C018SA-W4-S1

informatiques mathématiques

SEMAINE 4 : Contrôle d'Accès

1. **Introduction**
2. Modèle de contrôle d'accès discrétionnaire (DAC)
3. Modèle de contrôle d'accès basé sur les rôles (RBAC)
4. Modèle de contrôle d'accès obligatoire (MAC)

La sécurité des systèmes d'information

- Les bases de données stockent des données structurées, de grande qualité

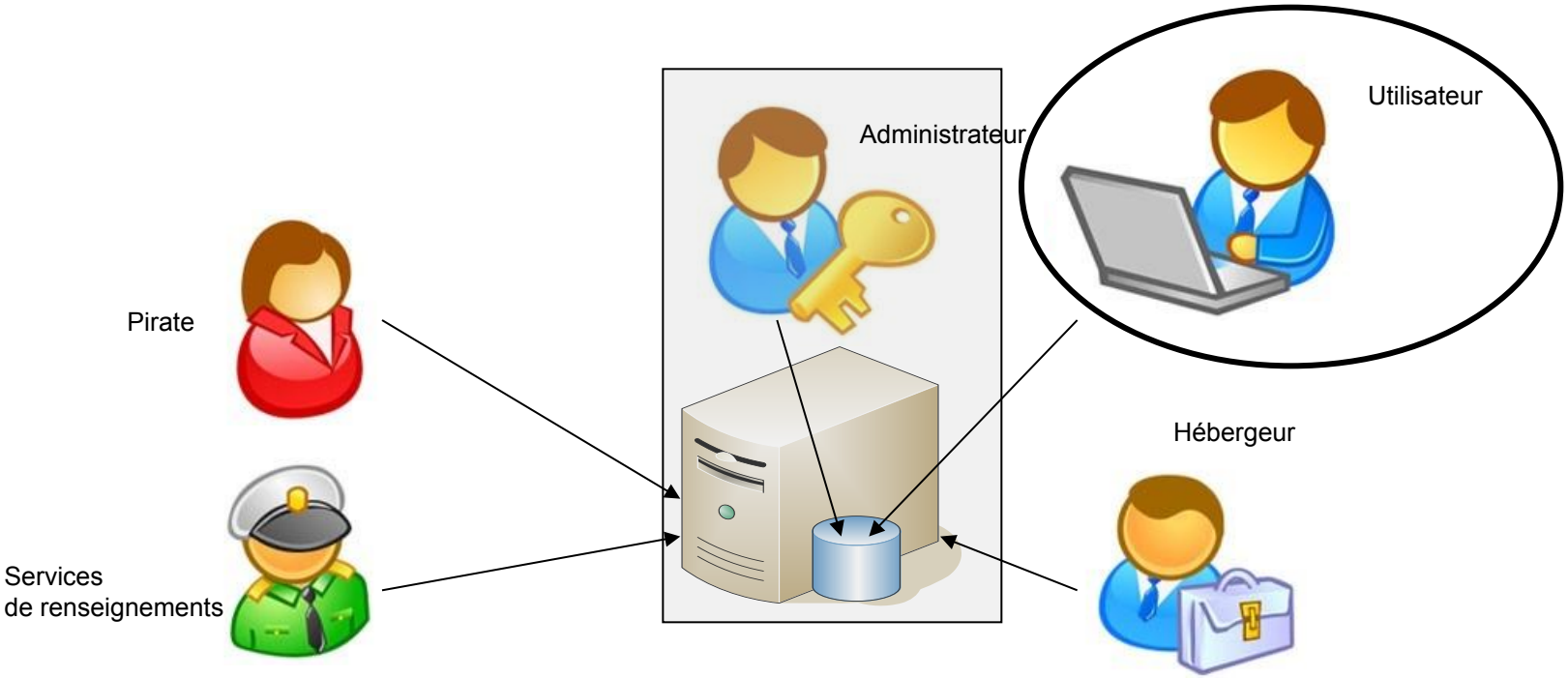
→Intérêt évident à les attaquer pour *dérober de l'information*

