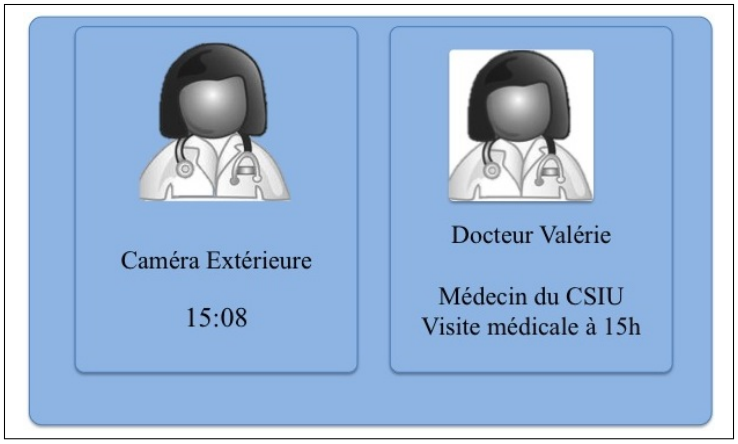

figure 4.5 – IHM de contextualisation d'une visite d'une personne connue

figure 4.6 – IHM de contextualisation d'une visite d'une personne inconnue

informations doivent être affichées sur l'IHM.

L'application du patron Juda permet d'afficher une photo du visiteur prise à l'extérieur au moment de s'authentifier ou de sonner, au côté de la photographie associée au profil du visiteur.

Conséquences

En appliquant ce patron, on dispose d'un moyen d'informer le patient sur le visiteur qui se trouve à la porte avant de l'ouvrir. On lui donne le choix de ne pas ouvrir la porte à toute personne inconnue.

Le patient voit le nom et l'affiliation de la personne qui le visite, ce qui peut le rendre plus à l'aise lorsqu'il s'agit d'une personne dont il aurait oublié le nom ou le rôle.

Limitations

Ce patron s'appuie sur l'utilisation du badge d'identification du personnel médical et des proches de l'entourage du patient. En l'absence de badge, ce patron ne peut fonctionner adéquatement. Ce patron ne protège pas contre l'usurpation d'identité si le patient n'est pas en mesure de distinguer la différence entre le visage de la personne à l'extérieur et le visage associé au titulaire du badge.

Patrons en lien

— **Juda** : Pour prendre une photo du visiteur qui sonne à la porte.

Références

[64] - Mario Mendez, Richard Martin, Kathleen Smyth et Peter Whitehouse. « Disturbances of Person Identification in Alzheimer's Disease : A Retrospective Study ». The Journal of Nervous and Mental Disease, 180(2), 1992.

[29] - Barbara Chenoweth et Beth Spencer. « Dementia : The Experience of Family Caregivers ». The Gerontologist, 26(3) :267–272, 1986.

Detector

Alias : aucun.
Type : Sûreté.

Résumé

Ce patron propose l'utilisation d'étiquettes et d'antennes d'identification par radiofréquence comme moyen de détection de déplacement et de localisation d'objets dans un espace ubiquitaire.

Problème

Parmi les pertes cognitives, la perte de mémoire est fréquente. Même une personne saine peut perdre ses clés chez elle et passer du temps à les retrouver.

Les troubles cognitifs augmentent les situations dans lesquelles le patient cherche ses affaires, oublie où celles-ci sont rangées, range un objet dans le mauvais placard ou tiroir, etc.

Un autre problème survient lors de la perte de mémoire sémantique. Dans ce cas, le patient ne sait plus à quoi sert un objet. Une application de reconnaissance des objets permettrait d'y remédier, mais il faut néanmoins un dispositif d'identification des objets pour cela.

Un système d'identification et de détection est nécessaire pour :

— Suivre l'utilisation d'un objet,
— Trouver un item dans l'HI,
— Vérifier les entrées/sorties de certains objets,

Detector

— Disposer d'un moyen d'alerter lorsqu'un item sort ou entre d'une espace spécifique,
— Consigner certaines utilisations, évaluer les quantités restantes d'une ressource, etc.

Particularités contextuelles

Santé : Pas de lien particulier.

TC : Le patient oublie où se trouve un objet, oublie de partir avec un objet ou de le laisser à l'HI. Localiser un objet permet d'assister à la réalisation de tâche en localisant les ressources utiles.

HI : Espace ubiquitaire dans lequel on peut intégrer aisément des antennes d'identification par radiofréquence.

Solution

La solution réside dans l'utilisation d'étiquettes et d'antennes d'identification par radiofréquence.

Pour cela il faut définir l'espace de détection en vue de l'équiper d'une ou plusieurs antennes. Il existe différentes tailles et puissances d'antennes. Certaines sont mieux adaptées à la détection de proximité (c'est-à-dire qu'il faut passer l'étiquette à quelques millimètres de l'antenne), d'autres offrent une plus grande distance de détection, de l'ordre de quelques centimètres à plus d'un mètre.

Le choix de l'antenne dépend de l'utilisation souhaitée. Par exemple, si l'on souhaite détecter les ingrédients disponibles dans un placard, une antenne disposant d'un champ de détection de quelques dizaines de centimètres convient parfaitement. Au-delà, il est difficile de distinguer le placard dans lequel l'ingrédient est rangé, si plusieurs antennes sont déployées dans des placards mitoyens.

Certaines étiquettes d'identification par radiofréquence ont la taille d'un timbre poste et peuvent être collées à peu près partout (des boîtes de céréales, le chéquier,

la télécommande de la télévision, etc.).

D'autres sont disposées dans des jetons ou des cartes de la même taille qu'une carte de crédit. Ces dernières peuvent être utilisées de moyen d'identification des personnes.

Conséquences

Ce patron offre un outil d'identification, de localisation et de repérage d'objet. Il aide à suivre l'utilisation et le déplacement d'objet dans la limite de détection des antennes installées.

Limitations

La détection d'objet peut-être limitée en fonction du type de technologie employée et en fonction de la puissance des antennes utilisées. De plus, l'étiquette utilisée pour la détection peut-être arrachée volontairement ou se décoller rendant l'objet indétectable.

Patrons en lien

Aucun.

Références

[88] - T. Sanpechuda et L. Kovavisaruch. « A review of RFID localization : Applications and techniques ». Dans Electrical Engineering/Electronics, Computer, Telecommunications and In- formation Technology, 2008. ECTI-CON 2008. 5th International Conference on, volume 2, pages 769–772, 2008.

[98] - Guang yao Jin, Xiao-Yi Lu et Myong-Soon Park. « An indoor localization mechanism using active RFID tag ». Dans Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006. IEEE International Conference on, volume 1, 2006.

Detector

[19] - M. Bouet et A.L. dos Santos. « RFID tags : Positioning principles and localization techniques ». Dans Wireless Days, 2008. WD '08. 1st IFIP, pages 1–5, 2008.

Porte-monnaie

Alias : Suivi des dépenses.
Type : Sûreté.

Résumé

Ce patron propose un moyen de suivre les dépenses du patient et offre une assistance pour prévenir le dépassement du montant maximum d'achat pour une transaction donnée ou une période de temps déterminée. Le patron Detector est utilisé pour détecter l'utilisation des moyens de paiement et déclencher une IHM d'assistance.

Problème

En fonction de son état de santé et de ses troubles cognitifs, un patient peut disposer de l'intégralité de ses capacités de paiement, seulement d'une partie ou ne pas être en mesure de gérer ses finances du tout. Le gestionnaire de cas, le tuteur ou curateur peut décider de laisser ses moyens de paiement au patient en imposant des limites de montant d'achat par semaine ou par mois et en contrôlant au besoin la nature des achats.

Il se peut qu'une limite soit mise en place sur une carte de débit ou de crédit au niveau de la banque. Cette limite n'est pas systématiquement applicable dans tous les cas et sur l'ensemble des moyens de paiement.

Autant que possible, il est préférable de laisser au patient une certaine autonomie financière tout en faisant attention à :

— Limiter l'impact d'une mauvaise utilisation ou d'un abus de la part d'un tiers,

— Éviter de dépenser tout le budget d'un seul coup,
— Pouvoir intervenir rapidement lorsque des abus sont constatés,
— Consigner les dépenses pour évaluation ultérieure.

Particularités contextuelles

Santé : Pas de lien particulier.

TC : L'incapacité de gérer ses dépenses fait partie des premiers signes de la maladie d'Alzheimer. Le patient peut avoir perdu une partie de ses capacités à gérer ses finances. Toute personne souhaite cependant conserver une autonomie dans la gestion de ses propres achats.

HI : L'HI dispose d'antennes d'identification par radiofréquence et d'écrans tactiles qui peuvent être utilisés pour l'implémentation de ce patron.

Solution

La solution est présentée en trois étapes. La première est l'application du patron Detector pour rendre les moyens de paiement détectables dans un environnement ubiquitaire. Ceci est fait en

— Collant des étiquettes sur le chéquier, les cartes de débit et de crédit, et sur le porte-monnaie,
— Déployant une antenne d'identification par radiofréquence dans les zones de rangement des moyens de paiement.

Ce dispositif permet détecter les entrées et sorties des moyens de paiement de leur zone de rangement et sert de déclencheur à l'interface de suivi des dépenses.

La seconde étape est le rassemblement des informations nécessaires au suivi des dépenses. Que ce soit fait par le gestionnaire de cas, un tuteur ou curateur, ou un membre de la famille, il faut savoir :

— Le montant maximum pour une période déterminée,
— Le montant maximum pour un achat,

- La somme disponible pour la période déterminée,
- Si le patient ne peut se déplacer, savoir si un membre de la famille va utiliser un moyen de paiement pour effectuer des achats à sa place,
- Les actions à réaliser lorsque le montant déclaré par le patient dépasse le montant restant pour la période courante ou le montant maximal par transaction. Ce peut être de :
  - Ne rien faire
  - Prévenir le patient qu'il dépasse l'un des montants maximums,
  - Prévenir une personne désignée,
  - Consigner le dépassement dans un journal des dépenses.

La troisième étape est la création d'une IHM qui :

- Se déclenche au moment de prendre ou de ranger les moyens de paiement,
- Rappelle les montants maximums pour la transaction en cours,
- Demande le montant de la dépense en cours ou à venir (si le montant n'est pas encore connu comme lors d'achats effectués à l'extérieur),
- Calcule si la somme déclarée ne dépasse pas les montants maximaux,
- Permet au tiers qui effectue des achats pour le patient de s'authentifier,
- Journalise les dépenses,
- Rappelle de ranger les moyens de paiement au retour du patient ou de l'aidant.

Création d'une IHM de suivi des dépenses :

- Établir un montant maximum pour une période déterminée
- Établir un montant maximum pour un achat
- Lancer l'IHM à la détection des moyens de paiement
- Au-delà d'un délai spécifique, rappeler de ranger le moyen de paiement si le patient est dans l'HI ou au retour de sa sortie.
- Demander au patient la somme et la raison de l'achat
- Avertir le patient en cas de dépassement et recommander de ne pas effectuer l'achat.
- Consigner les dépenses (utilisation d'un journal)

Conséquences

Après application de ce patron, le patient et la personne responsable du patient ont à leur disposition :

— Un système de suivi des dépenses tout en laissant une certaine liberté de gestion des dépenses au patient.

— Un outil d'évaluation sur les capacités de gestion des finances du patient.

Le gestionnaire de cas, le tuteur ou curateur peut vérifier a posteriori si des écarts se creusent entre les montants déclarés et les montants réels.

Ce système permet de prévenir essentiellement une mauvaise utilisation accidentelle des moyens de paiement, mais pas une mauvaise utilisation volontaire de la part d'un tiers.

Limitations

Ce patron est limité par les mêmes limitations que le patron Detector. Il dépend également de la volonté du patient de suivre les recommandations en matière de dépense. Si le patient décide d'ignorer l'assistance et qu'aucune limite n'est mise en place au niveau de ses moyens de paiements (par exemple, en plafonnant l'utilisation de sa carte de crédit), il n'y a plus de contrôle ou de suivi sur l'utilisation des moyens de paiement.

Patrons en lien

— **Detector** : Pour détecter le terminal e-Santé du patient (et lui rappeler de le prendre lorsqu'il l'oublie en sortant).

Références

[60] - D.C. Marson, S.M. Sawrie, S. Snyder, B. McInturff, T. Stalvey, A. Boothe, T. Aldridge, A. Chatterjee et L.E. Harrell. « Assessing financial capacity in patients with Alzheimer disease : A conceptual model and prototype instrument ».

[59] - Daniel C. Marson. « Loss of Financial Competency in Dementia : Conceptual and Empirical Ap- proaches ». Aging, Neuropsychology, and Cognition, 8(3) :164–181, 2001.

[33] - K.S. Earnst, V.G. Wadley, T.M. Aldridge, A.B. Steenwyk, A.E. Hammond, L.E. Harrell et D.C. Marson. « Loss of financial capacity in Alzheimer's disease : The role of working me- mory ». Aging, Neuropsychology, and Cognition, 8(2) :109–119, 2001. cited By (since 1996) 22.

Pickpocket

Alias : aucun.
Type : Sûreté.

Résumé

Ce patron combine les patrons Porte-monnaie, Concierge et Juda pour rassembler le plus d'informations possible sur le contexte d'utilisation des moyens de paiement. Sa mise en place permet d'enregistrer le moment, le type, le montant de l'achat ainsi que les personnes présentes lors de l'achat. Il est très utile pour protéger le capital d'une personne vulnérable en détectant de potentielles situations d'abus de faiblesse, même a posteriori.

Problème

Les personnes ayant des troubles cognitifs ont leur capacité de gestion de l'argent altérée. Par exemple, les personnes atteintes de la maladie d'Alzheimer oublient qu'ils ont déjà payé une facture et vont la payer à nouveau. Le patron Porte-monnaie fournit une aide en cas de mauvais usage des moyens de paiement par le patient en raison de ses troubles, mais ne protège pas en cas d'usage abusif de la part d'un tiers.

Bien souvent, les abus et détournement d'argent sont faits par des proches du patient, parfois même par des membres de la famille. Si ces abus peuvent être repérés, il est souvent difficile d'identifier les responsables et de disposer des preuves à leur encontre.

Particularités contextuelles

Santé : Le personnel soignant et de maintenance doit s'authentifier à leur arrivée.

TC : Le patient peut avoir perdu une partie de ses capacités à gérer ses finances, être en état de vulnérabilité et ne pas se rendre compte qu'il est en train d'être abusé par un proche.

HI : L'HI dispose d'antennes d'identification par radiofréquence, de système d'authentification à la porte, d'un service de suivi cette présence et d'une caméra à la porte d'entrée.

Solution

Ce patron combine les patrons Porte-monnaie, Concierge et Juda.

En implémentant le patron Porte-monnaie, on dispose des informations contextuelles suivantes :

— Le moment et le temps d'utilisation d'un moyen de paiement,
— Son type (chéquier, carte de débit ou de crédit, porte-monnaie),
— Le montant déclaré et la raison de l'achat.

En implémentant le patron Concierge, on dispose des informations contextuelles suivantes :

— Les personnes présentes durant l'utilisation des moyens de paiement (et si elles étaient authentifiées ou non reconnues),
— Si le patient était seul au moment d'en faire usage.

En implémentant le patron Juda, on dispose d'une photographie du visiteur.

L'emploi combiné de ces patrons permet de disposer d'une trace des personnes présentes autour du patient lors de l'utilisation d'un moyen de paiement.

Conséquences

Ce patron est le résultat de la combinaison de trois patrons dont l'utilisation conjointe permet de connaître le contexte d'une dépense.

Cela n'empêche pas forcément une fraude ou un abus de se réaliser, mais cela permet de la limiter dans la durée et d'empêcher qu'elle ne se reproduise, et permet également de constituer un dossier contre une personne essayant d'abuser de la vulnérabilité du patient.

Limitations

Ce patron est limité par les mêmes limitations que les patrons Concierge, Juda et Porte-Monnaie dont il dépend.

Patrons en lien

— **Juda** : Pour prendre une photo du visiteur qui sonne à la porte.
— **Concierge** : Pour le suivi des présences.
— **Porte-monnaie** : Pour le suivi des dépenses.

Références

[52] - Joan Langan et Robin Means. « Financial Management and Elderly People with Dementia in the U.K. : As Much a Question of Confusion as Abuse ? ». Ageing and Society, 16 :287–314, 4 1996.

[76] - Bridget Penhale. « The Abuse of Elderly People : Considerations for Practice ». British Journal of Social Work, 23(2) :95–112, 1993.

[63] - Robin Means et Joan Langan. « Money 'handling', financial abuse and elderly people with dementia : implica- tions for welfare professionals ».

Juda

Alias : aucun.
Type : Sûreté.

Résumé

Ce patron propose un moyen de journaliser les entrées des visiteurs en prenant une photographie d'eux au moment de leur entrée dans l'appartement à l'aide d'une caméra disposée à la porte d'entrée de l'HI.

Problème

Le patient est libre de faire entrer des visiteurs dans son appartement. Ce peut être aussi bien des membres de leur famille, des proches, des membres du personnel soignant ou de maintenance, que des démarcheurs ou d'autres personnes inconnues du patient ou du système de santé. Les personnes qui disposent d'un moyen d'authentification sont reconnues par le système, les autres ne sont pas clairement identifiables.

En cas d'abus de faiblesse envers une personne ayant des troubles cognitifs, ces derniers ne sont généralement pas capables de décrire les caractéristiques physiques de leur visiteur. Le service des présences n'est pas suffisant si la personne reste à la porte ou si le visiteur ne dispose pas de moyen d'authentification (ou ne l'utilise pas volontairement).

Un autre moyen de garder une trace des visiteurs qui sonnent à la porte de l'HI est nécessaire.

Particularités contextuelles

Santé : Pas de lien en particulier.

HI : L'HI dispose d'une caméra à la porte d'entrée et d'une sonnette qui génère un évènement auquel on peut associer une ou plusieurs actions telles que faire retentir une sonnerie à l'intérieur, allumer une lumière à l'entrée ou enclencher la caméra.

TC : Le patient peut être en état de vulnérabilité. Dans le cas des personnes souffrant de la maladie d'Alzheimer, elles ne se rendent pas forcément compte s'il s'agit d'un inconnu ou d'un proche à la porte. Ce ne sont pas les meilleurs témoins également en raison de leur âge avancé et de leurs pertes de mémoire.

Solution

L'HI est équipé de capteurs et d'effecteurs qui peuvent être utilisés pour détecter des évènements et en générer. Ainsi un détecteur de mouvement ou une sonnette placée à la porte d'entrée constituent un bon moyen de savoir qu'une personne est à la porte.

Récupérer les évènements liés à la présence d'une personne à la porte permet au développeur d'utiliser cette information pour déclencher une prise de vue depuis la caméra de la porte d'entrée. La photo est ensuite enregistrée sur le serveur de l'HI.

En appliquant le patron Greffier, le développeur consigne dans un journal des visites la date, l'heure et le chemin de la photographie.

Conséquences

Après application de ce patron, une photographie est prise lorsque la présence d'un visiteur est détectée à la porte d'entrée. La photographie et le moment de prise de vue sont enregistrés dans un journal des visites.

Limitations

Ce patron est limité par la prise de vue de la photo. Si la personne à l'extérieur tourne la tête lors de la prise de vue ou cache délibérément son visage en obstruant le capteur photographique, la photographie du visiteur ne sera pas utilisable.

Patrons en lien

— **Greffier** : Pour la journalisation des évènements.

Références

[47] - Achilles D. Kameas, Victor Callagan, Hani Hagras, Michael Weber, Wolfgang Minker, Abdelsalam Helal, Jeffrey King, Raja Bose, Hicham EL- Zabadani et Youssef Kaddourah. « Assistive Environments for Successful Aging ». Dans Advanced Intelligent Environments, pages 1–26. Springer US, 2009.

[32] - Angus Dickey, Jacob Slonim et Michael McAllister. « Enabling Ageing in Place through Visitor Recognition and Monitoring Tech- nology ». The International Journal of Science in Society, 1(2) :15–30, 2009.

Relanceur

Alias : aucun.
Type : Fiabilité et sûreté.

Résumé

Ce patron aborde le problème de la perte d'une requête lors de l'indisponibilité du service et propose un moyen pour la renvoyer une fois le service disponible à nouveau.

En cas d'indisponibilité d'un service web, la requête du client est perdue et ne sera pas envoyée à nouveau. Quand le message est important, il est préférable de l'envoyer à nouveau lorsque le service devient disponible.

Problème

Lorsqu'un client envoie une requête à un service web, celle-ci est acheminée jusqu'au serveur qui envoie ensuite la réponse. Si le service n'est pas disponible au moment de l'envoi, la requête est perdue. Au niveau du client, un message d'erreur survient. Celui-ci n'est pas nécessairement pris en compte dans le programme du client. Le programme du client peut ne pas savoir ce qu'il est advenu de la requête, ou peut mal fonctionner ou ne plus fonctionner du tout, si le dépassement de délai n'est pas pris en compte. L'utilisateur, de son côté, n'est pas averti et peut penser que sa requête a bien été envoyée ou appuyer continuellement sur le bouton d'envoi de l'interface.

Particularités contextuelles

Santé : Sur le plan médical, si une requête de demande d'intervention d'urgence ne parvient pas au centre de secours, il se peut que ce dernier n'apprenne la situation d'urgence que trop tard.

TC : Pour une personne ayant des troubles cognitifs, se retrouver face à une interface non responsive peut-être très frustrant. La personne peut ne pas comprendre pourquoi le système faisant appel au service web ne fonctionne pas.

HI : L'HI dispose de différents moyens d'interaction avec le patient tels que des écrans tactiles répartis dans l'habitat.

Solution

La première étape consiste à modifier le programme du client pour détecter que la requête n'est pas arrivée au serveur et optionnellement pour vérifier si le service est disponible ou non avant l'envoi de la requête. Détecter que la requête n'est pas arrivée au serveur est essentiel. Pour cela, le programme du client doit écouter les messages qui surviennent juste après l'envoi. Ces messages ont des codes spécifiques que l'on retrouve dans la RFC 2616 et qui incluent les codes du protocole HTTP. Parmi ces codes, on retrouve ceux du type

1. 2xx – Succès La requête est bien passée. Par exemple le code 200 qui signifie OK.
2. 4xx - Erreur du client Par exemple, le code 400 indique que la syntaxe de la requête est erronée.
3. 5xx - Erreur du serveur Par exemple, le code 500 indique une erreur interne du serveur et 503 indique que le serveur est temporairement indisponible.

Généralement, les erreurs du client sont repérées et corrigées lors de l'écriture du code et du débogage. Cependant les erreurs du serveur sont souvent ignorées.

La vérification préalable de la disponibilité du service peut se faire en appliquant le patron Pulsation. Par ailleurs, il se peut que le service soit disponible au moment de la

vérification, puis tombe en indisponibilité au moment d'envoyer la requête. Attraper l'exception et vérifier le dépassement de délai devient alors essentiel.

Pour réaliser ce patron, le développeur doit :

1. Garder en mémoire la requête jusqu'à l'obtention d'un message de type 2xx - Succès, ou des messages d'erreur de type 4xx ou 5xx,
2. Dans le cas de messages d'erreur, attendre un délai et envoyer à nouveau la requête,
3. Donner un retour à l'utilisateur de l'interface qui précise que la requête n'a pas été envoyée mais qu'une autre tentative aura lieu dans un délai donné,
4. Proposer des alternatives optionnellement, tel que l'envoi de la requête par message texte ou en téléphonant à une tierce personne.

Le client du service peut tester la disponibilité du service avant de l'envoyer. Dans le cas où le service est indisponible, la requête peut être mise en attente jusqu'à ce qu'il soit de nouveau opérationnel.

Conséquences

Après application de ce patron, le développeur dispose d'un moyen de vérifier si la requête a été envoyée avec succès ou non. Si la requête ne passe pas et que l'indisponibilité perdure, une alternative devra être utilisée. Son application a un impact en ce qui concerne la fiabilité du dispositif d'envoi d'alerte et la sûreté du patient.

