Analyse de la sécurité et de la protection de la vie privée des systèmes de gestion d'identités

Johann Vincent* † ‡ §, Kourosh Teimoorzadeh§, Christophe Rosenberger * † ‡, Marc Pasquet* † ‡
*Université de Caen Basse-Normandie, UMR 6072 GREYC, F-14032 Caen, France
†ENSICAEN, UMR 6072 GREYC, F-14050, Caen, France
{johann.vincent, christophe.rosenberger, marc.pasquet}@ensicaen.fr
‡CNRS, UMR 6072 GREYC, F-14032, Caen, France
§SFR, 1 place Carpeaux, Tour Séquoia, 92 915 Paris La Défense
{kourosh.teimoozadeh}@sfr.com

***Résumé*—L'un des enjeux majeurs de la dématérialisation de la notion d'identité concerne la sécurité et la protection des données privées. En effet, la multiplicité des identifiants numériques et la pluralité des modalités d'usage nécessitent la mise en place des mécanismes innovants de protection des données sensibles. Dans cette perspective, au-delà des modalités d'implémentation, des technologies d'identification et d'authentification existantes, il est primordial de déterminer une méthodologie "universelle" permettant de la modélisation des systèmes de gestion d'identité (SGI). Dans cet article, une telle méthodologie permettant d'analyser la sécurité et la protection de la vie privée dans les systèmes de gestion d'identités est proposée. Cette dernière repose sur une cartographie des acteurs et des fonctions présents dans les SGI, elle est illustrée sur les principaux systèmes de gestion d'identités existants, permettant ainsi de les comparer. Cette méthodologie est enfin illustrée sur les principaux systèmes de gestion d'identités existants et permet ainsi de les comparer.**

***Index Terms*—Identité numérique, sécurité, vie privée**

I. Introduction

Dans un système d'information, le problème de la confiance entre les différentes entités est récurrent. En sécurité informatique, ce problème de la confiance est traité à l'aide de politiques prédéfinies qui précisent les droits des entités du système. L'application de ces politiques dépend de l'échange d'attributs désignant une entité auquels sont associés un ou plusieurs droit d'accès. Ces ensembles d'attributs ou de revendications sont appelés identités numériques. La partie du système d'information en charge de ces identités est appelé système de gestion d'identité. On appelle plus généralement tous les systèmes en charge de traiter des données relatives à l'identité numérique : système de gestion d'identité (SGI). Le projet FIDIS [1] a classifié les SGI en trois types qui reprennent globablement leurs fonctions : authentification et autorisation pour le type 1, profilage pour le type 2 et enfin, gestion des mots de passe pour le type 3.

Les SGI du premier type, dédiés à l'authentification et à l'autorisation, sont ceux qui ont pour but d'assurer la création d'une relation de confiance entre entités. Leur fonction conditionnant l'application des politiques de sécurité, ces systèmes doivent tout d'abord être eux même sécurisés. De même, dans le cas où les entités désignées par ces identités numériques sont des individus, l'utilisation d'un SGI peut poser des problèmes vis à vis de la vie privée de ces personnes. Tous les SGI existants adressent ces deux problématiques que sont la sécurité et la protection de la vie privée de manière différente. Ces différences rendent difficiles la compréhension et la modélisation de ces SGI de même que leur comparaison.

L'objectif de cet article est de présenter une méthode destinée à modéliser les SGI de type 1 et 3. Nous commençons par présenter les méthodologies existantes qui permettent l'analyse d'une solution en regard de la protection de la vie privée et de la sécurité. Nous expliquons pourquoi notre méthode est un complément à celles existantes et en quoi elle est directement liée à la gestion d'identité. La méthode proposée ici consiste en une cartographie des acteurs et des fonctions des SGI. Nous expliquons comment notre modélisation permet de prendre en compte toutes les propriétés de sécurité et de protection de la vie privée attendues dans la gestion d'identité. Enfin, nous présentons une méthode d'évaluation des systèmes de gestion d'identité basée sur la cartographie et que nous illustrons sur les principaux protocoles et SGI actuels.

II. Etat de l'art

Les principaux efforts sur l'analyse de solutions en regard de la protection de la vie privée et de la sécurité sont conduits durant les premières phases de développement. La sécurité et la protection de la vie privée sont alors considérées comme des pré-requis non fonctionnels [2] [3] qui doivent être pris en compte dans les premières étapes de développement. Pour réaliser ces analyses et exprimer ces prérequis, plusieurs méthodes existent.

A. Approche orientée but et agents

L'approche orientée but[1] [4] consiste à exprimer les prérequis en matière de protection de la vie privée et de sécurité sous la forme de buts à atteindre. Les travaux utilisant cette approche se basent sur plusieurs taxonomies des propriétés de protection de la vie privée et en particulier sur les travaux de Pfitzmann [5]. Ces propriétés servent à exprimer directement

1. goal-oriented approach

les buts à atteindre. Cette approche est notamment celle de méthodologies comme KAOS [6] ou encore de la méthode PriS [7] spécifiquement dédiée à la protection de la vie privée. Cette dernière propose également au développeur un ensemble de techniques d'implémentation correspondant au but attendu. Il est intéressant de noter que dans cette approche, les systèmes de gestion d'identités constituent une de ces techniques. D'autres méthodologies s'appuient sur l'expression d'anti-buts ou de mauvais cas d'utilisation pour dériver les pré-requis, c'est le cas notamment de [8]. Plusieurs approches orientées agent [2] [9], [10], [11] viennent également compléter les méthodologies orientées but.

