Gestion des Risques dans les Systèmes d'Information Orientés Services

Vincent Lalanne (vincent.lalanne@univ-pau.fr)*
Manuel Munier (manuel.munier@univ-pau.fr)*
Alban Gabillon (alban.gabillon@upf.pf)†

Résumé : Les architectures orientées services (SOA) offrent de nouvelles possibilités pour l'interconnexion des systèmes d'information. L'ouverture du SI d'une entreprise sur l'extérieur n'est toutefois pas anodine du point de vue de la sécurité. Que ce soit pour utiliser des services proposés par des tiers ou pour offrir les siens, ces technologies introduisent de nouvelles vulnérabilités dans le SI et, par conséquent, de nouveaux risques. Nos travaux visent à initier une démarche de gestion de ces risques qui s'appuie sur un standard, la norme ISO/IEC 27005:2011. Nous proposons une évolution de cette norme afin qu'elle puisse prendre en compte pleinement le type "service". Suite à cette étude nous introduisons également un nouveau critère, la maîtrisabilité, pour qualifier la sécurité des systèmes d'informations.

Mots Clés : sécurité des systèmes d'information, gestion des risques, maîtrisabilité, ISO/IEC 27005, SOA, cloud, services web.

1 Introduction

Les systèmes d'informations présents dans les entreprises ont d'abord fonctionné en autarcie, c'est-à-dire fermés au monde extérieur et n'étant alimentés que par les données internes à l'entreprise. Très vite la nécessité de se connecter à d'autres systèmes est apparue, permettant ainsi d'accroître la quantité d'informations disponible, d'externaliser certains traitements et d'offrir de nouveaux services, tant au personnel (travail à domicile, itinérance,...) qu'aux clients (portails web, flux d'informations,...). L'usage de plus en plus fréquent des terminaux mobiles, smartphones et autres tablettes tactiles dans le monde professionnel (BYOD [1]) introduit également de nouveaux risques auxquels les entreprises se doivent de faire face : stockage d'informations, applications métier,...

Ces premières connexions ont été réalisées grâce à des liaisons privées mais, avec le déploiement d'Internet, le concepteur s'est orienté vers l'utilisation de ce réseau pour connecter ses différents systèmes d'informations. Cette évolution a permis de diminuer les coûts de connexion et d'apporter une grande souplesse dans le déploiement de telles infrastructures. Du point de vue du réseau proprement dit, les responsables sécurité ont dû mettre

*. LIUPPA, Université de Pau et des Pays de l'Adour, France
†. GePaSud EA 4238, Université de la Polynésie Française, France
1. BYOD : *Bring Your Own Device*

en œuvre différentes technologies pour maîtriser l'ouverture du réseau de l'entreprise sur Internet : routeurs, pare-feux, réseaux privés virtuels,...

L'interconnexion des systèmes d'information est une réalité en particulier avec le développement des architectures orientées services (SOA) car elles permettent la création de nouveaux services par la composition (orchestration, chorégraphie) de services existants sur Internet. Ceux-ci peuvent avoir des fonctionnalités très diverses : le calcul, le stockage des données, la consultation d'informations distantes (catalogues, horaires). Les services web (WS) sont une des technologies actuellement les plus utilisées pour de telles architectures.

La conception d'infrastructures faisant appel à des services extérieurs n'est pas sans soulever des problèmes quant à la sécurité des systèmes d'information (SSI). Cela concerne non seulement les critères classiques de confidentialité, d'intégrité et de disponibilité, mais également des notions telles que la traçabilité ou la confiance.

Après avoir détaillé différentes technologies mises en œuvre dans la sécurisation de ces services web, nous allons proposer une approche innovante mettant en œuvre une gestion des risques liée à l'utilisation de ces services. Cette approche s'appuie sur la norme ISO/IEC 27005:2011 [ISO11] que nous envisageons d'étendre aux services.

