# Sécurité Informatique

**Manuel Munier**

UPPA STEE - IUT des Pays de l'Adour - Département RT - **LIUPPA**
manuel.munier@univ-pau.fr
https://munier.perso.univ-pau.fr/teaching/m2ti-ssi/

**Master Technologie de l'Internet**
2026-2027

# Préambule

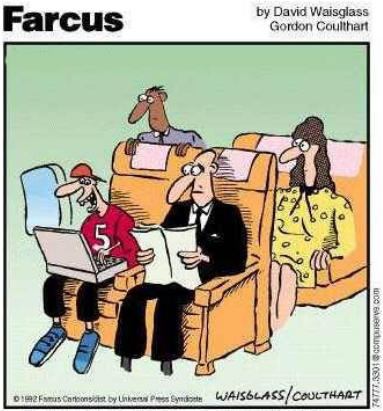
- Il faut améliorer la qualité des systèmes informatiques
  - les pannes informatiques paraissent insupportables
  - → les utilisateurs se sont habitués à une "informatique invisible" permanente
  - → les experts parlent d'un monde technologique que l'on ne peut plus débrancher...
- Importance économique du logiciel
  - importance croissante de l'informatique dans l'économie
  - coût du logiciel supérieur à celui du matériel
  - coût de la maintenance supérieur à celui de la conception

# Préambule

- Problèmes
  - Démarche ingénierie encore mal intégrée
    - ⇒ la non qualité des systèmes informatiques a des conséquences qui peuvent être très graves en cas de dysfonctionnements
  - L'informatique n'est pas prise au sérieux
    - quasiment tout le monde a un ordinateur, une tablette, un smartphone à la maison
    - ⇒ *"je sais l'utiliser"*, voire *"je sais tout"* ou *"j'ai un cousin qui...."*
    - ⇒ pas de distinction entre usage professionnel et usage privé
  - Les utilisateurs ne réalisent pas...
    - la **dépendance de leur métier** à l'outil informatique
    - la **valeur des informations** qu'ils manipulent

# "Qualité" des logiciels

- Les erreurs involontaires de conception et de codage représentent un tiers du coût des sinistres informatiques !
  - ⇒ Génie Logiciel
- Les défaillances/malveillances quant à elles causent 60% de ce coût...
  - ⇒ Sécurité des Systèmes d'Information (SSI) (aka sécurité informatique)
  - \+ **cybersécurité**




Yaahooo !!! J'ai réussi à faire planter le système de la tour de contrôle !!!

# Sécurité informatique ?

- Différentes facettes de la sécurité informatique

⇒ Différentes compétences

- ▷ génie logiciel ⇝ concevoir (proprement) des logiciels qui fonctionnent...
- ▷ sécurité système / sécurité réseau / sécurité du matériel
- ▷ sécurité logicielle ⇝ droits SQL, permissions Java, indicateurs de confiance, etc.
- ▷ **gestion des risques** ⇝ politique de sécurité, audits, etc.
- ▷ **droit & numérique**
- ▷ cybersécurité ⇝ détection, investigation, résilience, etc.

# Plan du cours

1. Introduction à la Sécurité Informatique
2. Gestion des Risques
3. Droit & Numérique
4. Conclusion

# Plan du cours

1. Introduction à la Sécurité Informatique
   - Présentation
   - Critères d'évaluation
   - Modèles de sécurité
   - Implémentation
2. Gestion des Risques
3. Droit & Numérique
4. Conclusion

# La sécurité en informatique

- Intuitivement : permettre uniquement les actions légitimes, c'est-à-dire empêcher qu'un utilisateur puisse exécuter des opérations qui ne devraient pas lui être permises

⇒ Pour définir quelles sont les opérations autorisées et celles qui sont interdites, il faut établir une **politique de sécurité**

- Les ITSEC [1] (standard européen) définissent une politique de sécurité comme étant

> *"l'ensemble des lois, règles et pratiques qui régissent la façon dont l'information sensible et les autres ressources sont gérées, protégées et distribuées à l'intérieur d'un système spécifique"*

1. Information Technology Security Evaluation Criteria

# La sécurité en informatique

- Pour construire une politique de sécurité il faut :
  - d'une part, définir un ensemble de propriétés de sécurité qui doivent être satisfaites par le système
    - → ex : *"une information classifiée ne doit pas être transmise à un utilisateur non habilité à la connaître"*
  - d'autre part, établir un schéma d'autorisation, qui présente les règles permettant de modifier l'état de protection du système
    - → ex : *"le propriétaire d'une information peut accorder un droit d'accès pour cette information à n'importe quel utilisateur"*

# Propriétés de sécurité

- Si la politique d'autorisation est **cohérente**, alors il ne doit pas être possible, partant d'un état initial sûr (c'est-à-dire satisfaisant les propriétés de sécurité), d'atteindre un état d'insécurité (c'est-à-dire un état où les propriétés de sécurité ne sont pas satisfaites) en appliquant le schéma d'autorisation
- Les ITSEC définissent 3 propriétés de sécurité :
  - la **confidentialité** → prévention de la divulgation non autorisée de l'information
  - l'**intégrité** → prévention de la modification non autorisée de l'information
  - la **disponibilité** → prévention d'un refus d'accès à une ressource ou à une information normalement autorisée (déni de service)

# Politique de sécurité → 3 directions

1. **physique** ⇒ ensemble de procédures et de moyens
   - protection des locaux et des biens contre des risques majeurs
     → *incendie, inondation,...*
   - contrôle des accès physiques aux matériels (info. & comm.)
     → *gardiens, codes, badges,...*
2. **administrative** ⇒ ensemble de procédures et moyens relatifs à la sécurité d'un point de vue organisationnel
   - structure de l'organigramme & répartition des tâches
     → *séparation des environnements de développement, d'industrialisation et de production des applicatifs*
   - propriétés de sécurité
     → *limiter les cumuls ou les délégations abusives de pouvoir*
     → *garantir une séparation des pouvoirs*

# Politique de sécurité → 3 directions

3. **logique** ⇒ gestion du contrôle d'accès logique ⇒ repose sur un triple service d'identification, d'authentification et d'autorisation
   - elle spécifie qui a le droit d'accéder à quoi, et dans quelles circonstances

   ⇒ avant de se servir du système, tout utilisateur devra décliner son identité (**identification**) et prouver qu'il est bien la personne qu'il prétend être (**authentification**)

   - une fois la relation établie, les actions légitimes que peut faire cet utilisateur sont déterminées par la politique d'**autorisation**

# Autorisation

⇒ Gérer et vérifier les droits d'accès aux ressources en fonction des règles spécifiées dans la politique de sécurité

- un **sujet** (entité qui demande l'accès → entité active) possède un droit d'accès sur un **objet** (entité à laquelle le sujet souhaite accéder → entité passive) si et seulement s'il est autorisé à effectuer la fonction d'accès (**action**) correspondante sur cet objet

- Exemple de mise en œuvre [2]
  - les droits d'accès peuvent être symboliquement représentés dans une **matrice de droits d'accès** dont les lignes représentent les sujets et les colonnes représentent les objets
  - une cellule de la matrice contient donc les droits d'accès d'un sujet sur un objet
  - la matrice est gérée conformément aux règles définies dans la politique de sécurité

2. cf. modèle HRU étudié plus loin

# Règlement de sécurité

- Les définitions précédentes supposent que ce qui est permis est connu
  - le **règlement de sécurité** définit ce qui est autorisé et ce qui ne l'est pas (les règles de la politique de sécurité)
  - un règlement de sécurité est généralement un ensemble de :
    - → **permissions**
      - *les enfants ont la permission de minuit*
      - *tout médecin a le droit d'accéder aux dossiers médicaux de ses patients*
    - → **interdictions**
      - *les enfants ont la permission de minuit, sauf la petite sœur*
      - *les médecins n'ont pas le droit d'effacer des diagnostics déjà établis*
    - → **obligations**
      - *les médecins sont obligés de conserver les dossiers médicaux pendant la durée fixée par la loi*

# Plan du cours

1 Introduction à la Sécurité Informatique
- Présentation
- Critères d'évaluation
- Modèles de sécurité
  - Modèles de contrôle d'accès discrétionnaires
  - Modèles de contrôle d'accès obligatoires
  - Modèles de contrôle d'usage
- Implémentation

# Critères d'évaluation

- Un système est sûr si et seulement si le règlement de sécurité ne peut pas être violé
- Les 1ers **critères d'évaluation de la sécurité** ont été définis aux États-Unis dans ce qui est couramment appelé le **Livre Orange** ou **TCSEC** [3]
  - → fondés à la fois sur des listes de fonctions de sécurité à remplir et sur les techniques employées pour la vérification, ces critères conduisent à classer les systèmes en sept catégories ou niveaux (D, C1, C2, B1, B2, B3, A1)

3. Trusted Computer System Evaluation Criteria

# TCSEC

- Pour chaque niveau, quatre familles de critères sont définies :
  - la **politique d'autorisation** stipule une politique précise à suivre en fonction des différents niveaux de certifications visés
  - les **critères d'audit** précisent les fonctions requises en matière d'identification, d'authentification et d'audit des actions
  - les **critères d'assurance** fixent des recommandations concernant des méthodes de conception et de vérification utilisées afin d'augmenter la confiance de l'évaluateur
    - → il s'agit de garantir que le système implémente bien la fonctionnalité qu'il prétend avoir
  - les **critères de documentation** spécifient les documents qui doivent être fournis avec le produit lors de l'évaluation

# TCSEC

- Caractéristiques principales des niveaux définis par les TCSEC :
  - → un système classé au niveau **D** est un système qui n'a pas été évalué
  - → jusqu'aux niveaux **C1** et **C2**, le système peut utiliser une politique discrétionnaire (cf. suite du cours)
  - → pour les niveaux **B1**, **B2**, et **B3** le système utilise une politique obligatoire (cf. suite du cours)
  - → un système classé **A1** est fonctionnellement équivalant à un système classé B3, sauf qu'il est caractérisé par l'utilisation de méthodes formelles de vérification pour prouver que les contrôles utilisés permettent bien d'assurer la protection des informations sensibles

# TCSEC

- Les TCSEC visaient d'abord à satisfaire les besoins du DoD (*Department of Defense*) des États-Unis, privilégiant ainsi la confidentialité des données militaires
- Le manque de souplesse et la difficulté de leur mise en œuvre, ont conduit d'autres pays à élaborer et adopter leurs propres critères d'évaluation
  - ex-Communauté Européenne → ITSEC (1991)
  - Canada → CTCPEC (1993)
  - Japon → JCSEC (1992)

# ITSEC

- Les **ITSEC**[4] sont le résultat d'harmonisation de travaux réalisés au sein de quatre pays européens : l'Allemagne, la France, les Pays-Bas et le Royaume-Uni
- Les ITSEC introduisent en plus la notion de **cible d'évaluation** (ou **TOE**[5])
  - une politique de sécurité
  - une spécification des fonctions requises dédiées à la sécurité
  - une définition des mécanismes de sécurité (optionnelle)
  - la cotation annoncée de la résistance minimum des mécanismes
  - le niveau d'évaluation visé

4. Information Technology Security Evaluation Criteria
5. Target Of Evaluation

# Critères Communs

- Harmonisation des critères canadiens (CTCPEC), européens (ITSEC) et américains (TCSEC)
  - ⇒ **critères communs** (en anglais *Common Criteria for Information Security Evaluation*)
  - ⇒ devenus maintenant une norme internationale (**ISO 15408**)
- Ces critères contiennent deux parties bien distinctes comme dans les ITSEC : fonctionnalité et assurance
- Les critères communs définissent également une cible d'évaluation (TOE) ainsi que les profils de protection

  *NB : déjà existants dans les critères fédéraux américains (Federal Criteria, 1992)*

# Plan du cours

1. Introduction à la Sécurité Informatique
   - Présentation
   - Critères d'évaluation
   - Modèles de sécurité
     - Modèles de contrôle d'accès discrétionnaires
     - Modèles de contrôle d'accès obligatoires
     - Modèles de contrôle d'usage
   - Implémentation

# Modèles de sécurité

- Pour sécuriser un système informatique il est donc important de définir un **modèle de sécurité**
- Un tel modèle de sécurité exprime les **besoins de sécurité** du système d'information ; il inclut :
  - un **règlement de sécurité**
  - un **modèle d'administration** spécifiant qui a le droit de mettre à jour le règlement de sécurité
- Il existe différents modèles de sécurité
  - les modèles **discrétionnaires**
  - les modèles **obligatoires** (ou de **contrôle de flux**)
  - les modèles de **contrôle d'usage**

# Modèles de sécurité

- Les modèles de contrôle d'accès discrétionnaires (ou **DAC** [6]) sont les plus répandus et implémentés mais sont vulnérables aux attaques par **cheval de Troie**
- Les modèles de contrôle d'accès obligatoires (ou **MAC** [7]) imposent des règles incontournables destinées à forcer le respect des exigences de sécurité
  - ils sont très formels, permettent d'atteindre un très haut niveau de sécurité (théoriquement) mais sont difficiles à implémenter
  - en général ils proposent des règlements qui visent à renforcer la propriété de confidentialité

6. Discretionary Access Control
7. Mandatory Access Control

# Modèles de sécurité

- MAC ⇒ **contrôle de flux** : ces modèles proposent des solutions pour l'identification et l'élimination des canaux cachés
  - → *"un canal caché est un chemin de communication pouvant être exploité par un processus de transfert d'information de telle sorte qu'il contourne les mécanismes de contrôle d'accès, et qu'ainsi il viole la politique de sécurité"*
- Les modèles de contrôle d'usage sont plus récents et ont été proposés afin de prendre en compte les nouveaux besoins de sécurité présents dans certaines applications telles que la **gestion des droits numériques** (ou **DRM** [8])
  - → les DRM multimédia ont été très controversés
  - → mais les DRM peuvent répondre à de nouveaux besoins en entreprise (**E-DRM** [9])

8. Digital Rights Management
9. Enterprise-DRM

# Plan du cours

1 Introduction à la Sécurité Informatique
- Présentation
- Critères d'évaluation
- Modèles de sécurité
  - Modèles de contrôle d'accès discrétionnaires
  - Modèles de contrôle d'accès obligatoires
  - Modèles de contrôle d'usage
- Implémentation

# Modèles de contrôle d'accès discrétionnaires

- Existent depuis les années 70 ; ont subi de nombreuses évolutions
  - un des premiers modèles proposés est celui de B. **Lampson** (structure de machine à états)

    *"Protection", 5th Princeton Symposium on Information Sciences and Systems, 1971*
  - progressivement amélioré → modèle **HRU** (M.A. Harrison, W.L. Ruzzo et J.D. Ullman)

    *"Protection in Operating Systems", Communication of the ACM, 19(8), pp. 461-471, 1976*
  - un des modèles les plus récents : **OrBAC** (Organization Based Access Control, 2003)

    *"Organization Based Access Control", IEEE 4th International Workshop on Policies for Distributed Systems and Networks (Policy 2003), Lake Come, Italy, June 4-6, 2003*

# Modèles de contrôle d'accès discrétionnaires

- Quelques autres modèles de contrôle d'accès :

RBAC Role Based Access Control
TBAC Task Based Access Control
VBAC View Based Access Control
TMAC TeaM based Access Control
...