B. Approche basée sur les arbres d'attaques

Les méthodes présentées sont principalement dédiées à l'expression de pré-requis lors des phases de développements et ne sont pas adaptées à l'étude de systèmes existants. Pour combler ce manque, plusieurs travaux proposent l'utilisation d'arbres d'attaque ou de menaces. La méthodologie SDL, basée sur les diagrammes de flux de données [12], en particulier est intéressante car elle se base sur une analyse des menaces appelée STRIDE (uSurpation, falsificaTion, Répudiation, divulgation d'Informations, Déni de service, et Elévation de privilèges). Dans [13], M. Deng propose une extension de la méthodologie SDL prenant en compte non seulement les menaces liées à la sécurité mais également celles liées à la vie privée à partir d'une analyse appelée LINDDUN (Linkability, Identifiability, Non-repudiation, Detectabiity, Disclosure of information, Content unawareness, policy and consent Noncompliance) basées principalement sur les propriétés proposées par Pfitzmann [5].

Aucune des méthodes présentées ne permet d'analyser directement à la fois la sécurité et la protection de la vie privée d'un SGI. Dans la partie suivante, nous présentont une telle méthode que nous avons appelée cartographie des acteurs et des fonctions.

III. Cartographie des acteurs et des fonctions

Les méthodes présentées ci-dessus peuvent s'appliquer au développement d'un SGI, cependant, elles proposent pour la plupart des contremesures qui ne sont pas adaptées aux spécificités des systèmes de gestion d'identités. Par exemple, la récursivité de la confiance n'est pas prise en compte. De plus, bien que certaines des méthodes soient dédiées à l'analyse, la plupart d'entres elles permettent avant tout l'expression de pré-requis. Il n'existe pas à notre connaissance de modèle spécifiquement dédié à l'analyse de SGI existants.

Dans cette partie, nous présentons un framework que nous avons appelé cartographie des acteurs et des fonctions [14][15] qui permet de faire ce type d'analyse. Notre framework s'inscrit comme un complément des méthodologies existantes et cherche à simplifier la compréhension des systèmes de gestion d'identités existants. Il est constitué d'un tableau des acteurs et des fonctions réalisées par ces derniers dans un processus de gestion d'identité.

A. Les acteurs

Les acteurs que nous présentons sont des rôles génériques que nous avons isolés dans chaque système de gestion d'identité. Ces rôles sont joués par des entités virtuelles au sein d'un système d'information. Nous détaillons ici les quatre rôles que nous avons identifiés. Lors de l'utilisation d'une identité, une entité pourra jouer plusieurs des rôles que nous présentons.

1) Le sujet: Comme nous l'avons indiqué, dans un système de gestion d'identité de type 1, l'identité numérique sert à établir une relation de confiance entre deux entités. Dans les SGI, le sujet représente l'entité désignée par l'identité numérique. Dans la littérature, le sujet est parfois appelé principal [16]. L'entité jouant le rôle du sujet est le plus souvent liée à un individu, mais elle peut aussi représenter tout autre type d'entité comme un groupe d'individus ou même un serveur de fichier.

2) Le fournisseur de service (SP): Dans un système d'information, le fournisseur de service est utilisé pour désigner une entité qui fourni un service basé sur la souscription à des particuliers ou des entreprises. Pour fournir ce service, ce dernier va devoir identifier le sujet qui en fait la requête. Dans un système informatique, il va chercher à identifier le sujet et s'assurer que ce dernier possède les bons droits d'accès. Un site internet, un système d'exploitation, une application d'entreprise sont autant d'exemples de fournisseurs de service.

3) Le fournisseur d'identité (IdP): Comme nous l'avons présenté, dans l'établissement d'une relation de confiance basée sur les politiques, le problème de la récursivité est adressé par l'ajout d'un tiers de confiance. C'est le cas par exemple dans les infrastructures de gestion de clés. De manière plus générale, l'entité qui joue ce rôle est appelé fournisseur d'identité. Ce fournisseur est en charge de l'attestation de l'identité. Dans ce modèle de confiance, pour que l'identité ainsi attestée permette au fournisseur de service de faire confiance au sujet, le fournisseur de service doit avoir pré-établi une relation de confiance avec ce fournisseur d'identité. Il est tout a fait possible que l'entité jouant le rôle de fournisseur d'identité joue également un autre rôle. Par exemple, un système d'exploitation gère habituellement les comptes des utilisateurs localement. Il est donc à la fois fournisseur de service et fournisseur d'identité. De même, en fonction du niveau de confiance attendu, un individu peut jouer le rôle du sujet et du fournisseur d'identité. Par exemple, lors de l'inscription sur un site de commerce éléctronique, le site laisse généralement l'utilisateur entrer ses coordonnées personnelles et lui fait confiance pour la véracité de ces dernières.