Limitations

Ce patron est limité par l'état du réseau et la disponibilité du service avec lequel il communique. Tant que la communication avec le service ne sera pas rétablie, la requête ne sera pas envoyée.

Relanceur

Patrons en lien

— **Garant** : Pour assurer la disponibilité d'un service web.
— **Pulsation** : Pour vérifier la disponibilité d'un service web.

Références

[38] - R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach et T. Berners-Lee. « Hypertext Transfer Protocol – HTTP/1.1 », 1999.

[55] - A. R. Luria. Human brain and psychological processes. Harper and Row (New York), 1966.

[69] - Donald A. Norman et Tim Shallice. « Attention to Action : Willed and Automatic Control of Behavior ». Dans R. J. Davidson, G. E. Schwartz et D. Shapiro, éditeurs, Consciousness and Self-Regulation, Volume 4, pages 1–18. Plenum Press, 1986.

Cerbère

Alias : Contrôle d'accès basé sur les rôles, RBAC, Role Based Access Control.
Type : Sécurité et sûreté.

Résumé

Ce patron présente le contrôle d'accès basé sur les rôles pour définir une politique de restriction d'accès dans un système d'information. Ce type de contrôle d'accès à l'avantage de réduire les coûts de maintenance des politiques de contrôles d'accès tout en offrant un moyen de définir et de différencier des droits d'accès selon les rôles attribués à un utilisateur.

Problème

Un système d'information donne accès à une grande diversité de ressources dont il faut protéger l'accès. Au sein d'un même organisme, tout le personnel n'a pas accès à l'ensemble des ressources, et ce pour des raisons de sécurité ou de confidentialité. C'est généralement le « besoin de savoir » qui justifie de donner les droits d'accès.

Une fois la personne authentifiée, il est donc nécessaire de différencier les accès auxquels elle a le droit des autres accès qui lui sont interdits.

Un tel système est assez simple à mettre en place de manière individuelle dans une très petite structure comprenant peu de personnes. Lorsque le nombre d'utilisateurs dépasse la centaine, entretenir la liste des droits pour chaque utilisateur devient trop complexe et trop coûteux à mettre un œuvre. Lorsqu'un utilisateur est ajouté ou

retiré du système d'information, la gestion des droits d'accès augmente en temps et en coût avec la taille des la structure et le nombre de ressources à protéger.

Un moyen plus pratique de contrôler l'accès est donc nécessaire avec les caractéristiques suivantes.

— Simple à mettre en place même dans une très grande structure,
— Permettant de différencier les droits d'accès entre groupes d'utilisateurs,
— Facile à entretenir lors de l'arrivée ou le départ d'un utilisateur.

Particularités contextuelles

Santé : Dans le domaine de la santé, le système informatique contient beaucoup d'informations sensibles dont il faut protéger l'accès. Ces accès sont déterminés par le poste occupé par l'utilisateur du système d'information.

TC : Pas de lien en particulier.

HI : Beaucoup d'informations sensibles sont générées par les capteurs. Comme pour le domaine de la santé, l'accès doit être protégé et donné seulement à des personnes autorisées.

Solution

Le contrôle d'accès basé sur les rôles a été introduit en 1992 par David Ferraiolo et Rick Kuhn [37] puis repris par Sandhu et al. en 1996 [86].

En 2000, à la demande du NIST, Sandhu, Ferraiolo et Kuhn intègrent leur travail et propose un modèle unifié de RBAC [87] appelé "NCIST RBAC model" qui sera par la suite adopté comme standard par le "InterNational Committee for Information Technology Standards" (INCITS) en 2004.

Il est devenu un modèle de contrôle d'accès prédominant grâce à une simplification des descriptions de politiques de contrôles d'accès avancés et de leur maintenance.

Avant RBAC, les organisations devaient maintenir des listes de contrôle d'accès ou "Access Control Lists" (ACL) pour autoriser l'accès à chacune de leurs ressources ou

de leurs applications. L'ajout ou le retrait d'un utilisateur entraînaient la modification de chacune des listes de contrôle associées aux ressources ou aux applications autorisées. Ce qui devenait très difficile à effectuer pour les administrateurs des systèmes d'information.

RBAC permet de faciliter cette gestion en attribuant des rôles aux utilisateurs et en définissant des permissions d'accès ou d'action pour ces rôles. Le principe de RBAC est le suivant :

— Un ou plusieurs rôles sont attribués à un utilisateur,
— Les autorisations sont associées à des rôles,
— Un utilisateur qui se voit attribuer un rôle possède les autorisations associées à ce rôle.

Selon un rapport effectué en 2010 [70] pour le compte du National Institute of Standards and Technology (NIST), ce type de contrôle d'accès est fortement utilisé dans les organisations de plus de 500 employés pour restreindre l'accès à certaines ressources ou fonctionnalités d'un système informatique aux utilisateurs autorisés. On retrouve des implémentations de RBAC dans de nombreux produits informatiques tels que Microsoft Active Directory, Microsoft SQL Server, SELinux, FreeBSD, Solaris, Oracle DBMS. RBAC est suffisamment flexible pour simuler les contrôles d'accès obligatoire, discrétionnaire [73] et basé sur les treillis [85].

Le contrôle d'accès basé sur des rôles est aujourd'hui très répandu notamment dans les domaines bancaires, de la santé et des télécommunications grâce à son faible coût de mise en œuvre et à sa facilité d'utilisation.

Une organisation définit des rôles (tels une fonction ou un poste) et des permissions (droit d'effectuer des opérations sur un ensemble d'objets. Par exemple, droit de lecture et d'écriture sur un document). Un utilisateur est un individu ou un système.

— Un utilisateur se voit attribuer un ou plusieurs rôles.
— Un rôle peut être attribué à plusieurs utilisateurs, et peut contenir plusieurs permissions.
— Une permission peut être assignée à une multitude de rôles.
— Une opération peut être assignée à une multitude de permissions.
— Une permission peut être assignée à une multitude d'opérations.

Lorsqu'il s'authentifie, une session est créée. Ce qui active les rôles de l'utilisateur

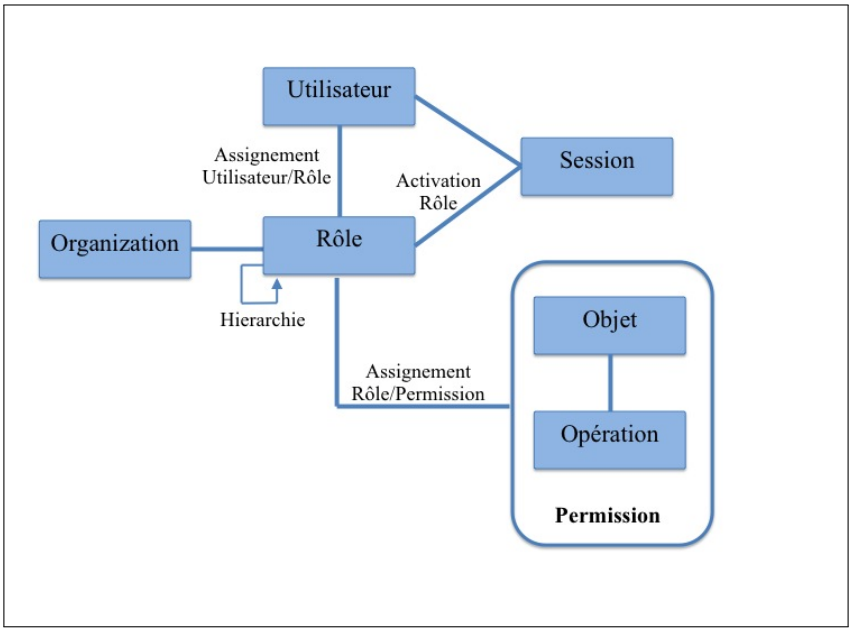

figure 4.7 – Modèle de contrôle d'accès basé sur les rôles.

qui peut à présent effectuer les opérations sur les objets selon les permissions dont disposent ses rôles comme illustrés sur la figure 4.7.

Conséquences

Après application de ce patron :

— Un utilisateur aura besoin d'avoir un rôle spécifique pour accéder à la ressource à laquelle il souhaite accéder.

— Ce rôle devra contenir la permission nécessaire pour effectuer l'opération sur cette ressource.

— Sans avoir un rôle permettant d'effectuer une opération sur une ressource, un utilisateur ne pourra pas effectuer cette opération.

— L'organisation n'a pas besoin de refaire sa politique d'accès quand une personne arrive ou quitte. Lui retirer ses rôles, puis effacer l'utilisateur suffira pour cela.

Limitations

Ce patron est limité par la qualité de l'authentification et de la gestion des rôles et des privilèges. Si le moyen d'authentification est subtilisé, il peut être utilisé tant qu'il n'est pas révoqué dans le système. Par exemple, si seul un badge est utilisé pour authentifier une personne et que ce badge est volé. L'auteur du vol aura accès à toutes les ressources autorisées pour les rôles associés au titulaire du badge jusqu'à ce que les autorisations du badge soient révoquées.

Patrons en lien

— **Patte Blanche** : Pour l'authentification des intervenants.
— **Dactylo** : Pour l'authentification à partir des empreintes digitales.
— **Brise-glace** : Pour outrepasser temporaire les restrictions d'accès à une ressource.
— **Greffier** : Pour la journalisation des accès à une ressource.

Références

[37] - Ferraiolo, D.F. and Kuhn, D.R. (October 1992). "Role-Based Access Control" (PDF). 15th National Computer Security Conference. pp. 554–563.

[86] - Ravi Sandhu, E.J. Coyne, H.L. Feinstein et C.E. Youman. « Role-Based Access Control Models ». IEEE Computer, 29(1) :38–47, August 1996.

[85] - Ravi Sandhu. « Role Activation Hierarchies ». Dans Proceedings of 3rd ACM Workshop on Role-Based Access Control, October 1998.

[73] - Sylvia Osborn, Ravi Sandhu et Qamar Munawer. « Configuring role-based access control to enforce mandatory and discretionary access control policies ». ACM Transactions on Information and System Security (TISSEC), pages 85–106, 2000.

[70] - Alan C. O'Connor et Ross J. Loomis. « Economic Analysis of Role-Based Access Control ». Rapport Technique, Research Triangle Institute, 2010.

[87] - Ravi Sandhu, David Ferraiolo et Richard Kuhn. « The NIST Model for Role Based Access Control : Toward a Unified Standard ». 5th ACM Workshop Role-Based

Cerbère

Access Control, pages 47–63, 2000.

Brise-glace

Alias : Bris de glace, élévation de privilège.
Type : Sécurité et sûreté.

Résumé

Ce patron propose un moyen de donner un accès à une ressource lorsqu'il est nécessaire pour un utilisateur d'outrepasser les restrictions dont il fait l'objet de manière temporaire et exceptionnelle. Cela revient à briser la vitre en cas d'urgence. L'utilisateur doit cependant se justifier par après, auprès de son responsable qui en est informé.

Problème

Certains membres du personnel ne devraient pas avoir accès à certaines ressources. Le contrôle d'accès basé sur les rôles permet justement de mettre en place une stratégie de sécurité en ce sens. Il est des situations plus complexes pour lesquelles leur travail requière, dans des cas exceptionnels, d'y accéder. Cependant, demander l'autorisation à un supérieur hiérarchique n'est pas toujours possible sur le coup, et est contraignant. Le supérieur peut être indisponible et n'a pas forcément la possibilité technique d'élever temporairement les privilèges d'une personne.

Le besoin d'accès se fait généralement sous une contrainte de temps ; lors d'une visite chez le patient par exemple. Le personnel a besoin d'accéder à la ressource sur le coup. Dans ce cas, il ne s'agit pas d'empêcher tout accès à la ressource, mais de la protéger contre tout accès qui pourrait être abusif. Le personnel pourrait accéder à la

ressource, mais devrait motiver l'utilisation de la ressource auprès de son responsable par la suite.

Tout en conservant l'emploi du contrôle d'accès basé sur les rôles, un moyen technique est nécessaire pour :

— Permettre d'outrepasser une restriction d'accès temporairement,
— Prévenir l'usager qu'il outrepasse ses privilèges et qu'il devra rendre des comptes à son responsable,
— Prévenir le responsable lorsque ce type d'accès est utilisé.

Particularités contextuelles

Santé : Pour outrepasser temporairement l'accès au réseau de capteurs et obtenir des informations significatives sur l'état de santé du patient (prise de médicament, hygiène corporelle, etc.).

TC : Pour outrepasser temporairement l'accès au réseau de capteurs et obtenir des informations significatives sur l'état de santé mental du patient (sortie de l'appartement, hygiène corporelle, etc.).

HI : Le réseau de capteur peut fournir des informations à considérer dans l'évaluation de l'état de santé du patient, par exemple à savoir si le patient prend bien ses médicaments, s'il sort de l'appartement de temps en temps, etc.

Solution

XACML (eXtensible Access Control Markup Language) est un langage pour le contrôle d'accès, dérivé du XML et indépendant de l'implémentation. Il sert à :

— Supporter les politiques d'autorisation,
— Décrire les conditions d'autorisation,
— Combiner des politiques,
— La circulation des règles de contrôles d'accès,
— L'administration de la politique de sécurité des systèmes d'information,

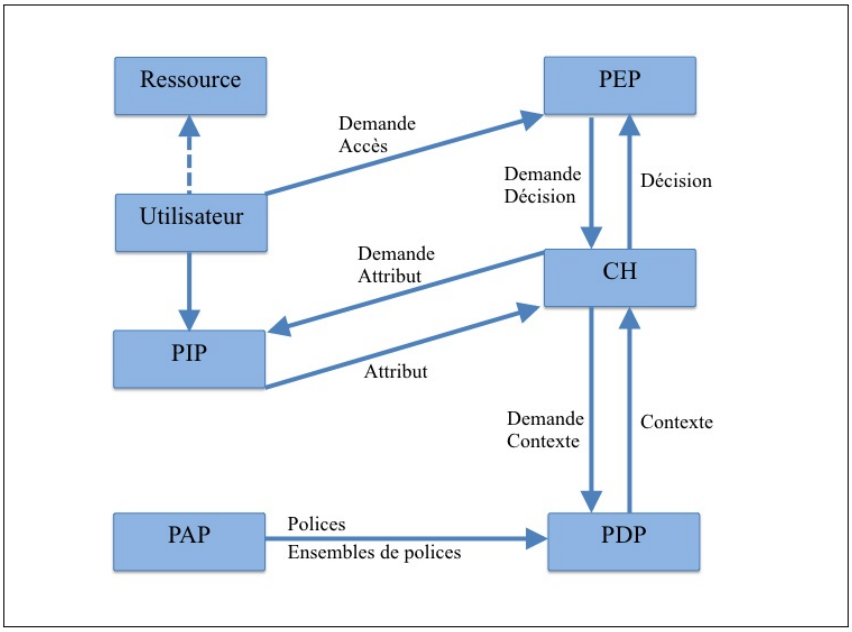

figure 4.8 – XACML

— La résolution de conflits des règles.

Le contrôle d'accès basé sur les rôles peut être implémenté en XACML.

XACML définit les composants suivants, comme illustré sur la figure 4.8 :

— PEP (Policy Enforcement Point) : Le point d'application de la décision exerce le contrôle d'accès en faisant des requêtes de décision et en appliquant les décisions d'autorisation. Il protège l'application ciblée.

— PIP (Policy Information Point) : Le point d'information répond aux demandes d'attribut. Par exemple, à la question « quel est le rôle de l'utilisateur ? ». Le PIP répond « infirmier ».

— PDP (Policy Decision Point) : Le point de décision évalue les politiques applicables et rend une décision d'autorisation.

— PAP (Policy Administration Point) : Le point d'administration des politiques est l'endroit ou les politiques ou ensembles de politiques sont créés et édités.

— Context Handler : Ce dispositif sert à la conversion des requêtes de décision du format natif au format XACML et des décisions d'autorisation du format XACML au format natif, et se coordonne avec le PIP pour ajouter des attributs au contexte de la requête.

Brise-glace

Le contexte XACML est le protocole utilisé par le PEP pour demander au PDP une décision d'autorisation. Il définit l'élément <xacml-context :Request> qui transmet la requête et l'élément <xacml-context :Response> pour la réponse. La requête contient quatre éléments pour l'autorisation :

- Le sujet est l'utilisateur qui fait la demande d'accès.
- L'action à faire sur la ressource telle que la lecture ou la modification.
- La ressource sur laquelle le sujet souhaite faire l'action.
- L'environnement est optionnel et peut contenir des attributs supplémentaires non fournis dans les éléments précédents, par exemple, la date et l'heure de la requête.

Le PEP envoie la requête d'autorisation au PDP en utilisant un contexte XACML qui contient les quatre éléments précédents. Cela revient pour le PEP à poser la question suivante au PDP : « A-t-on l'autorisation pour l'utilisateur donné d'effectuer l'action spécifiée sur la ressource indiquée dans le l'environnement donné ? ». Ce à quoi le PDP répond à la requête en définissant les trois éléments suivants dans sa réponse.

- La décision peut prendre quatre valeurs : « Permit » signifie que le PEP autorise la requête, « Deny » que le PEP la refuse, « Indeterminate » qu'une erreur est survenue ou qu'une donnée manque pour prendre une décision, et « Not Applicable » que la requête ne peut être répondue par ce service.
- Le statut correspond aux codes d'erreur.
- Les obligations sont optionnelles et sont ce que le PEP doit obligatoirement faire avant ou après d'autoriser ou de refuser la requête.

La solution réside dans l'utilisation de l'élément « Obligations » pour effectuer l'action d'écrire dans le journal. La lecture du journal permet par la suite de prévenir le responsable qu'un accès a eu lieu comme le montre l'exemple de règle de contrôle d'accès suivant 4.1.

programme 4.1 – Exemple de règle de contrôle d'accès en XACML

```
1 Allow access to resource DossierMedical with attribute patientID=x
        if Subject match MedecinDeFamillle and action is read
3 with obligation
        on Permit: doLog_Warning(patientID, Subject, time)
```

```
5           on Deny   : doLog_UnauthorizedLogin(patientID, Subject, time)
```

Conséquences

Après la mise en place de ce patron, on dispose d'un moyen de protéger l'accès à une ressource. Cette restriction peut-être outrepassée par certains utilisateurs spécifiés dans les règles de contrôle d'accès. Les responsables de ces utilisateurs seront notifiés de cet accès et pourront demander à ces utilisateurs de justifier leurs actions.

Limitations

Ce patron est limité par les mêmes limitations que le patron Cerbère sur lequel il s'appuie.

Patrons en lien

— **Patte Blanche** : Pour l'authentification des intervenants.
— **Dactylo** : Pour l'authentification à partir des empreintes digitales.
— **Cerbère** : Pour le contrôle d'accès basé sur les rôles.
— **Greffier** : Pour la journalisation des accès à une ressource.

Références

[53] - Markus Lorch, Seth Proctor, Rebekah Lepro, Dennis Kafura et Sumit Shah. « First experiences using XACML for access control in distributed systems ». Dans Proceedings of the 2003 ACM workshop on XML security, XMLSEC '03, pages 25–37. ACM, 2003.

[49] - Basel Katt, Xinwen Zhang, Ruth Breu, Michael Hafner et Jean-Pierre Seifert. « A general obligation model and continuity : enhanced policy enforcement engine for usage control ». Dans Proceedings of the 13th ACM symposium on Access control models and technologies, SACMAT '08, pages 123–132. ACM, 2008.

Brise-glace

[8] - J. Alqatawna, E. Rissanen et B. Sadighi. « Overriding of Access Control in XACML ». Dans Policies for Distributed Systems and Networks, 2007. POLICY '07. Eighth IEEE International Workshop on, pages 87–95, 2007.

Greffier

Alias : Journalisation des évènements, historique des évènements, logging.
Type : Sécurité et sûreté.

Résumé

Ce patron présente la journalisation des évènements. Ce procédé permet de conserver dans un journal les informations sur l'état du système, les erreurs qui surviennent et toutes informations utiles à conserver pour une relecture future.

Problème

De nombreuses situations requièrent de regarder en arrière pour comprendre ou simplement savoir ce qui s'est passé. D'où le besoin de garder des traces des évènements importants ayant un impact sur :

— La sûreté de la personne.
— La sécurité du système d'information.
— Le débogage des applications.
— Le respect du cadre légal.

Afficher à l'écran ce qui se passe n'est pas toujours possible surtout lorsque le programme tourne en tâche de fond ou lorsqu'il plante. Il est nécessaire de disposer d'un moyen de conserver une trace en dehors de l'application.

Greffier

Particularités contextuelles

Santé : Journaliser les actes médicaux, les visites à domicile, les accès permis ou refusés à une ressource

TC : Journaliser les visites à domicile, les demandes d'assistances, les évènements en lien avec l'état de santé physique ou mentale du patient

HI : Journaliser les entrées et sorties, les accès aux informations sensibles, etc.

Solution

La journalisation consiste en l'enregistrement séquentiel et chronologique dans un journal de tous les évènements affectant un processus particulier. Le journal étant soit un fichier, soit une base de données.

Développeurs, concepteurs du système doivent déterminer le type d'information à mettre dans le journal et déterminer leur signification. Il est important d'assigner une entrée du journal au bon niveau de journalisation, autrement de fausses alertes induiraient les administrateurs du système dans l'erreur.

Dans la majorité des systèmes de journalisation, on retrouve les niveaux suivants :

- Information : Message informatif qui indique l'état actuel du système ou l'état d'avancement d'une opération.
- Débogage : Message informatif précis relatif au débogage de l'application.
- Alarme : Désigne des évènements susceptibles d'être nocifs au bon fonctionnement de l'application.
- Erreur : Message concernant une erreur de fonctionnement.
- Fatale : Désigne une erreur très sévère dont on peut présumer qu'elle entraînera le plantage de l'application,
- Trace : Message informatif encore plus précis que celui du débogage de l'application.

Le développeur précise le niveau de journalisation de l'évènement au moment de l'enregistrer, et précise le niveau de journalisation que l'on souhaite donner à

l'application au moment de l'exécuter.

Une entrée du journal doit contenir les informations suivantes :

— Qui : Le nom de l'application ou de l'utilisateur.

— Quand : La date et l'heure de l'entrée.

— Où : Le contexte, la page web, le service, la base de données ...

— Quoi : La commande ou l'opération

— Résultat : Le résultat de la commande ; permission, refus, exception, etc.

La journalisation peut avoir un impact considérable sur les performances de l'application. Si l'application enregistre beaucoup d'évènements, ses performances peuvent s'en trouver fortement ralentie.

La journalisation peut également prendre beaucoup d'espace disque. Lors de l'usage de fichiers, celui-ci peut devenir tellement important en espace disque qu'il ralentit les performances. Mettre en place une rotation est nécessaire pour éviter de manipuler des fichiers atteignant un trop gros volume d'espace disque. Pour cela, le système de journalisation peut être programmé pour fermer le fichier, le renommer avec la date et l'heure de la création du fichier puis utiliser un nouveau fichier.

Pour des raisons de sécurité, légales ou d'audit, la sauvegarde et l'entreposage des journaux pendant plusieurs semaines, mois voir des années est parfois à considérer.

Conséquences

Après application de ce patron, les évènements importants sont enregistrés. La sélection du niveau de journalisation et le choix des évènements à enregistrer vont permettre de garder une trace des évènements significatifs.

Limitations

Ce patron est limité par la qualité des informations sélectionnées qui sont enregistrées dans le journal. De plus, il ne protège pas contre la corruption de fichier dû à un bris mécanique, un bogue, un virus ou une personne qui modifie le journal. Si la taille maximale d'un fichier ou la capacité maximale du disque dur sont atteintes,

les évènements ne sont plus enregistrés. Ceci peut même provoquer un plantage de la machine sur lequel est exécuté ce patron.

Patrons en lien

Aucun.

Références

[50] - Karen Kent et Murugiah P. Souppaya. « Guide to Computer Security Log Management ». Rapport Technique, NIST, Gaithersburg, MD, United States, 2006.

