Security and Privacy 3.0

Karima Boudaoud

karima.boudaoud@univ-cotedazur.fr

Université Côte d'Azur-I3S/CNRS

Plan

- Tour de table
- Contenu du module
- Brainstorming

Security and Privacy 3.0

- **Responsable : Karima Boudaoud**
  - Privacy, GDPR and Privacy By-design (K. Boudaoud)
  - Privacy and IoT (K. Boudaoud)
  - Smartphone Privacy (Vincent Roca – INRIA)
  - Ethics and Law (Estelle De Marco)
  - Android Security + 2 Labs (Jeremy Matos)
  - Security of software applications (Laurent Gomez- SAP)
  - Security of software applications – 2 Labs (Yves Roudier)

Vie privée et le concept de Privacy-by-Design

Karima Boudaoud

karima.boudaoud@unice.fr

I3S-University of Nice Sophia Antipolis/CNRS

Plan

- Qu'est ce que la « Privacy » ?
- Qu'est ce qu'une donnée personnelle?
- GDPR
- Différence entre « Privacy » et Sécurité ?
- Le concept de « Privacy by Design »

Qu'est ce que la « Privacy » ?

Qu'est ce que la « Privacy » ? (1/3)

- **Quelques definitions**
  - "… right to be left alone" [Warren and Brandeis, 1890]
  - "… right not to be annoyed" [Varian, 1996]
  - "control communication of personal data" [Westin 1967]
  - "control of interpersonal boundaries" [Altman 1976]
- **Mais il y en a plein d'autres** et la "privacy" est un concept multi-disciplinaire très complexe, et a de multiple dimensions…
  - Technique, economique, légal, socio-economique, philosophique,

Pas une seule définition …

Qu'est ce que la « Privacy » ? (2/3)

- **Privacy** a **de multiple perspectives dépendant du type d'acteurs**
  - Utilisateurs, entreprises en-ligne, autorités publiques, régulateurs, etc.
- Pour les utilisateurs, **Privacy** a une définition qui dépend de chaque individu et peut dépendre
  - Contexte d'usage (e.g. localisation de l'utilisateur, application, données personnelles)
  - Expérience en ligne et les violations de privacy d'un utilisateur
  - Culture et l'attitude des utilisateurs par rapport à la privacy

Qu'est ce que la « Privacy » ? (3/3)

- Protection de la **Privacy** est un challenge pour les individus
  - **Demande des efforts et nécessite très souvent une compréhension et connaissance technique**
  - N'est pas directement gratifiante (court terme) et non perceptible (Calcul de la Privacy)
  - **Est très souvent demandée par beaucoup d'acteurs, mais sans la volonté de faire l'effort** (Paradoxe de la Privacy)
  - **Ne peut probablement jamais être externalisée ("outsourced") ou automatisée**
  - Mais peut être rendu possible avec un minimum d'efforts

Privacy Online vs. Offline

- **Privacy Offline**
  - Dans le monde « offline » les individus sont capables de maintenir leur privacy de manière intuitive
- **Privacy Online**
  - Dans le monde « online », la privacy
    - Doit être maintenue en configurant des paramètres de privacy parfois complexes
    - Mais ne peut être maintenue par tous les individus
      - les données personnelles peuvent être collectées même à leur insu

Challenges pour la Privacy dans le monde Online

- **Internet** **n'oublie pas** ou parfois il n'est pas autorisé à le faire (rétention de données)
- **Internet** permet de **corréler très facilement les** **rôles sociaux** ou **identités partielles**, qui auraient été séparés dans le monde offline
- **Profilage** est **facile** et peut être fait **automatiquement**. Gérer les données personelles est **complexe** et doit être fait **manuellement**

Quelle est la définition de données personnelles?

Définition de données personnelles

- **Données personnelles**
  - **Eu Data Protection Directive (96/46/EC)/ CNIL**

According to the law, personal data means any information relating to an identified or identifiable individual; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number (e.g. social security number) or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (e.g. name and first name, date of birth, biometrics data, fingerprints, DNA…)

Protection des données personnelles d'un point de vue légal

Régulation Européenne (1/3)

- **General Data Protection Regulation (GDPR)**
  - Adoptée en Mai 2016 et entrée en vigueur en Mai 2018
  - **Eléments clés ***
    - ✓ **Augmentation de la portée territoriale :** "*apply to all companies processing personal data of personal subjects residing in EU, regardless the company's location*"
    - ✓ **Pénalités :** "*4% du chiffre d'affaires annuel global de l'entreprise ou 20 Millions d'euros*"
    - ✓ **Consentement** : consentement valide pour collecter les données data. clair, non ambigu, format facilement compréhensible.
    - ✓ **Délégué à la protection des données personnelles (Data Protection officer - DPO)** : point de contact avec l'autorité de contrôle

Régulation Européenne (2/3)

General Data Protection Regulation (GDPR)

Eléments clés *

- ✓ **Notification de violation** : autorité de contrôle (Supervisory Authority) (dans les 72h)+ personne concernée (Data subject)
- ✓ **Droit d'accès (Right to access)** aux données personnelles
- ✓ **Droit à l'oubli (right to be forgotten)** : droit d'effacer les données
- ✓ **Portabilité des données (Data Portability)** : droit de transférer les données personnelles + données fournies par le responsable de traitements des données (data controller) dans un format compréhensible

Régulation Européenne (3/3)

General Data Protection Regulation (GDPR)