4) L'opérateur technique (TOp): Les trois acteurs présentés précédemment sont habituels pour le domaine de l'identité. Ainsi, on les retrouve dans tous les cas, même dans le monde physique. Par exemple, un commerçant, le fournisseur de service, peut demander à un acheteur, le sujet, de lui prouver qu'il est majeur si ce dernier souhaite acheter de l'alcool. L'acheteur va alors présenter une pièce d'identité qui aura été

2. agent-oriented approach

émise par un organisme, le fournisseur d'identité, en lequel le marchand à confiance (carte nationnale d'identité, permis de conduire, ...). On voit au travers de cet exemple que les trois précédents acteurs sont assez facilement identifiables. Cependant, un quatrième acteur que nous avons appelé l'opérateur technique est toujours présent dans un système d'information.

En effet, les identités numériques étant des données, elles sont transportées sur les réseaux d'un opérateur technique qui pour ses besoins enrichit cette identité avec des revendications contextuelles. Par exemple, sur le réseau Internet, chaque ordinateur possède une adresse IP unique qui permet de communiquer avec lui. Cette adresse IP peut être considérée comme une revendication contextuelle liée à toutes les identités numériques qui seront utilisées sur cet ordinateur. De même, comme pour toutes les données, le stockage des identités numériques entraine également l'ajout de revendications contextuelles. C'est le cas, par exemple des, clés primaires des bases de données. Ces revendications techniques nécessaires sont donc émises par un acteur particulier que nous avons décidé d'appeler l'opérateur technique.

B. Les fonctions

Pour permettre l'établissement d'une relation de confiance, les acteurs que nous avons présentés vont assurer un certain nombre de fonctions. Nous avons identifié quatre types de fonctions :

- Les fonctions de requêtes qui traitent les requêtes émises par les différents acteurs
- Les fonctions d'enregistrement qui sont appelées dans les phases d'inscription ou d'enregistrement d'identité
- Les fonctions d'usage qui sont appelées lorsque le sujet utilise une identité numérique pour établir une relation de confiance.
- Les fonctions terminales qui traitent la fin de la relation de confiance ou la suppression d'une identité numérique.

Ces fonctions sont réalisées par un ou plusieurs acteurs et dépendent d'un contexte d'exécution. Une fonction peut ainsi réaliser un traitement différent en fonction de ce contexte. Par exemple, le traitement de la requête faite à un fournisseur d'identité peut différer en fonction de l'origine de la requête. C'est pourquoi nous avons également découpé les fonctions en actions élémentaires qui dépendent du contexte. Une action consiste en une entrée, un traitement et une sortie. Dans cette partie, nous allons présenter plusieurs fonctions de la cartographie en détaillant les actions qu'elles réalisent et en présentant le contexte dans lequel cette fonction est appelée. Nous avons isolé en tout 36 fonctions différentes réparties selons les quatres classes présentées. Comme nous le montrons dans la partie suivante, certaines de ces fonctions ne sont pas actuellement utilisées dans les systèmes de gestion d'identité. Cependant, elles nous ont semblé importantes pour la gestion du cycle de vie des identités ainsi que pour la protection de la vie privée.

La figure 1 présente le détail de la fonction "contrôle" de l'identité. Cette action est réalisée par le fournisseur de services qui veut s'assurer de la validité d'une identité avant de fournir son ou ses services. Nous avons identifié deux contextes dans lequel cette fonction est réalisée qui dépendent de l'acteur qui a fourni l'identité du sujet. La fonction a donc été divisée en deux actions qui diffèrent par leurs entrées. Les deux actions traitent une identité attestée qui provient soit du sujet directement soit du fournisseur d'identité. Leur sortie est identique et il s'agit d'un contexte de sécurité chez le fournisseur de service. Le traitement réalisé est également identique, il consiste à vérifier la validité de l'identité, à créer un contexte de sécurité et à autoriser le service. Dans notre outil, les traitements sont liés à la fonction suivante désignée par son id, ici la fonction suivante est la fourniture du service (SP25).

IV. Evaluation de la sécurité et de la protection de la vie privée

A. Modèle général

La cartographie en tant que telle permet de représenter un système de gestion d'identité et de comprendre le graphe des fonctions qui sont réalisées. Cependant, elle ne permet pas d'assurer qu'un SGI prenne en compte la protection de la vie privée ou qu'il soit sécurisé. Pour évaluer les SGI selon ces deux hypothèses, nous avons opté pour une démarche similaire à [13] en analysant les attaques possibles sur ces fonctions. Nous avons proposé pour chaque fonction un ensemble d'hypothèses de sécurité et de protection de la vie privée. Ces hypothèses reprennent les efforts de recherche actuels sur le sujet.

B. Evaluation d'un SGI

Afin d'évaluer la sécurité globale d'un SGI, nous vérifions pour chaque fonction traversée les hypothèses respéctées ou non. Pour chacune de ces hypothèses, nous attribuons une note entre 0 et 1 selon la règle suivante :

$$\begin{cases} Note = & 0 & \text{si l'hypothèse n'est pas respectée} \\ Note = & 0.5 & \text{si l'hypothèse est optionnelle} \\ Note = & 1 & \text{si l'hypothèse est respectée} \end{cases}$$

Cette notation permet d'obtenir un pourcentage des hypothèses respectées par rapport au total des hypothèses pour les fonctions utilisées.