[54] - Teresa F. Lunt. « Automated Audit Trail Analysis and Intrusion Detection : A Survey ». Dans Proceedings of the 11th National Computer Security Conference, pages 65–73, 1988.

Patte blanche

Alias : Authentification.
Type : Sécurité et sûreté.

Résumé

Un problème récurrent lors d'échange de message entre deux individus sur un réseau informatique est de vérifier que la personne a bien l'identité qu'elle prétend avoir. Ce patron aborde le sujet de l'authentification et présente des solutions couramment rencontrées pour vérifier l'identité d'un individu ou d'un système.

Problème

L'identification est le moyen de connaître l'identité d'un individu ou d'un système. Cependant, il est très facile d'utiliser une identité factice ou empruntée à une autre personne. Par exemple, le nom d'utilisateur d'un site internet identifie l'individu, tandis que le mot de passe authentifie que l'utilisateur est bien la personne qu'il prétend être.

Il est donc nécessaire d'employer un moyen de vérification d'identité. Ce procédé est l'authentification.

Particularités contextuelles

Santé : L'authentification du personnel médical est obligatoire pour des raisons légales, de responsabilités et de confidentialité.

TC : L'authentification du patient est utile, mais peut devenir une difficulté en raison de ses troubles cognitifs. En effet, les pertes de mémoire rendent problématique la mémorisation d'un mot de passe ou l'usage d'un badge.

HI : L'HI est un espace ubiquitaire dans lequel on peut interconnecter différents moyens d'authentification de l'HI avec ceux du domaine de la santé.

Solution

L'authentification est utilisée pour vérifier que l'information vient d'une source connue en qui on a confiance.

On distingue trois types d'authentification de l'identité d'un individu ou d'un système, en vérifiant :

1. ce qu'il connait, tels un mot de passe ou un identifiant personnel,
2. ce qu'il possède, tel un jeton de sécurité,
3. ce qu'il est, telles une caractéristique physique comme une empreinte digitale.

Les techniques les plus rencontrées sont les suivantes :

1. Mot de passe : L'utilisation d'un nom d'usager et d'un mot de passe est très répandue comme forme d'authentification sur internet. Pour un maximum de sécurité, la communication entre le poste client et le serveur doit être chiffrée et le mot de passe doit être assez complexe pour ne pas être deviné facilement. Cependant ce moyen peut être problématique pour des personnes avec des troubles de mémoire.
2. Carte de sécurité : C'est une carte avec un code unique remis à l'utilisateur. Cela va de la carte à bande magnétique, à radio-identification, à la carte munie d'une puce informatique.
3. Signature électronique : La signature électronique est basée sur une méthode de chiffrement par clé publique. La clé privée n'est connue que par le signataire du document.

4. Biométrie : L'individu est authentifié par une ou plusieurs caractéristiques morphologiques grâce à des techniques de reconnaissance d'empreinte digitale, faciale, vocale ou rétinienne.

Conséquences

L'authentification permet de s'assurer de l'identité d'un individu ou d'un système. Elle protège en assurant que la personne est bien celle qu'elle prétend être. D'autres moyens sont employés en plus de l'authentification pour contrôler l'accès à une ressource, protégé contre l'écoute illégale et l'altération de message.

Limitations

Ce patron est limité par la qualité du moyen d'authentification utilisé. Un mot de passe trop court ou trop facile peut être trouvé facilement par exemple. Ce patron ne prévient pas contre l'usurpation d'identité si le vol du badge n'est pas reporté ou si le mot de passe est connu par exemple. Utiliser un moyen d'authentification n'est pas suffisant pour garantir le contrôle d'accès des données et la sécurité des données lors de leur transit sur le réseau.

Patrons en lien

— **Dactylo** : Pour l'authentification à partir des empreintes digitales.
— **Cerbère** : Pour le contrôle d'accès basé sur les rôles.
— **Notaire** : Pour la signature électronique.

Référence

[103] - M. Zviran et W. J. Haga. « A Comparison of Password Techniques for Multilevel Authentication Mecha- nisms ». The Computer Journal, 36(3) :227–237, 1993.

[68] - B.C. Neuman et T. Ts'o. « Kerberos : an authentication service for computer networks ». Communications Magazine, IEEE, 32(9) :33–38, 1994.

[92] - Richard E. Smith. Authentication : from passwords to public keys. Addison-Wesley Longman Publishing Co., Inc., 2002.

[67] - R. Molva, D. Samfat et G. Tsudik. « Authentication of mobile users ». Network, IEEE, 8(2) :26–34, 1994.

Dactylo

Alias : Dactylogramme, reconnaissance des empreintes digitales.
Type : Sécurité et sûreté.

Résumé

Ce patron traite de la reconnaissance des empreintes digitales comme moyen d'authentifier une personne à partir de ces empreintes digitales. Un des moyens de valider l'identité d'une personne consiste à vérifier ce qu'elle est, c'est-à-dire vérifier une de ces caractéristiques physiques. La reconnaissance des empreintes digitales est une technique très répandue et efficace dans ce but.

Particularités contextuelles

Santé : L'authentification du personnel médical est obligatoire pour des raisons légales, de responsabilités et de confidentialité.

TC : L'authentification du patient est utile, mais peut devenir une difficulté en raison de ses troubles cognitifs. L'usage d'un moyen d'authentifier le patient par la biométrie présente de nombreux intérêts, pas de mot de passe à retenir et pas de badge à conserver sur soi.

HI : L'HI est un espace ubiquitaire dans lequel on peut interconnecter différents moyens d'authentification de l'HI avec ceux du domaine de la santé.

Dactylo

Problème

Pour accéder à une ressource informatique de façon sécurisée, l'utilisateur doit s'authentifier auprès du système qui vérifie et valide ses droits d'accès. Dans certaines situations, retenir un mot de passe ou porter un badge sécurisé est problématique. Un autre moyen d'authentifier un individu est donc nécessaire.

Ce patron aborde la reconnaissance biométrique des empreintes digitales comme moyen d'authentification.

Particularités contextuelles

L'authentification du patient peut devenir une difficulté en raison de ses troubles cognitifs. En effet, les pertes de mémoire rendent problématique la mémorisation d'un mot de passe qu'il risque d'oublier ou l'usage d'un badge qu'il risque de perdre.

L'utilisation des empreintes digitales est simple et intuitive, et constitue un meilleur moyen d'authentifier un patient avec des troubles cognitifs.

Solution

La reconnaissance par biométrie permet d'authentifier un individu en s'appuyant sur les caractéristiques morphologiques d'un individu. Certaines caractéristiques sont uniques, ce qui procure un moyen de contrôle d'accès simple et efficace. C'est le cas des empreintes digitales. L'empreinte digitale présente les caractéristiques suivantes :

1. Universalité : Chaque personne a des empreintes digitales.
2. Caractère distinctif : Les empreintes digitales sont distinctes d'une personne à une autre.
3. Permanence : Les empreintes ne changent pas au fil du temps.
4. Perceptibilité : La caractéristique doit pouvoir être mesurée quantitativement.

L'empreinte d'une personne peut être reconnue par un lecteur d'empreintes digitales. Parce qu'il est facile à mettre en place, ce procédé est largement répandu et on

le retrouve sur des ordinateurs portables et une multitude d'autres périphériques informatiques.

Dans un système de reconnaissance biométrique, un appareil saisit et enregistre les caractéristiques en question, et un logiciel interprète les données et détermine l'acceptabilité de la personne. Les systèmes de reconnaissance biométrique fonctionnent à trois niveaux :

1. un capteur prend une observation de la caractéristique biométrique ;
2. le système traduit l'observation en termes mathématiques et produit une signature biométrique ;
3. l'ordinateur introduit la signature biométrique dans un algorithme et la compare à une ou plusieurs autres signatures biométriques entreposées dans la base de données du système.

Les empreintes sont souvent enregistrées dans le boîtier qui compose le lecteur. Il existe dorénavant des systèmes qui stockent l'empreinte chiffrée dans un boîtier à part que l'utilisateur porte avec lui. L'avantage réside dans le fait que l'empreinte reste sous le contrôle de l'utilisateur.

Conséquences

La personne est identifiée et authentifiée, et peut avoir accès à certaines ressources sans avoir à retenir un mot de passe et sans avoir à porter un badge.

Limitations

Ce patron est limité par les mêmes limitations que le patron Patte Blanche. Il est également limité par le type de lecteur d'empreinte employé. Certains lecteurs ont des taux de faux positifs différents, certains ne protègent pas contre une falsification de l'empreinte.

Patrons en lien

— **Patte Blanche** : Pour l'authentification des intervenants.
— **Cerbère** : Pour le contrôle d'accès basé sur les rôles.
— **Notaire** : Pour la signature électronique.

Références

[30] - John Chirillo et Scott Blaul. Implementing Biometric Security. Hungry Minds, Incorporated, 1 édition, 2003.

[48] - Lalita Acharya ; Tomasz Kasprzycki ;. La biométrie et son usage par l'État. Ottawa] : Bibliothèque du Parlement, 2010.

[45] - A.K. Jain, A. Ross et S. Prabhakar. « An introduction to biometric recognition ». Circuits and Systems for Video Technology, IEEE Transactions on, 14(1) :4–20, 2004.

[44] - A.K. Jain, L. Hong, S. Pankanti et R. Bolle. « An identity-authentication system using fingerprints ». Proceedings of the IEEE, 85(9) :1365–1388, 1997.

[79] - N.K. Ratha, J.H. Connell et R.M. Bolle. « Enhancing security and privacy in biometrics-based authentication systems ». IBM Systems Journal, 40(3) :614–634, 2001.

Enigma

Alias : Chiffrement des communications, encryption, cryptage, SSL/TLS.
Type : Sécurité et sûreté.

Résumé

Ce patron propose une solution de chiffrement des messages transmis par le réseau Internet pour pallier le problème de confidentialité et d'intégrité. Sur Internet, les communications effectuées en clair risquent d'être écoutées voir altérées par des personnes non autorisées.

Problème

Lors de l'échange de messages via le réseau Internet, ceux-ci sont par défaut transmis en clair. Ils peuvent être interceptés et écouter par des personnes non autorisées. Ces messages peuvent également être altérés et retransmis sur le réseau après modification. Transmettre les messages en clair engendre donc des problèmes de confidentialité et d'intégrité.

Particularités contextuelles

Santé : Dans le domaine de la santé, il est recommandé d'utiliser un certificat fourni par une autorité de certification. Un hôpital ou un centre de réhabilitation doit pouvoir prouver son identité sur le web auprès de ces utilisateurs.

TC : Il n'y a pas vraiment de relation entre ce patron et les troubles cognitifs, à l'exception de l'usage de certificat auto signé qui engendrerait un message d'avertissement dans le navigateur et qui pourrait être mal interprété par le patient.

HI : Pour les serveurs installés du côté de l'HI, il pourrait s'avérer très coûteux d'utiliser des certificats provenant d'une autorité de certification. Dépendamment des moyens financiers alloués à l'installation des HI et si les utilisateurs des serveurs sont l'hôpital et les proches du patient, l'utilisation d'un certificat auto signé peut convenir.

Solution

TLS (Transport Layer Security pour Sécurité au niveau de la couche transport) est un protocole permettant à une application client-serveur de communiquer par le réseau de telle sorte à prévenir l'écoute illégale et l'altération des messages. Il s'agit d'un protocole de chiffrement qui fournit une sécurité des communications en chiffrant les données au niveau de la couche transport. La communication commence par un échange de clé en utilisant un chiffrement asymétrique, puis le chiffrement symétrique est utilisé pour assurer la confidentialité et l'intégrité.

TLS est un standard de l'IETF (Internet Engineering Task Force pour groupe de travail d'ingénieure d'Internet), dernièrement mis à jour dans la RFC 5246 et basé sur les premières spécifications SSL développées par Netscape Communications

Il est généralement implémenté au-dessus des autres protocoles de la couche de transport et encapsule ceux spécifiques aux applications tels que HTTP, FTP, SMTP, NNTP et XMPP. Il est principalement utilisé avec le protocole de transport TCP, mais certaines implémentations supportent également le protocole UDP.

TLS s'appuie beaucoup sur les autorités de certification. À l'ouverture d'une page sécurisée par le navigateur, celui-ci récupère la clé publique et le certificat, et vérifier les trois choses suivantes :

— Que le certificat fasse partie d'un tiers en qui l'on a confiance,
— Que le certificat soit présentement valide,
— Que le certificat ait une relation avec le site web d'ou il provient.

Le navigateur utilise ensuite la clé publique du certificat pour chiffrer une clé symétrique choisie aléatoirement. Le chiffrement par clé publique étant plus coûteux en temps de calcul, la plupart des implémentations utilisent une combinaison de chiffrement par clé publique et clé symétrique. Le navigateur envoie ensuite la clé symétrique chiffrée au serveur qui pourra la déchiffrer. Le navigateur et le client peuvent ensuite utiliser cette clé symétrique pour chiffrer les communications entre eux. Ce faisant, la confidentialité de l'échange est assurée et l'intégrité des données validée.

Une fois la session terminée, la clé symétrique utilisée est effacée. Une nouvelle session verra la création d'une nouvelle clé symétrique.

Pour mettre en place TLS, il n'y a rien à faire sur le navigateur. C'est le serveur qui doit être configuré adéquatement. Il faut :

— Créer et installer un certificat : Il y a deux façons de créer un certificat. La première se fait en passant par une autorité de certification telle que Thawte.com ou TrustCenter.de, qui créera le certificat. La seconde se fait en créant par soi-même un certificat auto signé. Passer par une autorité de certification a un coût financier, mais il est recommandé de procéder ainsi pour des organisations importantes pour des raisons de sécurité. Ainsi un utilisateur aura l'assurance que le certificat aura été délivré pour le bon organisme ou la bonne entreprise. Dans le cas du certificat auto signé, c'est une procédure simple et gratuite. L'inconvénient réside dans le fait qu'il ne prouve pas l'identité du l'organisme ou de l'entreprise qui l'utilise. De plus, les navigateurs affichent un message d'avertissement pour prévenir qu'il s'agit d'un certificat auto signé. Ce type de certificat est recommandé pour des applications web utilisées par un petit groupe de personne ou pour des démonstrations. L'installation du certificat dépend du serveur web utilisé et est expliquée dans la documentation du serveur.

— Configurer le serveur : la configuration du serveur dépend du serveur web utilisé et est expliquée dans la documentation du serveur. Les points importants sont le choix du port utilisé pour TLS, par exemple le port 443 est généralement utilisé pour le protocole HTTP, faire le lien vers le fichier du certificat, préciser le mot de passe pour accéder à la clé du certificat, etc.

— Rediriger les connexions non sécurisées vers des connexions sécurisées : cette

étape est à faire lors de la configuration du serveur également. Il s'agit de rediriger les connexions non sécurisées des connexions sécurisées de manière automatique. Autrement, les deux types de connexions seront possibles, créant des problèmes de sécurité si le mode non sécurisé est utilisé par inadvertance. Par exemple, si l'adresse saisie dans le navigateur est http :url, le serveur peut automatiquement la rediriger vers https :url.

Conséquences

Après application de ce patron, les communications entre une application-client et un serveur :

— bénéficieront d'un haut niveau de chiffrement,
— seront protégées contre l'écoute illégale (respect de la confidentialité),
— seront protégées contre l'altération des données (intégrité des messages)

Limitations

Un message peut être intercepté mais ne peut être lu ou modifié sans la clé. Par contre, il peut être enregistré et envoyé de nouveau sur le réseau à un moment ultérieur. Si la clé privée n'est plus secrète, l'écoute et la modification du contenu sont possibles lors du transport sur le réseau. De plus, la puissance du chiffrement dépend de la taille de la clé. Une clé trop petite peut être cassée facilement. Une clé même grande peut également être cassée à l'aide de machine disposant de très fortes puissances de calcul (super ordinateur).

Patrons en lien

— **Notaire** : Pour la signature électronique.

Références

[5] - SSL and TLS : designing and building secure systems. Addison-Wesley Longman Publishing Co., Inc., 2001.

[97] - Haidong Xia et José Carlos Brustoloni. « Hardening Web browsers against man-in-the-middle and eavesdropping at- tacks ». Dans Proceedings of the 14th international conference on World Wide Web, WWW '05, pages 489–498. ACM, 2005.

Notaire

Alias : Signature électronique, signature digitale, non-répudiation, authenticité.
Type : Sécurité et sûreté.

Résumé

Ce patron présente la signature électronique comme moyen de garantir l'authenticité, l'intégrité et la non-répudiation d'un message. La solution s'appuie sur une technologie de cryptographie asymétrique avec des clés publiques et privées.

Problème

Lors de l'échange d'un message entre deux personnes sur un réseau informatique, celui-ci est susceptible d'être intercepté et modifié durant le transport (attaque de l'homme du milieu). L'expéditeur peut également usurper l'identité d'une autre personne et se faire passer pour quelqu'un d'autre auprès du destinataire. Enfin, l'expéditeur du message peut également se rétracter et prétendre ne pas avoir envoyé le message.

Le destinataire d'un message a besoin d'être assuré que l'expéditeur de celui-ci est bien la personne qu'elle prétend être (la signature du message est authentique, l'identité de l'auteur est vérifiée), que le message n'a pas été altéré durant le transport (l'intégrité du message a été respectée) et que l'expéditeur ne puisse pas nier être l'auteur du message (la non-répudiation est garantie).

Notaire

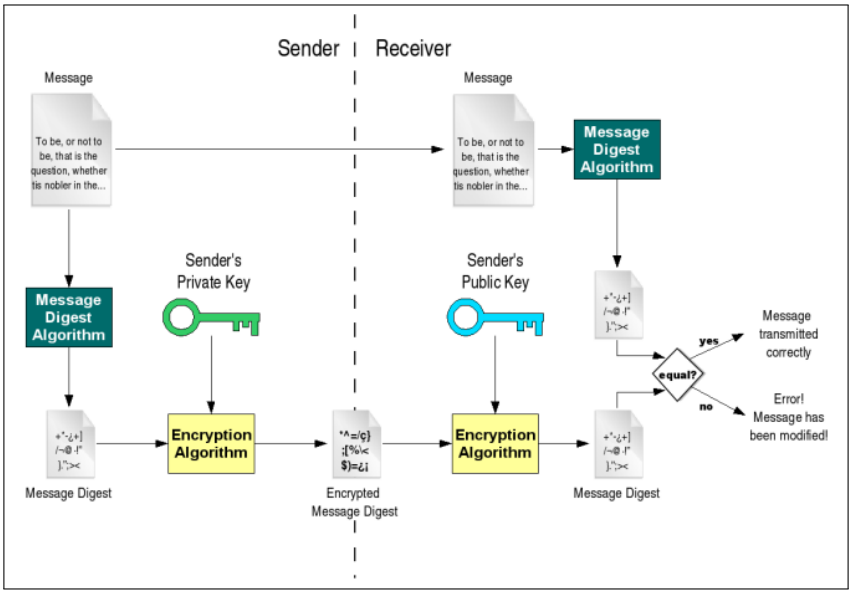

figure 4.9 – Signature électronique

Particularités contextuelles

Santé : Le personnel soignant doit signer des actes et des formulaires. Quand il accepte de prendre en charge un patient, il a une responsabilité légale.

TC : Pas de lien en particulier.

HI : Pas de lien en particulier.

Solution

La signature électronique peut-être utilisée pour répondre au besoin de garantir l'authenticité, l'intégrité et la non-répudiation du message. Lorsque la signature est valide, le destinataire à de bonnes raisons de croire que le message a été créé par un expéditeur connu, authentifié et qui ne peut nier l'avoir envoyé et que le message n'a pas été altéré.

La signature électronique est couramment utilisée dans les situations ou il est important de détecter la falsification ou l'usage de faux.

Notaire

Il s'agit d'une technique de cryptographie asymétrique comme le montre la figure 4.9.

Au préalable, une paire de clés publique/privée est générée. L'expéditeur dispose de la clé privée qu'il garde secrète et le destinataire dispose de la clé publique de l'expéditeur.

L'expéditeur génère l'empreinte numérique du message à l'aide d'une fonction de hachage cryptographique appliquée sur le message. L'empreinte est ensuite chiffrée à l'aide de la clé privée de l'expéditeur. Le résultat de cette opération est la signature électronique du message. La signature est jointe au message.

Le destinataire reçoit le message et la signature électronique de l'expéditeur. La signature est décryptée à l'aide de la clé publique pour obtenir l'empreinte numérique du message calculée par l'expéditeur. Le destinataire génère ensuite l'empreinte numérique du message reçu et la compare avec celle provenant de la signature. En cas de correspondance entre elles, cela signifie que le message a bien été signé par le détenteur de la clé privée, que le message n'a pas été modifié durant le transport et qu'il est authentique. Autrement, il s'agit d'un faux.

La qualité de la signature dépend de la taille de la clé générée et de l'algorithme utilisé.

Le chiffrement et la signature peuvent être utilisés conjointement ou séparément. Dans ce cas :

1. Si le message est codé, mais non signé, seul le détenteur de la clé peut le lire, mais sans savoir avec certitude qui en est l'auteur.
2. Si le message est signé, mais non codé, tout le monde peut savoir qui en est l'auteur et tout le monde peut le lire.
3. Si le message est codé puis signé, seul le détenteur de la clé peut le lire, mais tout le monde peut savoir qui en est l'auteur.
4. Si le message est signé puis codé, seul le détenteur de la clé peut le lire, et seul lui peut en connaître l'auteur.

Conséquences

Si l'empreinte du message calculée par le destinataire correspond à celle obtenue par le décryptage de la signature, cela signifie que les qualités suivantes de la signature sont respectées :

— Authentique : L'identité de l'expéditeur est connue de manière certaine.
— Infalsifiable : La signature n'a pas été falsifiée, et il n'y a pas eu usurpation d'identité.
— Non réutilisable : La signature fait partie du message signé et ne peut être réutilisée pour un autre message.
— Inaltérable : Le message signé ne peut plus être modifié.
— Irrévocable : L'expéditeur qui a signé ne peut nier être l'auteur du message.

La signature électronique protège de l'attaque « Attaque de l'homme du milieu », mais pas contre « l'écoute clandestine » pour laquelle il faut chiffrer également le message.

Limitations

Un message peut être intercepté mais ne peut être lu ou modifié sans la clé. Par contre, il peut être enregistré et envoyé de nouveau sur le réseau à un moment ultérieur. Si la clé privée n'est plus secrète, contrefaire la signature est possible. De plus, la puissance du chiffrement dépend de la taille de la clé. Une clé trop petite peut être cassée facilement. Une clé même grande peut également être cassée à l'aide de machine disposant de très fortes puissances de calcul (super ordinateur).

Patrons en lien

— **Enigma** : Pour le chiffrement des messages.

Références

[82] - R. L. Rivest, A. Shamir et L. Adleman. « A method for obtaining digital signatures and public-key cryptosystems ». Commun. ACM, 21(2) :120–126, février 1978.

[102] - Jianying Zhou et Dieter Gollmann. « Evidence and non-repudiation ». Journal of Network and Computer Applications, 20(3) :267 – 281, 1997.

[101] - Jianying Zhou et D. Gollman. « A fair non-repudiation protocol ». Dans Security and Privacy, 1996. Proceedings., 1996 IEEE Symposium on, pages 55–61, 1996.

[61] - Ueli Maurer, Mihir Bellare et Phillip Rogaway. « Lecture Notes in Computer Science ». Dans Advances in Cryptology —EUROCRYPT '96, volume 1070, pages 399–416. Springer Berlin Heidelberg, 1996.

Garant

Alias : Disponibilité des services web.
Type : Fiabilité et sûreté.

Résumé

Ce patron aborde le problème de la disponibilité des services web et présente une série de mesures pour la garantir.

Lorsqu'un service web est essentiel au bon déroulement d'opérations critiques, toute interruption de service peut avoir des conséquences graves. Des mesures existent pour minimiser le temps d'indisponibilité.

Problème

La disponibilité est l'aptitude d'une entité à être en état d'accomplir une fonction requise dans des conditions données à un instant donné. La disponibilité est compromise lorsque l'information recherchée ne peut être obtenue du système lors d'un besoin ponctuel.