2 Services Web et Sécurité

L'interconnexion de différents systèmes d'information via des services web peut être réalisée soit sur des infrastructures propriétaires soit au travers d'Internet. Pour des raisons évidentes de coût, l'utilisation d'Internet et de ses standards est de plus en plus fréquente. Il existe plusieurs protocoles d'échange, dont en particulier XML-RPC [2] [Use99], REST [3] et SOAP [4] [W3C03]. REST est le mode natif du protocole HTTP. La sécurité des informations transmises est assurée par le protocole de transport HTTPS. SOAP utilise quant à lui le format XML avec HTTP comme protocole de transport sur Internet.

2.1 SOAP : Simple Object Access Protocol

Le protocole SOAP [W3C03] définit le cadre général pour l'échange de données complexes structurées en XML. SOAP est indépendant des langages de programmation (C, JAVA, PHP, NET, PERL,...) ou des systèmes d'exploitation sur lesquels il est implémenté. Un message SOAP est une transmission unidirectionnelle entre des nœuds SOAP, d'un émetteur SOAP vers un récepteur SOAP, mais les messages SOAP sont supposés être combinés par les applications pour implémenter les séquences plus complexes d'interactions, de la requête-réponse aux échanges multiples "conversationnels" dans un sens et dans l'autre.

Au-delà du protocole SOAP nous pouvons identifier un certain nombre de mesures de sécurité existantes. Des spécifications supplémentaires ont été définies au dessus de la pile XML/SOAP [BMPS10, BFKH05, OAS06] pour renforcer la sécurité des infrastructures utilisant des services web (cf. pile de spécifications des web services (WS-*) [GPC05]).

Les technologies de base autour d'XML sont toutes définies par le World Wide Web Consortium (W3C). C'est le cas par exemple pour XML Encryption [ER02] et XML

2. XML-RPC : *XML Remote Procedure Call* ; n'est plus maintenu depuis 1999
3. REST : *REpresentational State Transfert*
4. SOAP : *Simple Object Access Protocol*

Signature [BBF+08], permettant de régler respectivement la question de la confidentialité (chiffrement des données) et de l'intégrité des données (authentification du message et/ou du signataire). À partir de ces standards, des organismes de normalisation tels que l'OASIS ont développé des spécifications telles que Web Service Security [NKHB+06]. C'est un lot d'extensions SOAP qui garantit au message son intégrité et sa confidentialité. Cette spécification est flexible et peut être accommodée de modèles de sécurité aussi variés que PKI, Kerberos et SSL. Un certain nombre de spécifications sont associées à WS-Security dont notamment WS-Trust [5], WS-SecureConversation [6], WS-Federation [7], WS-Authorization [8] et WS-Privacy [9].

D'autres spécifications concernent plus particulièrement les phases d'authentification et d'autorisation. L'authentification est le processus pour valider les identités, tandis que l'autorisation est un processus visant à déterminer qu'une partie authentifiée peut accéder à ce type de ressources ou d'effectuer ce type d'actions. La spécification SAML [10] [CKPM05] définit un cadre de travail pour échanger des informations d'authentification et d'autorisation entre les partenaires d'affaires. SAML prend en charge l'authentification unique (SSO) pour les sites affiliés. La spécification XACML [11] [MG03] définit quant à elle un langage pour le contrôle d'accès, la circulation des règles et l'administration de la politique de sécurité des systèmes d'information.

2.2 Un Monde de Services

Il n'est plus possible, à l'heure actuelle, de dissocier les services web d'un autre concept qui leur est proche : le "cloud". En effet ce concept fait appel à de nombreux services dans le domaine du traitement, du stockage, de la transformation de l'information. Le modèle du cloud reprend des concepts déjà connus dans le monde des services mais avec un discours marketing agressif et un nouvel acronyme : les SOA.