C. Illustration sur une fonction

A titre d'exemple, nous illustrons cette partie sur la fonction "Politique de requête de l'identité" en charge d'exprimer les attentes d'un fournisseur de service en terme d'identité et à l'exprimer sous la forme de politique. Nous avons utilisé le terme de politique pour rester général mais le fait de demander un login mot de passe sur un site Internet constitue en soit une politique d'identité. Les actions de cette fonction sont présentées sur la figure 3. On constate que cette fonction peut être appelée dans deux contextes différents, soit le fournisseur de service est directement lié à un fournisseur d'identité et va envoyer sa politique directement à ce dernier

Check Identity						
Id fonction : SP22						
Id Action :	Contexte		Acteur		Hypothèses de sécurité	Hypothèse de privacy
a1	Le sujet fournit une identité qui a été attestée par un IdP.	ENTREE	Sujet	Identité numérique attestée.	Le SP fait confiance à l'IdP.	
		SORTIE	SP	Une session sécurisée chez le SP.		
		FONCTION	Vérifie la validité de l'identité fournie et autorise le service pour			La vérification est confidentielle.
a2	Un IdP fournit l'identité d'un sujet.	ENTREE	IdP	Identité numérique attestée.	Le SP fait confiance à l'IdP.	
		SORTIE	SP	Une session sécurisée chez le SP.		
		FONCTION	Vérifie la validité de l'identité fournie et autorise le service pour			La vérification est confidentielle.

FIGURE 1. Détail de la fonction "Contrôle de l'identité"

Sécurité		Vie privée	
Attaques	**Hypothèses**	**Attaques**	**Hypothèses**
Usurpation	Authentification	Identification	Anonymat
Modification	Intégrité	traçabilité	Inassociabilité
Vol d'information	Confidentialité	Vol d'information	Confidentialité
Elevation de privilèges	Autorisation	Détection Observation	Indétectabilité Inobservabilité
Répudiation	Non-Répudiation	Non-Répudiation	Répudiation
Usage d'une identité incorrecte	Revocabilité	Usage d'informations éronnée	Conscience du contenu
		Usage incorrect des données personnelles	Conformité à une politique, conscience du contenu

FIGURE 2. Hypothèses de sécurité et de protection de la vie privée

soit il va la soumettre au sujet qui contactera ensuite un IdP.

La première attaque exhibée lors de l'étude de cette fonction est une attaque d'usurpation d'identité du SP (phishing). En effet, le sujet ainsi que l'IdP qui vont traiter la politique n'ont pas la possiblité en l'état de vérifier que cette dernière provient bien d'un fournisseur de service honnête. Afin de contrer ce type d'attaque, la première hypothèse proposée a donc été de demander à ce que cette politique contienne l'identité publique du SP. Ceci permet de vérifier sa provenance à l'aide d'une signature par exemple. Dans le cas où la politique est destinée à un IdP bien précis, il est également important pour le SP d'authentifier ce dernier avant de lui soumettre une demande. L'authentification de l'IdP par le SP constitue donc la deuxième hypothèse de sécurité que nous proposons pour cette fonction.

La fonction intervient avant que le sujet ait été authentifié par le fournisseur de service, il est donc important qu'aucune collecte d'information le concernant ne soit faite. Ceci constitue la première hypothèse de protection de la vie privée que nous présentons, à savoir que l'anonymat du sujet soit préservé. La requête d'identité se fait à travers l'expression d'une politique d'identité. Cette dernière doit être générale et ne pas pouvoir être liée à un sujet en particulier. De même, le fournisseur de service se doit d'expliquer dans sa requête quels usages il va faire des informations recueillies afin d'assurer la propriété de conformité à une politique et de consentement de l'utilisateur. Le tableau 3 présente ces hypothèses pour les actions de la fonction "Politique de requête de l'identité".

D. Récursivité

Comme nous l'avons présenté, un des problèmes de la compréhension d'un système de gestion d'identité est la recursivité de l'identité. En effet, dans l'exemple présenté au dessus, nous avons énoncé l'hypothèse que le fournisseur d'identité devait être authentifié par le fournisseur de services. Cette authentification, constitue la création d'une autre relation de confiance entre le SP et l'IdP et peut donc être modélisée sur une autre cartographie. Afin de représenter l'ensemble d'un processus de gestion d'identité, plusieurs cartographies sont donc nécessaires et sont chaînées entres elles au travers des hypothèses de sécurité ou de vie privée. La représentation de la figure 4 permet de rendre compte de cette récursivité. Si on considère un système de gestion d'identité à analyser, chacune des fonctions déclenchées dispose d'un identifiant unique dans une cartographie, par exemple X_{15} pour la fonction "Politique de requête de l'identité" de la cartographie X. Un système complet consiste donc en un vecteur dont les coordonnées sont les fonctions utilisées tour à tour dans les cartographies utilisées.

