Contrôle d'accès – Contrôle de flux – Contrôle d'usage – Le projet ANR FLUOR

Alban Gabillon

Université de la Polynésie Française

Plan

- Objectifs de la Sécurité Informatique
- Modèles de Sécurité
- Modèle de Contrôle d'accès
- Modèle de Contrôle des flux
- Modèle de Contrôle d'usage & DRM
- Le projet ANR FLUOR

Sécurité Informatique

- La sécurité informatique recouvre 3 types d'objectifs
  - 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 déni non autorisé d'accès à une information ou à une ressource

Modèles de Sécurité

- Pour sécuriser un système informatique il est important de définir un modèle de sécurité. Un modèle de sécurité exprime les besoins de sécurité du système d'informations. Il inclut:
  - Un règlement de sécurité
  - Un modèle d'administration spécifiant qui a le droit de mettre à jour le règlement de sécurité

Modèles de Sécurité

- Le règlement de sécurité définit ce qui est autorisé et ce qui ne l'est pas.
- Un règlement de sécurité est un ensemble de:
  - Permissions
  - Interdictions
  - Obligations
- Un système est sûr si et seulement si le règlement ne peut être violé

Modèles de Sécurité

- La nature du règlement de sécurité définit la nature du modèle de sécurité
  - Modèle de Contrôle d'accès
  - Modèle de Contrôle des flux
  - Modèle de Contrôle d'usage

Modèle de Contrôle d'Accès

- Modèle fondé sur le paradigme sujet, action, objet
  - Sujet est une entité manipulant l'information au sein du système informatique
    - Utilisateur
    - Processus (programme en cours d'exécution)
  - Action est une action pouvant être réalisée au sein du système informatique
    - Lecture
    - Ecriture
    - Exécution …
  - Objet est une ressource du système informatique sur laquelle le sujet réalise une action
    - Fichier …

Modèle de Contrôle d'Accès

- L'objectif du modèle de contrôle d'accès est de contrôler tout accès direct des sujets aux objets via l'utilisation des actions
  - Le règlement correspond à un ensemble de 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

Modèle de Contrôle d'Accès

- Le modèle d'administration du modèle de contrôle d'accès utilise la 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