Le nombre de services disponibles sur le cloud est en perpétuelle augmentation. Les infrastructures (Infrastructure as a Service, IaaS), les plates-formes (Platform as a Service, PaaS), les logiciels (Software as a Service, SaaS) sont d'abord apparus, n'étant souvent qu'une déclinaison des services web déjà existants, pour laisser place maintenant à la supervision (Monitoring as a Service, MaaS), les communications (Communication as a Service, CaaS), les données (Data as a Service, DaaS), les informations (inFormation as a Service, FaaS), etc... Les XaaS (Anything as a Service) sont nés et regroupent l'ensemble des services informatiques directement accessibles depuis Internet et qui se développent sur le business model du cloud computing. À noter que nous pouvons distinguer deux notions : le cloud privé et le cloud public. Si dans un cloud privé (interne à l'entreprise) il est possible de maîtriser l'infrastructure, ce n'est pas toujours le cas dans un cloud public.

5. WS-Trust : spécification pour la génération, le renouvellement et la validation de *security tokens*
6. WS-SecureConversation : création et partage de contextes de sécurité (via un *security context token*)
7. WS-Federation : définition de mécanismes de fédération d'espaces de confiance hétérogènes
8. WS-Authorization : expression des autorisations
9. WS-Privacy : modèle pour indiquer comment les besoins de confidentialité et les pratiques liées aux données privées sont transmises entre organisations
10. SAML : Security Assertion Markup Language
11. XACML : XML Access Control Markup Language

3 L'ISO/IEC 27005 Appliquée à la Gestion des Risques dans les Systèmes d'Information Orientés Services

Les entreprises ayant de nombreux échanges de données avec d'autres sociétés (nationales ou internationales) ou avec de nombreux partenaires et clients, ont senti depuis une dizaine d'années la nécessité de s'accorder sur des normes pour aider à sécuriser l'information et les processus d'échanges. L'ISO/IEC 27005 est la norme la plus récente en matière de gestion de la sécurité de l'information. Elle est appelée à être très utilisée dans le domaine des SMSI [12]. En 1995 la BSI publie la norme BS 7799 [BSI95] qui s'articule autour de dix grands chapitres qui énumèrent les mesures (une centaine) qui peuvent être prises en matière de sécurité de l'information. En 2000 l'ISO l'adopte officiellement sous la référence ISO 17799 [ISO05a] qui porte désormais le nom de ISO 27002. En 2005 apparait la série des normes ISO 27000 avec la création de l'ISO 27001 [ISO05b] ; il s'agit de la norme BS 7799 à laquelle s'ajoutent les exigences auxquelles doit répondre un organisme pour mettre en place un SMSI, le tout dans une une démarche proche de l'ISO 9001 [ISO08]. En 2008 l'ISO 27005 est mise en place ; c'est une norme de gestion des risques ; elle répond, lorsqu'elle est appliquée, à toutes les exigences de l'ISO 27001. Nous ne détaillerons pas cette norme dans cet article mais nous invitons le lecteur à consulter le site de l'ISO [ISO11] pour en comprendre les mécanismes.

Les difficultés rencontrées pour la gestion des risques dans les systèmes d'information distribués SOA sont fondamentalement liées à la nature même des SOA. Une telle architecture "logique" concerne à la fois les aspects matériel (les serveurs du prestataire de service), logiciel (systèmes d'exploitation, implémentation du protocole SOAP, services eux-mêmes) et réseau (internet, réseau local, routeurs). Certes la norme ISO/IEC 27005:2011 peut déjà prendre en compte ces aspects dans le périmètre d'étude, mais généralement de manière individuelle : datacenter, liaisons, ordinateurs, applicatifs,... Les solutions techniques existantes pour améliorer la sécurité des SI abordent d'ailleurs elles aussi ces points de manière individuelle : redondance de serveurs, liaisons doublées, outils de chiffrement, administration des systèmes, suivi des applicatifs,...

Suite à ce constat nous avons décidé de mener notre étude suivant une démarche de Risk Manager conforme à l'ISO/IEC 27005:2011 avec comme objectif de définir une annexe dédiée à l'interconnexion des SI dans une SOA afin d'enrichir les annexes C et D de la norme avec, respectivement, des menaces et des vulnérabilités spécifiques aux SOA.