V. ILLUSTRATION DE LA MÉTHODOLOGIE

Dans cette partie, nous illustrons notre framework sur les principaux systèmes de gestion d'identités existants à savoir : Oauth[17], OpenId[18], Shibboleth (basé sur SAML2) [19] et Infocard [20]. Dans un premier temps, la méthode présentée dans le papier sera entièrement explicitée sur le système Oauth puis les résultats de la méthode sur les autres systèmes seront présentés. L'objectif est tout d'abord de comprendre ces derniers à l'aide des graphes de fonctions mais également de

SP Identity Request Policy						
Id Fonction : SP15						
Id Action	Contexte		Acteur		Hypothèses de sécurité	Hypothèses de privacy
a1	Le SP a reçu une demande de service de la part d'un sujet. Ce SP possède suit une politique d'accès à ce service.	ENTREE	SP	Requête de service		Le sujet qui a fait la requête est anonyme.
		SORTIE	SP	Une demande d'identité suivant une politique prédéfinie.	La demande d'identité doit préciser l'identité publique du SP.	La politique ainsi que la demande doivent être inassociable au sujet.
		FONCTION	Request the Identity of the subject with the identity policy to #S14.a1			La demande doit comporter une politique de protection de la vie privée.
a2	Le SP a reçu une demande de service de la part d'un sujet. Ce SP possède suit une politique d'accès à ce service qui précise l'IdP qui doit attester l'identité et va demander cette attestation directement.	ENTREE	SP	Requête de service		Le sujet qui a fait la requête est anonyme.
		SORTIE	SP	Une demande d'identité suivant une politique prédéfinie.	La demande d'identité doit préciser l'identité publique du SP.	La politique ainsi que la demande doivent être inassociable au sujet.
		FONCTION	Request the Identity of the subject with the identity policy to #I1.a3			La demande doit comporter une politique de protection de la vie privée.

FIGURE 3. Détail de la fonction "Contrôle de l'identité"

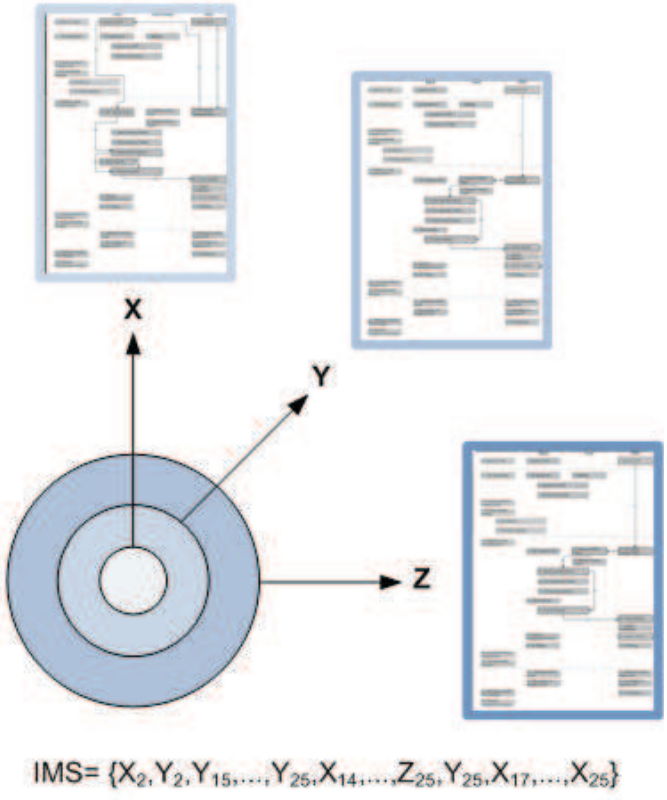

FIGURE 4. Représentation recursive avec la cartographie

les évaluer en regard des hypothèses de protection de la vie privée et de sécurité.

A. Analyse complète d'Oauth

Oauth est le protocole que nous analysons avec la cartographie. Il s'intéresse directement à l'autorisation et pas uniquement à l'authentification comme le fait OpenId par exemple. Dans ce protocole, un site appelé consommateur va jouer le rôle du fournisseur de service. Le fournisseur de service au sens Oauth joue par ailleurs le rôle de fournisseur d'identités sur la cartographie alors que l'utilisateur joue le rôle du sujet.

1) Mapping sur la cartographie: La première fonction appelée est *Inquiry to SP* chez le fournisseur de services. Le fournisseur de service va alors demander à l'utilisateur de choisir son fournisseur d'identités, cela constitue un appel à la fonction *SP Identity request policy*, et demander une créance temporaire appelée jeton de requête. Cette demande est traitée par la fonction *Inquiry to IdP* du coté de l'IdP. Une fois ce jeton reçu (*SP Identity Request Policy*), le SP va rediriger le sujet chez l'IdP avec ce jeton de requête (*Inquiry to IdP*). L'IdP va alors authentifier le sujet en appelant la fonction *Authenticate Subject* puis lui demander son consentement, ce que nous avons assimilé à la fonction *Select Identity Claims*. L'IdP va alors signer (*Attest Identity*) et émettre (*Provide identity*) une autorisation pour le service provider qui va l'utiliser pour requêter un jeton d'accès (*Inquiry to IdP*) auprès du fournisseur d'identité. Ce dernier analyse la demande (*IDP Identity Policy*) et atteste (*Attest Identity*) puis fournit (*Provide identity*) un jeton d'accès pour le SP qui va pouvoir l'utiliser pour obtenir les resources voulues (*Deliver service*).