  - Attaques internes (45% d'après le FBI)
  - Attaques externes

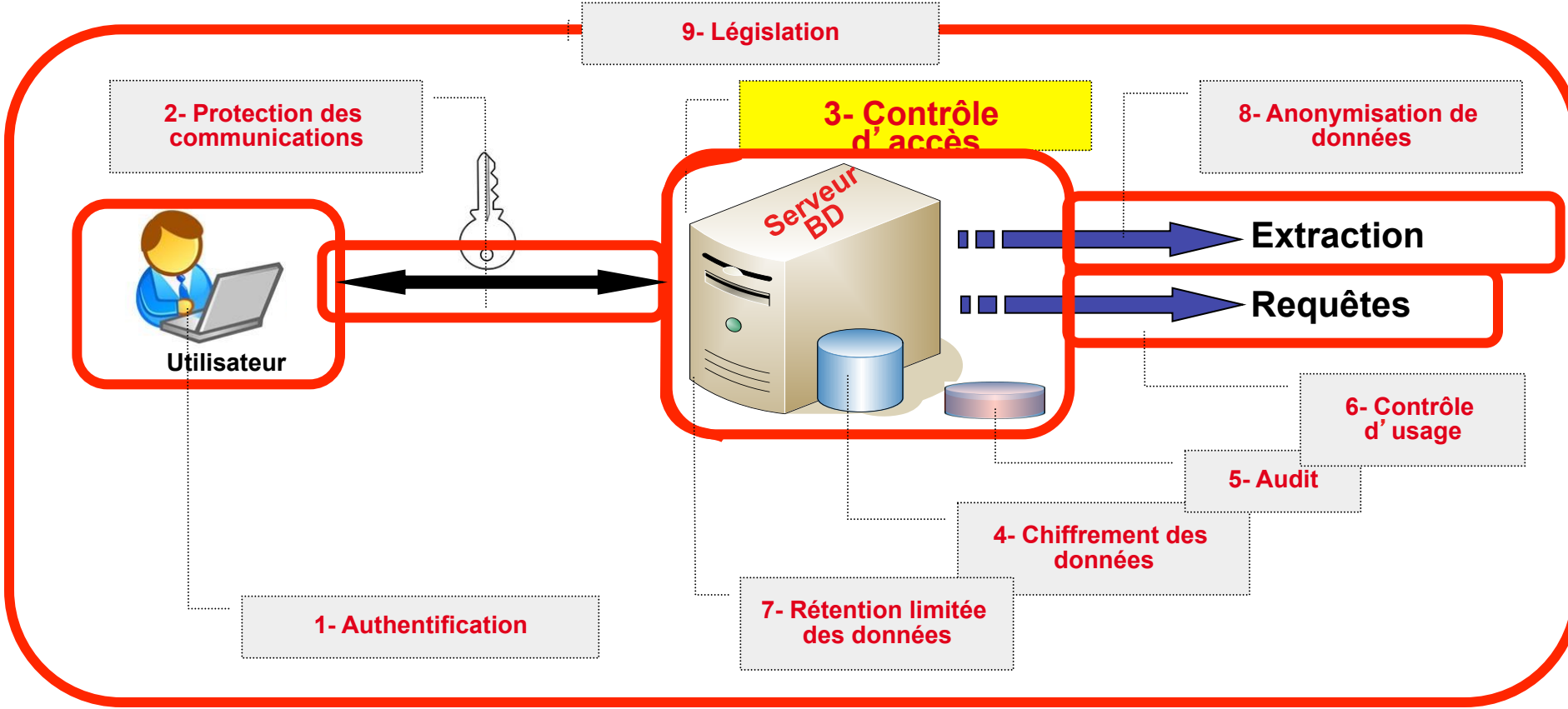
- Nombreux sites à lister les attaques sur les SGBD
  - DatalossDB
  - Zataz
  - …
- Sont évalué selon des standards :

e.g. Common Criteria for Information Technology Security Evaluation (Common Criteria ou CC), norme ISO/CEI 15408