# Modèles de contrôle d'accès discrétionnaires

## HRU

- Le modèle HRU aurait pu s'appeler IBAC (Identity Based Access Control) car il repose sur l'identité des entités actives du système d'information
- Il introduit les concepts de **sujet**, **action** et **objet**

sujet : c'est l'entité active ; il désigne un utilisateur, le système lui même, un processus s'exécutant pour le compte d'un utilisateur ou un processus système

objet : c'est l'entité passive ; il désigne une information ou une ressource à laquelle un sujet peut accéder pour réaliser une action

action : désigne l'effet recherché lorsqu'un sujet accède à un objet (ex : lire, écrire)

# Modèles de contrôle d'accès discrétionnaires

## HRU

- L'objectif du modèle HRU est de contrôler tout accès direct des sujets aux objets via l'utilisation des actions
- Le règlement (politique d'autorisations) correspond à un ensemble d'autorisations positives (permissions) du type :
  - → *"le sujet **s** a la permission de réaliser l'action **a** sur l'objet **o**"*
- La **politique d'autorisation par défaut** est **fermée**
  - ⇒ par défaut tous les accès sont interdits
  - → *"tout ce qui n'est pas explicitement autorisé est interdit"*

# Modèles de contrôle d'accès discrétionnaires

## HRU

- Le règlement est formalisé à l'aide d'une **matrice de contrôle d'accès**
  - les lignes représentent les sujets
  - les colonnes représentent les objets
  - une cellule (intersection d'une ligne et d'une colonne) contient l'ensemble des actions qu'un sujet a la permission d'effectuer sur un objet
- Le modèle HRU a été implanté dans la plupart des systèmes d'exploitation actuels tels que Windows ou Unix

# Modèles de contrôle d'accès discrétionnaires

## HRU

- La matrice n'est pas directement implanté ; il existe en fait deux approches selon que l'implantation repose sur une décomposition en colonnes ou en ligne de la matrice :
  - la décomposition en colonnes consiste à associer à chaque objet un descripteur appelé **liste de contrôle d'accès** (ou **ACL** [10])
    - → une ACL représente l'ensemble des sujets ayant des droits d'accès sur l'objet considéré avec pour chaque sujet l'ensemble des actions que ce sujet peut réaliser sur l'objet
  - la décomposition en lignes consiste à associer à chaque sujet une **liste de capacités**
    - → un ensemble de capacités associé à un sujet représente l'ensemble des objets auxquels le sujet considéré a accès avec pour chaque objet la liste des actions que peut réaliser le sujet

10. Access Control List

# Modèles de contrôle d'accès discrétionnaires

## HRU

| | Sam | Joe | Code | Data |
|---|---|---|---|---|
| **Sam** | | | read,write,execute | read,write |
| **Joe** | | | read,execute | read |

- ACL
  - → ⟨Code,(Sam,(r,w,x)),(Joe,(r,x))⟩
  - → ⟨Data,(Sam,(r,w)),(Joe,(r))⟩
- Capacités
  - → ⟨Sam,(Code,(r,w,x)),(Data,(r,w))⟩
  - → ⟨Joe,(Code,(r,x)),(Data,(r))⟩

# Modèles de contrôle d'accès discrétionnaires

## HRU

- Notion de **propriétaire**
  - le propriétaire d'un objet est celui qui a créé l'objet
  - le propriétaire d'un objet dispose de tous les droits sur l'objet
  - le propriétaire d'un objet peut **déléguer** à un autre sujet les droits sur son objet

# Modèles de contrôle d'accès discrétionnaires

## HRU

- Le modèle d'administration du modèle HRU consiste en un ensemble de **règles** définissant dans quelles conditions la matrice peut être modifiée ; ces règles utilisent les **primitives** suivantes :
  - donner un droit **r** à un sujet **s** sur un objet **o**
  - créer un sujet **s**
    - → *ajouter une ligne et une colonne car le sujet est aussi un objet*
  - créer un objet **o**
    - → *ajouter une colonne*
  - enlever un droit **r** à un sujet **s** sur un objet **o**
  - détruire un sujet **s**
  - détruire un objet **o**

# Modèles de contrôle d'accès discrétionnaires

## HRU

- Le modèle HRU a été fréquemment implémenté

Unix
- objets = fichiers/répertoires
- actions = {`r`,`w`,`x`}
- permissions représentées sous forme d'ACL
- administration → commande `chmod`

SQL
- objets = tables/vues
- actions = {`select`,`update`,`delete`,`insert`}
- administration → commandes `grant` et `revoke`

# Modèles de contrôle d'accès discrétionnaires

## HRU

- Avantages du modèle HRU
  - simple, souvent implémenté
    - → Unix, Windows, SQL,...
  - administration décentralisée de la règlementation
- Limites du modèle HRU : règlement complexe à exprimer et à administrer
  - énumération des autorisations $\langle sujet, action, objet \rangle$
    - → fastidieux, coûteux en mémoire
  - ⇒ constitution de **groupes** d'utilisateurs pour réduire la taille de la matrice
    - → maintenance des groupes délicate car un sujet peut appartenir à plusieurs groupes
  - mise à jour du règlement à chaque création de sujet et d'objet

# Modèles de contrôle d'accès discrétionnaires

## HRU

- Limites du modèle HRU
  - problème de la fuite des droits (*safety*)
    - → considérant un état de la matrice, il est impossible de s'assurer qu'un sujet ne pourra jamais recevoir un droit particulier sur un certain objet
  - vulnérable aux attaques par cheval de Troie
    - → le modèle HRU est vulnérable aux attaques par cheval de Troie effectuant des recopies de fichiers (cf. sécurité multi-niveaux)
    - → défaut aggravé par le fait que les systèmes informatiques sont maintenant tous interconnectés (Internet)

# Modèles de contrôle d'accès discrétionnaires

## RBAC

- Le modèle RBAC [11] propose de structurer le règlement autour du concept de **rôle**
  → un rôle est un concept organisationnel **structurant les sujets**
    - des rôles sont affectés aux utilisateurs conformément à la fonction que ces utilisateurs jouent dans l'organisation
    - les autorisations (droits d'effectuer des actions sur des objets) sont affectées aux rôles
- Le modèle RBAC ne considère que des autorisations positives et suppose une politique par défaut fermée

11. Sandhu (1996)

# Modèles de contrôle d'accès discrétionnaires

## RBAC

- Le modèle RBAC introduit la notion de **session**
  - tout utilisateur doit initier une session avant de pouvoir accéder aux objets
  - dans le cadre de cette session il peut activer un ou plusieurs rôles parmi tous les rôles qui lui ont été attribués
    - → les droits (privilèges) de l'utilisateur seront alors les droits appartenant au(x) rôle(s) activé(s)
- Les rôles peuvent être organisés **hiérarchiquement**
  - ⇒ les rôles **héritent** des autorisations des rôles hiérarchiquement inférieurs

    *Ex : "cardiologue" et "radiologue" héritent de "médecin"*

# Modèles de contrôle d'accès discrétionnaires

## RBAC

- Le modèle RBAC introduit la notion de **contrainte** permettant de spécifier des réglementation de type **séparation de tâches**
  - une séparation de tâches **statique** prévoit que 2 rôles (par exemple médecin et infirmier) ne peuvent pas être assignés à un même utilisateur
  - une séparation de tâches **dynamique** prévoit que 2 rôles (par exemple médecin libéral et chirurgien) ne peuvent être activés en même temps par un même utilisateur

# Modèles de contrôle d'accès discrétionnaires

## RBAC

- Le modèle RBAC initial ne définissait pas de modèle d'administration
  - → en particulier, il ne prévoyait pas qui avait le droit de créer et mettre à jour les rôles
- Pour combler cette lacune, le modèle ARBAC (Administrative Role Based Access Control) a été proposé
  - le modèle ARBAC est un modèle d'administration pour le modèle RBAC
  - il est lui aussi basé sur les rôles

# Modèles de contrôle d'accès discrétionnaires

## RBAC

- Avantages du modèle RBAC
  - structuration du règlement de sécurité
  - de plus en plus implémenté
    - → versions récentes de SQL
    - → Unix Solaris v8
    - → API Authorization Manager RBAC de Windows Server 2003
- Inconvénients
  - ce modèle est toujours vulnérable aux attaques par cheval de Troie
  - il nécessite de mettre en place une procédure d'administration des rôles

# Modèles de contrôle d'accès discrétionnaires

- Les systèmes d'information actuels devenant de plus en plus sophistiqués, de nouveaux modèles de sécurité sont apparus
- Les nouveaux modèles dérivés de HRU et RBAC introduisent de nouvelles possibilités
  - → workflows, vues, contextes,. . .

# Modèles de contrôle d'accès discrétionnaires

## Contextes

- En pratique, de nombreuses autorisations ne sont pas statiques mais dépendent de conditions qui, si elles sont satisfaites, permettent d'activer dynamiquement les autorisations

⇒ On parle d'**autorisations contextuelles**

  - contexte **temporel** → permission pendant les heures de travail
  - contexte **géographique** → permission uniquement à l'intérieur de l'enceinte sécurisée
  - contexte **provisionnel** → permission si d'autres actions ont été réalisées comme dans le cas d'un workflow

- Pour prendre en compte ces besoins, différents modèles à base de règles ont été définis (modèles de type Rule-BAC)
  - un règlement correspond alors à un ensemble de règles du type *condition* → *permission*

# Modèles de contrôle d'accès discrétionnaires

## Interdictions

- De nouveaux modèles de contrôle d'accès permettent d'exprimer des autorisations négatives (**interdictions**) sont apparus
- Utiliser des interdictions peut souvent répondre à un besoin
  - certaines règlementations sont plus faciles à exprimer à l'aide d'interdictions
    - → vidéo interdite au moins de 18 ans
  - combiner des permissions et des interdictions permet de spécifier de manière concise des autorisations souffrant d'**exceptions**
    1. les infirmiers ont l'interdiction d'accéder au dossier médical des patients
    2. en situation d'urgence, les infirmiers ont la permission d'accéder au dossier médical du patient

# Modèles de contrôle d'accès discrétionnaires

## Interdictions

- Utiliser simultanément des permissions et des interdictions peut créer des **conflits** dans la règlementation
  - → dans l'exemple précédent, la règle 1 est en conflit avec la règle 2 dès lors que nous sommes dans un contexte d'urgence
- Pour résoudre ces conflits diverses approches ont été proposées :
  - les interdictions (ou les permissions) l'emportent toujours
  - les règles reçoivent des niveaux de priorité
  - le plus spécifique l'emporte
  - ordre dans lequel les règles sont écrites (*first-matching applies*)

# Modèles de contrôle d'accès discrétionnaires

## OrBAC

- Actuellement, il n'existe pas de modèle de contrôle d'accès permettant de répondre à tous les besoins de sécurité énoncés
- Néanmoins le modèle OrBAC [12] est certainement un des modèles de contrôle d'accès les plus complets

https://motorbac.sourceforge.net/

12. Organization Based Access Control (2003)

# Plan du cours

1. Introduction à la Sécurité Informatique
   - Présentation
   - Critères d'évaluation
   - Modèles de sécurité
     - Modèles de contrôle d'accès discrétionnaires
     - Modèles de contrôle d'accès obligatoires
     - Modèles de contrôle d'usage
   - Implémentation

# Modèles de contrôle d'accès obligatoires

- Depuis 1975 on sait que les modèles de contrôle d'accès ne permettent pas de prendre en compte les applications piégées par un cheval de Troie (opérant par recopie de fichiers)
- Afin de prendre en compte cette possibilité, des modèles dits de contrôle des flux ont été définis parallèlement à la définition des modèles de contrôle d'accès
- Le premier modèle de contrôle des flux est le modèle de **Bell & LaPadula** (1975) (cf. sécurité multi-niveaux)
- D'autres modèles plus sûrs que le modèle de Bell & LaPadula ou répondant à des objectifs différents ont été proposés depuis
  → *non Interférence, Bell & LaPadula étendu, causalité, Biba,. . .*

# Modèles de contrôle d'accès obligatoires

- Appelés modèles **obligatoires** car le règlement de sécurité est simple et s'impose à tous les utilisateurs (il ne contient pas de règle adressant un utilisateur en particulier)
- Pour comprendre l'intérêt des modèles de contrôle des flux, il est nécessaire de revenir à la notion de sujet :
  - → *un sujet est un **utilisateur** ou un **processus** s'exécutant pour le compte d'un utilisateur*

# Modèles de contrôle d'accès obligatoires

- Tous les modèles de sécurité font implicitement les hypothèses suivantes sur les sujets :
  - un utilisateur peut potentiellement chercher à violer le règlement en tentant d'accéder à des objets pour lesquels il n'a pas d'autorisation
  - un utilisateur est supposé **de confiance**
    - ⇒ un utilisateur ne va pas délibérément divulguer de l'information à laquelle il a légalement accès
  - la plupart des processus ne sont pas de confiance car ils peuvent être potentiellement piégés et contenir un cheval de Troie
    - pb : un processus hérite des droits de l'utilisateur pour le compte duquel il s'exécute...
    - les seuls processus supposés de confiance sont ceux implantant les mécanismes de sécurité (les contrôles d'accès par exemple)

# Modèles de contrôle d'accès obligatoires

## Cheval de Troie

- Considérons un médecin qui utiliserait une application médicale piégée
  - ⇒ le cheval de Troie pourrait, **à l'insu du médecin**, transmettre le contenu d'un dossier médical par Internet à une personne non autorisée
- Les modèles de contrôle d'accès ne permettent pas d'empêcher de telles actions malveillantes
  - en effet le piège introduit dans l'application médical ne viole pas la réglementation de sécurité
    - le médecin (et donc l'application médicale) a le droit d'accéder à un dossier médical
    - le médecin (et donc l'application médicale) a le droit d'accéder à Internet (à un dictionnaire médical en ligne par exemple)

# Modèles de contrôle d'accès obligatoires

## Sécurité multi-niveaux

- Objectif de sécurité : **confidentialité**
- Système informatique représenté par le modèle Sujet-Objet
  - chaque sujet reçoit un niveau d 'habilitation
    - → Public, Confidentiel, Secret,...
  - chaque objet reçoit un niveau de classification
    - → Public, Confidentiel, Secret,...
- Règlement de sécurité (1 phrase)
  - un sujet $s$ est autorisé à **connaître** la valeur de l'objet $o$ si et seulement si $hab(s) \geq class(o)$
    - ⇒ un utilisateur **habilité** C aura le droit de connaître une information **classifiée** P ou C mais n'aura pas le droit de connaître une information **classifiée** S