3.1 Déroulement de la Norme ISO/IEC 27005:2011

3.1.1 Établissement du contexte

Contrairement aux travaux que nous pouvons trouver dans la littérature, nous ne nous orientons pas vers l'étude de la sécurisation des services web eux-mêmes. Nous étudions l'impact d'une architecture orientée services sur la sécurité des systèmes d'information (SSI) du point de vue des risques liés à la sécurité de l'information. Car si des technologies telles que les services web apportent de nouvelles fonctionnalités, voire sont à même de générer de nouveaux besoins, elles introduisent néanmoins de nouvelles vulnérabilités au sein du SI et, par conséquent, de nouveaux risques pour la Sécurité du SI.

12. SMSI (anglais : ISMS) : Système de Management de la Sécurité de l'information

Notre domaine d'étude concerne l'interconnexion de différents systèmes d'information (au sens large) via l'utilisation de services web. Notre préoccupation n'est pas la sécurité "interne" de ces services web (ex : injection de paramètres erronés) mais l'impact d'une "défaillance" d'un service web sur le SI.

3.1.2 Identification des actifs

Dans ce contexte, les actifs que nous sommes amenés à considérer peuvent être classés en deux catégories : les services web (graphe des flux de données en entrée et en sortie, processus métier qu'ils implémentent,...) et l'infrastructure de communication (systèmes, machines, OS, réseau, plateformes logicielles,...)

3.1.3 Identification des menaces

D'après le glossaire des termes de sécurité de l'information clé du NIST [NIS11], une menace (en anglais *threat*) est définie comme "toute circonstance ou événement susceptible de nuire aux opérations de l'organisation (y compris les missions, les fonctions, l'image, ou à la réputation), aux actifs de l'organisation ou des individus à travers un système d'information via un accès non autorisé, la destruction, la fermeture, la divulgation, la modification de l'information, et/ou déni de service".

Au sens des normes ISO, une menace est un événement qui peut se produire sur un actif ou un ensemble d'actifs. La menace est un événement qui cible un actif en exploitant une ou plusieurs vulnérabilités que possède l'actif. Cet événement peut être de nature délibérée (ex : vandalisme, piratage), accidentelle (ex : rupture d'un câble suite à des travaux de voirie) ou naturelle. Un risque est le potentiel d'une menace à exploiter avec succès une ou plusieurs vulnérabilités particulières et ainsi causer des dommages au système d'information ou à l'organisation. Il se mesure en termes de combinaison des probabilités d'un événement et de ses conséquences. En ce qui concerne notre domaine d'étude, voici une liste (bien évidemment non exhaustive) de menaces qui pourraient altérer le fonctionnement des services web :

- un incident sur le réseau entraîne des dysfonctionnements (délais trop longs, perte de connexion)
- une personne mal intentionnée intercepte des messages et forge de nouveaux messages pour nuire au SI et/ou accéder à certaines informations
- une erreur logicielle (accidentelle ou délibérée) sur un WS provoque l'envoi de réponses erronées

3.1.4 Identification des vulnérabilités

Une vulnérabilité peut être définie comme une "faiblesse dans le système d'information, les procédures de sécurité du système, les contrôles internes, ou la mise en œuvre qui pourraient être exploités ou déclenchés par une source de menace". Cette définition considère non seulement les vulnérabilités des composants logiciels, mais aussi également les aspects organisationnels.

Quand on parle de vulnérabilités des architectures orientées services (SOA) on doit se pencher sur les faiblesses inhérentes à ces technologies et pointer les vulnérabilités maintenant connues (OWASP [OWA], MITRE et le projet CVE [13] [CVE]), mais également

13. CVE : *Common Vulnerabilities and Exposures* ; ce système fournit une méthode de référence pour les vulnérabilités et les expositions (liées à la sécurité de l'information) connues du public.

prendre en compte tous les composants faisant partie de cette technologie et qui sont victimes d'attaques (WS-attacks.org) : le client du web service, le serveur, le moteur BPEL, les intermédiaires, le parseur XML, la validation de schéma (XML), la vérification de la signature, le chiffrement et le déchiffrement.