Principaux attaquants

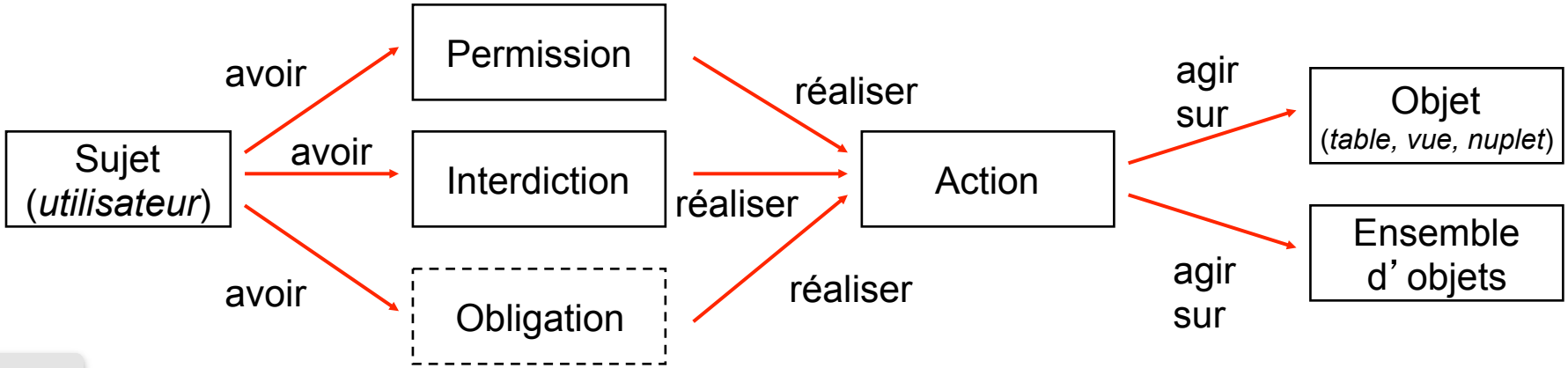


Principaux mécanismes de défense



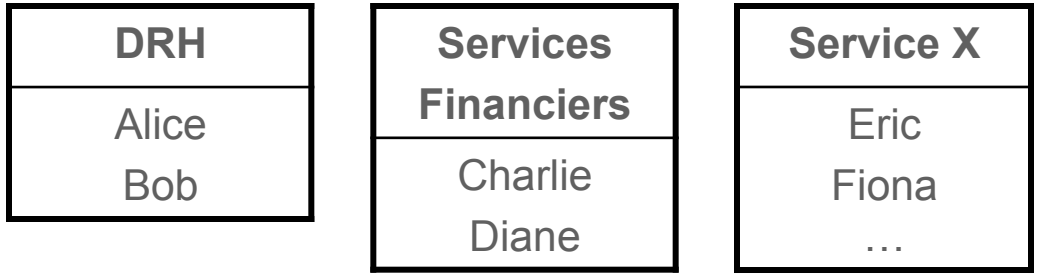
Le contrôle d'accès

- Précise :
  - dans **quelles conditions**
  - est autorisé à faire **quoi** (lectures, écritures, etc…)
  - sur **quelles données** (tables, nuplets, …)
  - dans **quelles conditions**
- Format des règles :

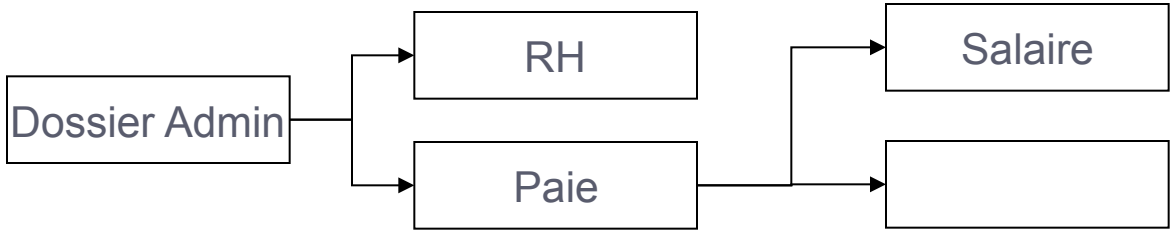


Exemple : système de paie dans une entreprise

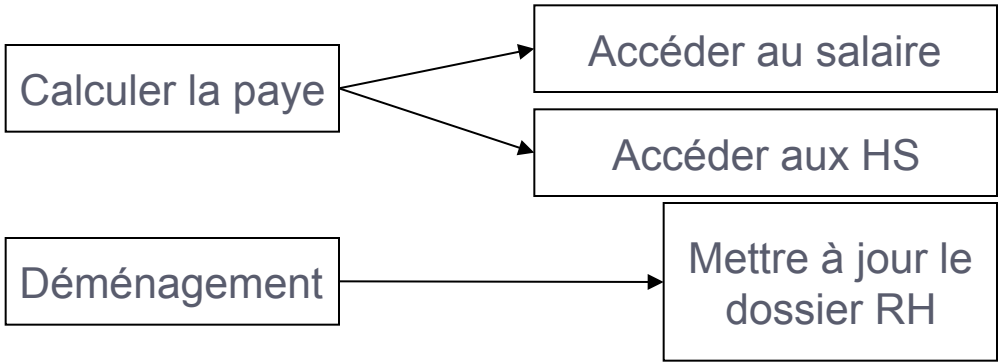
Sujets =
Employés de l'entreprise



Objets =
Information sur les employés



Actions :



Exemples de règles

- **Indépendantes du contenu de lobjet auquel on accède**
  - **Alice** et **Bob** ont le droit de lire et modifier toutes les informations RH des dossiers admin tous les employés
  - **Charlie** et **Diane** ont le droit de lire toutes les informations Salaire des employés
  - **Diane** a le droit de lire toutes les informations Heures Sup des employés