Un service web peut à tout moment tomber en panne et provoquer une interruption de service. Plusieurs causes peuvent provoquer ces pannes. Une panne peut être d'ordre matériel, par exemple, un bris d'un composant du serveur qui héberge le service, d'ordre logiciel, comme lors d'un plantage de la plateforme logicielle qui supporte le service. Elle peut également être d'origine humaine suite à une erreur ou à un acte volontaire d'interrompre le service, ou d'origine naturelle, comme lorsque qu'une catastrophe naturelle frappe l'endroit ou le serveur se situe.

Garant

Lors d'une défaillance, le service devient alors indisponible jusqu'à l'identification et la résolution du problème. Ceci prend du temps et provoque une interruption de service. Cette période d'indisponibilité de service peut engendrer des problèmes graves pour les personnes ou systèmes qui en dépendent.

Particularités contextuelles

Santé : La disponibilité d'un service web peut être critique pour les utilisateurs qui en dépendent. Par exemple, l'indisponibilité d'un service web d'accès au dossier médical du patient peut rendre le suivi médical problématique dans le meilleur des cas, et avoir des répercussions très graves lors de situations d'intervention d'urgence. La responsabilité en cas d'inaccessibilité peut être imputée à l'organisme de santé qui le fournit.

TC : Pour une personne ayant des troubles cognitifs, se retrouver face à une interface non responsive peut-être très frustrant. La personne peut ne pas comprendre pourquoi le système faisant appel au service web ne fonctionne pas.

HI : Pas de lien en particulier.

Solution

Bien qu'il n'existe pas de solution miracle pour empêcher toutes les pannes, il est possible de réduire le temps d'indisponibilité en employant certaines mesures d'ordre matériel, logiciel ou stratégique. Ces mesures visent généralement à remettre en route le service au plus vite ou à dupliquer le service pour que l'interruption de l'un d'eux soit invisible et sans conséquence pour les utilisateurs.

Parmi les mesures les plus utilisées, on retrouve les suivantes :

1. **Redondance du matériel :** Cette mesure implique de multiplier le matériel informatique pour qu'un composant soit automatiquement disponible lorsqu'un similaire tombe en panne [62].Avoir deux serveurs sur deux sites différents per-

mettra la redondance de l'information en divisant le risque de panne. Une organisation du système en grappe est toutefois nécessaire pour automatiser le basculement d'un site à l'autre.

2. **Sécurisation des données :** Pour prévenir la perte de données, la redondance des données sur disques durs ou la prise d'un instantané des données sont préconisées [28]. Les données sont automatiquement synchronisées à plusieurs endroits différents de sorte qu'un point de stockage des données soit toujours disponible si l'un devait devenir inaccessible.
3. **Réduction du temps moyen de remise en service :** Cette mesure vise à minimiser le temps nécessaire à la remise en route du service web [72] en cas d'évènement majeur tel la perte de données ou le bris de matériel. Par exemple, en cas de bris d'un composant du serveur web, disposer d'un composant de remplacement et d'un technicien disponible en quelques minutes permet de réduire le temps durant lequel le serveur est en panne.
4. **Support des applications :** Empêcher l'exploitation de bogues ou résoudre rapidement les failles de sécurité pour éviter qu'elles ne provoquent des ralentissements voir des arrêts de service [95].

Cette liste n'est pas exhaustive est d'autres mesures sont à prendre en considération en supplément ou en alternative pour augmenter la disponibilité [93].

Conséquences

Plus les mesures seront mises en œuvre, plus le risque d'avoir des périodes d'indisponibilité est faible. La liste des moyens mis en œuvre doit être réévaluée régulièrement et être mise à jour dans un document.

Limitations

Les limitations dépendent des moyens mis en œuvre par rapport aux objectifs de taux de disponibilités. Par exemple, si les moyens techniques de redondance des services sont dans le même bâtiment, la disponibilité des services n'est pas garantie

en cas d'incendie. De plus, si l'ensemble des services sont victime d'une attaque de type déni de service (*DOS attack* ou *DDOS attack* si elle est distribuée) au même moment, les services peuvent devenir difficiles d'accès voir totalement indisponibles.

Patrons en lien

— **Pulsation** : Pour vérifier la disponibilité d'un service web.
— **Relanceur** : Pour relancer la requête une fois le service web disponible à nouveau.

Références

[12] - Barry Barber. « Patient data and security : an overview ». International Journal of Medical Informatics, 49(1) :19–30, 1998

[13] - Barry Barber, Alison Treacher, Kees Louwerse et C. P. Louwerse. Towards Security in Medical Telematics : Legal and Technical Apsects. IOS Press, 1996.

[35] - Amado L. Espinosa. « Availability of health data : requirements and solutions ». International Journal of Medical Informatics, 49(1) :97–104, 03 1998.

[57] - Evan Marcus et Hal Stern. Blueprints for high availability (Second ed.). John Wiley and Sons, 2003.

[62] - N.R. May, H.W. Schmidt et I.E. Thomas. « Service Redundancy Strategies in Service-Oriented Architectures ». Dans 35th Euromicro Conference on Software Engineering and Advanced Applications 2009 (SEAA '09) , pages 383 –387, aug. 2009.

[95] - Ju An Wang et Minzhe Guo. « OVM : An Ontology for Vulnerability Management ». Dans Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research : Cyber Security and Information Intelligence Challenges and Strategies, CSIIRW '09, pages 34 :1–34 :4. ACM, 2009.

[72] - Susan Orge et Tom Kippola. « Reduce Mean Time to Repair with Expert Systems ». Penton's Controls and Systems, 39(6) :42, 1992.

[28] - Peter M. Chen, Edward K. Lee, Garth A. Gibson, Randy H. Katz et David A. Patterson. « RAID : High-Performance, Reliable Secondary Storage ». ACM

Computing Surveys, 26 :145–185, 1994.

[77] - Floyd Piedad et Michael Hawkins. High availability : Design, techniques, and processes. Prentice Hall PTR, 2001.

[93] Maria Toeroe et Francis Tam, éditeurs. Service Availability : Principles and Practices. Wiley, 2012.

[55] - A. R. Luria. Human brain and psychological processes. Harper and Row (New York), 1966.

[69] - Donald A. Norman et Tim Shallice. « Attention to Action : Willed and Automatic Control of Behavior ». Dans R. J. Davidson, G. E. Schwartz et D. Shapiro, éditeurs, Consciousness and Self-Regulation, Volume 4, pages 1–18. Plenum Press, 1986.

Pulsation

Alias : Détection d'indisponibilité de service, heartbeat.
Type : Fiabilité et sûreté.

Résumé

Lorsqu'un service web devient indisponible, l'interruption n'est pas détectée par le client sur le coup. L'indisponibilité peut n'être remarquée qu'au moment où un client tente de l'utiliser, voir ne pas être détectée du tout laissant l'utilisateur devant une interface non responsive.

Ce patron aborde le problème de l'indisponibilité de service web et propose un moyen de la détecter.

Problème

La connexion entre un client et un service web ne perdure qu'un temps très court lorsque le client sollicite le service. Le reste du temps, le client ne maintient pas de connexion active avec le service web et ne peut savoir si celui-ci est accessible ou non. Une interruption de service peut avoir lieu, puis être résolue sans que le client ne remarque rien à raison qu'il ne sollicite pas le service. Lorsque le client sollicite un service indisponible, celui-ci reste sans réponse jusqu'à ce qu'un dépassement de délai ne survienne. Ce dépassement de délai peut être pris en compte par le client ou non. S'il est pris en compte par le client, l'interface du client peut prévenir l'utilisateur. Autrement, il se peut que l'interface reste sans réponse et gèle, laissant son utilisateur

dans l'embarras. Dans les deux cas, l'utilisateur est pris au dépourvu. Repérer l'indisponibilité permet au client de prévenir son utilisateur d'une part, et permet également d'anticiper voir de remédier à cette situation avant qu'elle ne gène les utilisateurs.

Particularités contextuelles

Santé : La disponibilité d'un service web peut être critique pour les utilisateurs qui en dépendent. Par exemple, l'indisponibilité d'un service web d'accès au dossier médical du patient peut rendre le suivi médical problématique dans le meilleur des cas, et avoir des répercussions très graves lors de situations d'intervention d'urgence. La responsabilité en cas d'inaccessibilité peut être imputée à l'organisme de santé qui le fournit.

TC : Pour une personne ayant des troubles cognitifs, se retrouver face à une interface non responsive peut-être très frustrant. La personne peut ne pas comprendre pourquoi le système faisant appel au service web ne fonctionne pas.

HI : Pas de lien en particulier.

Solution

La solution consiste en l'implémentation d'une méthode supplémentaire qui retourne un message au client comme le montre la figure 4.10. Cette méthode ne requière pas de paramètre particulier et ne devrait pas nécessiter de mécanisme de sécurité particulier pour simplifier son utilisation lors des phases d'intégration et de débogage. Elle peut soit retourner un code spécifique, soit retourner à l'identique le message du client, telle une méthode de type echo.

Le client peut appeler cette méthode pour prendre le « pouls » du service, afin de savoir si celui-ci est opérationnel et joignable à son adresse connue. Cette méthode permet simplement au client de vérifier que le service existe et est en état de marche. En appelant cette méthode à intervalle régulier, le client peut détecter l'indisponibilité du service et prévenir l'usager d'un dysfonctionnement.

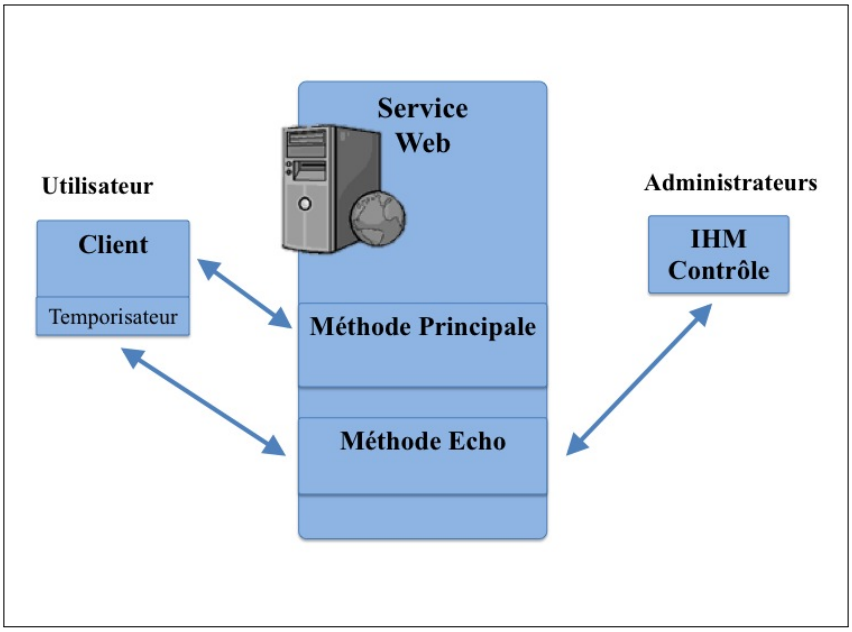

figure 4.10 – Détection d'indisponibilité de service

Conséquences

Lorsque l'indisponibilité devient détectable, des dispositifs peuvent être mis en place pour anticiper les nuisances qui en résultent. Les administrateurs peuvent également mettre en place un système de contrôle de disponibilité des services web dont ils sont responsables et émettre une alerte lorsqu'un service ne répond plus. Un indicateur d'indisponibilité du service peut-être affiché sur l'interface personne-machine du client. Des alternatives peuvent être utilisées pour compenser l'utilisation du service web, telle l'utilisation de la ligne téléphonique pour prévenir les secours en cas d'urgence par exemple.

Limitations

L'indisponibilité d'un service est détectée par le client qui la vérifie au niveau local. Cela peut être le service devenu indisponible, la connexion entre le client et le service, le réseau local auquel le client est connecté ou la machine sur lequel tourne le client qui pose problème.

Patrons en lien

— **Garant** : Pour assurer la disponibilité d'un service web.
— **Relanceur** : Pour relancer la requête une fois le service web disponible à nouveau.

Références

[55] - A. R. Luria. Human brain and psychological processes. Harper and Row (New York), 1966.

[69] - Donald A. Norman et Tim Shallice. « Attention to Action : Willed and Automatic Control of Behavior ». Dans R. J. Davidson, G. E. Schwartz et D. Shapiro, éditeurs, Consciousness and Self-Regulation, Volume 4, pages 1–18. Plenum Press, 1986.

Chapitre 5

Application des patrons de sécurité, de fiabilité et de sûreté dans les scénarios

Ce chapitre présente la deuxième partie des résultats, soit l'application des patrons de sécurité, de fiabilité et de sûreté dans les cinq scénarios du Chapitre 2. La première partie étant le catalogue du Chapitre 4.

À partir des scénarios illustrés dans le Chapitre 2, nous avons identifié des besoins de sécurité, de fiabilité et de sûreté auxquels les développeurs doivent répondre dans leurs applications destinées aux habitats intelligents pour personnes ayant des troubles cognitifs. À partir de ces besoins, nous avons trouvé des solutions que nous avons exprimées sous la forme de patrons de sécurité, de fiabilité et de sécurité. Ces patrons ont été regroupés dans le catalogue de patrons de sécurité, de fiabilité et de sécurité présenté dans le Chapitre 4.

Ce chapitre reprend les cinq scénarios un à un et établit une correspondance, entre les besoins identifiés et les patrons ou les combinaisons de patrons qui répondent à ces besoins. Certaines implémentations complexes de patrons y sont également détaillées. Ce chapitre est organisé en sections correspondants à la présentation des résultats scénario par scénario à l'exception des deux premiers qui partagent l'implémentation commune d'un patron.

5.1 Scénario 1 - Assistance médicale à domicile et scénario 2 - Intervention d'urgence

Cette section présente l'application des patrons de sécurité, de fiabilité et de sûreté du catalogue dans le scénario 1 - Assistance médicale à domicile et dans le scénario 2 - Intervention d'urgence pour répondre aux besoins identifiés dans le Chapitre 2.

Les scénarios de demande d'assistance médicale et d'intervention d'urgence ont des services essentiels à leur bon déroulement en commun, leur regroupement au sein de la même section permet de présenter ces services et leur organisation au même endroit.

Ces scénarios démarrent par l'envoi d'une requête adressée au CSIU et se termine au CSIU également par le rapport du dernier intervenant ayant pris en charge le patient. Entre temps, différents services et intervenants participent à la prise en charge du patient, ce qui en nécessite la coordination par le CSIU.

Les points de départ, soient les requêtes d'alerte sont similaires à la différence que l'une est moins urgente que l'autre. Les points de terminaisons sont similaires également, le rapport de fin d'intervention ou d'assistance est envoyé au CSIU, ce qui termine la prise en charge du patient. Afin de coordonner ces services et les intervenants de façon sécuritaire, un processus d'orchestration commun est mis en place au CSIU.

Cette section est organisée ainsi : les correspondances entre les besoins des scénarios 1 et 2 et les patrons qui y répondent sont présentées dans un tableau (Section 5.1.1), puis les services web spécifiques à l'élaboration de la prise en charge du patient par le CSIU sont détaillés (Section 5.1.2). Enfin, nous détaillons l'orchestration des services web (Sous-Section 5.1.3).

5.1.1 Application des patrons dans les scénarios 1 et 2

L'application des patrons issus du catalogue de patrons de sécurité, de fiabilité et de sûreté pour répondre aux besoins des scénarios 1 et 2 est détaillée dans les tableaux suivants. Le Tableau 5.1 répond à la première partie des besoins et le Tableau 5.2 répond à la deuxième partie des besoins. Ces tableaux sont organisés de manière

Besoin 1 : Les services du CSIU doivent être disponibles en tout temps.
Patron 17 - Garant : Pour assurer la disponibilité des services web critiques. Patron 18 - Pulsation : Pour détecter l'indisponibilité d'un service web critique. Patron 9 - Relanceur : Pour mettre en mémoire une requête et la relancer quand le service devient disponible à nouveau.
Besoin 2 : L'intervenant qui accepte la prise en charge en assume la responsabilité et ne peut répudier la prise en charge par la suite.
Patron 16 - Notaire : Pour que la signature électronique serve à garantir la non-répudiation.
Besoin 3 : Respecter le caractère privé des transmissions de données sensibles et en garantir la confidentialité, l'authenticité et l'intégrité.
Patron 15 - Enigma : Pour chiffrer les communications et en assurer la confidentialité et l'intégrité. Patron 16 - Notaire : Pour que la signature électronique serve à garantir l'authenticité de la transmission.
Besoin 4 : Les intervenants qui participent à la prise en charge doivent être authentifiés.
Patron 13 - Patte blanche : Pour que l'intervenant utilise un moyen d'authentification. Patron 14 - Dactylo (optionnel) : Pour que l'authentification soit effectuée au moyen de la reconnaissance des empreintes digitales.
Besoin 5 : Prévenir l'accès au DME aux personnes non autorisées.
Patron 10 - Cerbère : Pour appliquer un contrôle d'accès au DME basé sur les rôles. Patron 12 - Greffier : Pour journaliser l'accès au DME.
Besoin 6 : Le patient doit porter les capteurs et son terminal e-Santé à l'extérieur.
Patron 5 - Detector : Pour détecter le port des capteurs et du terminal à la sortie de l'appartement.
Besoin 7 : Respecter un temps de réponse court même lorsqu'aucun médecin n'est disponible.
Patron 17 - Garant : Pour assurer la disponibilité des services web critiques. Patron 18 - Pulsation : Pour détecter l'indisponibilité d'un service web critique. Patron 1 - Chef d'orchestre : Pour orchestrer les services web de prise en charge du patient. Voir la liste des services web (Section 5.1.2) et les détails de l'orchestration (Section 5.1.3).

tableau 5.1 – Correspondances (1/2) entre les besoins des scénarios 1 et 2 et les patrons issus du catalogue.

Besoin 8 : Le bon déroulement des différentes étapes de la prise en charge doit être garanti par le CSIU.
Patron 1 - Chef d'orchestre : Pour orchestrer les services web de prise en charge du patient. Voir la liste des services web (Section 5.1.2) et les détails de l'orchestration (Section 5.1.3).
Besoin 9 : Le patient doit être localisé avant d'envoyer les secours.
Patron 3 - Petit Poucet : Pour retrouver la localisation du patient.
Besoin 10 : Prévenir l'accès à la localisation du patient aux personnes non autorisées.
Patron 10 - Cerbère : Pour appliquer un contrôle d'accès à la localisation du patient basé sur les rôles. Patron 12 - Greffier : Pour journaliser l'accès à la localisation du patient.

tableau 5.2 – Correspondances (2/2) entre les besoins des scénarios 1 et 2 et les patrons issus du catalogue.

verticale par besoin auquel est associé le patron ou l'ensemble de patrons qui répond à ce besoin.

5.1.2 Les services de prises en charge du patient

Cette section présente les services web du CSIU et du HI nécessaires à la prise en charge du patient.

Dans le cas de l'assistance médicale, on cherche à mettre en lien le patient avec un médecin, son médecin traitant de préférence, ou un autre médecin disponible autrement. Le médecin qui prend en charge le patient se charge de le contacter directement, et en fonction des données physiologiques enregistrées par les capteurs du médecin, peut décider ou non d'envoyer les secours.

Dans le cas de l'intervention d'urgence, le principe est similaire, à la différence que ce sont les secours qui prennent en charge le patient et qu'il est parfois nécessaire de localiser le patient, ce qui nécessite de mettre en œuvre un moyen de déterminer sa position.

— **SW_Alerte :** Ce service est appelé par le patient ou par l'habitat lui-même en cas de demande d'assistance ou de demande d'intervention urgente. Accessible

sur le serveur de CSIU, ce service initie la prise en charge du patient.

- **SW_Medecin :** Ce service est responsable de trouver un docteur disponible pour le patient. En premier lieu, c'est le médecin traitant qui est sélectionné, puis son remplaçant s'il y en a un, puis n'importe quel médecin disponible. Un médecin est assigné pour la prise en charge du patient s'il répond favorablement à la requête de prise en charge envoyée par le service web dans un intervalle de temps donné. En l'absence de réponse ou en cas d'impossibilité de sa part, le médecin suivant est notifié. Le service procède ainsi jusqu'à l'acceptation d'un médecin disponible ou jusqu'à un temps limite à la fin duquel la demande d'assistance est transférée au service de secours.
- **SW_Localisation :** Lorsque la requête d'intervention ne contient pas la position actuelle du patient, le service de localisation du CSIU est responsable de la trouver. Ce service permet de notifier le CSIU qu'une requête d'intervention d'urgence est en attente de l'obtention de la position du patient.
- **SW_Secours :** Ce service notifie les sauveteurs qu'une intervention d'urgence est nécessaire. Le nom du patient et ses coordonnées leur sont spécifiés.
- **SW_Rapport :** Ce service permet aux acteurs de la prise en charge du patient de reporter leur intervention au CSIU. Ce service archive le rapport et met fin au processus de prise en charge du patient.
- **SW_HI_Evenements :** Les derniers évènements détectés par le réseau de capteurs sont accessibles par ce service disponible dans l'habitat intelligent. Il est utilisé pour localiser le patient à l'intérieur de l'habitat intelligent et il est uniquement accessible par le CSIU.

À l'exception du service web WS_HI_Evenements, la totalité des services précédents sont déployés au CSIU et font partie intégrante du processus de prise en charge du patient (Figure 5.1). Ce processus est décrit dans la section suivante.

5.1.3 Orchestration des services de prise en charge du patient

Cette section présente l'orchestration des services web mis en place dans les Scénarios 1 et 2. L'orchestration de ses services correspond à l'application du patron Chef d'orchestre (Patron 1 du catalogue).

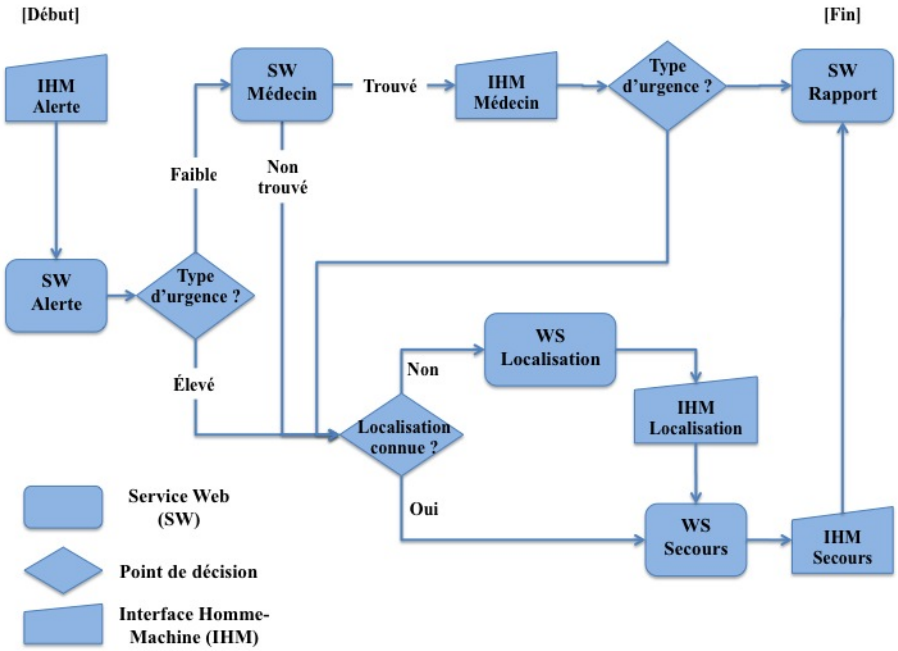

figure 5.1 – Processus d'orchestration des services web de prise en charge du patient

Les services de prise en charge du patient présentés dans la section précédente sont coordonnés par un processus d'orchestration de service web (Figure 5.1). L'orchestration est décrite avec BPEL (Business Process Execution Language, un langage d'execution de processus métier) et exécutée par le moteur d'exécution ActiveBPEL sur un serveur Tomcat du CSIU.

