Discipline(s) : Infomatique et télécommunications

DATA SECURITY FOR INTELLECTUAL PROPERTY AND PRIVACY

Nature	UE

RESPONSABLES

Guillaume Piolle

OBJECTIFS

Dans ce module nous présentons les motivations, issues de la propriété intellectuelle et de la protection des données personnelles, qu'il peut y avoir à mettre en place des architectures spécifiques et des mesures techniques de protection des données. Une première partie détaille les techniques classiques comme plus avancées pour le tatouage numérique et la protection des contenus, en particulier multimédia. Les impératifs de contrôle d'usage, de détection des violations et de protection de la vie privée des usagers y sont présentés comme des objectifs complémentaires. La deuxième partie du module se focalise sur les méthodologies et les techniques dédiées à la protection de la vie privée et des données personnelles dans les systèmes informatiques, notamment via la protection des communications ou les technologies d'autorisations préservant la vie privée. Les principes du Privacy by Design y sont détaillés, ainsi que la problématique de protection de la vie privée dans les bases de données et la differential privacy, en tant qu'outil spécifiquement adapté à cette fin.

MOTS-CLÉS

Digital Rights Management, tatouage numérique, traçage de traîtres, vie privée, données personnelles, anonymat, pseudonymat, privacy by design

PRÉREQUIS

Connaissances de base en sécurité informatique, en réseau, en bases de données

CONTENU

Contexte juridique de la protection des données (propriété intellectuelle, données personnelles et autres cadres réglementaires)
Partie 1 – protection de la propriété intellectuelle

- Utilisation du chiffrement pour la protection du droit d'auteur (notamment lors de la transmission de données, via des techniques DRM ou non-DRM)
- Tatouage numérique (protection pérenne des données après déchiffrement)
- Codes anti-collusion (traçage des utilisateurs malhonnêtes)
- Protocoles de distribution de contenus (combinaison de traçabilité et de respect de la vie privée)

Partie 2 – protection de la vie privée et des données personnelles

- Privacy by design et principes de conception (minimisation, souveraineté, protection au long du cycle de vie…)
- Protection de la vie privée dans les bases de données (anonymat, réidentification, assainissement, private information retrieval…)
- Protection des communications (outils et infrastructures garantissant confidentialité, intégrité, anonymat, répudiabilité…)
- Autorisations préservant la vie privée (Digicash, IDEMIX, uProve…)

COMPÉTENCES ACQUISES

Savoir

- Principes et outils du tatouage numérique
- Traçage de traîtres, codes anti-collusion
- Propriétés techniques et outils pour la protection de la vie privée
- Métriques pour la protection de la vie privée

Savoir-faire

- Élaborer et implanter une stratégie de protection de contenu multimédia
- Prendre en compte la protection de la vie privée dans la conception d'un système
- Analyser les propriétés d'une technique de protection de la vie privée
- Mettre en place et évaluer une procédure d'assainissement de base de données

APPARTIENT À

- Master 2 informatique parcours Science Informatique

Mise à jour le 17 juillet 2017

CONTACT(S)

Département Informatique et télécommunications
École normale supérieure de RennesCampus de Ker LannAvenue Robert Schuman
35170 BRUZ
Tél. : 02 99 05 52 43
E-mail
Site Internet