Modèle de Contrôle d'Accès

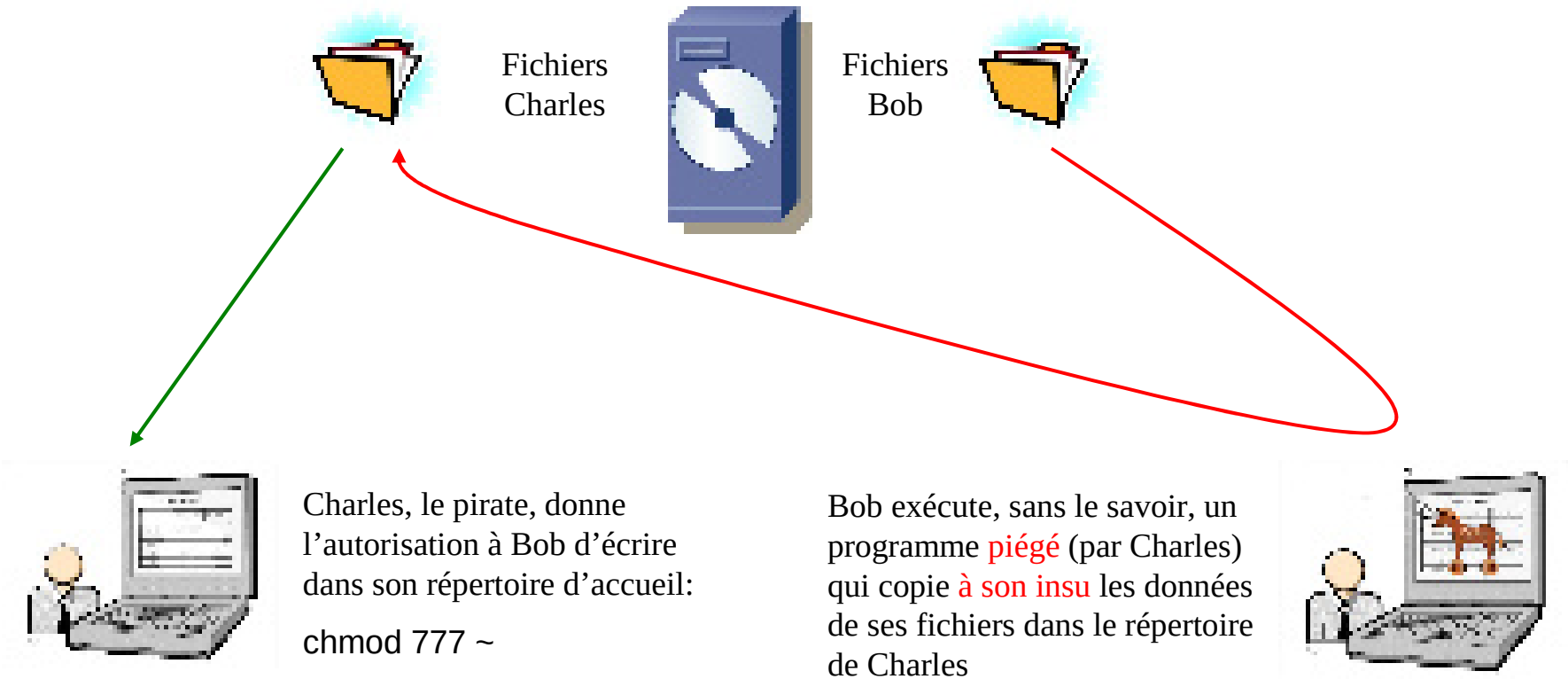
- Le modèle de contrôle d'accès a subi de nombreuses évolutions depuis sa première version …
  - Modèle HRU (Harrison Ruzzo et Ullman – 1976)
- … à sa dernière où les sujets sont organisés en rôles
  - Modèle RBAC (Sandhu - 1996)
- Il est implanté dans la plupart des systèmes informatique
  - Unix
  - Windows

Modèle de Contrôle d'Accès

- Les principaux avantages du modèle de contrôle d'accès sont
  - la simplicité
  - La souplesse
- Le principal défaut du modèle de contrôle d'accès est la vulnérabilité aux chevaux de Troie
  - Défaut aggravé par le fait que les systèmes informatiques sont maintenant tous interconnectés (Internet)

Modèle de Contrôle d'Accès

- Vulnérabilité aux chevaux de Troie.



Modèle de Contrôle de Flux

- Depuis 1975 on sait que le modèle de contrôle d'accès ne permet pas de prendre en compte les applications piégées par un cheval de Troie opérant par recopie de fichiers
  - Le modèle de contrôle des flux constitue une alternative au modèle de contrôle d'accès.