# Modèles de contrôle d'accès obligatoires

## Sécurité multi-niveaux

- Modèle de Bell & LaPadula ⇒ les deux propriétés suivantes sont **nécessaires** (mais pas suffisantes) pour garantir le règlement de sécurité :

No Read-up un sujet $s$ ne peut **lire** le contenu d'un objet $o$ que si $hab(s) \geq class(o)$

⇒ un utilisateur habilité C a le droit de lire une information classifiée P ou C mais n'a pas le droit de lire une information classifiée S

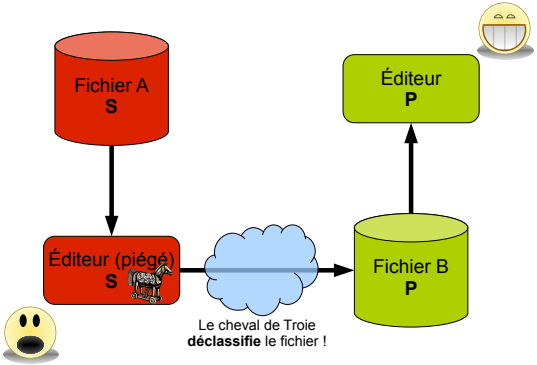
No Write-down un sujet $s$ ne peut **modifier** le contenu d'un objet $o$ que si $hab(s) \leq class(o)$

⇒ un utilisateur habilité C a le droit de modifier une information classifiée C ou S mais n'a pas le droit de modifier une information classifiée P

# Modèles de contrôle d'accès obligatoires

## Sécurité multi-niveaux

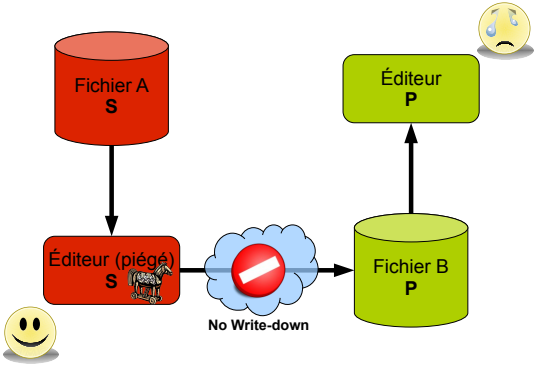
- Cheval de Troie



# Modèles de contrôle d'accès obligatoires

## Sécurité multi-niveaux

- Avec le modèle Bell & LaPadula



# Modèles de contrôle d'accès obligatoires

## Sécurité multi-niveaux

- Un utilisateur **habilité** à un niveau l peut initier une session à tout niveau **dominé** par le niveau l

  ex : un utilisateur habilité `Secret` se connecte au niveau `Secret` pour accéder à des informations secrètes mais se connecte au niveau `Public` pour modifier des informations publiques

  ⇒ permet de **déclassifier** certaines informations

# Modèles de contrôle d'accès obligatoires

- Avantages des modèles de contrôle de flux :
  - permettent de lutter contre les chevaux de Troie opérant par recopie de fichiers
  - ⇒ procurent un niveau de sécurité supérieur aux modèles de contrôle d'accès
- Inconvénients :
  - le règlement est très rigide
  - ⇒ modèles généralement réservés à des usages **militaires**
  - implémentation plus complexe

# Autres modèles

- Les deux conditions de modèle de Bell & LaPadula sont **nécessaires** mais **pas suffisantes**
  - les modèles de Non Interférence et de Causalité prennent en compte beaucoup plus de pièges que le modèle de Bell & LaPadula mais ils sont pratiquement impossibles à implémenter
  - le modèle de Biba est l'équivalent du modèle de Bell & LaPadula pour l'intégrité

⇒ Il est nécessaire de contrôler **tous** les flux d'information :
  - contrôle des canaux cachés
  - contrôle de l'inférence

# Contrôle des canaux cachés

- Un canal caché est un **canal de communication non prévu** mais pouvant potentiellement servir à communiquer de l'information de façon illégale
- Les canaux cachés résultent très souvent de particularités liées à l'**implémentation**

  ⇒ il est difficile d'en tenir compte dans un modèle théorique représentant un certain niveau d'abstraction

# Contrôle des canaux cachés

- Exemples de canaux cachés :
  - un processus piégé exécuté au niveau S peut accéder à une ressource quelconque pour transmettre des infos sensibles ; un sujet P peut observer ces accès et en déduire ces infos sensibles
  - un processus piégé exécuté au niveau S peut moduler son temps d'exécution pour transmettre des infos sensibles → canal caché temporel
  - on peut observer la consommation d'énergie d'un processus pour en déduire des infos sensibles

# Contrôle des canaux cachés

## Ils espionnent un ordinateur grâce aux ondes générées par. . .l'USB

- Fin 2013 → Edward Snowden → NSA → **COTTONMOUTH**
  - Article 01net du 01/09/2016
  - Un petit mouchard matériel qui vient se loger dans une prise USB et qui permet d'exfiltrer des données par ondes radio d'un ordinateur qui n'est pas connecté sur un réseau informatique
  - Alternative USBee : Le bus de données en USB s'appuie sur deux fils électriques dont la tension peut s'inverser. Si la tension s'inverse, alors c'est un «0», sinon c'est un «1».
  - Les chercheurs ont alors eu l'idée de n'envoyer que des zéros vers le matériel USB → la succession de changements de tension crée une belle onde électromagnétique.

# Contrôle des canaux cachés

## Ils espionnent un ordinateur grâce aux ondes générées par. . .l'USB (suite)

- Moduler la fréquence avec des zéros
  - Les chercheurs ont alors développé un algorithme qui permet de moduler la fréquence de cette onde en jouant sur la longueur des séries de «0» envoyées.
  - Répéter par exemple un bloc constitué d'une douzaine de «0» et d'une douzaine de «1» (111111111111000000000000) donnera une fréquence différente qu'une banale succession de «0» (000000000000000000000000).
  - La modulation de la fréquence permet ensuite de coder le message à exfiltrer. Pour capter le message, il suffit d'avoir une antenne et un logiciel d'analyse spectral tel que GNU Radio. Ce qui représente un investissement d'une trentaine de dollars.

# Contrôle des canaux cachés

## Ils espionnent un ordinateur grâce aux ondes générées par. . .l'USB (suite)

- Débit & utilisation
  - Les tests effectués ont permis de faire passer des messages d'une pièce à l'autre avec un débit compris entre 20 et 80 octets par seconde → regarder un film en HD est donc totalement hors de portée, mais c'est suffisant pour envoyer une clé de chiffrement en peu de temps.
  - COTTONMOUTH n'est pas encore à mettre au placard pour autant, car ce mouchard de la NSA est capable non seulement d'émettre, mais aussi de recevoir des données. Ce qui n'est pas le cas d'USBee → 2ème version ?

# Contrôle des canaux cachés

## Ils espionnent un ordinateur grâce aux ondes générées par. . .l'USB (fin)

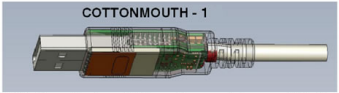
TOP SECRET//COMINT//REL TO USA, FVEY

**COTTONMOUTH-I**

ANT Product Data

**(TS//SI//REL)** COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.

**08/05/08**




**(TS//SI//REL)** CM-I will provide air-gap bridging, software persistence capability, "in-field" re-programmability, and covert communications with a host software implant over the USB. The RF link will enable command and data infiltration and exfiltration. CM-I will also communicate with Data Network Technologies (DNT) software (STRAITBIZARRE) through a covert channel implemented on the USB, using this communication channel to pass commands and data between hardware and software implants. CM-I will be a GENIE-compliant implant based on CHIMNEYPOOL.

**(TS//SI//REL)** CM-I conceals digital components (TRINITY), USB 1.1 FS hub, switches, and HOWLERMONKEY (HM) RF Transceiver within the USB Series-A cable connector. MOCCASIN is the version permanently connected to a USB keyboard. Another version can be made with an unmodified USB connector at the other end. CM-I has the ability to communicate to other CM devices over the RF link using an over-the-air protocol called SPECULATION.

COTTONMOUTH CONOP

# Contrôle des canaux cachés

## Câble USB O.MG

- Un "simple" câble USB... (⇨)
  - ... mais avec un implant
  - dispo en version *basic* ($119.99) ou en version *elite* ($179.99)

### O.MG CABLE FEATURES

**Easy WiFi Control**
Full control with your web browser. Desktop or mobile.

**Keystroke Injection**
Instant DuckyScript payloads. No compiling, just click run!

**Lots of Payload slots**
Basic model comes with 8 slots. Elite has extra storage allowing up to 200 slots!

**Global Keymaps**
With 192 keymaps already built in, you can target machines across the world.

**Built in IDE**
The WebUI not only provides 100% of the controls, but also gives you helpful feedback to catch syntax errors while rapidly building payloads.

**Mobile Payloads**
Cables with a USB-C active end, or Directional C to C, can automatically transmit to mobile devices with a USB-C connector. Connect just the active end!

**Stealth**
The implant stays dormant until a payload is deployed. No logs. No detections. The cable behaves just like a normal USB 2.0 cable. (5v charging, 480mps data transfer)

**Hardware Keylogger**
Plus & Elite contain a passive hardware keylogger designed for FullSpeed USB keyboards with detachable cables. Store up to 650,000 keystrokes. For tested keyboards & more info go here.

**Covert Exfil**
Elite models: send data from the host back into the O.MG Cable over a covert channel.

**Air Gap Comms**
Elite models: setup a bidirectional tunnel from Target Host > O.MG > Control Machine.

**Networked C2**
Elite models: Manage your O.MG Cables with a network attached C2 server.

**Self-Destruct**
Make your legal team happy by ensuring sensitive payloads & loot are gone, and the O.MG Cable is fully inert. (recoverable with O.MG Programmer)

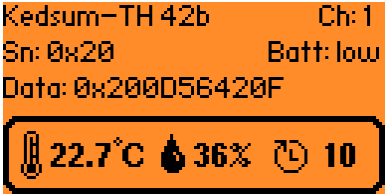
**Geo-Fencing**
Trigger payloads or other actions based on location. Keep your tool from falling out of scope! Ex: self-destruct if someone takes the O.MG Cable home.

**WiFi Triggers**
Trigger payloads at long range with a single beacon.

# Contrôle des canaux cachés

## Hack RF ⇝ Flipper Zero

- Le Flipper Zero se présente comme le couteau suisse des geeks, des hackers et des testeurs, avec l'ambition d'**exposer les vulnérabilités informatiques**. Une sorte de « rayon X pour la cybersécurité ». Son code est open-source, ce qui permet à quiconque de l'examiner.



# Contrôle des canaux cachés

## Hack RF ⇝ SDR (Software Defined Radio)

- SDR = radio logicielle ⇝ boîtier permettant de recevoir et d'envoyer des données radio depuis un ordinateur
  - HackRF One
  - Adalm-Pluto

# Contrôle des canaux cachés

## Et encore d'autres infos...

- Article *"Comment la NSA peut bidouiller votre iPhone, votre wifi, votre PC, votre écran..."* (➪)

- En IoT, comment usurper l'identité d'un capteur RF 433MHz pour envoyer de fausses informations au récepteur
  - tutoriel utilisant, entre autres, le Flipper Zero (➪)
  - stage BUT2 R&T 2024 (➪)

# Contrôle de l'inférence

- Un utilisateur peut **déduire** des informations sensibles en utilisant des informations qu'il est autorisé à connaître

  ex : un médecin est tenu au secret médical

  pourtant il délivre une ordonnance qui peut être aisément lue par des tiers (pharmacien, famille, clients dans la pharmacie,...)

  → la lecture de cette ordonnance peut révéler, par déduction, la nature de la maladie du patient

⇒ Problème difficile à résoudre complètement dans la mesure où il est difficile de recenser toutes les connaissances possédées par l'utilisateur

# Contrôle de l'inférence

- Pour déduire (ou inférer) des informations sensibles un utilisateur peut utiliser :
  - des informations présentes dans le système informatique et auxquelles il a légalement accès
    - ⇒ contrôle de l'inférence possible
  - des connaissances générales non représentées dans le système informatique
    - ⇒ contrôle de l'inférence difficile

# Plan du cours

1. Introduction à la Sécurité Informatique
   - Présentation
   - Critères d'évaluation
   - Modèles de sécurité
     - Modèles de contrôle d'accès discrétionnaires
     - Modèles de contrôle d'accès obligatoires
     - Modèles de contrôle d'usage
   - Implémentation

# Modèles de contrôle d'usage

- L'objectif du contrôle d'usage est de contrôler non seulement l'accès au document mais également l'**usage qui en est fait**
  - ex : initialement, le contrôle d'usage visait principalement (mais pas seulement) à contrôler la recopie des fichiers
- Idée[13] : contrôle d'usage ≡ obligations

13. dixit F. & N. Cuppens

# Modèles de contrôle d'usage

- Les modèles de contrôle d'usage dont la première version est le modèle UCON [14] permettent d'énoncer des règles de sécurité qu'il est difficile d'implanter avec des mécanismes classiques de contrôle d'accès :
  - → l'acheteur de ce morceau de musique ne pourra l'écouter que 10 fois au plus
  - → l'utilisateur de ce document ne pourra effectuer qu'une seule copie de sauvegarde
  - → le médecin aura l'obligation de mettre à jour le dossier médical du patient avant de pouvoir imprimer l'ordonnance

14. Park, Sandhu (2004)

# Modèles de contrôle d'usage

- La mise en œuvre d'un règlement de contrôle d'usage se fait généralement en utilisant des techniques de DRM

  NB : les DRM se caractérisent par le fait que les contrôles de sécurité s'effectuent non pas du coté du serveur mais **du coté du client**

- La partie du logiciel client qui effectue les contrôles de sécurité (noyau de sécurité) **doit être de confiance**

  → **par définition**, le noyau de sécurité ne peut être contourné et est dépourvu de failles, vulnérabilités, cheval de Troie,...