À partir de ces éléments il est possible de pointer quelques exemples de vulnérabilités et de menaces associées : recopie d'un processus de login vers une autre ressource (usurpation d'identité), usurpation de métadonnées (fichier WSDL, WS-security-policy) (abus de droit), modification du WS-Addressing avec modification du routage (vol de document), le moteur BPEL est sensible aux nombreuses requêtes SOAP (XML flooding).

De manière générale, au sens de la norme ISO/IEC 27005:2011 annexe D, toutes ces vulnérabilités font parties, des types "matériel", "logiciel" ou "réseau" et sont donc déjà implicitement référencées. En outre, un certain nombre de standards et de technologies associées permettent déjà de renforcer la sécurité des WS sur ces aspects (cf. section 2.1).

Notre objectif est de travailler à un niveau de granularité plus élevé et de nous intéresser à la sécurité de l'information en tant que telle (structure du contenu, chaîne de production et de consommation, enjeux économiques et juridiques de l'information) et non pas en tant que "simple" paramètre d'entrée/sortie circulant au sein du SI. Si l'on regarde le service de traitement de l'information (stockage, transformation, transport,...), il est certain que de nombreuses vulnérabilités et menaces se font jour en particulier avec les services de plus en plus présents qui sont communément appelés "**cloud**". Ainsi, il est possible de classer ces vulnérabilités suivant plusieurs catégories :

- ***La qualité de service :*** malgré les conventions de type SLA [14] il n'est pas rare d'être confronté à des pannes fréquentes, des services rendus indisponibles (Amazon EC2, avril 2012), pouvant toucher des milliers d'utilisateurs de par le monde. La seule compensation possible est d'ordre financière alors que votre image a été lourdement dégradée. De même qu'en est-il du client ? Peut-il migrer vers un autre opérateur de services ? Y a-t-il interopérabilité, portabilité, transférabilité lorsque le client veut reprendre ses informations ?
- ***La localisation des données et des traitements :*** ces services externalisés peuvent être situés dans le monde entier, sans qu'il soit possible de pouvoir choisir le pays. Dans la plupart des cas, le prestataire de cloud ignore lui-même où sont les données et où sont exécutés les traitements de l'information ! Un service immédiat et de qualité nécessite une grille de machines sur l'ensemble de la planète, or certaines informations peuvent être acceptables dans un pays mais interdites dans un autre.
- ***La perte de contrôle de l'information*** dont l'origine peut avoir des causes bien différentes. En cas d'***incident*** chez le prestataire de services, est-il toujours possible de récupérer ses données ? Est-ce aux clients ou au fournisseur de services de faire des sauvegardes ? De plus qu'en est-il de la ***réversabilité*** qui est censée permettre au client de reprendre possession de ses données, à tout moment, sans justification. D'autre part en cas de textit**résiliation** du contrat, l'effacement physique des données est rarement complet.
- ***La propriété de l'information :*** quand on traite des informations dans le cloud, on confie le capital de l'entreprise à un tiers. Que se passe-t-il en cas de litige (ex : non-paiement, injonction), s'il cesse son activité (ex : faillite, rachat),... ? Le prestataire a-t-il la possibilité de garder vos données ? A-t-il contractuellement le droit de les

14. *Service Level Agreement*

exploiter ?

– ***La nature de l'information :*** outre les données classiques qui peuvent être traitées dans une entreprise, il en est qui sont particulièrement sensibles : les données stratégiques (recherche-développement) et les données personnelles. En ce qui concerne des données personnelles, elles peuvent être ouvertes par des lois dans un pays alors qu'elles sont fermées dans d'autres (ex : USA Patriot Act, FISAAA [15]), ce qui peut impacter le respect de la vie privée.

3.1.5 Identification des conséquences

À partir de cette liste (non exhaustive) de vulnérabilités nous pouvons maintenant présenter quelques scénarios élémentaires illustrant l'occurrence d'une menace qui exploite une vulnérabilité d'un service avec ses conséquences sur le système d'information. Nous avons distingué les vulnérabilités "classiques" (•) qui peuvent être résolues à l'aide des technologies et mesures de sécurité existantes (cf. section 2.1) des vulnérabilités "organisationnelles" (◦) qui concernent la sécurité de l'information en elle-même.