La figure 5.1 montre les services web (les formes carrées), les IHM (les formulaires de saisie de données) et les points de décision (les losanges).

Les IHM représentent les interventions humaines durant le processus, par exemple, l'acceptation du médecin de la prise en charge du patient. Lorsque la main est donnée à une IHM, le processus est interrompu. La soumission d'une réponse depuis l'IHM permet la reprise du processus.

Les points de décisions sont des conditions vérifiées par le moteur d'exécution BPEL qui vont déterminer la direction du processus. Par exemple, le niveau d'urgence est-il faible (demande d'assistance) ou élevé (intervention d'urgence) ou la localisation du patient est-elle connue ?

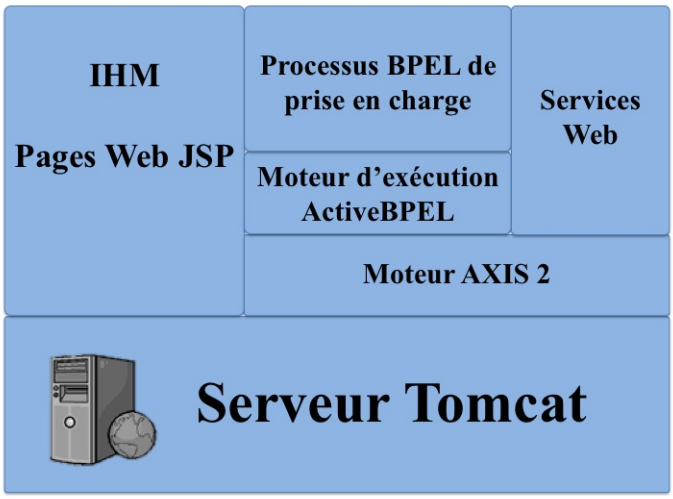

figure 5.2 – Architecture supportant le processus d'orchestration des services web

L'architecture qui supporte le processus BPEL est la suivante (Figure 5.2) : le moteur d'exécution BPEL est ActiveBPEL [94], il tourne sur le serveur Tomcat et le moteur d'exécution de web service Axis 2, ActiveBPEL étant un service web, il se déploie de la même manière qu'un service web dans Axis 2.

Les scénarios 1 et 2 ont été implémentés dans le cadre d'une collaboration avec SAP Labs France et de la participation au projet européen SERENITY [3]. Ils ont fait l'objet de démonstrations lors du European Research towards Trusted Ambient intelligence (EuroTRUSTAmI'08) à Sophia Antipolis en France.

5.2 Scénario 3 - Visite à domicile des intervenants

Cette section présente l'application des patrons de sécurité, de fiabilité et de sûreté du catalogue dans le scénario 3 - Visite à domicile des intervenants pour répondre aux besoins identifiés dans le Chapitre 2.

Cette section est organisée ainsi : les correspondances entre les besoins du scénario 3 et les patrons qui y répondent sont présentées dans la section 5.2.1, puis le prototypage du scénario 3 est détaillé dans la section 5.2.2.

Besoin 1 : Les services du CSIU doivent être disponibles en tout temps.
Patron 17 - Garant : Pour assurer la disponibilité des services web critiques. Patron 18 - Pulsation : Pour détecter l'indisponibilité d'un service web critique. Patron 9 - Relanceur : Pour mettre en mémoire une requête et la relancer quand le service devient disponible à nouveau.
Besoin 2 : L'intervenant qui accepte la prise en charge en assume la responsabilité et ne peut répudier la prise en charge par la suite.
Patron 16 - Notaire : Pour que la signature électronique serve à garantir la non-répudiation.
Besoin 3 : Respecter le caractère privé des transmissions de données sensibles et en garantir la confidentialité, l'authenticité et l'intégrité.
Patron 15 - Enigma : Pour chiffrer les communications et en assurer la confidentialité et l'intégrité. Patron 16 - Notaire : Pour que la signature électronique serve à garantir l'authenticité de la transmission.
Besoin 4 : Les intervenants qui participent à la prise en charge doivent être authentifiés.
Patron 13 - Patte blanche : Pour que l'intervenant utilise un moyen d'authentification. Patron 14 - Dactylo (optionnel) : Pour que l'authentification soit effectuée au moyen de la reconnaissance des empreintes digitales.

tableau 5.3 – Correspondances (1/2) entre les besoins du scénario 3 et les patrons issus du catalogue.

5.2.1 Application des patrons dans le scénario 3

L'application des patrons issus du catalogue de patrons de sécurité, de fiabilité et de sûreté pour répondre aux besoins du scénario 3 est détaillée dans les tableaux suivants. Le Tableau 5.3 répond à la première partie des besoins et le Tableau 5.4 répond à la deuxième partie des besoins. Ce tableau est organisé de manière verticale par besoin auquel est associé le patron ou l'ensemble de patrons qui répond à ce besoin.

Besoin 11 : L'affichage du DME au domicile du patient, seuls le patient et le médecin doivent être dans la pièce utilisée pour la consultation.
Patron 2 - Concierge : Pour le suivi des présences. Patron 10 - Cerbère : Pour appliquer un contrôle d'accès au DME basé sur les rôles. Patron 12 - Greffier : Pour journaliser l'accès au DME. Patron 13 - Patte blanche : Pour que l'intervenant utilise un moyen d'authentification.
Besoin 12 : L'identité de l'intervenant et le but de sa visite doivent être connus pour rappel au patient.
Patron 4 - Memento : Pour le rappel du contexte d'une visite. Patron 13 - Patte blanche : Pour que l'intervenant utilise un moyen d'authentification. Patron 14 - Dactylo (optionnel) : Pour que l'authentification soit effectuée au moyen de la reconnaissance des empreintes digitales.
Besoin 13 : Un intervenant disposant d'un accès limité aux réseaux de capteurs peut avoir une nécessité ponctuelle et limitée dans le temps d'avoir accès à plus d'information.
Patron 10 - Cerbère : Pour appliquer un contrôle d'accès aux réseaux de capteurs basé sur les rôles. Patron 11 - Brise-glace : Pour permettre à l'intervenant d'outrepasser temporairement ses droits d'accès aux réseaux de capteurs. Patron 12 - Greffier : Pour journaliser l'accès aux réseaux de capteurs. Patron 13 - Patte blanche : Pour que l'intervenant utilise un moyen d'authentification.

tableau 5.4 – Correspondances (2/2) entre les besoins du scénario 3 et les patrons issus du catalogue.

5.2.2 Le prototypage du scénario 3

Le scénario 3 (Visite à domicile des intervenants) a fait l'objet d'un prototypage dans le cadre du projet SERENITY. Le prototype a été démontré lors du rendez-vous européen de la recherche dans le domaine des technologies de l'information et de la communication (TIC) à Lyon, France en 2008 (ICT Lyon 2008).

Le prototype et certains patrons sont décrits dans l'article paru dans le journal IJSH *International Journal of Smart Home* [23] (voir Annexe B).

L'article présente le scénario de la visite à domicile, les acteurs et l'environnement du scénario, une sélection de besoins de sécurité à considérer puis présente le concept de patron de sécurité et le projet SERENITY. Finalement la solution mise au point pour combler le besoin 11 - *L'affichage du DME au domicile du patient, seuls le patient et le médecin doivent être dans la pièce utilisée pour la consultation* est détaillée avec l'ensemble de patrons qui la compose.

5.3 Scénario 4 - Accès à l'appartement

Cette section présente l'application des patrons de sécurité, de fiabilité et de sûreté du catalogue dans le scénario 4 - Accès à l'appartement pour répondre aux besoins identifiés dans le Chapitre 2.

L'application des patrons issus du catalogue de patrons de sécurité, de fiabilité et de sûreté pour répondre aux besoins du scénario 4 est détaillée dans le tableau 5.5. Ce tableau est organisé de manière verticale par besoin auquel est associé le patron ou l'ensemble de patrons qui répond à ce besoin.

5.4 Scénario 5 - Utilisation des moyens de paiement

Cette section présente l'application des patrons de sécurité, de fiabilité et de sûreté du catalogue dans le scénario 5 - Utilisation des moyens de paiement pour répondre aux besoins identifiés dans le Chapitre 2.

Besoin 14 : L'accès à l'appartement doit se faire sans clé.
Patron 12 - Greffier : Pour journaliser l'accès à l'appartement. Patron 14 - Dactylo : Pour que l'authentification effectuée au moyen de la reconnaissance des empreintes digitales serve à déverrouiller la porte d'entrée.
Besoin 15 : Restreindre l'accès à l'appartement aux personnes autorisées seulement.
Patron 10 - Cerbère : Pour appliquer un contrôle d'accès à l'appartement basé sur les rôles. Patron 12 - Greffier : Pour journaliser l'accès à l'appartement. Patron 13 - Patte blanche : Pour que l'intervenant utilise un moyen d'authentification. Patron 14 - Dactylo (optionnel) : Pour que l'authentification soit effectuée au moyen de la reconnaissance des empreintes digitales.
Besoin 16 : Autoriser un intervenant ou un groupe spécifique d'intervenant à accéder à l'appartement dans une situation d'urgence.
Patron 10 - Cerbère : Pour appliquer un contrôle d'accès à l'appartement basé sur les rôles. Patron 11 - Brise-glace : Pour permettre à l'intervenant d'outrepasser temporairement ses droits d'accès à l'appartement. Patron 12 - Greffier : Pour journaliser l'accès à l'appartement. Patron 13 - Patte blanche : Pour que l'intervenant utilise un moyen d'authentification.
Besoin 17 : Garder une liste des personnes qui entrent dans l'appartement.
Patron 2 - Concierge : Pour le suivi des présences. Patron 8 - Juda : Pour la prise d'une photographie du visiteur qui sonne à la porte. Patron 12 - Greffier : Pour journaliser l'accès à l'appartement.
Besoin 18 : Prévenir la présence ou la fréquence de visite de certains visiteurs.
Patron 2 - Concierge : Pour le suivi des présences. Patron 8 - Juda : Pour la prise d'une photographie du visiteur qui sonne à la porte. Patron 12 - Greffier : Pour journaliser l'accès à l'appartement.

tableau 5.5 – Correspondances entre les besoins du scénario 4 et les patrons issus du catalogue.

Besoin 4 : Les intervenants qui participent à la prise en charge doivent être authentifiés.
Patron 13 - Patte blanche : Pour que l'intervenant utilise un moyen d'authentification. Patron 14 - Dactylo (optionnel) : Pour que l'authentification soit effectuée au moyen de la reconnaissance des empreintes digitales.
Besoin 12 : L'identité de l'intervenant et le but de sa visite doivent être connus pour rappel au patient.
Patron 4 - Memento : Pour le rappel du contexte d'une visite. Patron 13 - Patte blanche : Pour que l'intervenant utilise un moyen d'authentification. Patron 14 - Dactylo (optionnel) : Pour que l'authentification soit effectuée au moyen de la reconnaissance des empreintes digitales.
Besoin 19 : Savoir quand un moyen de paiement est utilisé.
Patron 5 - Detector : Pour détecter l'utilisation d'un moyen de paiement. Patron 12 - Greffier : Pour journaliser l'utilisation d'un moyen de paiement.
Besoin 20 : Prévenir toute dépense au-delà d'un certain montant.
Patron 6 - Porte-monnaie : Pour le suivi des dépenses. Patron 12 - Greffier : Pour journaliser l'utilisation d'un moyen de paiement.
Besoin 21 : Prévenir le gestionnaire de cas ou le tuteur lors de l'utilisation de moyens de paiement en présence de personnes inconnues ou en présence de personnes spécifiques.
Patron 7 - Pickpocket : Pour la contextualisation des moyens de paiement. Patron 12 - Greffier : Pour journaliser l'accès à l'appartement et l'utilisation d'un moyen de paiement.

tableau 5.6 – Correspondances entre les besoins du scénario 5 et les patrons issus du catalogue.

L'application des patrons issus du catalogue de patrons de sécurité, de fiabilité et de sûreté pour répondre aux besoins du scénario 5 est détaillée dans le tableau 5.6. Ce tableau est organisé de manière verticale par besoin auquel est associé le patron ou l'ensemble de patrons qui répond à ce besoin.

5.5 Conclusion

Dans ce chapitre, nous appliquons les patrons du catalogue de patrons de sécurité, de fiabilité et de sûreté présenté dans le Chapitre 4 aux besoins identifiés dans les scénarios du Chapitre 2.

Scénario par scénario, nous avons montré qu'un patron ou un ensemble de patrons peut répondre à un besoin des développeurs d'applications dédiées aux habitats intelligents (HI) pour personnes ayant des troubles cognitifs.

La nouveauté de ce catalogue, ce qu'il apporte à la communauté des développeurs d'HI, ses limites et des pistes de développement futur sont discutés dans le Chapitre 6.

Chapitre 6

Discussion

Ce chapitre présente plusieurs axes de réflexions sur le travail réalisé durant cette thèse et le remet en perspective par rapport aux objectifs et aux travaux similaires réalisés dans d'autres domaines. La première section discute les résultats (Section 6.1) tandis que la deuxième section termine le chapitre par des perspectives de travaux futurs pour compléter le catalogue (Section 6.2).

6.1 Discussion des résultats

Cette thèse a permis l'élaboration d'un catalogue de sécurité, de fiabilité et de sûreté. Le catalogue contient 18 patrons. Le catalogue regroupe des patrons qui répondent aux besoins des cinq scénarios vus au Chapitre 2.

Cette section aborde l'approche de la création des patrons à partir de scénarios (Section 6.1.1), de la description des patrons et du choix des éléments qui les composent (Section 6.1.2), de la maturité ou du manque de maturité des patrons (Section 6.1.3), de la présence ou non d'implémentations jointes aux patrons (Section 6.1.4), enfin la dernière section discute des considérations légales (Section 6.1.5).

6.1.1 Approche par scénarios

Dans [39], Gamma est allé chercher des bonnes pratiques en réponse à des problèmes de conception logicielle puis les a regroupés sous forme de patrons. L'approche ici est assez similaire et consistait à observer des scènes de la vie quotidienne d'un résident dans un habitat intelligent et d'en extraire les besoins en termes de sécurité, de fiabilité et de sûreté.

L'avantage de l'approche par scénarios et qu'elle permet d'illustrer facilement les besoins. Les scénarios prennent en compte l'aspect médical (suivi à domicile et urgence), les troubles cognitifs, la réalité du vieillissement de la population (les fraudes, la problématique de la gestion de l'argent) et les problèmes d'intégrité physique du résident.

Une approche par scénarios n'est pas exhaustive, mais permet de couvrir beaucoup de situations. Cependant, certaines ne sont pas couvertes, car les habitats intelligents sont une technologie encore trop jeune pour que l'on dispose de suffisamment d'informations sur les problèmes couramment rencontrés et surtout sur les bonnes pratiques pour les contrer.

Nous sommes encore dans une phase de projection et de prédiction en ce qui a trait au quotidien d'un résident dans une telle installation.

L'approche par scénarios a été très utile car elle nous permet d'anticiper ce que sera la vie du résident d'un HI. Par la suite, l'usage des HI sera plus répandu, nous pourrons bénéficier de l'expérience des préposés aux bénéficiaires et du personnel soignant pour identifier de nouveaux besoins.

6.1.2 Éléments et description des patrons

Les patrons du catalogue comprennent relativement peu de sections : alias, résumé, problème, solutions, particularités contextuelles, conséquences, liens avec les autres patrons, références. Dans d'autres collections de patrons, on trouve davantage de sections notamment celles liées à l'implémentation où d'autres situations ou le patron est utilisé.

En ce qui a trait à l'implémentation, il existe des sections qui présentent la solution à l'aide d'un diagramme de classe. Bien que ce ne soit pas une implémentation en

langage informatique, la solution reste toujours très proche du développement informatique. Le patron s'appuie parfois plus sur une solution technique et concrète que sur une solution de conception de logiciel représenté par un diagramme.

Surtout pour les patrons de sûreté, pour lesquels des capteurs et des effecteurs vont entrer dans la conception de la solution.

Dans le projet SERENITY, les patrons intégraient une ou plusieurs implémentations. Cependant c'était le but du projet que de fournir une implémentation et un déploiement clé en main au développeur. Ceci avait un impact sur la description des patrons puisque le contexte technique et l'implémentation jouent un rôle plus important dans ce cas que la description de la solution.

Les éléments choisis pour décrire les patrons de sécurité, de fiabilité et de sûreté offrent l'avantage d'être facile à utiliser, quel que soit le type de patron à décrire. Cependant, d'autres sections pourraient être ajoutées parfois pour décrire davantage la solution et son usage. Il faudrait qu'elles soient optionnelles et non obligatoires pour laisser une certaine cohérence et souplesse dans la description des patrons du catalogue.

6.1.3 Maturité des patrons

Les patrons de sécurité et de fiabilité sont pour la plupart issus de bonnes pratiques éprouvées et couramment employées. La description du problème ou les particularités contextuelles ont été développées dans notre catalogue en gardant en tête la problématique du maintien à domicile des personnes ayant des troubles cognitifs.

Ces solutions ont été sélectionnées puis adaptées pour le contexte des HI et des troubles cognitifs. On peut considérer ces solutions comme étant matures.

Dans le cas des patrons de sûreté, les solutions répondent à des projections et n'ont pas toutes encore été éprouvées dans notre domaine ou d'autres. Il faudra du temps pour avoir un retour sur ces solutions et les perfectionner ou trouver des solutions nouvelles. Ces solutions sont pour le moment à considérer comme jeunes ou adolescentes.

6.1.4 Implémentation

Dans le projet SERENITY, les patrons de sécurité sont décrits de sorte à inclure une description abstraite de la solution technique puis intègrent une série d'implémentation possible en fonction de la plateforme logicielle utilisée ou du langage de programmation employé.

Dans notre catalogue, nous avons choisi de ne pas intégrer d'implémentation mais de décrire davantage la solution technique. Ce choix dépend de l'usage que l'on souhaite faire des patrons. Dans le cas du projet SERENITY, le déploiement automatique était pris en compte. Décrire précisément la solution technique qui est déployée automatiquement n'a pas de sens.

Nos patrons n'ont pas cette vocation. Il se pose alors la question du niveau d'abstraction du patron. Notre choix était de garder un niveau d'abstraction suffisamment élevé pour toucher un public plus large et ne pas se rattacher à un langage de prédilection. C'est un choix aussi qui permet de maintenir une certaine simplicité dans le catalogue notamment par rapport aux patrons pour lesquels une implémentation est superflue (comme ceux de sûreté).

6.1.5 Considérations légales

L'usage des patrons implique l'acceptation des habitats intelligents auprès des résidents. Même si la technologie est bien acceptée, les résidents doivent signer un formulaire de consentement qui couvre la collecte et l'analyse de données issues de leur présence dans un HI en vue de leur fournir une assistance cognitive. Ce formulaire doit préciser que le personnel médical autorisé peuvent y avoir accès dans le but d'apporter des soins médicaux au patient. En fonction de la législation locale ou d'un comité d'éthique, des mesures peuvent être prises pour détruire ces données au-delà d'une période spécifiée ou du décès du patient.

Ce n'est pas le seul cas où des considérations légales ou éthiques peuvent entrer en ligne de compte, par exemple demander l'autorisation d'utiliser la position GPS ou d'aider à la gestion des moyens de paiements. Ces considérations légales ou éthiques jouent un rôle dans l'application des patrons ou leur conception.

Le patron ne devrait pas être mis en pratique sans le consentement donné par écrit

du patient ou du tuteur autorisant l'usage d'un appareil GPS. Il en est de même pour l'aide à l'utilisation des moyens de paiements. Les patrons sont sujets aux limitations d'un cadre légal.

Les itérations futures du catalogue pourraient prendre davantage en compte ces considérations pour aider le développeur à savoir s'il peut ou non intégrer le patron dans son application ou pour mettre au point un dispositif d'application ou non du patron en fonction d'une configuration qui prend en compte les considérations légales ou éthiques.

6.2 Perspectives d'évolution du catalogue

Cette section présente les perspectives d'évolution du catalogue. Elle couvre les aspects d'augmentation du nombre de patrons (section 6.2.1), la classification des patrons en fonction des troubles cognitifs des résidents (section 6.2.2) et le déploiement automatique des patrons (section 6.2.3).

6.2.1 Alimenter le catalogue

Le catalogue peut bénéficier de nombreux autres patrons autant en sécurité et fiabilité, qu'en sûreté. En ce qui concerne la sécurité et la fiabilité, bien que les solutions soient plus matures, certaines variantes et l'arrivée constante de nouvelles technologies poussent à une revue régulière de nouvelles solutions. Par exemple, en ce qui concerne l'authentification, celle-ci pourra se faire un jour de manière automatique et invisible par un dispositif de reconnaissance de la démarche de l'utilisateur sur une surface sensible à la pression. Cette technologie existe, mais est encore trop onéreuse à mettre en place. D'autres technologies verront le jour prochainement. Il est donc nécessaire d'entretenir le catalogue et d'y ajouter de nouvelles entrées lorsque c'est nécessaire. Ceci peut être fait à l'aide d'expert en sécurité en collaboration avec des développeurs d'applications pour habitat intelligent (HI).

En matière de sûreté, le travail restant est plus important. Il nécessite d'avoir plus de retours sur le séjour des résidents des HI de la part du personnel soignant, des préposés aux bénéficiaires, de la famille et des centres de réadaptation. L'usage des

HI par les personnes ayant des troubles cognitifs est encore trop récent pour évaluer les solutions de sûreté.

Les patrons pourront aussi répondre à des critères plus précis de troubles cognitifs, par exemple des patrons dédiés à la détection de crise pour les schizophrènes et être mis au point en collaboration avec des experts de ces troubles cognitifs particuliers.

6.2.2 Trier les patrons

Avec l'augmentation du nombre de patrons, plusieurs classifications deviendraient utiles. Une classification par troubles cognitifs permettrait au développeur de trouver les patrons existant pour une application ciblant des personnes ayant ce type de trouble précis. Par exemple, isoler les patrons en lien avec personnes atteintes de la maladie d'Alzheimer, les traumatisés crâniens ou les schizophrènes. Il est possible que des patrons concernent tous les troubles cognitifs, un ou plusieurs troubles en particulier ou n'en concernent aucun (c'est le cas des patrons qui concerne plus les particularités de l'habitat intelligent plutôt que celles du résident).

On peut également par la suite distinguer le type de déficit visé : trouble de mémoire, d'initiation, de planification etc.

Une classification en fonction du type d'installation d'HI peut s'avérer utile dans certains cas. Par exemple, distinguer les patrons en lien avec les résidences individuelles des patrons en lien avec les foyers. En effet, certains patrons fonctionnent dans un type d'installation, mais pas dans l'autre, ou nécessitent des adaptations particulières.

6.2.3 Déploiement automatique des patrons

À l'instar du projet SERENITY dans lequel les patrons comprennent une ou plusieurs implémentations que le développeur peut sélectionner et déployer automatiquement, les patrons de sécurité et de fiabilité pourraient bénéficier du même traitement.

Cette automatisation serait un gain d'effort considérable pour le développeur, mais nécessite l'élaboration d'un framework de sélection et de déploiement de patrons. Ce qui devrait prendre beaucoup de temps à mettre au point. De plus, cela nécessite qu'il y ait au moins une implémentation pour chacun patron du catalogue.

6.2. Perspectives d'évolution du catalogue

L'automatisation a un impact sur la description du patron. Des éléments devront être ajoutés pour permettre le référencement des patrons afin d'en automatiser la consultation et le déploiement des implémentations des solutions.

L'automatisation des patrons de sûreté est plus complexe, car leurs solutions intègrent généralement des capteurs et des effecteurs. S'ils ne sont pas déjà en place dans l'habitat intelligent, leur déploiement ne peut être automatisé, car ils nécessitent la pose de capteurs et d'effecteurs supplémentaires par un technicien et leur intégration au réseau de capteurs.

Conclusion

Cette thèse apporte le premier catalogue de patrons de sécurité, de fiabilité et de sûreté dédié aux habitats intelligents pour les personnes ayant des troubles cognitifs.