# Modèles de contrôle d'usage

- Applications des DRM :
  - Initialement orientés vers la protection des droits d'auteurs et des intérêts commerciaux des distributeurs de contenus multimédia (films, musique,...)
  - Maintenant, les DRM sont de plus en plus utilisés dans des applications dont l'objectif est de contrôler la distribution de contenus sensibles (*Entreprise-DRM*)

    ex : FLUOR, projet ANR-SESUR (2008-2011)
    *convergence du contrôle de **FL**ux et d'**U**sage dans les **OR**ganisations*

# Modèles de contrôle d'usage

## OrBAC

- Retour sur le modèle OrBAC :
  - → contrôle d'accès
  - → contrôle d'usage
- La politique de sécurité permet :
  - permissions
  - interdictions
  - obligations
  - règles contextuelles

https://motorbac.sourceforge.net/

# Plan du cours

1. Introduction à la Sécurité Informatique
   - Présentation
   - Critères d'évaluation
   - Modèles de sécurité
     - Modèles de contrôle d'accès discrétionnaires
     - Modèles de contrôle d'accès obligatoires
     - Modèles de contrôle d'usage
   - Implémentation

# Mise en œuvre des modèles

- Approche dite du **noyau de sécurité** (ou TCB [15])
  NB : côté serveur ou côté client (cf. DRM)
- Le noyau est supposé fiable (*trusted*), i.e. dépourvu de :
  - failles
  - vulnérabilités
  - pièges
  - ...

⇒ Idéalement il doit donc être le plus petit possible

15. Trusted Computing Base

# Mise en œuvre des modèles

- Les fonctions du noyau de sécurité sont :
  - → authentification des utilisateurs
  - → contrôle des accès (ACL, No Read-up, No Write-down,...)
  - → chiffrement & déchiffrement de données
  - → ...

⇒ Ces mécanismes de sécurité doivent garantir le règlement de sécurité (***policy enforcement***)

# Plan du cours

1 Introduction à la Sécurité Informatique

2 Gestion des Risques
- Introduction
- Vocabulaire
- ISO 27005 Risk Manager
- Bilan

3 Droit & Numérique

4 Conclusion

# Gestion des risques liés à la sécurité de l'information

- L'enjeu : atteindre ses objectifs (de sécurité) sur la base de décisions rationnelles
  - *Née dans le domaine financier dans les années 50 et étendue à de nombreux autres domaines tels que la gestion de projet, la sécurité des personnes, la sûreté de fonctionnement, le marketing, l'environnement ou encore la sécurité de l'information, la* ***gestion des risques*** *a toujours eu pour objectif de rationaliser des situations pour aider à une prise de décision éclairée.*
  - *Les choix effectués par les décideurs peuvent ainsi être faits au regard des éléments fournis par les* ***risk managers****. Et ces choix peuvent autant guider l'organisme vers l'atteinte de ses objectifs que faire évoluer sa stratégie.*

# Gestion des risques liés à la sécurité de l'information

- Gestion des risques par la pratique
  - → méthodologie empirique
  - → sources de désaccords

- Gestion des risques par la théorie
  - → formalisme & organisation
  - → différentes normes & méthodes
    - EBIOS 2010
    - suite ISO/CEI 27000
      *notamment ISO/CEI 27005:2011 Risk Manager*
  - → processus d'audit & de certification

# Gestion des risques liés à la sécurité de l'information

- Des pratiques différentes mais des principes communs
  - le risque est décrit par un événement, ses conséquences et sa vraisemblance
  - le processus de gestion des risques comprend une étude du contexte, l'appréciation des risques, le traitement des risques, la validation du traitement des risques, la communication relative aux risques, le contrôle, dans une amélioration continue
- Le besoin d'une méthode
  - disposer d'éléments de langage communs
  - disposer d'une démarche claire et structurée à respecter
  - se baser sur un référentiel validé par l'expérience
  - s'assurer d'une exhaustivité des actions à entreprendre
  - réutiliser la même approche en amélioration continue et sur d'autres périmètres...

# Gestion des risques liés à la sécurité de l'information

## Suite ISO/CEI 2700x

- 1ère norme de gestion des risques de la **Sécurité des Systèmes d'Information** (SSI)
  - standard international lié aux Systèmes de Management de la Sécurité de l'Information (SMSI)
- ISO 2700x ≡ famille des standards SMSI

ISO/CEI 27000 introduction et vue globale de la famille des normes, ainsi qu'un glossaire des termes communs (mai 2009)

ISO/CEI 27001 norme de certification des SMSI (publiée en 2005)

ISO/CEI 27002 guide des bonnes pratiques en SMSI (dernière révision en 2005)
*nb : précédemment connu sous le nom de ISO/CEI 17799, et avant BS 7799 Partie 1*

ISO/CEI 27005 norme de gestion de risques liés à la sécurité de l'information (publiée le 4 juin 2008, révisée en novembre 2022) → ***Risk Manager***

ISO/CEI 27006 guide de processus de certification et d'enregistrement (publié le 13 février 2007)

...

# Gestion des risques liés à la sécurité de l'information

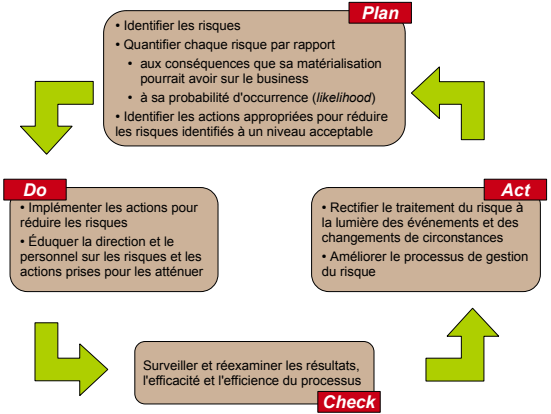
## Suite ISO/CEI 2700x

- Objectifs de l'ISO/CEI 27005:2011
  - la norme ISO 27005 explique en détail comment conduire l'appréciation des risques et le traitement des risques, dans le cadre de la sécurité de l'information
  - l'ISO 27005 propose une méthodologie de gestion des risques en matière d'information dans l'entreprise conforme à la norme ISO/CEI 27001
    - → *elle a donc pour but d'aider à mettre en œuvre l'ISO/CEI 27001 (certification d'un SMSI)*
  - la norme ISO 27005 peut néanmoins être utilisée de manière autonome dans différentes situations
  - elle applique à la gestion de risques le cycle d'amélioration continue PDCA (roue de Deming)

| | |
|---|---|
| PLAN | *identification des risques, évaluation des risques et définition des actions de réduction des risques* |
| DO | *exécution de ces actions* |
| CHECK | *contrôle du résultat* |
| ACT | *modification du traitement des risques selon les résultats* |

# Gestion des risques liés à la sécurité de l'information

## Suite ISO/CEI 2700x



# Gestion des risques liés à la sécurité de l'information

## EBIOS

- **E**xpression des **B**esoins et **I**dentification des **O**bjectifs de **S**écurité
- Méthode de gestion des risques élaborée par l'ANSSI [16]
  - marque déposée par le Secrétariat général de la défense et de la sécurité nationale
  - ⇒ norme franco-française...
- Màj majeure en 2018 ⇝ EBIOS RM (**Risk Manager**)
  - → harmonisation du vocabulaire vis-à-vis des normes ISO 27001, ISO 27005,...
- Origine : rédaction de FEROS

  nb : une **f**iche d'**e**xpression **r**ationnelle des **o**bjectifs de **s**écurité est requise dans le dossier de sécurité de tout système traitant des informations classifiées

16. **A**gence **N**ationale de la **S**écurité des **S**ystèmes d'**I**nformation
http://www.ssi.gouv.fr/

# Gestion des risques liés à la sécurité de l'information

## EBIOS

- Objectifs
  - fournir une base commune de concepts et d'activités pragmatiques à toute personne impliquée dans la gestion des risques, notamment dans la sécurité de l'information
  - satisfaire les exigences de gestion des risques d'un système de management de la sécurité de l'information (ISO 27001)
  - définir une démarche méthodologique complète en cohérence et en conformité avec les normes internationales de gestion des risques (ISO 31000, ISO 27005,...)
  - établir une référence pour la certification de compétences relatives à la gestion des risques
- Domaine d'application
  - secteur public / secteur privé
  - petites structures (PME, collectivités territoriales,...) / grandes structures (ministère, organisation internationale, entreprise multinationale,...)
  - systèmes en cours d'élaboration / systèmes existants

# Gestion des risques liés à la sécurité de l'information

## EBIOS

- Positionnement par rapport aux normes
  - la méthode EBIOS respecte les exigences de l'ISO 27001 (norme d'exigences pour un SMSI)
  - elle peut exploiter les mesures de sécurité décrites dans la norme ISO 27002 (catalogue de bonnes pratiques)
  - elle est compatible avec l'ISO 31000 (cadre général pour toutes les normes sectorielles de gestion des risques)
  - c'est une méthode pour mettre en œuvre le cadre défini dans l'ISO 27005 (cadre spécifique pour gérer les risques de sécurité de l'information)
  - elle permet d'exploiter l'ISO 15408 (critères communs)

# Gestion des risques liés à la sécurité de l'information

## EBIOS vs. ISO 27005 (à l'origine)

- EBIOS 2010
  - \+ gestion des risques sur le SI dans sa globalité (y compris locaux, personnes,...)
  - \- norme franco-française
  - \- contexte (trop) complet dès le départ
- ISO 27005:2011
  - \+ norme internationale
  - \+ processus de certification
  - \+ démarche incrémentale
  - \- uniquement le SI

# Gestion des risques liés à la sécurité de l'information

## EBIOS vs. ISO 27005 (actuellement, cf. Club EBIOS)

- La méthode EBIOS Risk Manager (EBIOS RM) a été mise à jour en 2024, et l'ISO 27005 en novembre 2022. Ces mises à jour sont majeures, et recentrent la gestion des risques autour des métiers, de la cybersécurité et de la protection de la vie privée.
- ISO 27005
  - Elle décrit les grandes lignes d'une gestion des risques dans un contexte cyber : définition du contexte d'analyse, identification et évaluation des risques encourus, possibilités de traitement ou d'acceptation de ces derniers. Elle introduit un processus d'appréciation des risques conforme à l'ISO 31000, sans pour autant proposer de méthode au sens strict.
  - Elle est construite en cohérence forte avec le couple de normes ISO 27001/27002 et reprenant le vocabulaire principalement défini dans l'ISO 27000, la norme ISO 27005 utilise comme nombre de systèmes de management la logique d'itération et d'amélioration continue.

# Gestion des risques liés à la sécurité de l'information

## EBIOS vs. ISO 27005 (actuellement, cf. Club EBIOS)

- EBIOS RM
  - La méthode EBIOS est une méthode d'analyse et d'évaluation des risques qui a aujourd'hui plus de 25 ans. Elle a été définie par l'ANSSI, avec le soutien du Club EBIOS. Elle décrit dans le détail la procédure à suivre pour dérouler une analyse des risques (démarche et bonnes pratiques).
  - La dernière version de la méthode a permis de mettre l'accent sur l'agilité, et de substituer à la recherche d'exhaustivité une volonté de représentativité : l'idée n'est plus d'identifier tous les risques, mais uniquement les plus significatifs dans une approche permettant représenter aussi largement que possible l'espace des risques. Elle se veut aussi plus flexible en fonction de la maturité et de l'objectif fixé.
  - EBIOS RM n'est pas une norme, mais une méthode. Elle décrit des techniques pratiques pour permettre à ses utilisateurs d'appliquer le modèle décrit dans l'ISO 27005. Dans les faits, lors d'une démarche de mise en œuvre d'un SMSI implémentant la famille de normes ISO 2700x, se pose immédiatement l'obligation d'identifier si oui ou non la méthode d'analyse de risques sélectionnée est bien compatible avec le cadre normatif choisi. EBIOS RM apporte une solution.

# Gestion des risques liés à la sécurité de l'information

## Objectif du cours

- Vous sensibiliser à la gestion des risques dans les systèmes d'information
  - ▷ adopter une démarche SSI **dès la phase de conception** du SI / des applications
  - ▷ comprendre les attentes des experts **lorsque vous serez audités**
  - ▷ transformer cet "effort" en "**avantage concurrentiel**" $\rightsquigarrow$ projets, clients, etc.

$\Rightarrow$ Présentation des principes généraux de la gestion des risques dans la SSI selon la norme ISO 27005

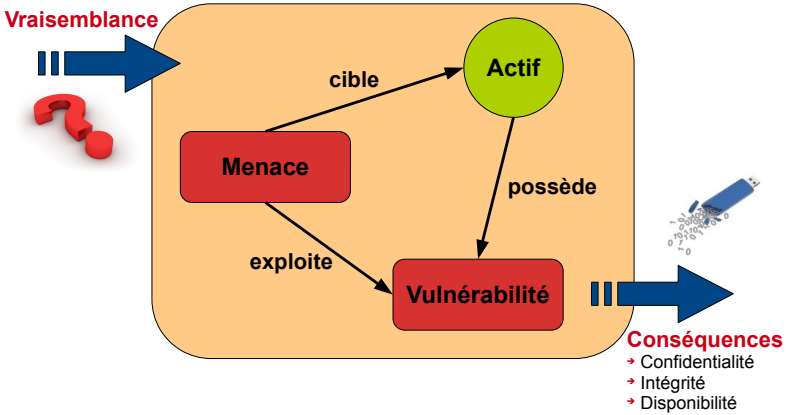
# Risque

- Concept multidisciplinaire
  - assurance
    - → concept fondamental
  - droit
    - → **événement éventuel**, **incertain**, dont la réalisation ne dépend pas exclusivement de la volonté des parties et pouvant causer des dommages
  - écologie
    - → **probabilité** de survenance d'un danger
- 2 notions fondamentales
  - incertitude
  - dommage

# Risque

- Risque informatique
  - → **probabilité plus ou moins grande** de voir une menace informatique se transformer en événement réel entraînant une perte
- Risque de sécurité de l'information
  - → **possibilité** (**éventualité**) qu'une menace donnée exploite une ou plusieurs vulnérabilités d'un actif ou d'un groupe d'actifs, causant ainsi des **préjudices** à l'organisme
    - il s'estime en termes de combinaison de la **vraisemblance** (probabilité d'occurrence) et de ses **conséquences**

# Risque en sécurité de l'information



# Plan du cours

- Modèles de contrôle d'accès discrétionnaires
- Modèles de contrôle d'accès obligatoires
- Modèles de contrôle d'usage

2 Gestion des Risques
- Introduction
- Vocabulaire
- ISO 27005 Risk Manager
- Bilan

# Vocabulaire

## Importance de la communication

- Dans la mise en œuvre d'un processus de gestion du risque, **la communication joue un rôle primordial**
- Le vocabulaire employé dans le cadre de ce processus doit être clairement défini
- C'est un langage commun pour l'ensemble des participants aux études

# Vocabulaire

## Quelques définitions

- Actif
  - ▷ actif primordial / valeur métier
    - ⇝ critères de sécurité
    - ⇝ besoins de sécurité
  - ▷ actif support
    - ⇝ vulnérabilités
- Scénario de menace
  - ⇝ source de risque
  - ⇝ mode opératoire
- Événement redouté
  - ⇝ impact
- Risque

