Gestion des risques appliquée aux systèmes d'information distribués

Vincent Lalanne
LIUPPA - EA 3000
Université de Pau et des Pays de l'Adour

Thèse de doctorat - ED 211

Sous la direction de
Alban Gabillon, PR (UPF) et **Manuel Munier**, MC (UPPA)

Jeudi 19 décembre 2013 - Mont de Marsan, UPPA

Introduction

Contexte et motivations

- La sécurité des systèmes d'information
- Les documents sécurisés
- Architecture Orientée Service - SOA, Cloud
- La gestion des risques en sécurité de l'information
- Les métadonnées

Introduction
Organisation de la présentation

Plan

Contrôle d'usage

Digital Rights Management - DRM

- Le contenu numérique peut être facilement copié, transmis et diffusé sur les réseaux.

- Un système de DRM protège la propriété intellectuelle :
  - par le cryptage des données
  - avec un filigrane numérique, de sorte que le contenu ne peut être distribué librement.
  - par un mécanisme de gestion du contenu qui facilite la transaction et le commerce
  - par la délivrance d'une licence d'utilisation

Contrôle d'usage
L'interopérabilité des DRM

La loi Française du 1er août 2006, dite **loi DADVSI**, relative au droit d'auteur et aux droits voisins dans la société de l'information dispose à son article L. 331-5 que :
"les mesures techniques ne doivent pas avoir pour effet d'empêcher la mise en œuvre effective de l'interopérabilité, dans le respect du droit d'auteur".

Contrôle d'usage
L'interopérabilité des DRM

Concrètement l'interopérabilité des systèmes de DRM dépend :

- des protocoles de communication entre les composants du système,
- du mécanisme de protection du contenu,
- du langage d'expression de droits (REL - Rights Expression Language) utilisé dans chacun des systèmes.

$\rightsquigarrow$ **SARSSI 2007**

Vers l'interopérabilité des Systèmes de DRM

Majirus Fansi, Vincent Lalanne, Alban Gabillon

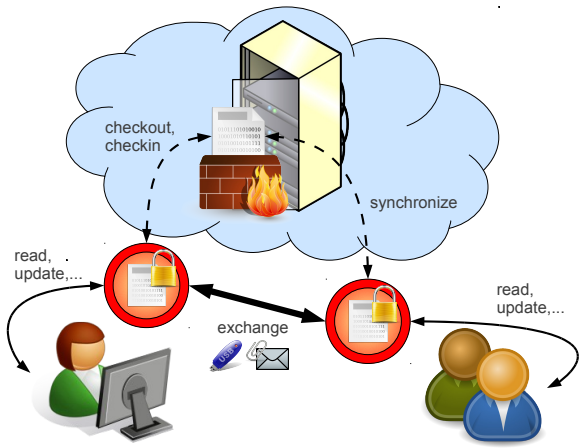
Seconde conférence jointe SAR [6ème Conférence sur la Sécurité des Architectures Réseaux - SAR] - SSI [4ème Conférence sur la Sécurité des Systèmes d'Information - SSI] organisée à Annecy du 12 aux 15 juin 2007.

Contrôle d'usage

Documents sécurisés : DRM d'entreprise

- Document complexe
- Document "intelligent"
  - document encapsulé
  - **données** : contenu du document en soi
  - **composants de sécurité** :
    - contrôles d'accès, d'usage,
    - traçabilité, contextes,
    - travail collaboratif,...

  $\Rightarrow$ métadonnées



$\rightsquigarrow$ **TrustCom 2012**

Self-Protecting Documents for Cloud Storage Security

Manuel Munier, Vincent Lalanne, Magali Ricarde[1]

11ème conférence IEEE TrustCom 2012 organisée à Liverpool (Grande Bretagne) du 25 au 27 juin 2012

1. Société BackPlan™

Contrôle d'usage

Les métadonnées dans les systèmes d'information

- Une métadonnée est une information "sur une information".
- Une métadonnée est une donnée servant à définir ou décrire une autre donnée quel que soit son support.
- Les exemples sont nombreux :
  - pour un fichier : la date de création, son titre, son auteur, etc.
  - pour une photo : les coordonnées GPS du lieu où elle a été prise, la focale de l'appareil, etc.
  - pour un workflow : données d'exécution du processus
- Les métadonnées permettent la traçabilité - Elles sont utiles en cas de litige.

