Ulrich Aïvodji – aivodji.ulrich@etsmtl.ca

Protection des renseignements personnels

Descriptif du cours

Le droit au respect de la vie privée est un droit fondamental universellement reconnu. À titre d'exemple, il est mentionné dans l'article 12 de la déclaration universelle des droits de l'Homme. Cependant, les changements introduits par notre manière d'utiliser les technologies de l'information et de la communication combinés aux avancées technologiques en analyse de données nous exposent à un nombre croissant de risques de bris de vie privées qui peuvent mettre à mal la garantie de ce droit fondamental.

Ce cours vise à présenter les enjeux de protection des renseignements personnels dans différents contextes d'utilisation des technologies de l'information et de la communication. Il permettra de familiariser l'étudiant.e. au potentiel d'inférence de ces données ainsi qu'aux différents principes et techniques de protection. En particulier, on abordera les méthodes d'anonymisation de données, les techniques d'analyse de données préservant la vie privée, les réseaux de communication anonymes, des primitives cryptographiques avancées telles que l'intersection respectueuse de la vie privée et le retrait privé d'information, ainsi que leurs applications.

Objectif du cours

Ce cours permettra à l'étudiant.e.

- De se familiariser avec les exigences légales et réglementaires relatives au traitement des renseignements personnels.
- D'identifier des menaces à la vie privée et d'effectuer des études d'impact sur la vie privée.

- De se familiariser avec les technologies améliorant de la confidentialité (TAC) et les principes de développement garantissant la protection des renseignements personnels.
- De développer des systèmes garantissant la protection des renseignements personnels dans différents contextes, incluant le développement web et mobile, l'internet des objets, les services basés sur la localisation et l'intelligence artificielle.

Stratégie pédagogique

Ce cours sera donné en classe inversée. Il s'agit d'une approche pédagogique dans laquelle les élèves étudient le matériel avant de venir en classe. Le matériel sera constitué de capsules vidéo et de lectures. Le temps de classe est réservé à des activités plus concrètes telles que des tutoriels en forme de notebooks, des démonstrations, des questions réponses. Le cours sera complété par des travaux pratiques effectués lors des séances de laboratoire.

Charge d'enseignement : 39 heures de cours, 24 heures de laboratoire.

Sur une base hebdomadaire, cela correspond à trois heures de cours, deux heures de laboratoires, et quatre heures et demi de travail hors classe. Soit un total de 145 heures de travail.

Cours

Séance	Principaux thèmes
1	Introduction à la protection des renseignements personnels - Définition de vie privée - Définition de renseignements personnels

Ulrich Aïvodji – aivodji.ulrich@etsmtl.ca

	- Cadre légal (nationale, internationale) - Propriétés de vie privée - Privacy by design
2	Type d'inférences selon les données - Historique de navigation web - Données mobiles - Données de localisation - Réseaux sociaux - Données de santé - Jeux vidéo et monde virtuels Data brokers et modèle économique
3	Technologies d'amélioration de la confidentialité (TACs) • Anonymisation des données (vue d'ensemble) - Psedonymisation - Quasi-identifiant - Unicité des quasi-identifiants - Généralisation et suppression - Randomisation
4	Anonymisation des données (détaillé) - Historique - Techniques k-anonymat, l-diversité, t-proximité …
5	Au-delà de l'anonymisation • Confidentialité différentielle - Définition - Propriétés - Application • Synthèse de données
6	Méthodes cryptographiques (PIR, PSI, …) - Modèle d'adversaire - Étude de cas : PSI by Apple
7	Interdependant privacy
8	Réseaux de communication anonyme - Mixnets

	- Tor
9	Vie privée et technologies web - Données de navigation - Cookie syncing - Browser fingerprinting - Trackers - Dilemme des plugins anti-tracking - Session replay - Email tracking
10	Technologies basées sur la localisation - Enjeux - Geoprivacy : protections des données de mobilités - Mix zone - Cloaking - Geo indistinguishability - Autres techniques d'anonymisation
11	Donnés de santé et biométriques - Enjeux - Quantify self et wearable-based services - Inférence de renseignements personnels - Contre-mesures
12	Réseaux sociaux, Technologies mobiles et Internet des objets - Enjeux - Inférence de renseignements - Contre-mesures
13	Vie privée et intelligence artificielle - Inférence de renseignements personnels - Contre-mesures - Question ouvertes

Ulrich Aïvodji – aivodji.ulrich@etsmtl.ca

Laboratoires

Séance	Principaux thèmes
1-2	Anonymisation k-anonymat, l-diversité, t-proximité - Atelier pratique en Python
3-4	Confidentialité différentielle - Atelier pratique en Python
5-6	Technologie web - OpenWPM
7-8	Réseaux sociaux - Gephi
9-10	Donnée synthétique - Mécanisme Laplace - Mécanisme Exponentiel
11-12	Apprentissage machine - Membership inference attack - Gradient descent préservant la vie privée