À partir de l'observation du vieillissement de la population et des problèmes que ce vieillissement engendre, nous avons abordé la problématique du maintien à domicile des personnes âgées avec les problèmes de sûreté que cela engendre : leurs problèmes de santé nécessitent un suivi médical régulier, ce sont des personnes vulnérables et isolées, etc. Cette situation est accentuée par les troubles cognitifs qui augmentent la vulnérabilité de ces personnes en perte d'autonomie.

Les habitats intelligents (HI) apportent une réponse aux besoins des personnes ayant des troubles cognitifs et qui se retrouvent en perte d'autonomie. Pour assurer le maintien à domicile de personnes ayant ce type de trouble, nous avons établi qu'il faudra résoudre les problèmes de sûreté auxquels les résidents d'un HI seront confrontés et les problèmes de sécurité et de fiabilité des applications et des services qui participent au suivi médical du patient.

À cette fin, nous avons présenté cinq scénarios. Ces mises en situation illustrent des scènes de vie d'un résident d'un HI. Nous montrons la dimension médicale du maintien à domicile et ses conséquences (accès au dossier médical, gestion de situations d'urgence), la dimension des troubles cognitifs et l'impact qu'ont ces troubles sur leur maintien à domicile. Finalement nous montrons la dimension de la vie privée et en quoi l'HI amène à la fois un défi pour la faire respecter et des outils pour mettre au point des dispositifs pour la garantir.

Pour le bon déroulement de ces scénarios, nous avons identifié des besoins de sécurité, de fiabilité et de sûreté à satisfaire et à intégrer dans le développement d'applications pour HI. Nous avons parcouru certaines solutions qui existent déjà et

sont applicables dans le domaine des HI et nous en avons créé de nouvelles.

Cependant les développeurs d'application pour HI ne sont pas forcément des experts dans ces domaines et ne sont pas tous en mesure d'appliquer ces solutions dans leurs applications. Nous avons mis ce problème en avant et avons proposé dans cette thèse un moyen de rendre ces solutions accessibles en les regroupant dans un catalogue de patrons de sécurité, de fiabilité et de sûreté.

Notre travail comprend une étude sur l'usage des patrons dans de nombreux domaines. En informatique, il existe des recueils de patrons de conception logicielle et de patrons de sécurité. Pour autant, aucun d'entre eux ne prend en compte la spécificité des troubles cognitifs et les particularités de l'infrastructure d'un HI.

L'approche par catalogue de patron est une première dans le domaine des HI. Le concept a fait l'objet d'un article lors de la conférence ICOST en 2010 [25].

Les retombées de cette thèse sont multiples. La communauté des HI dispose d'un premier catalogue qui lui est dédié et qui prend en compte les multiples facettes de notre contexte, à savoir la santé, les troubles cognitifs et les spécificités de l'informatique diffuse. Le catalogue compte 18 patrons qui répondent à des besoins de fiabilité, de sûreté et de sécurité.

Ces patrons peuvent être utilisés individuellement ou être combinés pour répondre aux besoins de notre contexte. La dernière partie de notre travail utilise les patrons du catalogue pour répondre aux besoins identifiés dans nos cinq scénarios.

L'approche par patron et les éléments descriptifs qui composent un patron rendent le catalogue extensible. De travaux futurs incluront une augmentation du nombre de patrons, une classification plus précise en fonction du type de troubles cognitifs auquel le patron s'adresse.

Les trois premiers scénarios ont fait l'objet d'un prototypage, ces prototypes ont servi d'environnement de test pour l'implantation des patrons. Ces prototypes ont été réalisés dans le cadre d'une collaboration avec SAP Lab France au sein du projet européen SERENITY [3].

Ces prototypes et les patrons mis au point durant le travail de cette thèse ont fait l'objet de multiples publications dans le cadre de conférences [22], [24] et dans des journaux spécialisés dans les habitats intelligents [23], [34].

Annexe A

Première annexe

Cette annexe présente l'article paru dans les proceedings de la conférence ICOST 2010 [25].

L'article décrit le concept des patrons de sécurité dans le contexte des habitats intelligents (HI). Il décrit des scénarios de la vie quotidienne de résidents d'HI et montre les besoins auxquels les développeurs doivent répondre pour garantir la sécurité de leurs applications. Le concept des patrons est détaillé. Finalement, nous montrons les avantages à créer un catalogue de patrons spécifique aux HI pour personnes ayant des troubles cognitifs.

Security, Privacy, and Dependability in Smart Homes: A Pattern Catalog Approach

Pierre Busnel, Sylvain Giroux,

University of Sherbrooke, DOMUS lab, Sherbrooke
J1K 2R1, QC, Canada

{Pierre.Busnel, Sylvain.Giroux}@USherbrooke.ca

Abstract. Security, privacy and dependability are crucial issues if one wants to build a real smart home. First, in addition to established home security requirements, smart home adoption requires to solve brand-new security vulnerabilities deriving from the automated facets of smart homes. Thereafter, pervasive computing and ambient intelligence allow to collect a lot of information, to analyze it to derive new facts, and make them explicit. Finally, systems that are usually safe and dependable can fail when their behavior is becoming controlled as the result of complex interactions between many intertwined information systems. Unfortunately, application developers in smart home environments are usually neither security experts, nor familiar with ethical and legal requirements related to privacy. Security patterns can help to anticipate, overcome, and document systematically these difficult issues in building pervasive information systems in smart homes for cognitively impaired people. In this paper, we illustrate how security patterns can be extended and applied to Smart Home to foster autonomy of elderly or cognitively impaired people, then, we sketch the structure of the catalog which will be populated with a few patterns.

Keywords: Security patterns, ubiquitous computing, health care, smart home, cognitively impaired people.

1 Introduction

Occidental countries are facing great challenges from a population of elders increasing rapidly while the birth rate cannot sustain it. According to U.S. Census Bureau estimations, there were more than 36 million people that are aged 65 and over in 2003, and this population is projected to increase to 72 million in 2030 [1]. Thus, it is easy to forecast an increase of health injuries related to normal and pathological aging that will lead toward loss of autonomy and greater fragility, which result in a reduction of quality of life. People may need continuous supervision when either injured, sick, cognitively impaired, elderly, or fragile. If resources are not adapted at home, then people are more often transferred to a hospital setting. Thanks to

ubiquitous and pervasive computing, Smart Homes (SH) can interact with residents to foster their autonomy and to provide for health monitoring [2].

Nonetheless, security, privacy and dependability are crucial issues to build a real SH. They must be equipped with privileged, secure, and dependable ambient information systems. This implies that traditional information systems must be adapted to ambient intelligence (AmI) specific requirements. First, in addition to established home security requirements, SH adoption requires to solve brand-new security vulnerabilities deriving from the automated facets of SH. For instance, a thief can intrude into a SH sensor network to learn about one's habits and be aware precisely when he is home, when he is not and for how much time. Second pervasive computing and ambient intelligence allow to collect a lot of information, to analyze it to derive new facts, and to make them explicit. Before the rise, in everyday life, of pervasive and connected systems, such information was latent or hidden. Indeed, pervasiveness will take place in everyday life transactions where technical systems are not involved at all like, for instance, taking a bath[1] or social relationship[2] [14]. Finally, systems that are usually safe and dependable, such as heating systems, can fail when their behavior is becoming controlled as the result of complex interactions between many intertwined information systems, e.g. user interfaces to set the temperature, ecological control systems for saving energy, electricity company controlling the overall demand in the city, etc.

Unfortunately, application developers in SH environments are usually neither security experts, nor familiar with ethical and legal requirements related to privacy. Security[3] patterns can help to anticipate, overcome, and document systematically these difficult issues in building pervasive information systems in smart homes for cognitively impaired people. They can enable SH to meet the required security, privacy, and dependability. A security pattern describes a particular recurring security issue that arises in specific contexts, and presents a well-proven generic solution for it. Several security patterns have already been written to assist developers to select and deploy security solutions in their applications. However, elements used to describe them and assist developers in their choice does not take into account the particular infrastructure of SH and the cognitive impairments of their residents.

In this paper, we show how security patterns can be extended and applied to SH to foster autonomy of elderly or cognitively impaired people. First, a simple case study is used to illustrate where security, privacy and dependability issues can arise in a smart home with health related services (§2). Then, an overview of security patterns is presented (§3). The current description of their structure is too generic to catch the peculiarities of smart homes. Thus, it is extended with facets specific to smart homes, health services, and cognitively impaired people. Once the description of security

---

[1] While you are on the way home, Smart Hydro can prepare your bath according to your preferences and inform you on your cell phone. http://www.ihouse.com.br/ and http://gadgets.softpedia.com/gadgets/Household-and-Office/The-Smart-Hydro--Intelligent--Bath-Tub-994.html

[2] When a friend is visiting you, what will happen if a note appears on your TV screen saying you rated his wife as boring on one of your preferred social network...

[3] For convenience, in the rest of the paper the term "security" encompasses information systems security, privacy and dependability.

patterns is well extended, the structure of the catalog is sketched and populated with a few patterns (§4).

2 Case study

Smart homes in a medical context raise difficult and complex security issues; often, programmers are not able to cope with these specific issues. Security patterns can then become an invaluable help. This section presents a case study involving a patient in his smart home, his physician, his daughter, and a health-monitoring center that allow us to pinpoint security requirements in smart homes. First, the profiles of the actors involved are sketched (§2.1). Then, a scenario about monitoring an elder is cut into small scenes, each one illustrating a specific security issue (§2.2).

2.1 Actors

The case study involves the following actors: the patient Bob, his smart home, his daughter Rachel, the doctor Andrew, and the Monitoring and Emergency Response Center systems (MERC) as shown in Fig. 1.

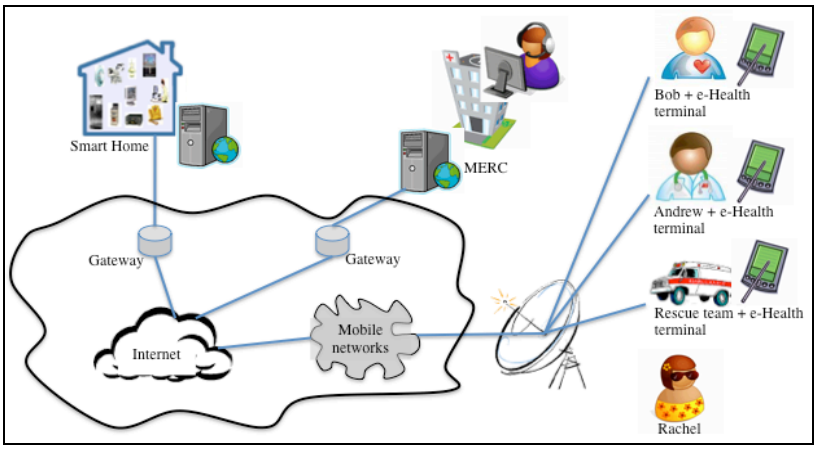

Fig. 1. Actors involved in the case study.

- *Bob* is a 70-year-old widowed man. Six months ago, he had a Cerebral Vascular Accident (CVA). Bob spent 4 months at the hospital after his accident. Since he still suffers from various troubles, his health status needs to be monitored daily. Before leaving hospital, he subscribed to a Smart Home (SH) program to get assistance in his daily activities and to make his heart rate monitored continuously.

- The *MERC* receives and handles emergency and assistance requests triggered by monitored patients. It also coordinates the activities of many other actors including doctors and social workers.
- Dr. *Andrew* is a physician working at the MERC. In the case study, Andrew is Bob's personal doctor, who is in charge of Bob's case.
- *Rachel* is Bob's daughter. Since her father's CVA, she often runs his errands and visits him twice a week. Rachel, in contrary to other visitors, is a privileged user and can enter the SH using her RFID tag and password, as approved by her father Bob.
- The *Smart Home* is a conventional apartment equipped with various types of sensors and effectors, to monitor and assist the patient in his Activities of Daily Living (ADL) [3], [4], [5]. Pressure mats, electro-magnetic sensors, infra-red and flow meters in the apartment, are used to recognize activities performed by the patient and prompt him with advices when necessary. *Microphones*, *speakers* and *cameras* are available to facilitate communications between the patient, the medical staff and his family. *RFID tag readers* are available at the Smart Home door for authenticating the access requesters among the medical staff, doctors, family and others during home visits.
- The *SH terminal* combines an interface to interact with the SH server and the MERC server. It displays a calendar accessible through the MERC for adding medical or maintenance visits. It also hosts an ADL assistant [4] and a communication interface with the MERC for emergency request or request for doctor assistance.

2.2 Scenario

The general scenario is exploring the management of security and privacy when people come into Bob's home. This scenario is divided in two main parts. In the first part, the visits of a doctor and a technician are planned and organized by the MERC. In the second part, the focus is put on the access by persons with different status at Bob's home.

According to Bob medical records, the MERC has to schedule weekly medical visits for Bob's check-up. The MERC also schedules regular maintenance visits for sensors check-up. So each week, a medical visit is assigned to an available doctor, and events detailing the arrival time of the doctor and his identity are added to Bob's calendar by the MERC. Therefore, Bob is always warned in advance and aware of these planned visits. Accordingly, when Dr. Andrew is assigned to visit Bob this week, Bob has to allow and acknowledge the visit thanks to his electronic calendar. The same procedure is used for the maintenance visit.

Next the scenario is divided into three small scenes that highlight security and safety issues that need to be solved when Bob receives visitors. The first scene corresponds to the medical visit at Bob's home. This visit involves known participants and is scheduled beforehand (Fig. 2). Then, in Scene 2, an unexpected visitor comes in while the doctor and Bob are watching private medical data (Fig. 3), and, finally,

Scene 3 describes an emergency situation when nobody, except Bob, is at home and someone has to get in (Fig. 4).

- **Scene 1: the doctor visit (Fig.2)**
  When Dr. Andrew arrives at the SH's door, the door bell rings as the RFID tag carried on his badge gets scanned and analyzed by the SH. At the same time, the outdoor webcam takes a picture of Dr. Andrew. Bob, notified by the doorbell, sees on his screen both the picture taken outside and the one corresponding to Dr. Andrew's identification badge and the MERC, and unlocks the door from his terminal. Then, the doctor logs in to access the medical record of Bob (1). The MERC retrieves the record, sends it to the SH and it is displayed on the TV screen (2). When Rachel arrives at the door, her authentication RFID tag is read and, since she has special access right, the door automatically unlocks and grants her access inside. Since confidential data are displayed on the TV screen and a new person is in the living room (3), the system immediately hides these data (4). Then, Andrew has to log in again to get access to the data (5).

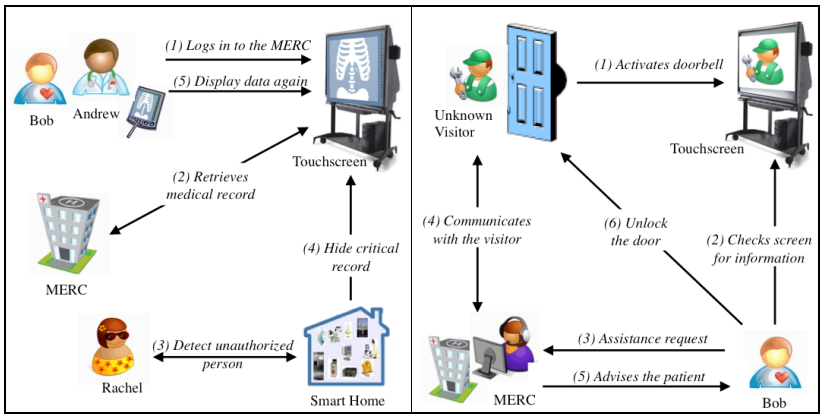

Fig. 2. Scene 1 – the doctor visit (left side) and scene 2 – the unknown visitor (right side)

Scene 1 and 2 illustrate security and privacy issues related to providing access inside the SH and to sensible data involving a mix of devices (RFID tag reader, camera, movement detectors, TV screen…) and information (photo, RFID tag number…), authorization policies and procedures (login and password, explicit authorization…).

- **Scene 2: the unknown visitor (Fig. 2)**
  Bob is in the living room when the doorbell rings (1). An unknown visitor picture appears on the screen situated next to him (2). Bob does not recognize this visitor and even after talking to him through the interphone, hesitates to open the door. He finally decides to ask assistance to the MERC (3) which communicates with the visitor (4) in order to advise Bob to grant access or not (5). Since the MERC advises Bob to grant access to the visitor, he unlocks the door (6).

- **Scene 3: the assistance request (Fig. 3)**
  Bob's is at home when he suddenly feels giddy and uses his e-health terminal to send an emergency request (1). The MERC forwards the assistance request to an available doctor (2). The doctor consults the medical record and the medical data recently collected by the SH sensors and sends a report to the MERC saying that an emergency team must be sent to help Bob (3). Thanks to the localization service, the MERC localizes Bob in his home. The localization service was granted special and temporary access rights to sensors data stocked in Bob's home server (4). The MERC sends an emergency intervention request to the rescue team (5). While the rescue team is on its way to the SH's door, the MERC grants temporary access to the SH's door to the members of the rescue team, in order to let them enter into Bob's home (6). This scene is treated more extensively in [6].

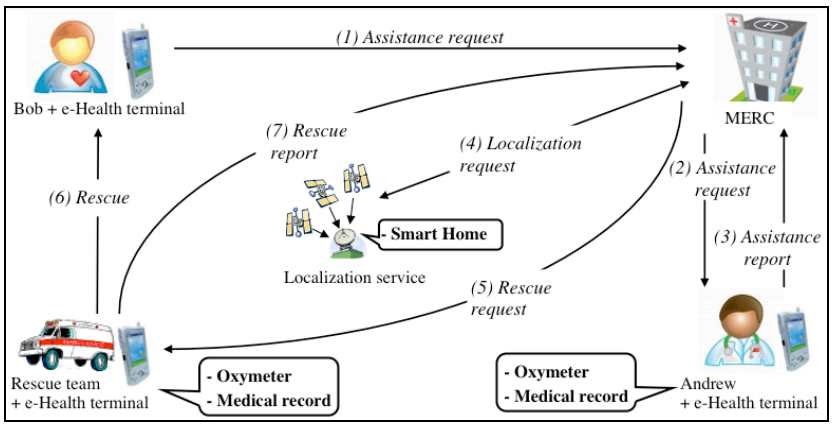

Fig. 3. Scene 3 – the assistance request

3 An overview of security patterns

The pattern approach has been adopted into software engineering as a method for object-based reuse [8]. Design patterns capture recurring solutions to common problems in software design. The following items describe a design pattern: *name*, *intent*, *alias*, *motivation*, *applicability*, *structure*, *participants*, *collaborations*, and *consequences*. Given the success of the Gang of Four in eliciting and organizing expert knowledge in object-oriented programming, a similar methodology was applied to security issues. Schumacher [9] applied the pattern approach to security problems by proposing a set of security patterns for the development process. Yoder and Barcalow [10] proposed architectural patterns that can be applied when introducing security into an application. Fernandez and Pan [11] described patterns

for the most common security models, such as *Authorization*, *Role-Based Access Control*, and *Multilevel Security*.

One of the main limitations of these proposals is that they neither capture explicitly the very nature of SH and pervasive systems, nor they take into account specific issues related to resident, for instance cognitive deficits. For instance, Table 1 presents an eXtensible Access Control Markup Language (XACML) based pattern that tries to make these peculiar requirements more explicit.

Table 1. XACML based access control pattern to enforce confidentiality.

Pattern name	XACML based access control pattern
Context	While confidentiality is enforced at the hospital to access medical information, such data need to be accessible outside with the same level of confidentiality. During home visits at the patient's smart home, medical staff needs to access the medical record and display it on the living room screen. The data displayed must only to be seen by the patient and the medical staff.
Legal issue	Medical data are confidential
Ethical issue	Not available
Problem	With the presence of others actors and family members having privileged access to the smart home, confidentiality while displaying medical data during a home visit is at risk.
Solution	The smart home sensors are used to identify any incoming visitors by using RFID badge at the main door of the apartment and using an XACML policy enforced both at the smart home and the MERC side.
Smart Home infrastructure requirements	An RFID reader must be deployed at the entrance of the door and connected to the smart home events server.

4 Towards a Catalog of patterns

Without a general classification scheme, design patterns would just have become a long list difficult to search in and understand. The beauty of the Gang of Four solution is that they also provide a general organization scheme to better understand, search and use design patterns. This organization takes the form of a classification table ordered into class and instance patterns on the rows side and creation, structure, and behavior aspects on the column side. Also, a graph shows the interrelations between patterns use. Then, a catalog of patterns becomes more than a collection of patterns and can offer guidance to select and use patterns. It is a tool for both patterns writers to organize their solutions and developers to find the adequate patterns to apply. Catalogs of patterns in domains such as code design [8] and security [9], [12], [13], already exist. However, no one is dedicated to Smart Homes.

We are currently working on such a catalog. This catalog of security patterns will assist SH developers to choose a security solutions adapted to their needs and their context of utilization. In our context, several elements such as the sensors network,

the use of mobile devices, the participation of healthcare workers and the cognitive troubles of SH residents are taken into account in order to explicit the consequences of the possible security solutions.

5 Conclusion and future work

This paper presented, by using a simple use case, the necessity to create security pattern and to structure them in a catalog dedicated to Smart Homes, in order to assist SH developers in the integration of security solutions in their application. Up to now, two patterns have been written and successfully implemented in remote healthcare prototype [6], [7]. Many patterns are on their way to a complete description. Future works will focus on the validation of new elements composing security patterns in the context of smart homes and on writing new security patterns in order to populate the catalog.

References

1. He, W., et al.: 65+ in the U.S.: Current Population Reports. In: Washington, DC: U.S. Bureau of the Census, pp. 23--209 (2005)
2. Jorge, J.: Adaptive tools for the elderly new devices to cope with age induced cognitive disabilities. In: Proceedings of the 2001 WUAUC, pp. 66--70 (2001)
3. Pigot, H., Mayers, A., Giroux, S.: The intelligent habitat and everyday life activity support. In: Proceedings of the 5th international conference on Simulations in Biomedicine, pp. 507--516, Slovenia (2003)
4. Bauchet, J., Vergnes, D., Giroux, S., Pigot, H.: A pervasive cognitive assistant for smart homes. In: Proceedings of the 2006 ICADI, pp. 228, USA (2006)
5. Bauchet, J., Mayers, A.: A modelisation of ADLs in its environment for cognitive assistance. In: Proceedings of the 2005 ICOST, pp. 221--228, Canada (2005)
6. Busnel, P., El Khoury, P., Giroux, S., Li, K.: Achieving Socio-Technical Confidentiality using Security Pattern in Smart Homes. In: 3rd International Symposium on Smart Home (SH08), China (2008)
7. El Khoury, P., Busnel, P., Giroux, S., Li, K.: Enforcing Security in Smart Homes using Security Patterns. In: International Journal of Smart Home (IJSH), Vol. 3, No. 2 (2009)
8. Gamma, E., Helm, R., Johnson, R., Vlissides, J.: Design patterns: Elements of Reusable Object-Oriented Software. Addison-Wesley Professional (1994)
9. Schumacher, M.: Security Engineering with Patterns: Origins, Theoretical Models, and New Applications. LNCS, vol. 2754, Springer, Verlag, (2003)
10. Yoder, J., Barcalow. J.: Architectural Patterns for Enabling Application Security. In: Conference on Pattern Languages of Programs (1997)
11. Fernandez, E., Pan, R.: A Pattern Language for Security Models. In: Conference on Pattern Languages of Programs (2001)
12 Schumacher, M., Roedig, U.: Security Engineering with Patterns. In: Conference on Pattern Languages of Programs, USA (2001)
13 Kienzle, D., Elder, M., Tyree, D., Edwards-Hewitt, J.: Security Patterns Template and Tutorial, http://www.securitypatterns.com/documents.html (2002).
14 Everyware: The Dawning Age of Ubiquitous Computing, Peachpit Press Publications; 2006, 272 p.

Annexe B

Deuxième annexe

Cette annexe présente l'article paru dans le journal IJSH *International Journal of Smart Home* [23].