$\rightsquigarrow$ **BackPlan^{tm}** [2]

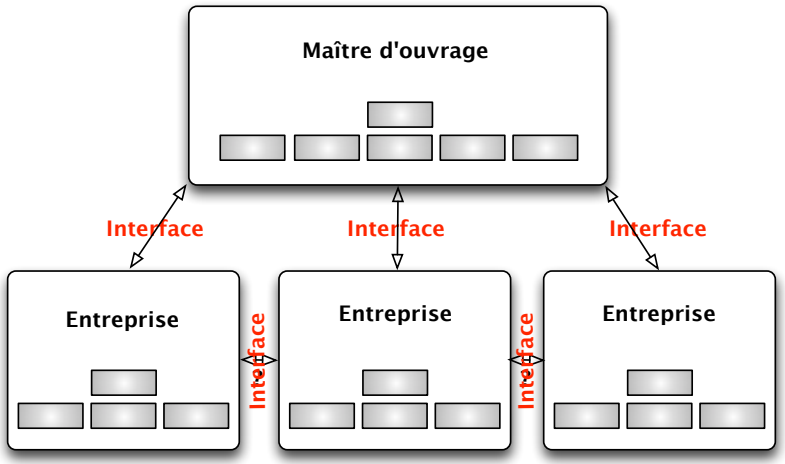
2. http ://www.backplan.fr

Plan

BackPlan™ entreprise innovante

La gestion d'interface

- Les projets industriels évoluent dans une organisation particulièrement complexe.
- Manque de visibilité globale sur l'organisation en mode projet



- Le manque d'anticipation en gestion d'interface provoque de nombreux retards et surcouts
- La coordination repose donc principalement sur l'expérience des chefs de projet

BackPlan™ entreprise innovante

Du projet à la création de la société

- Le projet BackPlan a débuté en 2008. Il a été accompagné par l'Incubateur Régional d'Aquitaine depuis mars 2009.
  - ⇝ **ENSC** [3]
  - ⇝ **UPPA** [4]
- Un contrat d'étude avec le laboratoire d'informatique de l'UPPA
  - ⇝ **Contrôle d'usage** - workflows
  - ⇝ **Métadonnées** - traçabilité
- Septembre 2009, l'équipe a intégré la technopole Hélioparc à Pau.
- Le lancement du site internet http://www.backplan.fr a eu lieu le 1er Décembre 2009 en même temps que la présentation du logo

BackPlan™
Project Communication Control

- Janvier 2011 - création de la société BackPlan™

3. École Nationale Supérieure de Cognitique - Bordeaux
4. Université de Pau et des Pays de l'Adour

BackPlan™ entreprise innovante

La politique de sécurité de l'information

- La société privilégie la qualité des informations
- Une priorité forte a été mise sur la sécurité de l'information.
- Les clients doivent avoir confiance dans la gestion de leurs informations.
- Des formations certifiantes :
  - Certification d'auditeur ISO 27001
  - Certification de mise en œuvre de la norme ISO 27 001
  - Certification **ISO/IEC 27005:2011** de management du risque