- Défaut "d'isolation" des services web au niveau du conteneur utilisé ⇝ la défaillance d'un WS peut perturber le fonctionnement des autres WS hébergés dans ce conteneur ⇝ impact potentiel sur la confidentialité, l'intégrité, la disponibilité.
- Usurpation d'identité ⇝ la recopie d'un message contenant les informations d'identification permet de réutiliser ce message une nouvelle fois pour obtenir de nouvelles ressources.
- Falsification des métadonnées du service Web ⇝ une personne malveillante peut falsifier ces métadonnées (WSDL, WS-Security Policy) pour réduire les exigences de sécurité du service web : une obligation de crypter les messages peut être transformée en une transmission des messages en clair permettant ainsi de lire leur contenu.
- ◦ Le fournisseur ne produit pas lui-même le service qu'il propose ; ce n'est qu'un mandataire (avec des sous-traitants) ⇝ problème d'identification des responsabilités en cas de litige.
- ◦ Les données sont stockées sur un territoire étranger ⇝ les lois et réglementations ne sont pas identiques dans tous les pays (ex : SA Patriot Act, FISAAA) ⇝ perte de confidentialité évidente, que les données soient personnelles ou non.
- ◦ Certains clients stockent des données "interdites" ⇝ le service peut être fermé du jour au lendemain (ex : Megaupload 2012, 2e2 2013) ⇝ perte des données même pour les clients respectueux de la loi.
- ◦ Le fournisseur est une entreprise financièrement fragile ⇝ si cette entreprise fait faillite, le service sera interrompu (ex : 2e2 2013).
- ◦ Les procédures de clôture du service (à la fin du contrat) ne sont pas clairement définies ⇝ quid de la réversabilité ? quid de l'effacement physique des données ?

3.2 Proposition d'Évolution de la Norme ISO/IEC 27005

Comme nous venons de le voir, nous traitons la sécurité de l'information dans son ensemble : du contenu jusqu'aux aspects économiques et juridiques. Cette vision de la sécurité de l'information ne remet pas en question les concepts établis dans l'ISO/IEC 27005:2011. Au contraire, elle en est complémentaire car notre proposition consiste à ajouter à l'annexe D de cette norme un nouveau type "service" avec les vulnérabilités et les menaces

15. FISAAA : Foreign Intelligence Surveillance Act Amendments Act

qui lui correspondent et qui tient compte de la technologie des services web mais aussi de l'offre même de service proposé : ce nouveau type "service" peut être vu comme étant un "sur-type" au-dessus des types existants "matériel" , "logiciel" et "réseau".

Ainsi, lorsque l'on fixe un type "service" dans cette nomenclature, les vulnérabilités, et par conséquent les menaces associées, sont vues sous un nouvel angle. Les scénarios sont plus respectueux des faits constatés : ici il est plutôt question de "déni de service" par exemple, plutôt que de "perte de connexion réseau" ; "prestataire de service fournissant des données erronées" au lieu de "défaillance logicielle". De ces vulnérabilités découlent alors des questions simples qui sont au cœur de tout utilisateur de services et qui lui permettent de garantir une certaine "maîtrisabilité" de ses données : Puis-je agir librement sur mes données ? Sais-je où sont mes données ? Sais-je qui a accès à mes données ? Ai-je la propriété de mes données ? Puis-je changer facilement de prestataire ? Dans quel pays sont stockées mes données ? Mes données sont-elles légales dans le pays où elles sont stockées ? Mon prestataire rappelle-t-il le respect de la propriété intellectuelle à tous ses clients et éviter ainsi de se faire fermer ?