# Vocabulaire

## Actif

- Toute ressource qui a de la valeur pour l'organisme et qui est nécessaire à la réalisation de ses objectifs
- Il en existe de deux types :
  - actifs primordiaux / valeurs métiers (biens essentiels, *primary assets*)
  - actifs support (biens supports, *supporting assets*)

# Vocabulaire

## Actif primordial

- Il s'agit d'un actif qui peut être de deux types :
  - informations
  - processus, fonctions, activité
- Les actifs primordiaux constituent la valeur ajoutée du système d'information pour l'organisme
- **Un actif primordial n'est pas porteur de vulnérabilité**

Ex Gestion des factures, liste des clients, liste des élèves

# Vocabulaire

## Critère de sécurité

- Caractéristique d'un actif primordial / d'une valeur métier permettant d'apprécier ses différents besoins de sécurité
  - confidentialité
  - intégrité
  - disponibilité
  - traçabilité

# Vocabulaire

## Besoin de sécurité

- Définition précise et non ambiguë du niveau d'exigences opérationnelles relatives à un actif primordial pour un critère de sécurité donné (confidentialité, intégrité, disponibilité,...)
- Exemples
  - doit être disponible dans la journée
  - ne doit être connu que du groupe projet

# Vocabulaire

## Actif support

- C'est un actif sur lequel reposent des actifs primordiaux
- **Les actifs supports sont porteurs de vulnérabilités**
- Exemples
  - service du personnel
  - salle machine
  - utilisateur, administrateur
  - réseau d'hébergement
  - ordinateur portable

# Vocabulaire

## Vulnérabilité

- Caractéristique d'un **actif support** qui peut constituer une faiblesse ou une faille au regard de la sécurité des systèmes d'information
- Exemples
  - absence de sensibilisation des utilisateurs à la sécurité
  - crédulité du personnel
  - faille de sécurité dans le logiciel Internet Explorer
  - serveur dépendant de l'électricité

# Vocabulaire

## Actifs supports vs. actifs primordiaux

- Les actifs primordiaux constituent la valeur ajoutée du système d'information pour l'organisme
- Ils reposent sur les actifs supports qui, potentiellement, sont porteurs de vulnérabilités
- Dans une analyse de risque, pendant la phase d'inventaire, il est nécessaire de réaliser un tableau qui croise les actifs supports et les actifs primordiaux

# Vocabulaire

## Source de risque

- Chose ou personne à l'origine de menaces
- Elle peut être caractérisée par son type (humain ou environnemental), par sa cause (accidentelle ou délibérée) et selon le cas par ses ressources disponibles, son expertise, sa motivation, etc.
- Exemples
  - virus
  - utilisateurs
  - ancien membre du personnel ayant peu de compétences techniques et peu de temps mais susceptible d'avoir une forte motivation
  - pirate avec de fortes compétences techniques, bien équipé et une forte motivation liée à l'argent qu'il peut gagner

# Vocabulaire

## Menace

- Moyen type utilisé par une source de menace
- Exemples
  - vol de supports ou de documents
  - piégeage du logiciel
  - atteinte à la disponibilité du personnel
  - écoute passive
  - crue, incendie,...

# Vocabulaire

## Impact

- Conséquence sur l'organisme de la réalisation d'une menace
- Exemples
  - perte d'image de marque vis-à-vis de la clientèle
  - perte financière à hauteur de 10% du chiffre d'affaires
  - infraction aux lois et aux règlements donnant lieu à des poursuites judiciaires à l'encontre du Directeur (le responsable des traitements)

# Vocabulaire

## Risque

- Utilisez les éléments précédents pour définir le risque...

# Vocabulaire

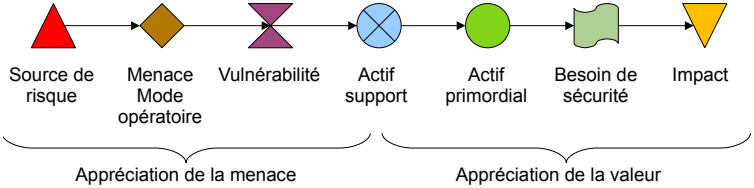
## Les 7 composantes du risque

- Il est d'usage de décomposer le risque en 7 composantes
  - la source du risque
  - la menace ou le mode opératoire
  - la vulnérabilité
  - l'actif support
  - l'actif primordial ou la valeur métier
  - le besoin de sécurité
  - l'impact

# Vocabulaire

## Les 7 composantes du risque

- Il est d'usage de décomposer le risque en 7 composantes
  - ▷ risque =

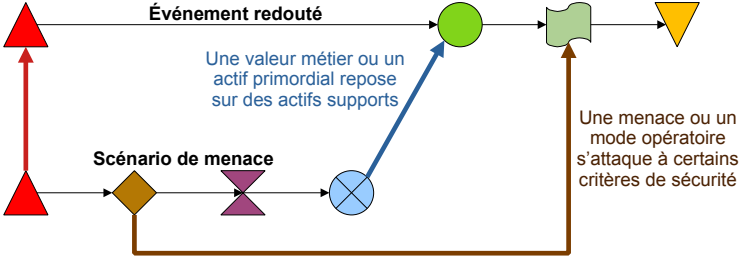



NB source : Fred Kustyan, Ministère de la Transition Écologique (MTE), France

# Vocabulaire

## Les 7 composantes du risque

- Croisement des événements redoutés et des scénarios de menace



# Plan du cours

- Modèles de contrôle d'accès discrétionnaires
- Modèles de contrôle d'accès obligatoires
- Modèles de contrôle d'usage

2 Gestion des Risques
- Introduction
- Vocabulaire
- ISO 27005 Risk Manager
- Bilan

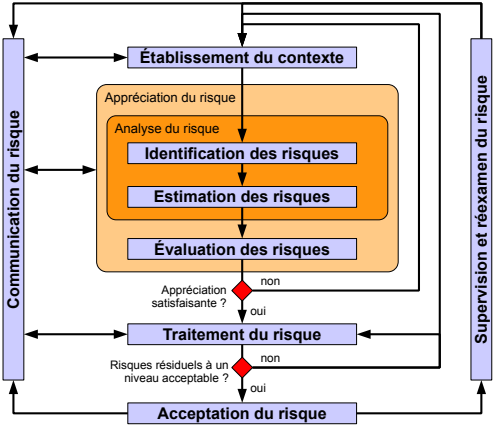
# Liens

- Sources de documentation
  - normes **ISO** (International Organization for Standardization)
    http://www.iso.org/
  - méthode **EBIOS**
    http://www.ssi.gouv.fr/
  - ~~documents **HSC** (Hervé Schauer Consultants)~~
    http://www.hsc.fr/
  - ➜ documents **HS2** (Hervé Schauer Sécurité)
    https://www.hs2.fr/

# Processus de gestion du risque

- Approche itérative
  - Établissement du contexte
  - Appréciation du risque
    - → Identification des risques
    - → Estimation des risques
    - → Évaluation des risques
  - Traitement du risque
  - Acceptation du risque
- La méthode définit aussi 2 tâches à mener en parallèle
  - Communication du risque
  - Supervision et réexamen du risque

# Processus de gestion du risque



# Processus de gestion du risque

- Une telle approche itérative...
  - améliore la finesse de l'analyse à chaque itération
  - fournit une bonne répartition entre le temps et l'effort fourni pour identifier les mesures de sécurité
  - permet de traiter les risques en fonction des ressources et des moyens qui sont disponibles
  - facilite les liens entre les risques et les conséquences sur les processus métier
  - permet d'avancer lorsque les interlocuteurs sont absents ou les livrables incomplets
  - facilite la gestion des susceptibilités et des aspects politiques (...) entre les interviewés, les propriétaires d'actifs et de processus métier
  - tend progressivement vers une maîtrise des risques de haut niveau et qui soit conforme aux besoins de l'organisme

# Terminologie

- Norme en anglais, traduite en français
  - risk analysis ⇝ analyse du risque
  - risk evaluation ⇝ évaluation du risque
  - risk estimation ⇝ estimation du risque
  - risk assessment ⇝ appréciation du risque

⚠ **Ne pas confondre**

- analyse du risque ≡ quels risques ? + quelles conséquences ? + scénarios
- appréciation du risque ≡ faut-il traiter le risque ?

# Présentation de la méthode

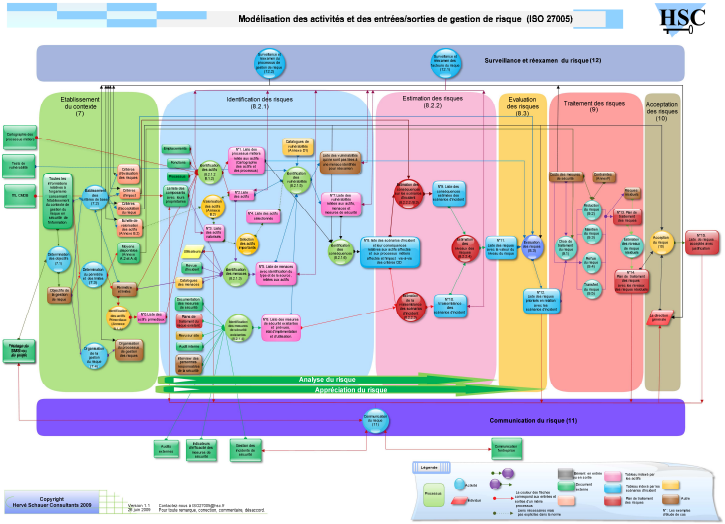
- L'ISO 27005 est une norme "non directive"
  - explicite comment faire (le processus général)
  - tout en laissant l'entière liberté de comment on exécute chaque étape

- L'ISO 27005 peut couvrir des situations très diverses
  - avantage d'une norme "consensuelle"
  - inconvénient : la 1ère itération peut être "plus longue"
    - → définition des différents critères,
    - → des règles,
    - → des formules de calcul,
    - → etc.

# Présentation de la méthode

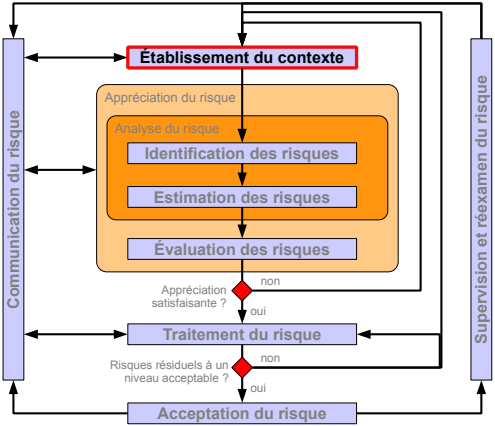
- Une bonne présentation des principes essentiels de la méthode ISO 27005
  → **Méthode de management des risques ISO 27005**
  Hervé Schauer Consultants
  Paris, 15 avril 2010

  - schéma modélisant chaque activité et sous-activité de la méthode proposée par la norme ISO 27005
  - cas d'étude illustrant les différentes étapes de la méthode
  - toutes les explications indiquent les références aux sections de la norme (version ISO 27005:2008)


Modélisation des activités et des entrées/sorties de gestion de risque (ISO 27005)
HSC
Surveillance et réexamen du risque (12)
Etablissement du contexte (7)
Identification des risques (8.2.1)
Estimation des risques (8.2.2)
Evaluation des risques (8.3)
Traitement des risques (9)
Acceptation des risques (10)
Analyse du risque
Appréciation du risque
Communication du risque (11)
Copyright
Hervé Schauer Consultants 2005

# Étape 1 : Établissement du contexte

## Processus



# Étape 1 : Établissement du contexte

## Objectifs

- Définition du périmètre de l'étude
  - définit "ce sur quoi va porter l'analyse de risques" et "comment on va mesurer"
  - étape d'identification $\rightsquigarrow$ actifs primordiaux, actifs en support
  - corrections possible aux étapes ultérieures
  - le contexte peut concerner un ensemble très large ou très resserré $\rightsquigarrow$ tout un système d'information ou juste un sous-ensemble du SI
    - cycle PDCA $\rightsquigarrow$ élargissement, intégration de nouveaux actifs

# Étape 1 : Établissement du contexte

## Définition des critères et échelles

- Critères de base
  - ▷ **critères d'impact** (seuil de prise en compte)
    - l'impact est-il assez important pour que le risque doive être pris en compte dans l'analyse de risques ?
    - → bas niveau : vis-à-vis de l'actif ⇝ impact de la perte ou de l'atteinte d'un critère de sécurité (**C**onfidentialité, **I**ntégrite, **D**isponibilité)
    - → haut niveau : vis-à-vis de l'organisme, du processus métier, du projet ⇝ échelle de mesure ou critère d'estimation des conséquences (financières, délais, image, etc.)
  - ▷ **critères d'évaluation des risques** (seuil de traitement)
    - le niveau de risque est-il assez élevé pour que le risque nécessite d'être traité ?
  - ▷ **critères d'acceptation des risques** (seuil d'acceptation)
    - le niveau de risque résiduel est-il acceptable par la direction ?

# Étape 1 : Établissement du contexte

## Définition des critères et échelles

- Pas d'échelles standard $\rightsquigarrow$ ce doit être "pertinent" pour l'entreprise
- Les critères peuvent changer d'une itération à l'autre
  - cycle PDCA $\rightsquigarrow$ adaptation à de nouveaux besoins
- D'autres échelles peuvent être utiles lors de l'analyse de risques
  - pas explicitement imposées lors de l'établissement du contexte
  - ex : échelle (ou critères) de valorisation des actifs
  - ex : échelles d'estimation...
    - des menaces (vraisemblance)
    - des vulnérabilités (difficulté d'exploitation)
    - d'appréciation de la vraisemblance des scénarios d'incidents

# Étape 1 : Établissement du contexte

## Définition des critères et échelles

- Étude de cas
  - critères d'impact CID go to example
    - impact sur un actif ou besoin sur cet actif
  - échelle de mesure des conséquences go to example
    - conséquences de l'occurrence d'un scénario d'incident sur l'organisme, le métier, le projet
  - critères d'évaluation des risques go to example
    - utilisés par le RSSI ou le gestionnaire de risques SI
  - critères d'acceptation des risques go to example
    - validés par la direction et utilisés par la direction

# Étape 1 : Établissement du contexte

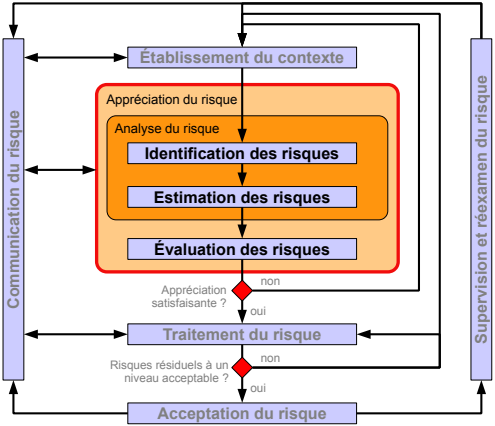
## Synthèse

- Définir...
  - ▷ l'objectif du processus de gestion des risques (vision claire de ce sur quoi va porter la gestion des risques)
  - ▷ sa portée ainsi que ses limites ⇒ **périmètre**
  - ▷ l'environnement dans lequel il s'inscrit (organisation, contraintes, etc.)