Eléments clés *

✓ Accountability

- Enregistrer les activités de traitement de données (coordonnées du Data Controller et du DPO, données personnelles traitées, destinataires des données, transfert internationaux, **durée de rétention des données**).
- Réaliser une analyse de risque concernant la « privacy » des données (data protection impact assessments - DPIA)
- Implémenter des politiques de protection des données

✓ Privacy by Design and Privacy by Default

- Configuration des paramètres de Privacy (privacy settings) : **par défaut un niveau élevé**

Protection des données personnelles d'un point de vue technologique

Protection de la Privacy d'un point de vue technique

- **Solutions techniques**
  - PET (Privacy Enhancing Technology)

    "*Privacy-Enhancing Technology is a system of ICT measures protecting informational privacy by **eliminating** or **minimising** personal data thereby preventing unnecessary or unwanted processing of personal data, **without** the **loss** of the **functionality** of the information system*"[van Blarkom, Borking & Olk, 2003]

    e.g. outils d'anonymisation
  - Outils de sécurité (cryptograhie,...)
- **Privacy by Design et plus encore ...**

Quelle est la différence entre Privacy et Sécurité ?

Différence entre Privacy and Securité*

- **Implementer la Sécurité** pour assurer **Privacy**
- **Utiliser la Sécurité** pour obtenir la **Privacy**
- **Securité** est **un process - Privacy** est une **conséquence**
- **Securité** est une **action - Privacy** est le résultat d'une **action réussie**
- **Securité** est une **condition – Privacy** est le **pronostic**
- **Securité** est la **strategie – Privacy** est le **résultat**

Les principes de Privacy-by-Design

Le concept de Privacy by Design

- **Qu'est ce que le Privacy By Design?***
  - Défini par Ann Canouvian dans les années 90 & publié en 2009
  - Garantit la privacy des données + ne peut être garantit en étant «comforme à une réglementation»
  - Les PETs (Privacy-Enhacing Technologies) ne sont pas suffisants
  - Doit être appliqué à tous les types de données personnelles (données sensibles: financières, médicales, etc.)
  - **7 principes** ont été définis

* Privacy by Design – The 7 Foundational Principles – Ann Canouvian

The 7 Foundational Principles (1/4)

1. **Proactive not Reactive; Preventative not Remedial**
   - *Prendre des mesures proactives et non pas réactives. PbD n'offre pas de solution corrective. Doit être considéré durant tout le cycle de vie d'un projet dès le début de sa conception. Anticiper les problèmes de privacy avant qu'ils n'arrivent*
2. **Privacy as the Default Setting**
   - *Règles par défaut*
   - *Les données personnelles des utilisateurs doivent protégées sans leur intervention. Protection des données implicite.*
   - ***Fait partie de la GDPR***
   - *Responsabilité des développeurs et des chefs de Project d'appliquer ce principe.*

The 7 Foundational Principles (2/4)

3. Privacy Embedded into Design

- *La Privacy des données doit être intégrée dans la conception et l'architecture des systèmes IT. Ne doit pas être fait a posteriori*
- *Protection de la privacy des données est un élément essentiel des fonctionnalités de base et principales. Doit faire partie du système sans avoir d' impact sur des fonctions.*

4. Full Functionality – Positive-Sum, not Zero-Sum

- *Tenir compte des intérêts et objectifs de tous en utilisant une approche gagnant-gagnant (e.g. e-santé, applications de vidéo surveillance/ domaine)*
- *Ne pas utiliser une approche "zero-sum", où des compromis non nécessaires seraient faits.*
- *Privacy by Design évite les fausses dichotomies, tel que privacy vs. sécurité, montrant qu'il est possible d'avoir les 2.*

The 7 Foundational Principles (3/4)

5. End-to-End Security –Full Life cycle Protection

- *Garantir la sécurité des données durant tout leur cycle de vie: données doivent être* ***stockées de manière sécurisée*** *+* ***détruites de manière sécurisée*** *à la fin du traitement.*
- ***Mécanismes de sécurité forts*** *requis du* ***début à la fin****: une sécurité de bout-en-bout des données stockées (de la collecte à la destruction)*

6. Visibility and Transparency –Keep it Open

- *Les composants du système et les opérations concernant la privacy* ***restent visibles et transparents****, aussi bien pour les* ***utilisateurs*** *que les* ***fournisseurs de services (providers)****.*
- *Vérification de la Privacy crée un* ***environnement de confiance****.*

Conclusion

- Régulation Européenne RGPD
- Les principes de Privacy-by-Design
- Application lors de la conception
  - Interfaces utilisateurs
  - Conception d'applications Web
  - Smart Grids

Liens intéressants

- **Privacy by Design**
  - **https://www.ipc.on.ca/english/Privacy/Introduction-to-PbD/**
- **W3C**
  - **Privacy Interest Group: http://www.w3.org/Privacy/**

Soyez conscients de la « privacy » de vos données et de celles des citoyens et utilisateurs lorsque vous concevez des applications logicielles!!!

Thank you, Go raibh maith agat, Merci, Grazie,

Gracias, Obrigado, Danke,

谢谢, ありがとう ございました,

Terima kasih

?

Example of Best Practices for Smart Grids Privacy By Design (2/2)*

4. **Smart Grids systems** must **avoid any unnecessary trade-offs between privacy and legitimate objectives** of Smart Grid projects.
5. **Smart Grids systems** must **build in privacy end-to-end**, throughout the **entire life cycle of any personal information** collected.
6. **Smart Grids systems** must be **visible and transparent to consumers** – engaging in accountable business practices – to ensure that new Smart Grid systems operate according to stated objectives
7. **Smart Grids systems** must be **designed with respect for consumer privacy**, as a core foundational requirement.