Type	**Exemples de vulnérabilités**	**Exemples de menaces**
Matériel	...	...
Logiciel	...	...
Réseau	...	...
Service	Pas de support à long terme du fournisseur de service	Le service n'est plus disponible
	Le cycle de vie et les politiques de mise à jour du fournisseur de service sont inconnus	Changement inattendu de l'interface du service
	Hébergement des services dans un pays inconnu	Espionnage, vol de données
	Ne se conforme pas avec les lois en vigueur	Le service n'est plus disponible
	Le fournisseur fait faillite	Le service n'est plus disponible
	Les lois sur la vie privée du pays d'hébergement sont différentes des lois du pays d'utilisation de ces données	Perte de confidentialité
	Permissivité des lois sur la sécurité de l'information	Espionnage, vol de données
	Sévérité des lois sur la sécurité de l'information sont	Le service n'est plus disponible
	ontrat de niveau de service inapproprié	Perte de maitrisabilité du SI
	Pas de procédure de récupération des données	Perte de maitrisabilité du SI
	Manque de réversibilité (migration, interopérabilité)	Perte de maitrisabilité du SI
	Absence de procédure d'effacement des données à la fin du contrat	Vol de données, utilisation non autorisée
	Absence de sécurisation des métadonnées du WS	Falsification du web service
	Possibilité d'appels multiples du WS	Usurpation d'identité
	Absence de traçabilité du service fourni	Absence de confiance dans l'information
Personnel	...	...
Site	...	...
Organisation	...	...

Table 1: Un nouveau type "service" dans l'annexe D de la norme ISO/IEC 27005:2011

Dans le tableau 1 nous avons repris le formalisme utilisé dans l'annexe D de la norme ISO/IEC 27005:2011 pour présenter une série (non exhaustive) de vulnérabilités et de menaces associées spécifiques au type "service". Ces vulnérabilités et menaces tiennent compte des propositions développées dans les sections précédentes.

La notion de "maîtrisabilité" apparaît du coup fondamentale dans la conception des systèmes d'information utilisant des services. L'architecte du SI doit absolument être certain de pouvoir organiser, gérer et donc "maîtriser" ses services, sous peine de rendre son système d'information inexploitable. Il est tout à fait envisageable à partir de ce postulat de définir en plus des trois critères de sécurité fondamentaux CID, un quatrième bien spécifique aux services :

1. **Confidentialité** : prévenir la divulgation non autorisée de l'information (ex : accès en lecture illicite)
2. **Intégrité** : garantir l'exactitude, l'exhaustivité, la validité et la non modification illicite de l'information
3. **Disponibilité** : garantir la continuité de service et de performance du système
4. **Maîtrisablité** : garantir le contrôle total des services utilisés

4 Conclusion

Les modèles d'architectures orientées services (SOA) sont de plus en plus utilisés au regard des bénéfices qu'ils procurent. D'un point de vue gestion des risques du système d'information, ces technologies introduisent néanmoins de nouvelles vulnérabilités de part les accès réseau, l'utilisation de services externes dont nous n'avons pas la maîtrise, les responsabilités liées à la fourniture d'un service, etc... Il existe bien évidemment des solutions pour tenter de sécuriser ces échanges et pour concevoir des services web "fiables". Nos travaux sont complémentaires puisque nous intervenons au niveau de la sécurité de l'information au sens de la norme ISO/IEC 27005:2011. Notre objectif est d'affiner ce processus de gestion des risques sur les spécificités liées aux services dans une SOA en prenant en compte l'information dans sa globalité (jusqu'aux aspects économique et juridique).

Après avoir mis en évidence un certain nombre de scénarios ne pouvant être évités via les mécanismes de sécurité existants, la deuxième phase de nos travaux consistera à proposer un modèle de sécurité pour les communications inter-SI. Nous envisageons pour cela une approche orientée contrôle d'usage telle que nous l'avons déjà expérimentée dans nos travaux [MLR12, Mun11, M. 10] sur les documents intelligents (cf. *Enterprise Digital Right Management*). L'utilisation de métadonnées pour la traçabilité des communications (via ces services) nous permettra également de remonter des indicateurs qui pourront, par exemple, être utilisés pour superviser le système d'information. Ainsi ces mécanismes permettront de protéger l'information lors de son hébergement chez un fournisseur de service. Avec ce modèle nous pourrons ainsi garantir non seulement la Confidentialité, l'Intégrité et la Disponibilité des données, mais également la **Maîtrisabilité** de l'information.