- Organiser et diriger la gestion des risques
  - ⇝ intervenants, rôles, chemins de décision, etc.

# Étape 2 : Appréciation du risque

## Processus



# Étape 2 : Appréciation du risque

## Objectifs

- Identifier et évaluer
  - les actifs associés au contexte et leur propriétaire
  - les menaces qui pèsent sur ces actifs
  - les mesures de sécurité existantes
  - les vulnérabilités possibles
  - les conséquences de ces dernières
- Évaluer ≡ donner une note

⇒ Débouche sur l'élaboration de scénarii d'incidents

# Étape 2 : Appréciation du risque

## Identification des risques

- Que peut-il arriver aux actifs qui composent le contexte ?
  - ⇝ réunions, brainstorming
  - ⇝ réflexions individuelles
  - ⇝ approches scénarisées
  - ⇝ entretiens
  - ⇝ lectures
  - ⇝ expériences vécues, ...

# Étape 2 : Appréciation du risque

## Identification des risques

- Critères d'évaluation pour les actifs, menaces, conséquences
  - qualitatifs
  - quantitatifs
  - financiers
  - etc.
- Les critères peuvent être quelconques
- Objectif = obtenir une note pour les différents éléments

# Étape 2 : Appréciation du risque

## Identification des risques : quels actifs ?

- Identification des actifs ⇒ **cartographie des actifs**
  - ▷ actifs primordiaux [17]
    - processus métier, activités métier
    - information
  - ▷ actifs en support [18]
    - cadre organisationnel, site, personnel
    - réseau, logiciels, matériel, etc.
- Pour info : Annexe B de l'ISO 27005 + ISO 27002 + ISO 15408 (CC)

17. EBIOS ⇝ biens essentiels
18. EBIOS ⇝ biens support

# Étape 2 : Appréciation du risque

## Identification des risques : quels actifs ?

- Étude de cas
  - ▷ liste des actifs primordiaux go to example
  - ▷ liste des processus métier reliés aux actifs go to example
    - ⇝ quels sont les actifs en support nécessaires ?
  - ▷ liste des complète actifs (primordiaux et support) go to example

# Étape 2 : Appréciation du risque

## Identification des risques : quelle est la valeur de ces actifs ?

- **Valorisation des actifs**
  - ▷ il est important de déterminer la valeur de chaque actif go to example
  - ⇒ l'un actif doit-il être traité ou pas dans l'analyse de risques ? (seuil) go to example

| Échelle de valorisation des actifs | | |
|---|---|---|
| **Valeur** | | **Signification** |
| 1 | Faible | Actif facilement remplaçable<br>Coût d'achat faible<br>Coût de maintenance faible<br>Ne nécessite pas de compétences particulières |
| 2 | Moyen | Actif remplaçable dans la journée<br>Coût d'achat moyen<br>Coût de maintenance moyen<br>Nécessite des connaissances de base |
| 3 | Élevé | Actif remplaçable dans la semaine<br>Coût d'achat élevé<br>Coût de maintenance élevé<br>Nécessite des connaissances techniques particulières |
| 4 | Très élevé | Actif remplaçable dans le mois<br>Coût d'achat très élevé<br>Coût de maintenance très élevé<br>Nécessite des connaissances spécifiques |

# Étape 2 : Appréciation du risque

## Identification des risques : quelles menaces pèsent sur ces actifs ?

- **Identification des menaces**
  - une menace est susceptible d'endommager les actifs tels que des informations, des processus et des systèmes et, par conséquent, des organismes
  - les menaces peuvent être d'origine naturelle ou humaine et peuvent être accidentelles ou délibérées $\rightsquigarrow$ il convient d'identifier les sources de menace à la fois accidentelles et délibérées
  - une menace peut survenir de l'intérieur ou de l'extérieur de l'organisme
  - il convient d'identifier les menaces de manière générique et par type
    - ex : des actions non autorisées, des dommages physiques, des défaillances techniques
  - puis, lorsque cela est pertinent, des menaces individuelles particulières peuvent être identifiées au sein d'une classe générique

# Étape 2 : Appréciation du risque

## Identification des risques : quelles menaces pèsent sur ces actifs ?

- **Identification des menaces** (suite)
  - ▷ certaines menaces peuvent affecter plus d'un actif
    - ⇝ dans ce cas, elles peuvent avoir différentes conséquences selon l'actif affecté
  - ▷ comment identifier les menaces ?
    - référentiels : Annexe C de l'ISO 27005 + ISO 27002 + ISO 15408 (CC)
    - entretiens : propriétaires/utilisateurs d'actifs, RH, experts, etc.
    - expérience : incidents survenus, appréciation de menaces antérieures, etc.
    - veille techno : organismes dédiés, compagnies d'assurance, etc.

NB seulement sur les actifs en support go to example

⇒ **Aucune menace n'est négligée, même une menace imprévue** !

# Étape 2 : Appréciation du risque

## Identification des risques : quelles vulnérabilités de ces actifs ?

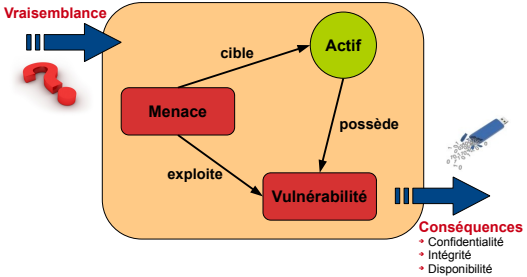
- Objectif = identifier les vulnérabilités susceptibles d'être exploitées par des menaces pour nuire aux actifs ou à l'organisme
- **Identification des mesures de sécurité existantes**
  - ▷ éviter des travaux ou des coûts inutiles dus, par exemple, à la redondance des mesures de sécurité
  - ▷ identifier les mesures + contrôler qu'elles fonctionnent ! ☺

  NB processus itératif ⇒ **réexamen régulier**
- **Identification des vulnérabilités**
  - ▷ rappel : vulnérabilité ≠ menace ≠ dommage/conséquence

# Étape 2 : Appréciation du risque

## Identification des risques : quelles vulnérabilités de ces actifs ?

- **Identification des vulnérabilités**
  - rappel : vulnérabilité ≠ menace ≠ dommage/conséquence




- Étude de cas

  go to example

# Étape 2 : Appréciation du risque

## Identification des risques : quels impacts et conséquences ?

- **Identification des conséquences**
  - Objectif = identifier les conséquences que des pertes de confidentialité, d'intégrité et de disponibilité peuvent avoir sur les actifs
  - reformuler sous forme de **scénario d'incident**
    - ⇝ valeurs `C,I,D` pour chaque actif impacté dans le scénario
    - ⇝ + indicateur global sur chaque actif (ex : `SOM(C,I,D)` )
    - ⇝ + indicateur global du scénario (ex : `MAX(SOM(C,I,D))` )
  - **occurrence** du scénario d'incident = **incident de sécurité**
    - un scénario d'incident est la description d'une menace exploitant une certaine vulnérabilité, ou un ensemble de vulnérabilités, pour impacter un actif, ou un groupe d'actifs, lors d'un incident de sécurité de l'information (cf. ISO 27002, article 13)
- Étude de cas go to example

# Étape 2 : Appréciation du risque

## Identification des risques : quelles mesures existantes ?

- **Identification des mesures de sécurité existantes**
  - liste des mesures existantes et prévues
  - état d'implémentation
  - état d'utilisation

NB 1ère itération ⇝ aucune mesure de sécurité existante

- Étude de cas go to example

# Étape 2 : Appréciation du risque

## Estimation des risques

- L'**estimation des risques** se fait en trois étapes :
  1. estimer l'importance des **conséquences** de l'occurrence d'un scénario go to example
     - voir l'échelle de mesure des conséquence (contexte) remind
  2. estimer la **vraisemblance** d'un scénario d'incident go to example
     - c'est ce qui va permettre de "relativiser" certains scénarios de risque qui, s'ils sont "catastrophiques" (ex : une météorite frappe la Terre et détruit un pays entier), ont néanmoins très peu de chance de se produire...
  3. estimer le **niveau de risque** (pour chaque scénario) go to example
     - objectif = donner une valeur à chaque risque afin de pouvoir ensuite les **classer** du plus critique au plus faible
     - exemple de formule : `MAX(SOM(C,I,D)) * Vraisemblance`

# Étape 2 : Appréciation du risque

## Estimation des risques : quelques rappels

- Libre à vous de définir vos propres échelles
  - non définies dans la norme
  - autres exemples d'échelles (resserrées) :
    - actifs : notés de 0 (jetable) à 4 (vital)
    - vraisemblance des menaces : 0 (peu vraisemblable) à 2 (très vraisemblable)
    - facilité d'exploitation : 0 (très difficile) à 2 (facile)
  - pb des échelles impaires : 2 est "pile au milieu" de l'échelle 0→4
  - une échelle peu être très large (ex : 0→100)
    - mais, par exemple, comment choisir entre les valeurs 64, 65 ou 66 dans ce cas ?

# Étape 2 : Appréciation du risque

## Estimation des risques : quelques rappels

- Idem pour les règle de calcul pour l'estimation des risques
  - absentes de la norme, donc à définir selon le projet, son contexte, la maturité de l'organisation
  - commencer avec des règles simples
    - ex : `MAX(SOM(C,I,D)) * Vraisemblance`
  - faciliter la comparaison avec d'autres situations et d'autres projets
  - autre exemple :
    - somme des pondérations des trois critères (probabilité, facilité, valeur)
    - 0 à 2 ⇝ bénin
    - 3 ou 4 ⇝ moyen
    - supérieur à 5 ⇝ grave

| | Probabilité d'occurrence du risque | Faible | | | Moyenne | | | Élevée | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 0 | | | 1 | | | 2 | | |
| | Facilité d'exploitation | F | M | E | F | M | E | F | M | E |
| | | 0 | 1 | 2 | 0 | 1 | 2 | 0 | 1 | 2 |
| Valeur de l'actif | 0 | 0 | 1 | 2 | 1 | 1 | 2 | 2 | 1 | 2 |
| | 1 | 1 | 2 | 3 | 2 | 2 | 3 | 3 | 2 | 3 |
| | 2 | 2 | 3 | 4 | 3 | 3 | 4 | 4 | 3 | 4 |
| | 3 | 3 | 4 | 5 | 4 | 4 | 5 | 5 | 4 | 5 |
| | 4 | 4 | 5 | 6 | 5 | 5 | 6 | 6 | 5 | 6 |

# Étape 2 : Appréciation du risque

## Évaluation des risques

- Étape de prise de décision go to example
  - faut-il traiter le (scénario de) risque ?
  - établir des priorités, fixer des seuils
- Analyse des risques ⇒ comprendre ceux-ci, les expliquer aux décideurs

NB On peut éventuellement "redresser" les résultats de l'estimation des risques du fait de contraintes qualitatives difficiles à chiffrer (obligations contractuelles, réglementation, notoriété, etc.)

# Étape 2 : Appréciation du risque

## Évaluation des risques

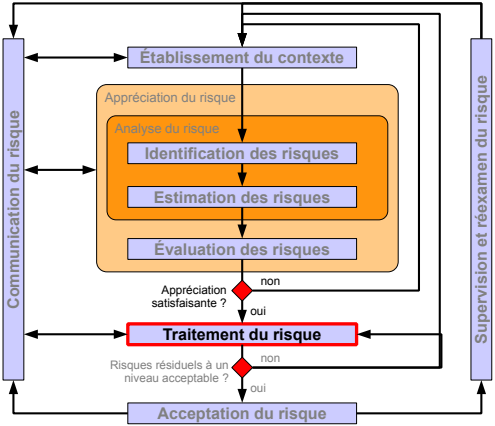
- Prise de décision ?
  - ▷ nous avons défini le **niveau de risque** pour chaque scénario (estimation des risques)
  - ▷ les critères d'évaluation des risques (établissement du contexte) et les formules de calcul nous ont permis de **prioriser ces risques**

⇒ **point de contrôle** : l'appréciation est-elle satisfaisante ?

oui ⇝ on passe à la définition du plan de traitement
non ⇝ on refait une itération

# Étape 3 : Traitement du risque

## Processus



# Étape 3 : Traitement du risque

## Définition du plan de traitement

- Pour définir les options de traitement :
  - mettre en adéquation le risque et le coût de traitement/réduction
  - intégration possible d'éléments non rationnels (ex : "11 septembre")
  - intégration des parties concernées
    - perception des risques par celles-ci
    - communication avec elles
    - les scénarios qui ont été définis permettent d'argumenter **de manière objective**

# Étape 3 : Traitement du risque

## Définition du plan de traitement

- 4 options pour traitement du risque (terminologie ISO 27005)
  - ▷ **évitement du risque** (*risk avoidance*)
    - ⇝ l'activité amenant le risque doit être éliminée
  - ▷ **réduction du risque** (*risk reduction*)
    - ⇝ le risque doit être diminué
    - ⇒ indiquer et chiffrer les mesures de sécurité à mettre en place
  - ▷ **transfert du risque** (*risk transfer*)
    - ⇝ le risque sera transféré à une autre "entité" capable de le gérer
      ex : assurance, sous-traitant, etc.
  - ▷ **maintien du risque** (*risk retention*)
    - ⇝ le risque est maintenu tel quel

NB Chaque option produit un **risque résiduel** à évaluer

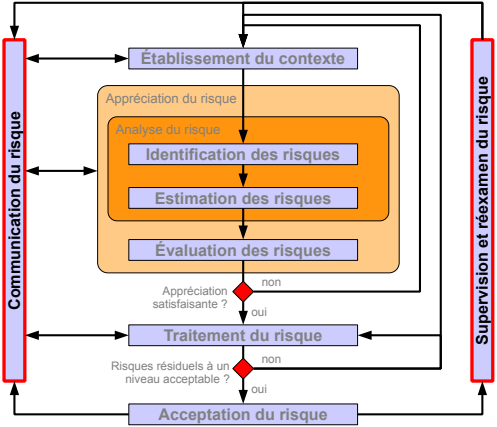
# Étape 3 : Traitement du risque

## Étapes vers le plan de traitement

- Pour chaque scénario d'incident identifié
  1. choix du traitement et mesures de sécurité à mettre en œuvre
     go to example
  2. calcul du risque résiduel (estimé)
     go to example
  3. validation par la direction des risques acceptés avec justification de leur choix
     go to example
     - peut déroger aux règles d'évaluation des risques (cf. critères d'acceptation)
       ex : coût jugé trop élevé, avantages intéressants à maintenir un risque, etc.
     - les dérogations doivent être justifiées et documentées
     ⇝ à prendre en compte à la **prochaine itération**

# Étape 4 : Communication & Surveillance

## Processus



# Étape 4 : Communication & Surveillance

## 2 étapes souvent négligées ☹

- La norme ISO 27005 définit 2 tâches supplémentaires malheureusement souvent sous-estimées !
  - ▷ **communication du risque**
    - une communication efficace entre les parties prenantes est essentielle puisqu'elle peut avoir une forte influence sur les décisions à prendre
    - cette communication garantit que les personnes responsables de la mise en œuvre de la gestion du risque et que les personnes ayant un intérêt direct comprennent les fondements sur lesquels les décisions sont prises et les raisons pour lesquelles des actions spécifiques sont nécessaires
    - cette communication est bidirectionnelle

    ⇒ **acceptabilité des décisions**

# Étape 4 : Communication & Surveillance

## 2 étapes souvent négligées ☹

- La norme ISO 27005 définit 2 tâches supplémentaires malheureusement souvent sous-estimées !
  - ▷ **surveillance et réexamen du risque**
    - il convient de surveiller et de réexaminer les risques et leurs facteurs (à savoir valeur des actifs, impacts, menaces, vulnérabilités et vraisemblance) pour identifier au plus tôt toutes les modifications dans le contexte de l'organisme et pour maintenir une cartographie complète des risques
    - de nouvelles menaces, vulnérabilités ou modif de la vraisemblance ou des conséquences peuvent accroître les risques appréciés auparavant comme des risques peu élevés

    ⇒ **supervision** & **évolution** du SI

    ⇒ **veille techno**, CERT (*computer emergency response team*), etc.