2) Evaluation: La fonction *Inquiry to SP* suppose que trois hypothèses de protection de la vie privée soient vérifiées : l'anonymat du sujet, l'inobservabilité et l'inassociabilité. Dans notre cas, on considère que l'anonymat de l'utilisateur est respecté. Cependant, la requête peut être associée à une autre requête et reste observable. La deuxième fonction traversée *SP Identity Request Policy*, suppose elle aussi l'anonymat du sujet et emet un jeton de requête pour le fourniseeur d'identités. Ce jeton ne contenant aucune information sur l'identité du sujet, l'hypothèse d'inassociabilité est donc respectée pour cette fonction. De même, le SP signe sa requête à l'aide d'une créance client et on peut considérer que cela constitue son identité publique. Par contre, Oauth ne propose pas de mécanisme pour exprimer une politique de protection de la vie privée à ce niveau.

La demande du jeton de requête est traitée par l'IdP avec la fonction *Inquiry to IdP*, cette dernière assure l'authentification du SP. Le protocole demande également l'utilisation d'une communication chiffrée afin d'assurer la confidentialité de la réponse de l'IdP, cependant le protocole n'assure pas directement cette fonctionnalité. C'est pour cette raison que nous avons noté ces hypothèses comme optionnelles dans le récapitulatif. Une fois le jeton de requête reçu (*SP Identity*

