

Rencontre « Vie privée et sécurité dans les données du futur »

Retours et perspectives

Journées nationales
GDR MaDICS 20/11/2018



Cédric Eichler, cedric.eichler@insa-cvl.fr

■ Contexte:

- Une exploitation accrue des données
 - De « nouveaux » paradigmes: données ouvertes, données liées, industrie 4.0...
- Nécessité privacy (et sécurité)
 - Demande du public
 - Réglementation (RGPD)

■ Objectif:

- Réunir tout-e acteur-trice, tout domaine
- Outils, techniques, contraintes, problèmes, données...

- 19/11/2018 après-midi
- ~ 15 manifestations d'intérêt, 12 inscrit-e-s, 9 participant-e-s
 - Académiques (dont 2 étudiants)
 - Informaticien-nes
 - IA, Web semantic, data-base, privacy, sécurité
 - Liris (Lyon), Lifo (Orléans), iCube (Strasbourg), Cristal (Lille), Irit (Toulouse), IMT (Toulouse), Irisa (Rennes), Sorbonne (Paris)
- Format:
 - 3 présentations
 - une table ronde

- Obj: détection attaques multi-étapes
 - E.g. WannaCry
 - Industrie 4.0
 - Orienté logs (5V)
- Investigation:
 - Identification de patterns
- Modélisation
 - Arbre d'attaques
- Détection
 - En temps réel

- Obj:
 - Data mining, calcul sur graphes
 - Robuste et respectueux confidentialité
 - Appliqué à un use-case: calcul d'influence
- Tour d'horizon techniques anonymisation et types d'attaquants
 - Bruitage differentially private:
 - Résultats
 - Communications
 - Modification du graphe
- Compromis utilité/vie privée

- Obj:
 - Publication données RDF
 - Anonyme, même face à croisement (données liées)
- User-defined spécification
 - utilité et privacy via requête
- Modifs du graphe RDF
 - Suppression faits
 - Transformation en blank node
- Suppression d'identifiants/quasi identifiants sensibles à l'interlinkage

- Intérêt manifeste pour ces problématiques
 - Volonté pérennisation des échanges à l'échelle nationale
 - Mais homogène
 - Académique
 - Uni-disciplinaire
 - Périmètre?
 - « Sécurité » données/données pour la « sécurité »
 - Graphes
 - Des données?
 - Étudiants médecine
 - OSN
 - Comment pérenniser?
 - Propositions conférences
 - Divers GDRs (MADiCS, sécurité, IA, politique publique)
-