L'implémentation de ce modèle fait bien évidemment partie de nos perspectives. C'est pour cette raison que nous nous sommes orientés vers la technologie Web Services puisqu'un grand nombre de spécifications dédiées à la sécurité ont été développées autour du protocole SOAP. En outre, ces spécifications (présentées à la section 2.1) sont "ouvertes", c'est-à-dire que nous sommes libre de mettre en œuvre nos propres modèles et politiques de sécurité.

Références

[BBF+08] Mark Bartel, John Boyer, Barb Fox, Brian LaMacchia, and Ed Simon. XML Signature Syntax and Processing. Technical report, W3C Open Source Software, 2008.

[BFKH05] Konstantin Beznosov, Donald J. Flinn, Shirley Kawamoto, and Bret Hartman. Introduction to web services and their security. *Information Security Technical Report*, 10(1) :2 – 14, 2005.

[BMPS10] Elisa Bertino, Lorenzo D. Martino, Federica Paci, and Anna C. Squicciarini. *Security for Web Services and Service-Oriented Architectures*. Springer-Verlag Berlin Heidelberg, 2010.

[BSI95] BSI British Standards. BS 7799 :Part 1 :1995 - Code of practice for information security management systems. Technical report, BSI British Standards, 1995.

[CKPM05] Cantor, Kemp, Philpott, and Maler. Security Assertion Markup Language (SAML). Technical report, OASIS, 2005.

[CVE] CVE : Common Vulnerabilities and Exposures. Technical report.

[ER02] Donald Eastlake and Joseph Reagle. XML Encryption Syntax and Processing. Technical report, W3C, 2002.

[GPC05] Christian Geuer-Pollmann and Joris Claessens. Web services and web service security standards. *Information Security Technical Report*, 10(1) :15 – 24, 2005.

[ISO05a] ISO/IEC. ISO/IEC 17799:2005 - Code of practice for information security management. Technical report, ISO/IEC, 2005.

[ISO05b] ISO/IEC. ISO/IEC 27001:2005 : Information security management systems. Published, ISO, 2005.

[ISO08] ISO/IEC. ISO/IEC 9001:2008 : Quality management systems. Published, ISO, 2008.

[ISO11] ISO/IEC. ISO/IEC 27005:2011 : Information security risk management. Published, International Organization for Standardization (ISO), Geneva, Switzerland, 2011.

[M. 10] M. Munier. A multi-view approach for embedded information system security. In *CRiSIS*, pages 65–72. IEEE, 2010.

[MG03] Tim Moses and Simon Godik. eXtensible Access Control Markup Language (XACML) Version 1.0. Technical report, OASIS, 2003.

[MLR12] Manuel Munier, Vincent Lalanne, and Magali Ricarde. Self-protecting documents for cloud storage security. In *TrustCom*, pages 1231–1238. IEEE, 2012.

[Mun11] Manuel Munier. A secure autonomous document architecture for enterprise digital right management. In *SITIS*, pages 16–23. IEEE, 2011.

[NIS11] NIST. NIST IR 7298 Rev. 1 : Glossary of Key Information Security Terms. Technical report, National Institute of Standards and Technology (NIST), Fév-2011.

[NKHB+06] A Nadalin, C Kaler, P Hallam-Baker, R Monzillo, and Et Al. Web Services Security : SOAP Message Security 1.0 (WS-Security 2004). *OASIS Standard*, 200401(February), 2006.

[OAS06] OASIS. Web Services Security (WSS). Technical report, OASIS, 2006.

[OWA] Owasp : The open web application security community. Technical report.

[Use99] UserLand. XML-RPC. Technical report, UserLand Software, Inc., 1999.

[W3C03] W3C. SOAP version 1.2. Technical report, W3C Open Source Software, june 2003.