Plan

Gestion des risques en sécurité de l'information

La norme ISO/IEC 27005:2011

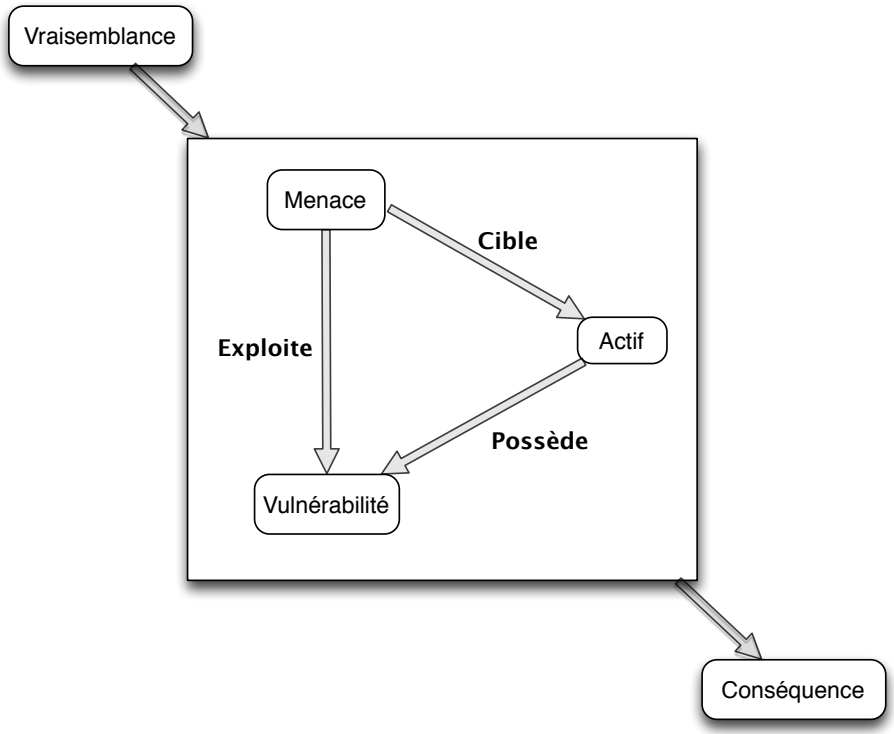
- Elle s'intègre dans la suite des normes ISO 2700x ou ISO 27k
- Elle décrit le processus de gestion des risques en sécurité de l'information.
- Elle applique à la gestion des risques le cycle d'amélioration continue PDCA [5]

5. Plan-Do-Check-Act : Cycle de Demming

Gestion des risques en sécurité de l'information

Le risque : au cœur du processus

Le risque est la vraisemblance (plus ou moins grande) de voir un événement ciblant un actif et exploitant une ou plusieurs vulnérabilités se réaliser en entraînant des impacts sur un ou plusieurs actifs et des conséquences pour l'organisme.



Modélisation du risque

Gestion des risques en sécurité de l'information

Pas de prise en compte de la notion de service

- Une gestion des risques où la notion de service est absente
- Pas de prise en compte des aspects socio-économiques :
  - Faiblesse du fournisseur de service : faillite, banqueroute, etc.
  - Espionnage : pays "poreux" avec la propriété de l'information
  - Loi permettant l'exploration des serveurs hébergés
- Des révélations qui montrent les risques encourus
  $\rightsquigarrow$ E. Snowden (juin 2013)
- PRISM, RIOT, etc...
- Perte des relations de confiance entre les organisations

$\rightsquigarrow$ **PASSAT 2013**

Information Security Risk Management in a World of Services

Vincent Lalanne, Manuel Munier, Alban Gabillon

5ème conférence IEEE PASSAT 2013 organisée à Washington DC (États Unis) du 8 au 14 septembre 2013

Gestion des risques en sécurité de l'information

Vers une maitrise des services

- Une nécessité de gérer les risques
- L'architecte du SI a de fortes contraintes :
  - Techniques : sécurité informatique de son système
  - Économiques : l'hébergement "chez soi" coute cher $\rightsquigarrow$ **Cloud**
- Une obligation de contrôle des services $\rightsquigarrow$ **Maitrisabilité**
  $\rightsquigarrow$ **PASSAT 2013**
- Collecte de métadonnées, établissement d'indicateurs
  $\rightsquigarrow$ **Aspects juridiques**

Plan

Collaboration avec les juristes

Métadonnées : des "données sensibles"

- Ces métadonnées sont "sensibles"
  - elles sont nécessaires d'un point de vue de la sécurité
    - contrôle d'usage, règles contextuelles
    - traçabilité, notion de preuve probante
  - mais peuvent être "détournées"
    - falsification
    - "surveillance" des utilisateurs (ex : géolocalisation)
    - déduction d'informations personnelles
    - calcul automatisé d'indicateurs (performance, confiance,. . .)
    - entrepôts de données (*DataWarehouse*)
    - Big data : ensemble de données