L'article décrit le scénario de la visite à domicile, les acteurs et l'environnement du scénario, une sélection de besoins de sécurité à considérer puis présente le concept de patron de sécurité et le projet SERENITY. Finalement la solution mise au point pour combler le besoin 11 - *L'affichage du DME au domicile du patient, seuls le patient et le médecin doivent être dans la pièce utilisée pour la consultation* est détaillée avec l'ensemble de patrons qui la compose.

An XACML-based Security Pattern to achieve Socio-Technical Confidentiality in Smart Homes

Pierre Busnel[1], Paul El-Khoury[2,3], Sylvain Giroux[1], Keqin Li[2]
[1]*University of Sherbrooke, DOMUS lab, Sherbrooke J1K 2R1, QC, Canada*
Email:{pierre.busnel, sylvain.giroux}@usherbrooke.ca
[2]*SAP Research, 805 avenue du Dr. Maurice Donat, 06250 Mougins, France*
Email:{paul.el.khoury, Keqin.li}@sap.com
[3] *LIRIS, University of Lyon I, 8, Bd Niels Bohr, 69622 Villeurbanne Cedex, France*
Email:paul.el-khoury@liris.cnrs.fr

Abstract

In this paper we discuss and address multifold security challenges involved in the implementation of remote healthcare in smart homes. These security challenges are derived from real-world, industrially relevant scenarios. Validated security techniques and mechanisms providing certain security properties can be captured and implemented in security patterns, which can be applied in order to satisfy security requirements in the smart home healthcare scenarios. The presented results are parts of our ongoing research effort aiming at the development of an integrated security framework for remote healthcare and ambient intelligence systems.

1. Introduction

Occidental countries are facing great challenges from a population of elders increasing rapidly while the birth rate cannot sustain it. According to U.S. Census Bureau estimations, the population aged 65 and over was 36 million persons in 2003 and is projected to increase to 72 million in 2030 [1]. Thus it is easy to forecast an increase of health injuries related to normal and pathological aging which will lead toward loss of autonomy and greater fragility, then reducing their quality of life. When injured, sick or cognitively impaired, aged and fragile, people will need continuous supervision. If resources are not adapted at home, this will mean more often a transfer to a hospital setting. Thanks to ubiquitous and pervasive computing, Smart Homes (SH) can interact with the resident to foster its autonomy and to provide for health monitoring [2].

Nonetheless security is a crucial if one want to build a SH for the real. They must be equipped it with privileged security setup adequate and adapted to Ambient Intelligent (AmI) security specific requirements. Indeed in addition to traditional home security requirements, SH adoption requires to solve brand-new security vulnerabilities deriving from the automated facets of SH. Unfortunately application developers in SH environments are usually not security experts. Security patterns can help overcome this and provide SH with the required security solutions. A security pattern describes a particular recurring security issue that arises in specific contexts, and presents a well-proven generic solution for it.

The SERENITY project (“System Engineering for Security and Dependability”) address exactly this kind of situation [3]. One of its essential proposals is to provide novice users with the SERENITY Security & Dependability (S&D) patterns package. This package comprises of the expert-validated security solutions and tested plug-n-play deployable implementations.

In this paper, we illustrate how SERENITY can be applied to SH thanks to a simple case study. First the case study is presented: a patient's health status is continuously monitored remotely through a SH. Of course, typical security problems such as confidentiality and privacy of the patient's medical data will arise. Several security requirements from such AmI environment are presented, and an AmI confidentiality requirement is fulfilled by applying security patterns. Section 3 presents an overview on security patterns. Next, we present the architecture of the authorization pattern and present an overview of the proposed security solution in section 4. Finally in section 5 we conclude and present future work.

2. Case study

SH in a medical context raises difficult security issue, the average programmer is not able to cope with. Security pattern can then become an invaluable help. To illustrate security requirements and present our solution made by security patterns, we first introduce our case study, and describe a couple of tightly related scenes. Finally, we highlight security requirements of business applications closely related to confidentiality and privacy of the patient's medical data.

2.1. Actors

The case study involves the following actors: the patient Bob, his daughter Rachel, the physician Andrew, and the *Monitoring and Emergency Response Center* systems (MERC).

Bob is a 70-year-old widowed man. Six months ago, he had a Cerebral Vascular Accident (CVA). Bob spent 4 months at the hospital after his accident. Since he still suffers from various troubles his health status needs to be monitored daily. Before leaving hospital, he subscribed to a Smart Home (SH) program to get assistance in his daily activities and to make his heart rate monitored continuously.

Bob's health status is electronically captured in an Electronic Health Record (EHR). The *EHR* refers to an individual patient's medical record in digital format which is composed of various pieces of information about the patient such as medicines prescribed, notes left by physicians and data recorded from medical sensors. The EHR is used by the *Monitoring and Emergency Response Center* systems (MERC) to coordinate the medical team participating in Bob's medical aid.

The *MERC* receives and handles emergency requests arisen by patients. It also coordinates the activities of many other actors including doctors and social workers.

Dr. *Andrew* is a physician working at the MERC. In our case study, Andrew is Bob's personal doctor, who is in charge of Bob's case.

The *Smart Home* is coordinated to other participating actors through the MERC. The Smart Home is a conventional apartment equipped with various types of sensors to monitor and assist the patient in his Activities of Daily Living (ADL) [4, 5, 6]. Sensitive rugs, electro-magnetic sensors, infra-red and flow meters set all over the apartment, are used to recognize activities performed by the patient and prompt him with advices when necessary. Patients interact with their environment using *touchable screens* available in most of the rooms. *Microphones*, *speakers* and *cameras* are available to facilitate communications between the patient, the medical staff and his family. *RFID tag readers* are available at the Smart Home door for authenticating the access requesters among the medical staff, doctors, family and others during home visit.

Rachel is Bob's daughter. Since her father CVA, she often runs his errands and visits him twice a week. Rachel in contrary to other visitors is a privileged user and can enter the SH using her RFID tag and password as approved by her father Bob.

The *SH's terminal* combines an interface to interact with the SH's server and the MERC's server. It displays a calendar accessible through the MERC for adding medical or maintenance visits. It also contains an ADL assistant [5] and a communication interface with the MERC for emergency request or doctor assistance request. A medical interface is also included for periodically uploading medical data from the patient's medical sensors to the MERC. Doctors may also use this interface to access patients EHR when visiting patients at home.

2.2. Scenario

In the general scenario, the MERC has scheduled weekly medical visits for Bob's check-up. Each week, medical visits are assigned to available doctors, and events detailing the arrival time of doctors and their identities are added to patients' calendars. Bob is then aware that Dr. Andrew will be the one assigned to visit him this week. Bob confirms his acknowledgement of the visit. Then the scenario is divided in the two scenes below to put in evidence some security issues. In scene 1, Andrew is alone with Bob. In scene 2, Rachel joins them.

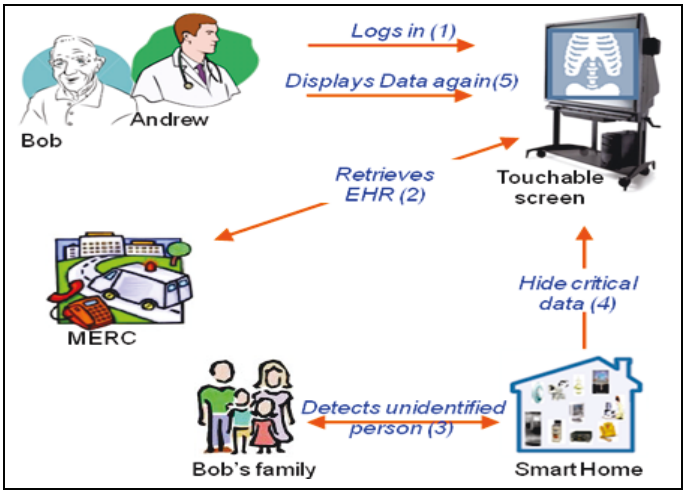

Figure 1 - Home visit case study

2.2.1. Scene 1: When Dr. Andrew arrives at the SH's door, the door bell rings as for the RFID tag carried on his badge gets scanned and analyzed by the SH. At the same time, the outdoor webcam takes a picture of Dr. Andrew. Bob, notified by the door bell, sees on his screen both the picture taken outside and the one corresponding to Dr. Andrew's identification badge, and unlocks the door from his terminal.

As shown in Figure 1, once inside Dr. Andrew logs onto the SH's terminal (1) to access Bob's EHR. The interface gives him access to notes left previously, health status monitored daily and previous prescriptions (2). Such information must be kept confidential between doctors and patient, cameras and microphones are turned off inside the Smart Home when medical information is being displayed and discussed.

2.2.2. Scene 2: The home visit goes on, Bob's daughter comes on her way back from running errands to visit her father at the SH. The sensor network detects (3) her RFID tag, signals Bob her approach, and allows her to enter. Yet Andrew is still examining Bob, and most data displayed on the smart home terminal are delicate and strictly personal. Upon Rachel's presence in the entrance, and since no explicit approval was provided by Bob, the SH terminal automatically hides (4) the delicate data on the screen. Dr. Andrew recognizes Bob's daughter and with Bob's approval displays the medical data again (5).

In addition to the traditional security and dependability requirements, the two presented scenes highlight some AmI security requirements discussed in next section.

2.3. Security requirements

This case study is typical of e-Health services. Table 1 highlights a few of critical security requirements: non repudiation, service availability, access control, integrity, confidentiality, privacy, and reliability.

Table 1 – Sample S&D requirements for the home visit case study

1.	The MERC shall be *available* and *reachable* 24 hours a day, 7 days a week.
2.	Each communication between the SH terminals and the MERC *shall guarantee messages delivery, integrity and confidentiality of the data exchanged, and mutual authentication*.
3.	The SH terminals shall always *be available* and *connected to the communication network*.
4.	The MERC shall continuously ensure the *reliable network connection* with the SH.
5.	Patient's data available at Smart Terminal shall be *kept confidential* and *accessible to authorized* requesters.
6.	Doctors shall *not repudiate scheduled home visit* after previous confirmation.
7.	The sensor network detection of unidentified persons approaching the examination area *shall be reliable*.
8.	To *ensure the patient's privacy*, cameras and microphones of the examination room shall be turned off during medical home visit.
9.	Data requesters have *to justify their need* to access patient's EHR, and *strictly least privileged access* will be granted, part of legal need-to-know principle [8].

The SERENITY security pattern approach can fulfill most of these identified security requirements. Indeed the security patterns described in this paper represent an excerpt of the library we are populating in the context of the SERENITY project. The security pattern library could serve as a reference in the design and deployment of systems having security requirements. Therefore it becomes clear that the fundamental plus value of the security pattern approach is providing security solutions to non-security experts [7].

3. An overview of security patterns

The pattern approach has been adopted into software engineering as a method for object-based reuse [9]. Following this particular path, Schumacher [7] applied the pattern approach to security problems by proposing a set of security patterns for the development process. Yoder and Barcalow [10] proposed architectural patterns that can be applied when introducing security into an application. Fernandez and Pan [11] described patterns for the most common security models such as Authorization, Role-Based Access Control, and Multilevel Security. One of the main problems of these proposals is the lack of tools that validate patterns with respect to expert knowledge. The usual natural language descriptions for security patterns open room for different interpretations of solutions provided and problems described by these patterns, as shown recently in [12].

SERENITY enables to capture security techniques and mechanisms into security artifacts. SERENITY's description for these artefacts enables the selection, adaptation, usage and monitoring at runtime by automated means of security techniques and mechanisms. There are three kinds of security artifacts, Security Classes, Security Patterns, and Security Implementations. Although this paper emphasizes the usage of security pattern artifact [13] and presents an intuitive and extensive description of all of them. SERENITY defines security patterns as detailed descriptions of abstract security solutions that contain all the information necessary for the selection, instantiation and adaptation of them. Such descriptions provide a precise foundation for the informed usage of the solution. An Integration Scheme (IS) is a special kind of security pattern defining the combination of security patterns. Complex security solutions relying on the usage and interactions of several patterns could be defined as integration schemes. In an IS, the relations among the participating security patterns are described in addition to other information.

In [14] two possible ways of capturing the security mechanism, i.e. authorization using XACML, were introduced, one as a security pattern, and the other as an integration scheme. In the next section we exploit this work to answer the confidentiality requirements identified in our AmI case study.

4. Socio-Technical Security Solution

In *traditional* and *smart* homes, top priority for people is the feeling of living safely and securely. In general, a full control over their homes' entry points is what ensures them the most. In remote healthcare assistance Bob and the MERC, an external organization compliant to the authorities' regulations remotely assisting the patient, has the full control of the SH entry points. As mentioned in §2, Bob's explicit approval for opening the SH entrance door to Rachel, his daughter, overrides the SH control and grants her immediate entrance.

The presented prototype is fully operational through Service Oriented Architecture (SOA) using Web Services (WS). Two alternatives of deploying authorization mechanism are considered, i.e., using SAML (Security Assertion Markup Language) or using XACML (eXtensible Access Control Markup Language). Ensuring confidentiality of SH resources as referred in Table 1, particularly in *Req 5, 8 and 9,* requires evaluating requests on fine-grained resources such as location and time. With this aim, authorization using XACML is recommended over authorization using SAML for fine-grained access control [15].

Table 2 – Summary of XACML as S&D pattern

S&D Pattern	S&D Requirement	S&D Solution
SP1	Confidentiality for fine-grained resources in SOA using WS.	Authorization using XACML, e.g., Sun's implementation.
SP2	Single Enforcement Point for extensive logging capabilities to facilitate audits.	Policy Enforcement Point, e.g., proxy web server
IS1	Confidentiality for fine-grained and distributed resources in SOA using WS.	Combination of SP1 and SP2**.** Authorization using XACML, e.g., our proposal in this paper with distributed PEPs with single PDP.

4.1. Authorization using XACML as Security Patterns

Our previous work [14] on capturing the access control solution using XACML in security patterns is applicable to satisfy the presented confidentiality requirements. In that work we focused on the XACML authorization model more than the language, specifically on the Policy Enforcement Point (PEP) and Policy Decision Point (PDP). The results indicated that XACML authorization model can be captured in one security pattern, or a combination of security patterns (i.e., integration scheme). A summary of both results is illustrated in Table 2. On the first hand, in local deployment of an XACML authorization solution, one S&D pattern is capable of capturing the validated conceptual model and providing a plug-n-play implementation. On the other hand a distributed deployment of the authorization using XACML as it is in our case requires one host for the evaluation engine (i.e., the MERC) and several hosts for the enforcement points (i.e., the MERC repository and the SH). This is captured by means of an integration scheme, where communications between the enforcement points and the evaluation points have to be secured.

A brief summary of the XACML model is depicted in Figure 2 – XACML authorization model and summarized hereafter. The PEP is the XACML's front-end that receives a subject's request, initializes its evaluation process, and sends back the answer. The PDP selects the applicable policies and computes the authorization response by evaluating the requests with respect to these policies. In order to provide access control decision, the PEP intercepts access requests, passes them to the Context Handler (CH) that queries them in XACML language to the PDP. The PDP loads the applicable policy (or set of policies) based on the resource targeted by the request, and then asks for the credentials required for the policy evaluation. Once all applicable policies are evaluated, the pre-selected policy combination algorithm decides the overriding evaluation. XACML defines several combination algorithms such as Deny-override and Permit-override. These combination algorithms are applied when combining access control rules to form a policy or when combining a set of policies. The access evaluation is passed back to the PEP for enforcement. Obligations are part of XACML language. Obligations are enforced by the PEP after a Permit decision. Actually, the PDP sends the authorization Permit back to the PEP with a list of obligations that the PEP has to fulfill as part of the authorization request. If the PEP is unable to fulfill an obligation, this does not affect the access control decision.

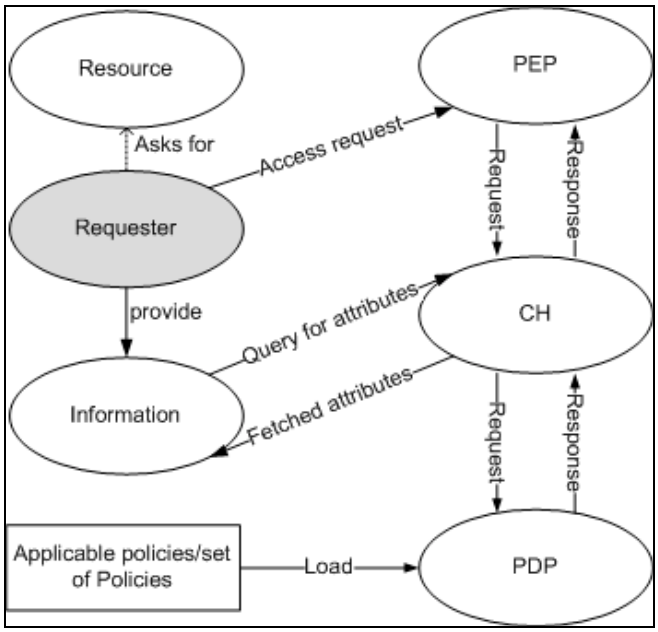

Figure 2 - XACML authorization model

4.2. Authorization using XACML as Integration Scheme for AmI confidentiality requirement

Clearly *Req 5, 8 and 9* of Table 1 matches better the *Confidentiality for fine-grained and distributed resources in SOA using WS* requirement of Table 2. In order to show the deployment of *IS1*integration scheme and the two *SP2* security patterns we identified the environments of our case study that has to be mapped to the security patterns. An illustration is depicted in Figure 3, where *conceptually* we show a deployment of the *IS1* made by two *SP2* patterns, namely PEP-1 and PEP-2, and one *SP1* that contains the decision point. The medical data are periodically sent to the SH; hence PEP-2 enforces access control to these data too. The main difference between PEP-1 and PEP-2 resides in their physical distribution. In our case study, the PEP-1 is hosted on the MERC server in SAP Labs France, while the PEP-2 is hosted at the DOMUS Laboratory in University of Sherbrooke. Each of these implementations has to be connected to the requesters' terminals, the information retrieval service(s), the resources and the evaluator.

In *Scene 1* of section 2.2, Dr. Andrew gets into Bob's SH in order to assist him during weekly visits. Technically speaking, the deployment of *IS1* does not reveal the interesting challenges as for the steps in setting up the policies for satisfying *Req. 5 and 9* from *Scene 1*. Dr. Andrew, using his RFID tag, authenticates himself to the SH. The access request sent by the RFID reader is sent to PEP-2 of the SH.

The PEP-2 creates the following token <*Dr. Andrew RFID tag identifier, his password and onetime generated passcode*, *an open action*, on the *resource door*> and passes it to the CH as the XACML illustration in Figure 2. The CH creates an XACML request and sends it to the PDP of the IS1. After succeeding the strong authentication, the first applicable XACML policy authorizes Dr. Andrew entrance. In fact, this policy satisfies *Req 9, by* checking the validity of Dr. Andrew's request with the Bob's scheduled medical visit. The second applicable policy requires Bob's decision on opening the door. As part of the obligation for this policy, the door bell rings. Bob looks to his e-Health terminal, sees Dr Andrew's request

for access, compares the photos, and responds positively. As a result the access to the SH is granted to Dr. Andrew.

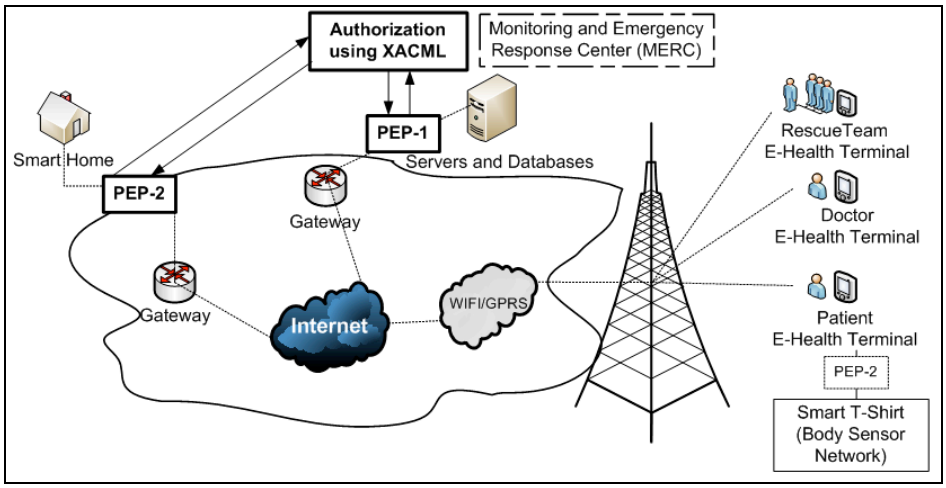

Figure 3 - Authorization using XACML Integration Scheme in the case study

Once inside, Dr. Andrew accesses Bob's EHR through the SH terminals. In the first phase, Dr. Andrew uses his username, password and the onetime generated *passcode* to be authenticated to the e-Health application provided by the MERC. In the second phase, Dr. Andrew requests to view and modify Bob's EHR (ref. Table 1, *Req. 5*). The terminal client page creates a message request to the PEP-1 of the MERC. The PEP-1 creates the following request <*Dr Andrew's identifier* and the *SH terminal*, *view and modify* as actions, and *Bob's EHR* as resource> to the CH. The applicable policy for fetching Bob's EHR checks whether the request was initiated from Bob's SH terminal (even if it is created by Dr. Andrew) or through his Laptop or his e-Health terminal. If Dr. Andrew's request was initiated from a terminal different from the ones previously mentioned, then *Req. 9* of Table 1 wouldn't have been satisfied. However, since Dr. Andrew's request is triggered from the SH's terminal, a Permit access is returned as it justifies his need to access Bob's EHR.

In *Scene 2* of section 2.2, Rachel's visit requires yet its share of the access control policies. Similarly to Dr. Andrew's case, Rachel's visit shall be checked from the SH's door until her entrance. Once at the door, within the authentication step, Rachel as already having Bob's consent for direct access does not require additional confirmation from her farther for entering. Nevertheless, the applicable policy takes into consideration Bob's privacy (*Req.* 8). It has to ensure that Bob's EHR is not displayed on any screen even when family members are within the SH without Bob's approval. This is interpreted in our policy as an *obligation* added to the grant permission. The obligation locks down the visualization of all connected e-Health terminals. Dr. Andrew after having Bob's acceptance has to re-authenticate himself to the SH terminal and unlock the screen.

5. Conclusion and future work

This paper presented a remote healthcare assistance case study. Most of the smart home security requirements are discussed extensively: non repudiation, service availability, access control, integrity, confidentiality, privacy, and reliability. Then an authorization solution is applied using the security pattern approach to satisfy security requirements typically existing

in such AmI environment. The presented prototype is fully implemented and operational (with additional scenes); the SH is hosted at the DOMUS laboratory in University of Sherbrooke and the MERC is hosted at SAP Labs France servers. The XACML implementation has been implemented and demonstrated at the ICT 2008 Exhibit in Lyon, France.

Future works will consider the combination of the presented security solutions with additional solutions operational at other layers, such as SSL at the network layer.

6. References

[1] He W. et al. 2005. "65+ in the U.S.: Current Population Reports" Washington, DC: U.S. Bureau of the Census, pp. 23-209.

[2] J. Jorge, "Adaptive tools for the elderly new devices to cope with age induced cognitive disabilities" in Proceedings of the 2001 WUAUC, 2001, pp. 66–70.

[3] A. Mana, C. Rodolph, G. Spanoudakis, V. Lotz, F. Massacci, M. Molideo, and J. S. Lopez-Cobo, Security Engineering for Ambient Intelligence: A Manifesto, IGI Publishing, 2007.

[4] H. Pigot, A. Mayers, and S. Giroux, "The intelligent habitat and everyday life activity support", Proceedings of the 5th international conference on Simulations in Biomedicine, Slovenia, April 2003, pp. 507–516.

[5] J. Bauchet, D. Vergnes, S. Giroux, and H. Pigot, "A pervasive cognitive assistant for smart homes", Proceedings of the International Conference on Aging, Disability and Independence (ICADI), USA, 2006, pp. 228.