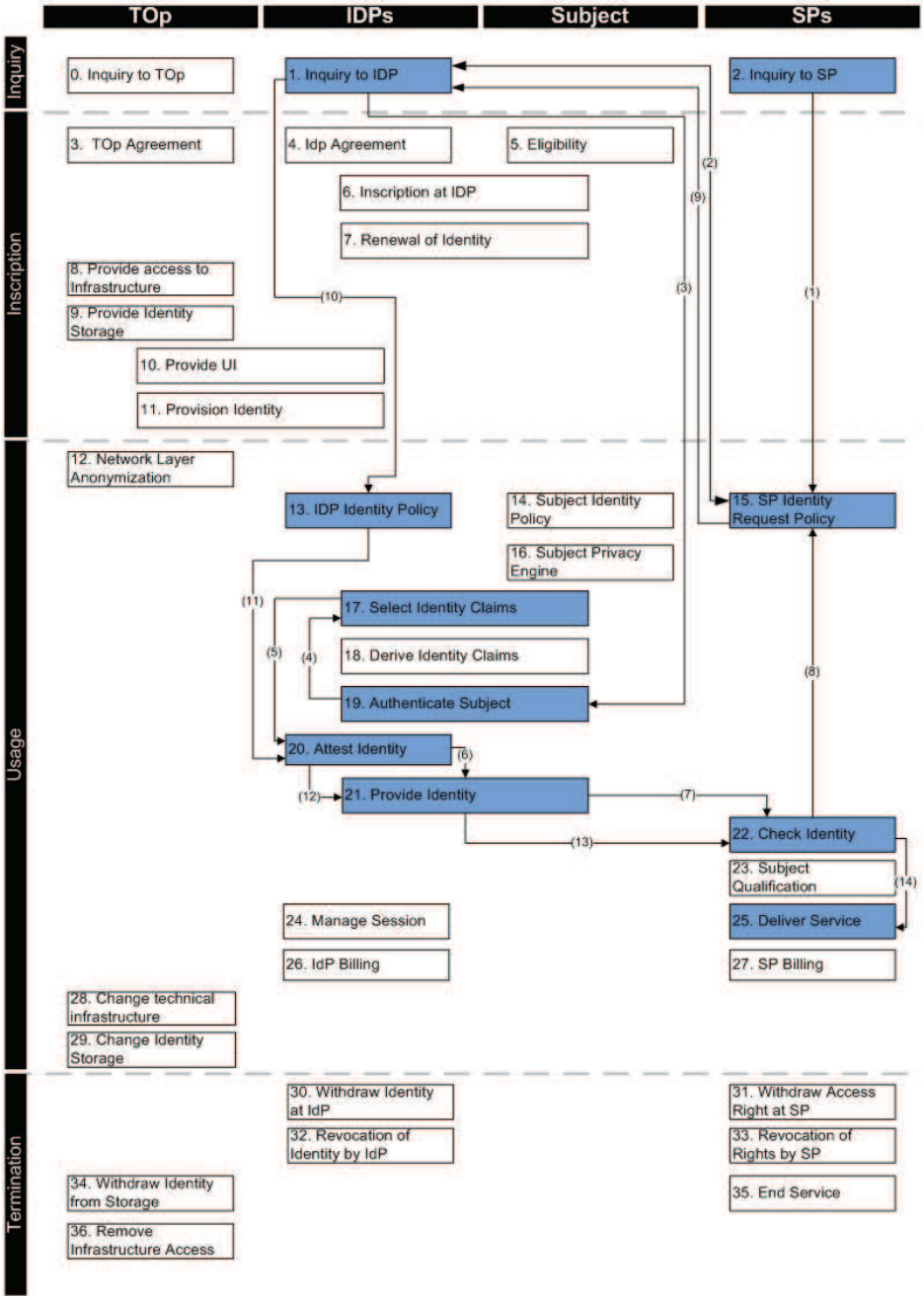

FIGURE 5. Mapping du protocole Oauth sur la cartographie

Request Policy), le SP redirige le sujet chez l'IdP avec ce jeton de requête (*Inquiry to IdP*). Là encore, l'hypothèse d'anonymat est respectée vis à vis de l'identité du sujet chez le SP de même que l'inassociabilité et ce dernier a été authentifié par l'IdP. La requête faite chez l'IdP contient également une politique sur l'accès demandé. Au niveau de la sécurité, l'authentification de son IdP par le sujet n'est pas prévue et comme précédemment l'utilisation d'une connexion chiffrée est optionnelle. L'étape suivante chez l'IdP est d'authentifier le sujet (*Authenticate Subject*), comme pour OpenId l'implémentation de cette fonction n'est pas précisée et on suppose donc qu'aucune hypothèse n'est couverte par Oauth. Le sujet va alors autoriser l'utilisation de ses resources par le fournisseur de services ce que nous qualifions de sélection d'identité (*Select Identity Claims*). L'hypothèse de protection de la vie privée attendue est le respect d'une politique d'identité, ce qui est réalisé puisque l'utilisateur a été confronté au choix de donner l'accès aux données. La propriété de non répudiation est également assurée. Dans la suite du protocole, Oauth atteste et marque le jeton temporaire avec l'autorisation de l'utilisateur (*Attest Identity*) et l'envoie au SP (*Provide identity*). Dans ces fonctions, les hypothèses de sécurité sont toutes respectées en dehors de l'hypothèse de confidentialité pour les mêmes raisons que précédemment.

Le fournisseur de service vérifie l'autorisation reçue (*Check Identity*) puis utilise la créance temporaire pour demander une créance d'accès à l'IdP (*SP Identity Request Policy* puis *Inquiry to IdP*). Pour la vérification de la créance temporaire, la confidentialité est attendue mais ne peut pas être respectée. Les hypothèses pour la demande de créance sont respectées elles aussi à part l'authentification de l'IdP. Une fois la requête reçue, l'IdP vérifie que cette dernière est conforme en appelant la fonction *IdP Identity policy* dont les hypothèses sont respectées. L'IdP atteste enfin un jeton d'accès qu'il va fournir au SP. Une fois encore les hypothèses sont respectées à l'excpetion de l'hypothèse de confidentialité qui reste optionnelle. Enfin, le SP vérifie ce jeton (*Check Identity*) et l'utilise pour requêter les données (*Deliver service*).

Au niveau de la sécurité, la principale limitation d'Oauth concerne la confidentialité de certaines fonctions. Ce problème permet à un observateur de lire les créances et par exemple de lancer des attaques offline (force brute). Dans les faits, le protocole Oauth ne présente pas de mécanisme pour adresser ce problème, cependant, il recommande à plusieurs reprises l'utilisation d'un canal sécurisé notamment par TLS. Un autre problème d'Oauth concerne l'authentification de l'IdP qui permet de réaliser des attaques de type phising. Malgré ces deux limitations, le protocole est bien sécurisé et obtient un score de 73%. Au niveau de la protection de la vie privée, Oauth souffre également du manque de confidentialité pour garantir l'inobservabilité. Cependant, il est important de noter que le protocole permet de réaliser une authentification de manière anonyme chez un SP. Avec notre méthodologie, Oauth obtient un score de 57% pour la protection de la vie privée.

B. Résultats des analyses des autres solutions

L'analyse a permis d'exhiber plusieurs hypothèses qui ne sont pas respectées dans le protocole OpenId. Ainsi, la solution obtient une note de 47% en sécurité et de 15% en protection de la vie privée. La principale limitation d'OpenId est l'absence de confidentialité lorsqu'il n'est pas utilisé au dessus d'un protocole comme TLS pour l'assurer. De même, l'absence d'authentification entre l'IdP et le SP et entre le sujet et son IdP rend possible des attaques de type phishing. Le score concernant la protection de la vie privée est également impacté par l'absence de confidentialité ainsi que par l'absence de politique de protection de la vie privée.

La solution de Shibboleth [19] propose un bon niveau de sécurité (71%) qu'il faut mettre en relation avec l'utilisation d'une liaison chiffrée avec TLS. Par ailleurs, le niveau de protection de la vie privée peut sembler assez faible (25%) mais il est principalement lié à la nature d'une solution de SSO qui suppose le minimum d'interaction avec l'utilisateur et ne propose pas de politiques pour la protection de la vie privée. Cependant, SAML permet l'utilisation d'identifiants éphemères ce qui permet potentiellement d'assurer l'anonymat des utilisateurs vis à vis des SPs.

La solution Infocard [20] obtient un très bon score au niveau de la sécurité (92%) ce qui s'explique par la réalisation des authentifications nécessaires entre IdP, SP et sujet et par l'intégration directe de la confidentialité dans le protocole. Inforcard obtient également un très bon score de protection de la vie privée (82%) qui s'explique principalement par l'intégration de politiques de la vie privée dans le protocole et par l'interaction de l'utilisateur qui sélectionne lui même son identité.