Collaboration avec les juristes

Métadonnées : des "données sensibles"

- Les métadonnées sont parfois plus importantes que les données auxquelles elles sont associées
  - données personnelles
  - données stratégiques de l'entreprise, patrimoine informationnel
  - relations inter-organisationnelles
- Quelles-sont les métadonnées que l'on a le droit de collecter ?
- Quelles-sont les métadonnées que l'on doit collecter afin de constituer une preuve ?
  $\rightsquigarrow$ Preuve en cas de litige, préconstitution de preuves,...
  $\rightsquigarrow$ Mémoire de Master Recherche [6]

6. La preuve par les métadonnées, *Camille Drouiller, juin 2013 sous la direction de Pierre-Yves Ardoy, UPPA*

Collaboration avec les juristes

Des résultats en commun

- Publications scientifiques
  - ⇝ **DPM 2013**

    Legal Issues about Metadata Data Privacy vs Information Security

    Manuel Munier, Vincent Lalanne, Pierre-Yves Ardoy, and Magali Ricarde

    8ème édition de l'atelier DPM qui s'est tenu à Egham (Grande Bretagne) au Royal Holloway, Université de Londres, le 12 et 13 Septembre 2013
  - ⇝ **CNR IUT 2013**

    Sécurité de l'Information Métadonnées & Aspects Juridiques

    Manuel Munier, Vincent Lalanne, Pierre-Yves Ardoy et Magali Ricarde

    2ème Congrès National de la Recherche en IUT CNR IUT 2013 (19ème édition) qui s'est tenu du 12 au 14 juin 2013 à l'IUT de Corté - Université de Corse - France.

Collaboration avec les juristes

Des résultats en commun

- Séminaires, colloques, formations,. . .
  - ⇝ 13/01/2012 : **Colloque** "Internet et le droit d'expression des salariés"
    6ème Journée de droit du travail
    Exposé sur "les technologies de surveillances de l'Internet"
    Colloque validé pour la formation continue des avocats
  - ⇝ 18/12/2012 : **Séminaire CRAJ** [7]
    Exposé sur les métadonnées
- Appel à projets
  - Rédaction et présentation d'un projet PEPS [8] CNRS

7. **C**entre de **R**essource et d'**A**nalyse **J**uridiques - EA 1929
8. Projets ExPloratoireS

Plan

Conclusions et perspectives

Conclusions

- Publications scientifiques :
  - **TrustCom 2012** :
    Proposition d'un document autonome sécurisé
  - **PASSAT 2013** et **SARSSI 2013** :
    - Prise en compte de la notion de service dans la mise en œuvre d'un gestion des risques en sécurité de l'information
    - Proposition du critère de maitrisabilité dans l'exploitation des services
  - **DPM 2013** :
    Prise en compte de l'aspect juridique dans la collecte des métadonnées - contrôle d'usage dans une architecture DRM
  - **CNR IUT 2013** :
    Affichage national d'une collaboration Juridique - Informatique et d'un partenariat avec entreprise locale

Conclusions et perspectives

Conclusions

- BackPlan™ :
  - Publications communes
  - Contrat de recherche
  - Statut Jeune Entreprise Universitaire
- Collaboration avec les juristes :
  - Publications communes
  - Mémoire sur les métadonnées
- Décembre 2012 : Début d'une thèse dont le thème est "Contrôle d'usage dans les architectures orientées services"

Conclusions et perspectives

Perspectives

- BackPlan™ :
  - Continuer les publications dans le domaine Oil & Gas
  - Contrat de recherche : mise en place et exploitation des métadonnées - formalisation du modèle
- Collaboration avec les juristes :
  - Ce n'est que le début : qualification des métadonnées d'un point de vue juridique
- Continuer les travaux en gestion des risques et sécurité de l'information car de nombreuses pistes ont été ouvertes

$\rightsquigarrow$ demander l'intégration au LIUPPA au titre de membre permanent

Merci de votre attention.

vincent.lalanne@univ-pau.fr