[6] J. Bauchet and A. Mayers, "A modelisation of adls in its environment for cognitive assistance", Proceedings of the 3rd International Conference on Smart Homes and Health Telematic (ICOST), Canada, 2005, pp. 221–228.

[7] M. Schumacher, Security Engineering with Patterns: Origins, Theoretical Models, and New Applications, Lecture Notes in Computer Science, LNCS 2754, Springer Verlag, August 2003.

[8] L. Compagna, P. E. Khoury, F. Massacci, R. Thomas, and N. Zannone. "How to capture, model, and verify the knowledge of legal, security, and privacy experts: a pattern-based approach", International Conference on Artificial Intelligence and Law, 2007, pp. 149–153.

[9] E. Gamma, R. Helm, R. Johnson, and J. Vlissides. Design patterns: Elements of Reusable Object-Oriented Software, Addison-Wesley Professional, 1994.

[10] J. Yoder and J. Barcalow. "Architectural Patterns for Enabling Application Security", Conference on Pattern Languages of Programs (PLoP), 1997.

[11] E. Fernandez and R. Pan, "A Pattern Language for Security Models", Conference on Pattern Languages of Programs (PLoP), 2001.

[12] A. Armando, R. Carbone, L. Compagna, J. Cuellar, L. T. Abad, "Formal Analysis of a SAML Web Browser Single Sign-On Protocol", to appear in the Formal Methods in Security Engineering, 2008.

[13] F. Sanchez-Cid and A. Mana. "Patterns for automated management of security and dependability solutions", 1st International Workshop on Secure systems methodologies using patterns (SPattern), 2007.

[14] F. Sanchez-Cid, A. Munoz, P. El Khoury, and L. Compagna, "XACML as a Security and Dependability (S&D) pattern for Access Control in AmI environments," Ambient Intelligence Developments (AmI.d), Springer, September 2007.

[15] OASIS XACML specification, http://www.oasis-open.org.

Bibliographie

[1] « Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ».

[2] « Fraud Target : Senior Citizens ».

[3] « SERENITY Project, System Engineering for Security and Dependability (Projet Européen 2006-2009) ».

[4] « W3C SOAP specifications ».

[5] *SSL and TLS : designing and building secure systems.*
Addison-Wesley Longman Publishing Co., Inc., 2001.

[6] « FTC Testimony : Identifying and Fighting Consumer Fraud Against Older Americans », July 2005.

[7] Christopher Alexander, Sara Ishikawa et Murray Silverstein.
A Pattern Language : Towns, Buildings, Construction.
Oxford University Press, 1977.

[8] J. Alqatawna, E. Rissanen et B. Sadighi.
« Overriding of Access Control in XACML ».
Dans *Policies for Distributed Systems and Networks, 2007. POLICY '07. Eighth IEEE International Workshop on*, pages 87–95, 2007.

[9] P. Amnuaykanjanasin et N. Nupairoj.
« The BPEL orchestrating framework for secured grid services ».
Dans *Information Technology : Coding and Computing, 2005. ITCC 2005. International Conference on*, volume 1, pages 348–353 Vol. 1, 2005.

[10] Joan Arehart-Treichel.
« Early Alzheimer's Patients Lose Routine Financial Skills ».
American Psychiatric Association, 43(7):43, April 2008.

[11] Alessandro Armando, Roberto Carbone, Luca Compagna, Jorge Cuellar et Llanos Tobarra.
« Formal analysis of SAML 2.0 web browser single sign-on : breaking the SAML-based single sign-on for google apps ».
Dans *Proceedings of the 6th ACM workshop on Formal methods in security engineering*, FMSE '08, pages 1–10. ACM, 2008.

[12] Barry Barber.
« Patient data and security : an overview ».
International Journal of Medical Informatics, 49(1):19–30, 1998.

[13] Barry Barber, Alison Treacher, Kees Louwerse et C. P. Louwerse.
Towards Security in Medical Telematics : Legal and Technical Apsects.
IOS Press, 1996.

[14] Jérémy Bauchet et André Mayers.
« A Modelisation of ADLs in its Environment for Cognitive Assistance ».
Dans Sylvain Giroux et Hélène Pigot, éditeurs, *3rd International Conference On Smart Homes and health Telematic (ICOST 2005)*, Assistive Technology Research Series, pages 221–228. IOS Press, July 2005.

[15] Jérémy Bauchet, Denis Vergnes, Sylvain Giroux et Hélène Pigot.
« A Pervasive Cognitive Assistant For Smart Homes ».
Dans *International Conference on Aging, Disability and Independance (ICADI 2006)*, February 2006.

[16] Bruno Stanislas Beauvais, Vincent Rialle et Juliette Sablier.
« MyVigi : An Android Application to Detect Fall and Wandering ».
Dans *The Sixth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies*, pages 156–160, 2012.

[17] A. Belapurkar, A. Chakrabarti, H. Ponnapalli, N. Varadarajan, S. Padmanabhuni et S. Sundarrajan.

Distributed Systems Security : Issues, Processes and Solutions.
John Wiley & Sons, 2009.

[18] Morad Benyoucef, Craig Kuziemsky, Afrasiabi AmirRad et Ali Elsabbahi.
« Modeling healthcare processes as service orchestrations and choreographies ».
Business Process Management Journal, 17(4):568–597, 2011.

[19] M. Bouet et A.L. dos Santos.
« RFID tags : Positioning principles and localization techniques ».
Dans *Wireless Days, 2008. WD '08. 1st IFIP*, pages 1–5, 2008.

[20] Frank Buschmann, Kevlin Henney et Douglas C. Schmidt.
Pattern Oriented Software Architecture Volume 5 : On Patterns and Pattern Languages.
Wiley, juin 2007.

[21] Frank Buschmann, Regine Meunier, Hans Rohnert, Peter Sommerlad et Michael Stal.
Pattern-Oriented Software Architecture : a system of patterns.
volume 1. John Wiley and Sons, 1996.

[22] Pierre Busnel, Paul El Khoury, Sylvain Giroux et Keqin Li.
« Achieving Socio-technical Confidentiality Using Security Pattern in Smart Homes ».
Future Generation Communication and Networking (FGCN 2008), 2:447–452, 2008.

[23] Pierre Busnel, Paul El Khoury, Sylvain Giroux et Keqin Li.
« An XACML-based Security Pattern to achieve Socio-Technical Confidentiality in Smart Homes ».
International Journal of Smart Home, 3(1):17–26, January 2009.

[24] Pierre Busnel, Paul El Khoury, Keqin Li, Ayda Saidane et Nicola Zannone.
« Security and Dependability Pattern Deployment at Organizational Level : A Prototype for Remote Healthcare System ».
Electronic Notes in Theoretical Computer Science, 244:27–39, 8/1 2009.

[25] Pierre Busnel et Sylvain Giroux.
« Security, Privacy, and Dependability in Smart Homes : A Pattern Catalog Approach ».
Dans Y. Lee, Z.Z. Bien, M. Mokhtari, J.T. Kim, M. Park, J. Kim, H. Lee et I. Khalil, éditeurs, *Aging Friendly Technology for Health and Independence, Proceedings of the 8th International Conference on Smart Homes and Health Telematics (ICOST 2010)*, pages 24–31, June 2010.

[26] S. Campadello, L. Compagna, D. Gidoin, P. Giorgini, S. Holtmanns, J. Latanicki, V. Meduri, J-C. Pazzaglia, M. Seguran, R. Thomas et N. Zanone.
« SERENITY Deliverable A7.D2.1 - Security and Dependability Requirements Specification ».
Rapport Technique, SERENITY Project, 2006.

[27] S. Campadello, L. Compagna, D. Gidoin, S. Holtmanns, V. Meduri, J-C. Pazzaglia, M. Seguran et R. Thomas.
« SERENITY Deliverable A7.D1.1 - Scenario Selection and Definition ».
Rapport Technique, SERENITY Project, 2006.

[28] Peter M. Chen, Edward K. Lee, Garth A. Gibson, Randy H. Katz et David A. Patterson.
« RAID : High-Performance, Reliable Secondary Storage ».
ACM Computing Surveys, 26:145–185, 1994.

[29] Barbara Chenoweth et Beth Spencer.
« Dementia : The Experience of Family Caregivers ».
The Gerontologist, 26(3):267–272, 1986.

[30] John Chirillo et Scott Blaul.
Implementing Biometric Security.
Hungry Minds, Incorporated, 1 édition, 2003.

[31] Dorothy E. Denning.
« A lattice model of secure information flow ».
Commun. ACM, 19:236–243, May 1976.

[32] Angus Dickey, Jacob Slonim et Michael McAllister.
« Enabling Ageing in Place through Visitor Recognition and Monitoring Tech-

nology ».
The International Journal of Science in Society, 1(2):15–30, 2009.

[33] K.S. Earnst, V.G. Wadley, T.M. Aldridge, A.B. Steenwyk, A.E. Hammond, L.E. Harrell et D.C. Marson.
« Loss of financial capacity in Alzheimer's disease : The role of working memory ».
Aging, Neuropsychology, and Cognition, 8(2):109–119, 2001.
cited By (since 1996) 22.

[34] Paul El Khoury, Pierre Busnel, Sylvain Giroux et Keqin Li.
« Enforcing Security in Smart Homes using Security Patterns ».
International Journal of Smart Home, 3(2):57–70, Arpil 2009.

[35] Amado L. Espinosa.
« Availability of health data : requirements and solutions ».
International Journal of Medical Informatics, 49(1):97–104, 03 1998.

[36] Eduardo B. Fernandez et Rouyi Pan.
« A pattern language for security models ».
Dans *Proceedings of the conference on Pattern Languages of Programs (PLoP 2001)*, 2001.

[37] David Ferraiolo et Richard Kuhn.
« Role Based Access Control ».
Dans *15th National Computer Security Conference*, pages 554–563, October 1992.

[38] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach et T. Berners-Lee.
« Hypertext Transfer Protocol – HTTP/1.1 », 1999.

[39] Erich Gamma, Richard Helm, Ralph E. Johnson et John Vlissides.
Design Patterns : Elements of Reusable Object-Oriented Software.
Addison-Wesley, 1994.

[40] Sylvain Giroux, Jérémy Bauchet, Hélène Pigot, Dany Lussier-Desrochers et Yves Lachappelle.
« Pervasive behavior tracking for cognitive assistance ».

Dans *Proceedings of the 1st international conference on PErvasive Technologies Related to Assistive Environments*, PETRA '08. ACM, 2008.

[41] Marlys J. Harris.
« Elder Fraud ».
Money Magazine, 24(11):144–154, November 1995.

[42] Wan He, Manisha Sengupta, Victoria A. Velkoff et Kimberly A. DeBarros.
« 65+ in the United States : 2005 ».
Rapport Technique Current Population Reports, Special Studies P23-209, U.S. Census Bureau, Washington, D.C., 2005.

[43] Liesi E. Hebert, Paul A. Scherr, Julia L. Bienias, David A. Bennett et Denis A. Evans.
« Alzheimer Disease in the US Population : Prevalence Estimates Using the 2000 Census ».
Arch Neurol, 60(8):1119–1122, 2003.

[44] A.K. Jain, L. Hong, S. Pankanti et R. Bolle.
« An identity-authentication system using fingerprints ».
Proceedings of the IEEE, 85(9):1365–1388, 1997.

[45] A.K. Jain, A. Ross et S. Prabhakar.
« An introduction to biometric recognition ».
Circuits and Systems for Video Technology, IEEE Transactions on, 14(1):4–20, 2004.

[46] J. A. Jorge.
« Adaptive tools for the elderly : new devices to cope with age-induced cognitive disabilities ».
Dans *WUAUC'01 : Proceedings of the 2001 EC/NSF workshop on Universal accessibility of ubiquitous computing*, pages 66–70. ACM Press, 2001.

[47] Achilles D. Kameas, Victor Callagan, Hani Hagras, Michael Weber, Wolfgang Minker, Abdelsalam Helal, Jeffrey King, Raja Bose, Hicham EL-Zabadani et Youssef Kaddourah.
« Assistive Environments for Successful Aging ».

Dans *Advanced Intelligent Environments*, pages 1–26.
Springer US, 2009.

[48] Lalita Acharya ; Tomasz Kasprzycki ;.
La biométrie et son usage par l'État.
Ottawa] : Bibliothèque du Parlement, 2010.

[49] Basel Katt, Xinwen Zhang, Ruth Breu, Michael Hafner et Jean-Pierre Seifert.
« A general obligation model and continuity : enhanced policy enforcement engine for usage control ».
Dans *Proceedings of the 13th ACM symposium on Access control models and technologies*, SACMAT '08, pages 123–132. ACM, 2008.

[50] Karen Kent et Murugiah P. Souppaya.
« Guide to Computer Security Log Management ».
Rapport Technique, NIST, Gaithersburg, MD, United States, 2006.

[51] Darrell M. Kienzle, Matthew C. Elder, David Tyree et James Edwards-hewitt.
« Security Patterns Template and Tutorial », February 2002.

[52] Joan Langan et Robin Means.
« Financial Management and Elderly People with Dementia in the U.K. : As Much a Question of Confusion as Abuse ? ».
Ageing and Society, 16:287–314, 4 1996.

[53] Markus Lorch, Seth Proctor, Rebekah Lepro, Dennis Kafura et Sumit Shah.
« First experiences using XACML for access control in distributed systems ».
Dans *Proceedings of the 2003 ACM workshop on XML security*, XMLSEC '03, pages 25–37. ACM, 2003.

[54] Teresa F. Lunt.
« Automated Audit Trail Analysis and Intrusion Detection : A Survey ».
Dans *In Proceedings of the 11th National Computer Security Conference*, pages 65–73, 1988.

[55] A. R. Luria.
Human brain and psychological processes.
Harper and Row (New York), 1966.

[56] Antonio Maña, Antonio Muñoz, Francisco Sanchez-Cid, Daniel Serrano, George Spanoudakis, Kelly Androutsopoulos et Luca Compagna.
« SERENITY Deliverable A5.D2.1 - Patterns and Integration Schemes Languages ».
Rapport Technique, SERENITY Project, 2006.

[57] Evan Marcus et Hal Stern.
Blueprints for high availability (Second ed.).
John Wiley and Sons, 2003.

[58] D. Marson et S. Briggsm.
« Assessing competency in Alzheimer's disease : Treatment consent capacity and financial capacity ».
Dans *Alzheimer's disease and related disorders annual 2001*, page 272. Cummings, J.L. and Gauthier, S., londre : martin dunitz ltd édition, 2001.

[59] Daniel C. Marson.
« Loss of Financial Competency in Dementia : Conceptual and Empirical Approaches ».
Aging, Neuropsychology, and Cognition, 8(3):164–181, 2001.

[60] D.C. Marson, S.M. Sawrie, S. Snyder, B. McInturff, T. Stalvey, A. Boothe, T. Aldridge, A. Chatterjee et L.E. Harrell.
« Assessing financial capacity in patients with Alzheimer disease : A conceptual model and prototype instrument ».
Arch Neurol, 57(6):877–884, June 2000.

[61] Ueli Maurer, Mihir Bellare et Phillip Rogaway.
« Lecture Notes in Computer Science ».
Dans *Advances in Cryptology —EUROCRYPT '96*, volume 1070, pages 399–416.
Springer Berlin Heidelberg, 1996.

[62] N.R. May, H.W. Schmidt et I.E. Thomas.
« Service Redundancy Strategies in Service-Oriented Architectures ».
Dans *35th Euromicro Conference on Software Engineering and Advanced Applications 2009 (SEAA '09)*, pages 383 –387, aug. 2009.

[63] Robin Means et Joan Langan.
« Money 'handling', financial abuse and elderly people with dementia : implications for welfare professionals ».
Health and Social Care in the Community, 4(6):353–358, 1996.

[64] Mario Mendez, Richard Martin, Kathleen Smyth et Peter Whitehouse.
« Disturbances of Person Identification in Alzheimer's Disease : A Retrospective Study ».
The Journal of Nervous and Mental Disease, 180(2), 1992.

[65] A. M'hamed.
« Safety, Security, Privacy and Trust Issues ».
Dans *Engineering Handbook of Smart Technology for Aging, Disability, and Independence*. John Wiley & Sons, 2008.

[66] Mounir Mokhtari, Mahmoud Ghorbel et Rachid Kadouche.
« Mobilité et services : Application aux aides technologiques pour les personnes handicapées. ».
Dans *International Symposium On Programming and Systems (ISPS 2005)*, May 2005.

[67] R. Molva, D. Samfat et G. Tsudik.
« Authentication of mobile users ».
Network, IEEE, 8(2):26–34, 1994.

[68] B.C. Neuman et T. Ts'o.
« Kerberos : an authentication service for computer networks ».
Communications Magazine, IEEE, 32(9):33–38, 1994.

[69] Donald A. Norman et Tim Shallice.
« Attention to Action : Willed and Automatic Control of Behavior ».
Dans R. J. Davidson, G. E. Schwartz et D. Shapiro, éditeurs, *Consciousness and Self-Regulation, Volume 4*, pages 1–18. Plenum Press, 1986.

[70] Alan C. O'Connor et Ross J. Loomis.
« Economic Analysis of Role-Based Access Control ».
Rapport Technique, Research Triangle Institute, 2010.

[71] U.S. Office of Justice Programs, Office for Victims of Crime et National Sheriffs' Association.
First response to victims of crime who have a disability [electronic resource] : a handbook for law enforcement officers on how to approach and help crime victims who have Alzheimer's disease, mental illness, mental retardation, or who are blind or visually impaired, deaf or hard of hearing / prepared by National Sheriffs' Association.
Office for Victims of Crime Resource Center (OVCRC), 2002.

[72] Susan Orge et Tom Kippola.
« Reduce Mean Time to Repair with Expert Systems ».
Penton's Controls and Systems, 39(6):42, 1992.

[73] Sylvia Osborn, Ravi Sandhu et Qamar Munawer.
« Configuring role-based access control to enforce mandatory and discretionary access control policies ».
ACM Transactions on Information and System Security (TISSEC), pages 85–106, 2000.

[74] J. Pasley.
« How BPEL and SOA are changing Web services development ».
Internet Computing, IEEE, 9(3):60–67, 2005.

[75] C. Peltz.
« Web services orchestration and choreography ».
Computer, 36(10):46–52, 2003.

[76] Bridget Penhale.
« The Abuse of Elderly People : Considerations for Practice ».
British Journal of Social Work, 23(2):95–112, 1993.

[77] Floyd Piedad et Michael Hawkins.
High availability : Design, techniques, and processes.
Prentice Hall PTR, 2001.

[78] Hélène Pigot, André Mayers et Sylvain Giroux.
« The intelligent habitat and everyday life activity support ».
Dans *5th international conference on Simulations in Biomedicine*, april 2003.

[79] N.K. Ratha, J.H. Connell et R.M. Bolle.
« Enhancing security and privacy in biometrics-based authentication systems ».
IBM Systems Journal, 40(3):614–634, 2001.

[80] B. Reisberg, S. H. Ferris, M. J. De Leon et T. Crook.
« The global deterioration scale for assessment of primary degenerative dementia ».
American Journal of Psychiatry, 139(9):1136–1139, 1982.
Cited By (since 1996) : 1514.

[81] Vincent Rialle, Catherine Ollivet, Pierre Rumeau, Audrey Serna, Hélène Pigot et Christian Hervé.
« Éthique des technologies émergentes pour l'aide aux malades "Alzheimer" et à leurs aidants ».
Dans *VIIIe Congrès international francophone de gérontologie et gériatrie*, octobre 2006.

[82] R. L. Rivest, A. Shamir et L. Adleman.
« A method for obtaining digital signatures and public-key cryptosystems ».
Commun. ACM, 21(2):120–126, février 1978.

[83] Francisco Sánchez-Cid et Antonio Maña.
« Patterns for Automated Management of Security and Dependability Solutions ».
Dans *18th International Workshop on Database and Expert Systems Applications (DEXA 07)*, pages 739–743. IEEE Computer Society, 2007.

[84] Ravi Sandhu.
« Lattice-based access control models ».
IEEE Computer, 26(11):9–19, 1993.

[85] Ravi Sandhu.
« Role Activation Hierarchies ».
Dans *Proceedings of 3rd ACM Workshop on Role-Based Access Control*, October 1998.

[86] Ravi Sandhu, E.J. Coyne, H.L. Feinstein et C.E. Youman.
« Role-Based Access Control Models ».
IEEE Computer, 29(1):38–47, August 1996.

[87] Ravi Sandhu, David Ferraiolo et Richard Kuhn.
« The NIST Model for Role Based Access Control : Toward a Unified Standard ».
5th ACM Workshop Role-Based Access Control, pages 47–63, 2000.

[88] T. Sanpechuda et L. Kovavisaruch.
« A review of RFID localization : Applications and techniques ».
Dans *Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, 2008. ECTI-CON 2008. 5th International Conference on*, volume 2, pages 769–772, 2008.

[89] Markus Schumacher.
Security Engineering with Patterns : Origins, Theoretical Models, and New Applications.
Lecture Notes in Computer Science, Vol. 2754. Springer, 2003.

[90] Markus Schumacher et Utz Roedig.
« Security Engineering with Patterns ».
Dans *Proceedings of the conference on Pattern Languages of Programs (PLoP 2001)*, 2001.

[91] K. Shimizu, K. Kawamura et Katsuyuki Yamamoto.
« Location system for dementia wandering ».
Dans *Engineering in Medicine and Biology Society, 2000. Proceedings of the 22nd Annual International Conference of the IEEE*, volume 2, pages 1556–1559 vol.2, 2000.

[92] Richard E. Smith.
Authentication : from passwords to public keys.
Addison-Wesley Longman Publishing Co., Inc., 2002.

[93] Maria Toeroe et Francis Tam, éditeurs.
Service Availability : Principles and Practices.
Wiley, 2012.

[94] Yuli Vasiliev.
SOA and WS-BPEL : Composing Service-Oriented Architecture Solutions with PHP and Open-Source ActiveBPEL.
Packt Publishing, 2007.

[95] Ju An Wang et Minzhe Guo.
« OVM : An Ontology for Vulnerability Management ».
Dans *Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research : Cyber Security and Information Intelligence Challenges and Strategies*, CSIIRW '09, pages 34 :1–34 :4. ACM, 2009.

[96] Timothy O. Woods, U.S. Office of Justice Programs et Office for Victims of Crime.
First response to victims of crime : a handbook for law enforcement officers on how to approach and help elderly victims, victims of sexual assault, child victims, victims of domestic violence, survivors of homicide victims.
Office for Victims of Crime Resource Center (OVCRC), 2001.

[97] Haidong Xia et José Carlos Brustoloni.
« Hardening Web browsers against man-in-the-middle and eavesdropping attacks ».
Dans *Proceedings of the 14th international conference on World Wide Web*, WWW '05, pages 489–498. ACM, 2005.

[98] Guang yao Jin, Xiao-Yi Lu et Myong-Soon Park.
« An indoor localization mechanism using active RFID tag ».
Dans *Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006. IEEE International Conference on*, volume 1, 2006.

[99] Joseph Yoder et Jeffrey Barcalow.
« Architectural Patterns for Enabling Application Security ».
Dans *Proceedings of the conference on Pattern Languages of Programs (PLoP 97)*, 1997.

[100] Steven H. Zarit, Karen E. Reever et Julie Bach-Peterson.
« Relatives of the Impaired Elderly : Correlates of Feelings of Burden ».
The Gerontologist, 20(6):649–655, 1980.

[101] Jianying Zhou et D. Gollman.
« A fair non-repudiation protocol ».
Dans *Security and Privacy, 1996. Proceedings., 1996 IEEE Symposium on*, pages 55–61, 1996.

[102] Jianying Zhou et Dieter Gollmann.
« Evidence and non-repudiation ».
Journal of Network and Computer Applications, 20(3):267 – 281, 1997.

[103] M. Zviran et W. J. Haga.
« A Comparison of Password Techniques for Multilevel Authentication Mechanisms ».
The Computer Journal, 36(3):227–237, 1993.