    ⇒ **retours d'expérience**

# Bilan de l'ISO 27005

## Ce qu'elle apporte

- S'intègre normalement dans un SMSI (ex : norme ISO 27001)
  - ▷ mais peut fonctionner de manière autonome, hors SMSI
  - ⇒ attention à ne pas oublier d'appliquer le plan de traitement !
- Un processus comme l'ISO 27005 permet de garder un historique significatif
  - ▷ des risques, hypothèses, scénarios envisagés
  - ▷ des analyses, évolutions du contexte et modifications associées des scénarios
  - ▷ des plans de traitement, dérogations, contraintes spécifiques
  - ⇒ maîtriser son SI !

# Bilan de l'ISO 27005

## Ses défauts

- C'est une norme
  - ⇒ payante
  - ⇒ difficile à faire évoluer
- Base de connaissance des risques minimale
  - ▷ une partie de la méthode en annexe(s) bien qu'indispensable au fonctionnement
  - ⇒ consulter également d'autres référentiels (ex : ISO 15408 (CC), EBIOS)
- Une certaine liberté
  - ⚠ ne pas faire une appréciation trop superficielle ou au contraire trop détaillée

# Bilan de l'ISO 27005

## Ses avantages

- Méthode compréhensible
  - ▷ aucune notion trop complexe
  - ▷ vocabulaire conforme au langage courant
  - ▷ vocabulaire cohérent de bout en bout
- Méthode pragmatique et accessible à tous
  - ▷ aucune étape infaisable même si la précédente n'est pas terminée
  - ▷ production d'un travail exploitable et utile rapidement
- Application de l'amélioration continue (cycle PDCA)
  - ▷ on peut commencer petit et améliorer progressivement
  - ⇒ adaptée aux changements (pas juste une appréciation des risques à l'instant t)
- Impose à la direction de prendre ses responsabilités !

# Plan du cours

- Modèles de contrôle d'accès discrétionnaires
- Modèles de contrôle d'accès obligatoires
- Modèles de contrôle d'usage

2 Gestion des Risques
- Introduction
- Vocabulaire
- ISO 27005 Risk Manager
- Bilan

# Bilan

- Vous savez maintenant faire une analyse de risques ! ☺
- L'ISO 27005 et EBIOS RM sont très proches
  - ▷ leurs processus sont organisés différemment, mais on retrouve globalement les mêmes étapes
  - ▷ leurs vocabulaires ont été harmonisés
  - ▷ sont dorénavant plus complémentaires que concurrentes
- Ce sont la pratique et l'expérience qui feront la différence entre les *risk managers*
  - ⇝ y compris les échecs...

# Digression vers l'IA

- L'IA est un nouvel outil informatique devenu incontournable ☺
- Tout outil introduit de nouvelles vulnérabilités et donc de nouvelles menaces
  - le digital classique est déterministe $\rightsquigarrow$ l'IAg est probabiliste
  - systèmes agentiques, vibe coding $\rightsquigarrow$ l'humain perd-il le contrôle ?
  - dépendance aux services IA, aux modèles disponibles (ex : géo-politique)
  - maîtrise des coûts ? (tokens, infra locale, etc.)
  - montée en compétence(s) en IA ? Perte de compétences sur les technos "classiques" !
  - souveraineté, responsabilités, flou juridique actuel, *shadow AI*, etc. ?
  - green IT, éco-responsabilité, ressources, etc. ?

# Plan du cours

1 Introduction à la Sécurité Informatique

2 Gestion des Risques

3 Droit & Numérique
- Introduction
- Protection des Données Personnelles
- Et bientôt...

4 Conclusion

# Droit & Numérique

- La prise en compte des aspects juridiques en SSI est multiple :
  - Droit d'auteur & propriété intellectuelle
  - Liberté d'expression (et ses limites)
  - Contrat de travail & obligation de loyauté envers l'employeur
  - Respect des différentes réglementations en vigueur
  - **Protection des données personnelles**

# Les textes fondateurs

- Loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Directive européenne n° 95/46/CE du 24 octobre 1995
- Charte des droits fondamentaux de l'Union Européenne
  - → Chapitre II : libertés
- Règlement Général pour la Protection des Données (RGPD)
  - → entré en vigueur le 25 mai 2018
  - → règlement européen
    - ⇒ pas de transposition nationale
    - ⇒ est "obligatoire dans tous ses éléments et directement applicable dans tout État membre"

# CNIL

- La France, pionnière en matière de données personnelles, a très vite réalisé les risques de l'informatique pour les libertés de la personne humaine et a réagi en se dotant depuis 1978 d'une législation traitant de la protection de ces données face aux dangers d'une informatique grandissante : la loi du 6 janvier 1978 dite "informatique et libertés".
- La Commission Nationale de l'Informatique et des Libertés (CNIL) est une autorité administrative indépendante née de l'adoption de la loi précitée.
- La mission générale de la CNIL est, face aux dangers de l'informatique, de protéger la vie privée et les libertés individuelles ou publiques.

# CNIL

- La CNIL est une autorité administrative indépendante qui fonctionne avec une dotation du budget de l'État.
- Elle informe et conseille les personnes sur leurs droits : elle reçoit les réclamations, pétitions, plaintes relatives aux traitements de données personnelles et répond par des avis, délibérations ou recommandations.
- Elle régule et recense les fichiers de données personnelles : elle autorise ou non la création des fichiers.
- Elle peut opérer des contrôles dans les entreprises, des enquêtes, des auditions de personnes.
- La CNIL n'est pas un juge. Il faut saisir le juge pour obtenir des dommages-intérêts au titre de la responsabilité civile en cas de préjudice.

# Notion de données sensibles

- **Attention** (→ responsables de traitements) : En pratique une confusion est parfois opérée entre :
  - *"les données qui sont sensibles pour une organisation"* (ex : des données financières pour une entreprise)
  - le régime juridique des *"données sensibles, au sens de la loi de 1978"*
- Des données sensibles pour une entreprise (l'évolution de son chiffre d'affaire, ses processus d'acquisition de clientèle,...) ou une administration (organisation interne, dossiers politiquement et médiatiquement sensibles,...) ne sont pas nécessairement des données sensibles au sens de la loi de 1978.

# Notion de données sensibles

- Cette distinction est importante car seul le traitement de *données sensibles au sens de la loi informatique et libertés* devra répondre au régime juridique décrit ci-après.
- Peu importe qu'une organisation traite des *données qui lui sont sensibles*, dès lors que ces données ne sont pas des données personnelles.

# Droits et principes fondamentaux

**Loi "informatique et libertés"**

La loi de 1978, dite loi "informatique et libertés", instaure de nombreux droits et principes fondamentaux relatifs **"à la protection des personnes physiques à l'égard des traitements de données à caractère personnel"**.

- Principe de **finalité**
  - Les données personnelles ne peuvent être collectées, traitées, conservées ou transmises à des tiers qu'en vue de réaliser des finalités déterminées, légitimes et compatibles entre elles.

# Droits et principes fondamentaux

- Principe de **loyauté** et de **transparence**
  - La collecte, le traitement, la conservation des données personnelles et leur transmission éventuelle à des tiers doivent s'effectuer de manière loyale.
  - Cela suppose que les données ne soient pas collectées et traitées à l'insu de la personne concernée et que les personnes soient informées de l'identité et du lieu d'établissement de la personne qui traite ces données, des finalités poursuivies, du caractère obligatoire ou facultatif du traitement des données, des destinataires des informations, ainsi que toute information nécessaire à l'exercice de leurs droits.

# Droits et principes fondamentaux

- Principe de la **pertinence** et de l'**exactitude** des données
  - Les données personnelles faisant l'objet d'un traitement doivent être pertinentes au regard des finalités poursuivies. Elles doivent être exactes et mises à jour.
- Principe du **consentement** pour les traitements de données sensibles
  - Lorsque des traitements portent sur des données sensibles (religion, opinion politique ou philosophique, appartenance syndicale, origine raciale et ethnique, santé et vie sexuelle), celles-ci ne peuvent être collectées qu'avec le consentement des personnes.

# Droits et principes fondamentaux

- Principe d'**accès**, de **rectification** et d'**opposition**
  - Les personnes doivent se voir reconnaître les droits d'accéder, sans subir de coût dissuasif, à toute donnée les concernant, de corriger les données incomplètes ou inexactes et de s'opposer sans avoir à se justifier à l'exploitation de leurs données à des fins commerciales.
- Principe de **sécurité**
  - Le code pénal incrimine le traitement, sans que soient prises les mesures de précaution, et prévoit des sanctions à l'encontre de l'administrateur ne protégeant pas assez efficacement son système (délit de manquement à la sécurité).

# Droits et principes fondamentaux

- Principe du **droit à l'oubli**
  - Le code pénal incrimine le fait, sans l'accord de la CNIL, de conserver une information sous la forme nominative au-delà de la durée prévue à la demande d'avis ou à la déclaration préalable.
- Principe de **protection de la considération et de l'intimité**
  - Le fait de porter à la connaissance d'un tiers des images portant atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée est condamnable.
  - Cette divulgation est sanctionnée encore plus sévèrement si elle a été faite par imprudence ou négligence (délit d'atteinte à la considération ou à l'intimité).

# Résumé droits & obligations

- Les droits des personnes
  - **Droit à l'information**
    *Toute personne a le droit de savoir si elle est fichée et dans quels fichiers elle est recensée.*
  - **Droit d'accès**
    *[...] a le droit d'interroger le responsable d'un fichier pour savoir s'il détient des informations sur elle et d'en obtenir la communication.*
  - **Droit de rectification**
    *[...] a le droit de contrôler l'exactitude des données et de les faire rectifier.*
  - **Droit d'opposition**
    *[...] peut s'opposer pour des motifs légitimes à figurer dans un fichier ou de voir communiquer des informations sur elle à des tiers. Les personnes peuvent saisir la CNIL en cas de difficultés dans l'exercice de leurs droits.*

# Résumé droits & obligations

- Les obligations des responsables du traitement
  - ▷ **Obligation d'information préalable** des personnes concernées dont on doit obtenir le consentement exprès.
  - ▷ **Obligation d'assurer la sécurité et la confidentialité** des données collectées et traitées.
  - ▷ **Obligation d'une collecte et d'un traitement** ayant une finalité précise et effectués de façon licite et loyale.
  - ▷ **Obligation de déclaration préalable à la CNIL** des traitements informatiques de données personnelles.

# Données à caractère personnel

- Points clés
  - Les données sont des données à caractère personnel dès lors qu'elles portent sur une **personne identifiée ou identifiable**, la personne concernée.
  - Une personne est identifiable si des informations complémentaires peuvent être obtenues sans effort déraisonné, permettant l'identification de la personne concernée.
  - L'authentification s'entend du fait de démontrer qu'une certaine personne possède une certaine identité et/ou est autorisée à exercer certaines activités.
  - NB : **identification $\neq$ authentification**

# Données à caractère personnel

- Points clés
  - Il existe des catégories particulières de données, appelées "données sensibles", énumérées dans la directive relative à la protection des données, qui requièrent une protection accrue et, par conséquent, sont soumises à un régime juridique spécial.
  - Les données sont anonymisées si elles ne contiennent plus d'identifiants ; elles sont pseudonymisées si les identifiants sont cryptés.
  - Contrairement aux données anonymisées, les données pseudonymisées sont des données à caractère personnel.

# Caractère identifiable d'une personne

- Dans le droit de l'UE, une information contient des données sur une personne si :
  - ▷ une personne est identifiée dans cette information

  ou ▷ si une personne, bien que non identifiée, est décrite dans cette information d'une manière permettant de découvrir qui est la personne concernée en menant d'autres recherches

- Les deux types d'informations sont protégés de la même manière par le droit européen en matière de protection des données.
  - noms non uniques ⇒ date et lieu de naissance, numéros de citoyens,...
  - ère du numérique ⇒ données biométriques (empreintes digitales, photos numériques, aspects rétiniens) pour l'identification des personnes

# Authentification

- L'authentification est la procédure par laquelle une personne peut prouver qu'elle possède une certaine identité et/ou est autorisée à faire certaines choses.
  - Par la comparaison de données biométriques (une photo ou les empreintes digitales d'un passeport) avec les données de la personne qui se présente à un contrôle d'immigration.
  - En demandant des informations que seule la personne possédant une certaine identité ou autorisation devrait connaître (numéro d'identification personnel (PIN) ou un mot de passe).
  - En demandant la présentation d'un certain objet qui devrait exclusivement se trouver en la possession de la personne ayant une certaine identité ou autorisation (une carte magnétique spéciale ou la clé d'un coffre en banque).

# Authentification

- L'authentification est la procédure par laquelle une personne peut prouver qu'elle possède une certaine identité et/ou est autorisée à faire certaines choses.
  - Outre les mots de passe ou cartes magnétiques, parfois associés à des codes PIN, les signatures électroniques sont un outil particulièrement utile pour identifier ou authentifier une personne dans des communications électroniques.
- NB : L'authentification ne nécessite pas de stocker les données personnelles (ex : empreinte digitale) sur le serveur, contrairement à l'identification.