VI. Conclusion

Dans cet article, nous avons présenté les outils et méthodes existants permettant de comparer des systèmes en regard de la protection de la vie privée et de la sécurité. Les méthodes présentées s'intéressaient principalement à l'expression de pré-requis lors des premières phases de développement. Ainsi, nous avons constaté qu'aucune de ces méthodes n'était directement utilisable pour représenter les systèmes de gestion d'identités existants. Dans un second temps, nous avons donc proposé un outil appelé "Cartographie des acteurs et des fonctions" permettant d'atteindre ce but.

La cartographie proposée liste 36 fonctions appelées par 4 acteurs différents et permettant de représenter tout système de gestion d'identités. Plusieurs de ces fonctions (23) ont été proposées pour la cartographie et ne sont actuellement pas utilisées dans la plupart des SGI de la littérature. Il s'agit par exemple des fonctions d'enregistrement de l'identité dont dépend pourtant la confiance en une identité. La cartographie permet de lier les fonctions entres elles au moyen d'actions élémentaires qui sont soumises à des hypothèses de sécurité et de protection de la vie privée. Le respect ou non de ces hypothèses permet d'évaluer un SGI et de lui attribuer une note sur sa réponse à ces deux problématiques.

La cartographie peut également servir à l'expression de pré-requis pour le développement d'un système de gestion d'identités. Ainsi, nous comptons l'utiliser pour décrire une future architecture de gestion d'identité utilisant la spécificité de l'opérateur télécom et proposant des implémentations particlière de certaines des fonctions. La cartographie permettra également de positionner notre solution par rapport aux autres SGI en matière de protection de la vie privée et de sécurité.

Références

[1] M. Bauer, M. Meints, and M. Hansen. FIDIS Deliverable D3. 1–Structured Overview on Prototypes and Concepts of Identity Management Systems. *Frankfurt aM*, 2005.

[2] L. Chung. Dealing with security requirements during the development of information systems. In *Advanced Information Systems Engineering*, pages 234–251. Springer, 1993.

[3] J. Mylopoulos, L. Chung, and B. Nixon. Representing and using nonfunctional requirements : A process-oriented approach. *IEEE Transactions on Software Engineering*, pages 483–497, 1992.

[4] A. van Lamsweerde. Goal-oriented requirements enginering : a roundtrip from research to practice [enginering read engineering]. In *Requirements Engineering Conference, 2004. Proceedings. 12th IEEE International*, pages 4–7. IEEE, 2004.

FIGURE 6. Récapitulatif de l'analyse des besoins de sécurité et de protection de la vie privée

[5] A. Pfitzmann and M. Hansen. Anonymity, unlinkability, unobservability, pseudonymity, and identity management-a consolidated proposal for terminology, 2005.

[6] A. Dardenne, A. Lamsweerde, and S. Fickas. Goal-directed requirements acquisition. *Science of computer programming*, 20(1-2) :3–50, 1993.

[7] C. Kalloniatis, E. Kavakli, and S. Gritzalis. Addressing privacy requirements in system design : the pris method. *Requirements Engineering*, 13(3) :241–255, 2008.

[8] A. Van Lamsweerde, S. Brohez, R. De Landtsheer, and D. Janssens. From system goals to intruder anti-goals : attack generation and resolution for security requirements engineering. *Requirements Engineering for High Assurance Systems (RHAS'03)*, page 49, 2003.

[9] Y. Shoham. Agent-oriented programming. *Artificial intelligence*, 60(1) :51–92, 1993.

[10] L. Liu, E. Yu, and J. Mylopoulos. Security and privacy requirements analysis within a social setting. In *Proceedings of the 11th IEEE international Conference on Requirements Engineering*, page 151. Citeseer, 2003.

[11] J. Castro, M. Kolp, and J. Mylopoulos. Towards requirements-driven information systems engineering : the tropos project. *Information systems*, 27(6) :365–389, 2002.

[12] E. Yourdon and L.L. Constantine. *Structured design*. Yourdon, Inc., 1976.

[13] M. Deng. *Privacy Preserving Content Protection*. PhD thesis, Katholieke Universiteit Leuven, 2010.

[14] J. Vincent, J-P. Wary, and M. Pasquet. Cartography of actors and roles in identity management solutions. 2010.

[15] J. Vincent and W. Pasquet, M.and Chaisantikulwat. Security and privacy analysis of a physical access control solution. 2011.

[16] L. Alliance. Liberty alliance project. *Web page at http ://www. projectliberty. org*.

[17] E. Hammer-Lahav and D. Recordon. The oauth 1.0 protocol. *Internet Engineering Task Force (IETF) RFC5849*, pages 2070–1721, 2010.

[18] D. Recordon and D. Reed. Openid 2.0 : a platform for user-centric identity management. page 16, 2006.

[19] T. Scavo and S. Cantor. Shibboleth architecture. *Internet2, Technical Overview June*, 2005.

[20] M.B. Jones. A guide to using the identity selector interoperability profile v1. 5 within web applications and browsers. *Microsoft Corporation*, 2008.