- **Dépendantes du contenu**
  - **Eric** et **Fiona** ont le droit de lire les informations de salaire de leur propre dossier

- **Délégation**
  - **Diana** a le droit d'autoriser **Charlie** à lire les informations Heures Sup

Le contrôle d’accès

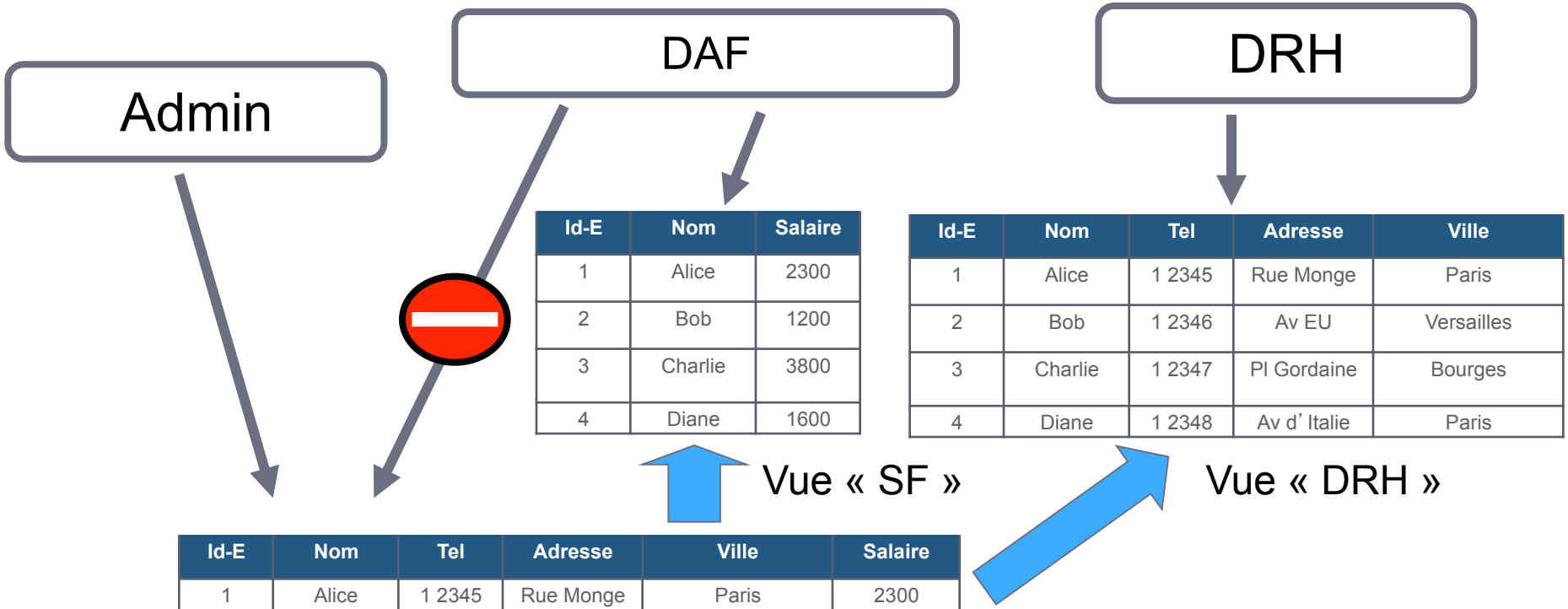
Objectif :

- Ne permettre l’accès et la modification des données qu’aux personnes autorisés

Plusieurs méthodes :

  - Contrôle d’accès obligatoire (MAC)
  - Contrôle d’accès discrétionnaire (DAC)
  - Contrôle d’accès basé sur les rôles (RBAC)
- Plus ou moins flexibles et plus ou moins sécurisées
- DAC est implémenté dans tous les SGBDs

Contrôle d'accès via des vues



Id-E	Nom	Salaire
1	Alice	2300
2	Bob	1200
3	Charlie	3800
4	Diane	1600

Id-E	Nom	Tel	Adresse	Ville
1	Alice	1 2345	Rue Monge	Paris
2	Bob	1 2346	Av EU	Versailles
3	Charlie	1 2347	Pl Gordaine	Bourges
4	Diane	1 2348	Av d' Italie	Paris

Id-E	Nom	Tel	Adresse	Ville	Salaire
1	Alice	1 2345	Rue Monge	Paris	2300
2	Bob	1 2346	Av EU	Versailles	1200
3	Charlie	1 2347	Pl Gordaine	Bourges	3800
4	Diane	1 2348	Av d' Italie	Paris	1600