# Catégories particulières de données à caractère personnel

- Il existe des catégories particulières de données qui, par leur nature, peuvent faire courir un risque aux personnes concernées quand elles font l'objet d'un traitement et requièrent donc une protection accrue :
  - ▷ données à caractère personnel révélant l'origine raciale ou ethnique
  - ▷ données à caractère personnel révélant les opinions politiques, convictions religieuses ou autres convictions
  - ▷ données à caractère personnel relatives à la santé ou à la vie sexuelle

# Données anonymisées et pseudonymisées

- Principe de la conservation des données pendant une durée limitée :
  - ▷ les données doivent être conservées *"sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement"*

⇒ Il pourrait être nécessaire d'anonymiser des données si un responsable du traitement souhaite les conserver alors qu'elles ne sont plus d'actualité et qu'elles ne servent plus leur finalité initiale.

# Données anonymisées et pseudonymisées

- **Données anonymisées**
  - Des données sont anonymisées si tous les éléments identifiants ont été supprimés d'un ensemble de données à caractère personnel.
  - Les informations ne doivent plus contenir aucun élément qui soit susceptible, au moyen d'un effort raisonnable, de servir à réidentifier la ou les personnes concernées.
  - Lorsque des données ont été correctement anonymisées, elles ne sont plus des données à caractère personnel.

# Données anonymisées et pseudonymisées

- **Données pseudonymisées**
  - Les informations personnelles contiennent des identifiants, tels que le nom, la date de naissance, le sexe ou l'adresse.
  - Lorsque des informations personnelles sont pseudonymisées, les identifiants sont remplacés par un pseudonyme.
  - La pseudonymisation est notamment obtenue par cryptage des identifiants figurant dans les données à caractère personnel.
  - Il ne doit pas être possible de relier facilement les données et les identifiants. Pour quiconque ne possède pas la clé de décryptage, les données pseudonymisées peuvent être difficilement identifiables.
  - Le lien avec l'identité demeure sous la forme du pseudonyme associé à la clé de décryptage. Pour toute personne habilitée à utiliser la clé de décryptage, une nouvelle identification est possible aisément $\Rightarrow$ **données personnelles**

# Une constante évolution

- Règlement Général pour la Protection des Données (**RGPD**) le 25 mai 2018
- Règlement **ePrivacy** (25 mai 2018 ?)
  - → réforme la directive 2002/58/CE du 12 juillet 2002
  - → relatif au traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques
- Plusieurs référentiels de sécurité informatique seront rendus opposables "dès 2018"
  - → source Agence des Systèmes d'Information Partagés de santé (ASIP Santé)
  - → ex : référentiels d'interopérabilité
- Publication récente de plusieurs règlements sur la **donnée**

# RGPD

- Rien de révolutionnaire !
  - en France nous avions déjà la loi "informatique et libertés"
  - modifiée par la loi du 6 août 2004 afin de transposer en droit français les dispositions de la directive 95/46/CE
- Dans les grandes lignes, le RGPD cherche à renforcer la responsabilité des sociétés amenées à gérer des informations personnelles. Ses différentes dispositions cherchent donc à assurer la protection de ces données, mais aussi leur traçabilité, et le suivi précis des traitements qui en seront faits.

# RGPD

- Le poste de **DPO** (Data Protection Officer) s'inscrit dans le prolongement de ce que la CNIL avait déjà initié avec son Correspondant Informatique et Libertés (**CIL**), avec un niveau de responsabilité similaire mais des prérogatives étendues.
- Ce pilote en interne est censé cartographier l'ensemble des traitements de données personnelles réalisés par l'entreprise pour identifier les carences et proposer une optimisation des processus.

NB : La CNIL recommande également la création d'une documentation permettant de justifier des mesures entreprises en cas d'enquête de conformité.

# RGPD & PIA

- L'Étude d'Impact sur la Vie Privée (**EIVP**) était la traduction utilisée par la CNIL pour le Privacy Impact Assessment (**PIA**).
- L'application du nouveau règlement européen RGPD impose (en partie) la réalisation d'une analyse d'impact relative à la protection des données (ou **DPIA** pour Data Protection Impact Assessment).
- Cette démarche, repose sur une analyse de risques sécurité orientée uniquement sur les risques visant les données personnelles et leurs impacts sur les droits et libertés des personnes concernées par ces données.

# RGPD & PIA

- Le DPIA n'est pas obligatoire pour l'ensemble des traitements, mais uniquement pour les traitements présentant *"un risque élevé pour les droits et libertés des personnes physiques"*
  - → les traitements à grande échelle
  - → la surveillance systématique à grande échelle d'une zone accessible au public (notamment la vidéosurveillance)
  - → les décisions automatiques produisant des effets juridiques (pour des offres de prestations, ou le choix de contractualisation)
  - → le traitement de données sensibles (données de santé, opinions politiques, orientation sexuelle)
  - → l'évaluation ou la notation basée sur des données personnelles, y compris le profilage et la prédiction
  - → le traitement de données biométriques, de données relatives à des condamnations pénales et à des infractions

# ePrivacy

- Là où le RGPD s'attache à la protection des données personnelles dans leur ensemble, ePrivacy se concentrera plus précisément sur l'exploitation des données issues des communications.
  - Avec ce texte, la Commission européenne affiche sa volonté de remettre au premier plan la notion de consentement de l'internaute, en particulier pour ce qui concerne la question des cookies.
  - Il sera difficile d'esquiver son impact sur les pratiques en matière de marketing...

# ePrivacy

- Aujourd'hui, la norme est au cas par cas, ce qui signifie que chaque éditeur se charge de recueillir le consentement du visiteur avant de distribuer les traceurs dédiés aux opérations de ciblage.
- Demain, le règlement ePrivacy prévoit que le consentement se fasse au niveau des options du navigateur Web, de façon globale.

# ePrivacy

- Lourde de conséquence pour l'ensemble des acteurs du Web, la mesure sera âprement discutée jusqu'à l'adoption définitive du règlement ePrivacy, (qui était) prévue pour la fin de l'année 2017. Il ne restera(it) ensuite que six mois pour se mettre en conformité...
- Le 07/10/2024 le CEPD (Comité Européen de la Protection des Données) a adopté la version finale des lignes directrices sur le champs d'application technique des dispositions sur le "traçage" de la directive ePrivacy...
- En février 2025 la directive **n'a pas été adoptée** et a été retirée par la Commission européenne

# Domaine de la santé

- Le 6 octobre 2017, le directeur général de l'Agence des systèmes d'information partagés de santé (ASIP Santé) a assuré qu'*"au moins trois référentiels de sécurité informatique seront publiés par arrêtés ministériels et rendus opposables dès 2018"*.
- Élaboration d'un cadre d'interopérabilité des systèmes d'information de santé, la création d'un espace de confiance "pour l'ensemble des interactions supposées par l'e-santé", notamment via :
  - les messageries sécurisées de santé (MSSanté)
  - l'adoption d'une politique générale de sécurité des systèmes d'information de santé (PGSSI-S)

# Domaine de la santé

- Parmi les référentiels qui seront rendus opposables dès 2018 par arrêté ministériel (dixit) :
  - l'un porte sur l'identification
  - l'autre sur l'authentification
  - le troisième sur la gouvernance de la sécurité
- Parallèle avec les actions menées sur la sécurité informatique
  - → la loi prévoit aussi que les référentiels d'interopérabilité soient rendus opposables juridiquement
- En 2019 l'ASIP Santé devient l'agence du numérique en santé et... rien...

# Partage de données

- Avec l'émergence des environnements connectés, IoT, smart-*, IA & ML le législateur propose de nouveaux règlements :
  - **RGPD** → Règlement Général sur la Protection des Données (25/05/2018)
    https://fr.wikipedia.org/wiki/Règlement_général_sur_la_protection_des_données
  - **LRN** → Loi pour une République Numérique (07/10/2016)
    https://fr.wikipedia.org/wiki/Loi_pour_une_République_numérique
  - **Une stratégie européenne pour les données** (19/02/2020)
    https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52020DC0066
  - **DGA** → Data Governance Act (24/09/2023)
    https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX%3A52020PC0767
  - **Data Act** (11/01/2024)
    https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN

# Partage de données

- Voire également de nouveaux concepts :
  - **Open Data**
  - **Communs numériques**
- En s'adaptant aux nouveaux usages :
  - **AI Act** → Artificial Intelligence Act (08/2024)
  - **DSA** → Digital Services Act (02/2024)
    *fixe un ensemble de règles pour responsabiliser les plateformes numériques et lutter contre la diffusion de contenus illicites ou préjudiciables ou de produits illégaux : attaques racistes, images pédopornographiques, désinformation, vente de drogues ou de contrefaçons...* ⇝ *succède à la directive dite e-commerce du 8 juin 2000, devenue dépassée*

# Plan du cours

1 Introduction à la Sécurité Informatique

2 Gestion des Risques

3 Droit & Numérique

4 Conclusion

# D'autres facettes de la sécurité informatique

- Dans ce cours nous nous sommes essentiellement intéressés à la sécurité informatique au niveau applicatif
  - → règlement & politique de sécurité
  - → ~~sécurité dans les bases de données~~
  - → ~~sécurité dans les applications Java~~
- Voire même à un niveau encore supérieur...
  - → gestion des risques dans les systèmes d'informations
  - → droit & numérique
- Mais la Sécurité des Systèmes d'Information (SSI) recours à bien d'autres techniques & technologies

# Sécurité réseau

- Modèle OSI (Open Systems Interconnect) en 7 couches

**application** c'est le programme qui a besoin du réseau pour communiquer
ex : navigateur web (HTTP), logiciel de messagerie (POP, IMAP, SMTP) ou de transfert de fichier (FTP), telnet,...

**présentation** responsable de la représentation des données (de telle sorte qu'elle soit indépendante du type de microprocesseur ou du système d'exploitation par exemple) et, éventuellement, du chiffrement (ex : HTML)

**session** en charge d'établir et maintenir des sessions (ie. débuter le dialogue entre 2 machines : vérifier que l'autre machine est prête à communiquer, s'identifier,...)

**transport** en charge de la liaison d'un bout à l'autre ; s'occupe de la fragmentation des données (fichiers) en petits paquets et vérifie éventuellement qu'elles ont été transmises correctement et dans l'ordre (ex : TCP, UDP)

**réseau** en charge du transport, de l'adressage et du routage des paquets entre extrémités distantes, à travers le réseau (ex : IP)

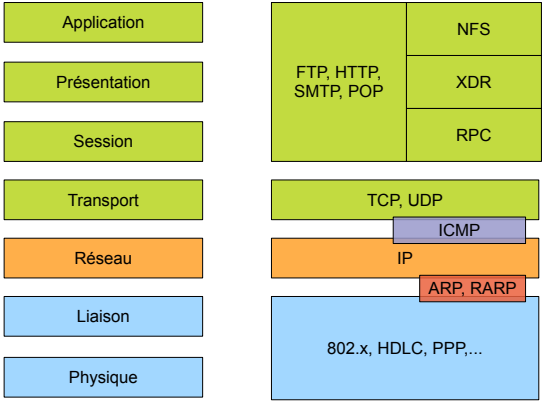
**liaison** en charge de transmettre des trames ; fournit également la détection d'erreur (retransmission) et la synchronisation (ex : transmission de trames entre nœuds d'un segment Ethernet)

**physique** responsable de la transmission de bits : codage, modulation,... (ex : normes des modems V23, V92,...)

**support** c'est le support de transmission lui-même : un fil de cuivre, une fibre optique, les ondes hertziennes, une liaison infrarouge,...

# Sécurité réseau

- Comparaison modèle OSI & modèle TCP/IP



# Sécurité réseau

- De nombreux mécanismes existent pour sécuriser le réseau du système d'information
  - sécurité du médium de communication
    - → *Wi-Fi sécurisé (ex : WPA & WPA2), sauts de fréquence,...*
  - architecture du réseau
    - → *VLANs, routage, firewall, DMZ, NAT, PAT, VPN,...*
  - sécurité des services réseau
    - → *SSL, HTTP, FTP, WebDAV, NFS, Samba, DNS, DHCP, SSH, telnet, NTP, proxy,...*
  - supervision du réseau
    - → *SNMP, Nagios, Syslog, IDS,...*

# Sécurité système

- Bien évidemment, la sécurité informatique concerne également l'administration système
  - système d'exploitation
    - → *mises à jour de l'OS, patchs de sécurité, services activés,...*
  - logiciels liés à la sécurité
    - → *antivirus, détection des fichiers système modifiés, surveillance des processus exécutés,...*
  - politique de sécurité
    - → *gestion des utilisateurs & des groupes, permissions, GPO sous Windows,...*
    - → *horaires & lieux de connexion, traçabilité,...*

# Sécurité système

- Sécurité & aspects matériels
  - tolérance aux pannes
    - → *onduleur & alim. de secours, alim. redondante, RAID*
    - → *virtualisation, clusters de serveurs, multi-sites,. . .*
  - reprise après "sinistre" la + rapide possible
    - → *gestion des sauvegardes*
    - → *maquettes pour réinstaller les OS, les applis, les licences*
  - sécurité des locaux
    - → *accès, protection incendie, inondation,. . .*
  - renouvellement du matériel
    - → *garantie, suivi constructeur, dispo. des mises à jour,. . .*
    - → *anticiper les besoins, prévoir les évolutions,. . .*

# Sécurité applicative

- Certains mécanismes de sécurité son implémentés au niveau des couches applicatives
  - protocoles de communication
    - → *RMI, CORBA, Web Services, WSS,...*
      - ▷ chiffrement des échanges
      - ▷ signatures & certificats ⇒ authentification de l'émetteur & intégrité
      - ▷ transaction, session, *security token*,...
      - ▷ "intercepteurs" pour mettre en place des politiques de sécurité particulières
  - mécanismes d'authentification applicative
    - → *SSO, CAS, Radius,...*
      - ▷ authentification unique de l'utilisateur ⇒ session
      - ▷ *security token* ⇒ attributs, permissions,...
      - ▷ objectif : décharger les applis web & services réseau de l'authentification

# Communication & formation

- Comme le précisent clairement les différentes méthodes de gestion des risques (quel que soit le domaine d'ailleurs), la sécurité ne peut être assurée sans la "participation" des utilisateurs
  - communication
    - → *expliquer/justifier les mécanismes mis en œuvre*
    - → *informer les utilisateurs des enjeux, des ressources sensibles*
    - → *établir des procédures*
    - → *rassurer & mettre en confiance les partenaires, clients,...*
  - formation
    - → *former les utilisateurs aux outils & logiciels*
      - ▷ limiter les erreurs liées à une mauvaise utilisation
    - → *sensibiliser les utilisateurs aux objectifs de sécurité (cf. CID) pour certaines données*
      - ▷ appliquer la PSSI, les procédures,...

# Veni, Vidi, Security