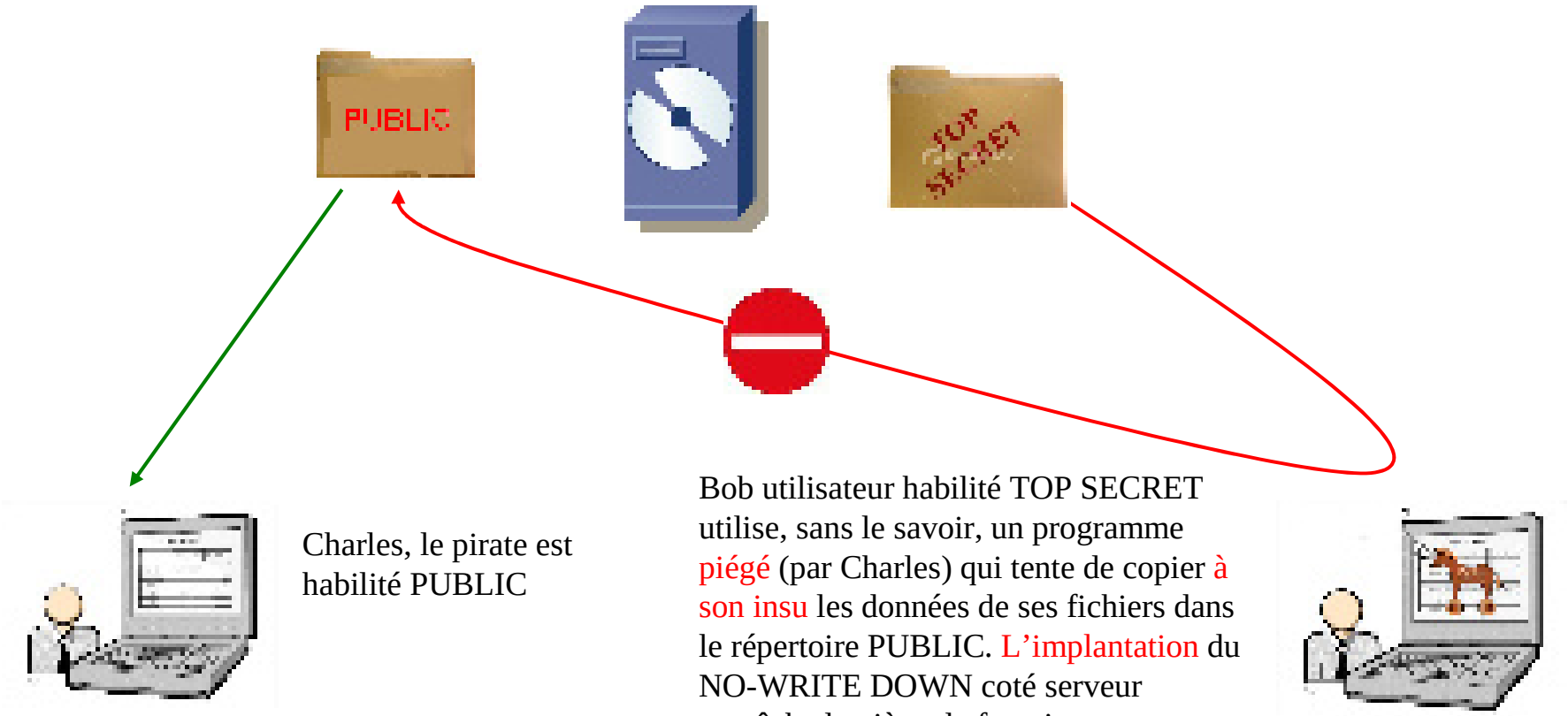
Modèle de Contrôle de Flux

- 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 a le droit de connaître une information *classifiée* P ou C mais n 'a pas le droit de connaître une information *classifiée* S.

Modèle de Contrôle de Flux

- 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.

Modèle de Contrôle de Flux



Charles, le pirate est habilité PUBLIC

Bob utilisateur habilité TOP SECRET utilise, sans le savoir, un programme piégé (par Charles) qui tente de copier à son insu les données de ses fichiers dans le répertoire PUBLIC. L'implantation du NO-WRITE DOWN coté serveur empêche le piège de fonctionner.

Modèle de Contrôle de Flux

- Le principal avantage du modèle de contrôle des flux est qu'il permet de lutter contre les chevaux de Troie opérant par recopie de fichiers
- Le principal désavantage de ce modèle est que le règlement est très rigide et le réserve à des applications militaires.

Modèle 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.
  - Le contrôle d'usage vise principalement (mais pas seulement) à contrôler la recopie des fichiers

Modèle de Contrôle d'Usage

- Le modèle de contrôle d'usage dont la première version est le modèle UCON (Park – Sandhu 2004) permet 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

Modèle de Contrôle d'Usage

- En général, l'implantation d'un règlement de contrôle d'usage se fait en utilisant des techniques DRM (Digital Right Management)
  - 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.

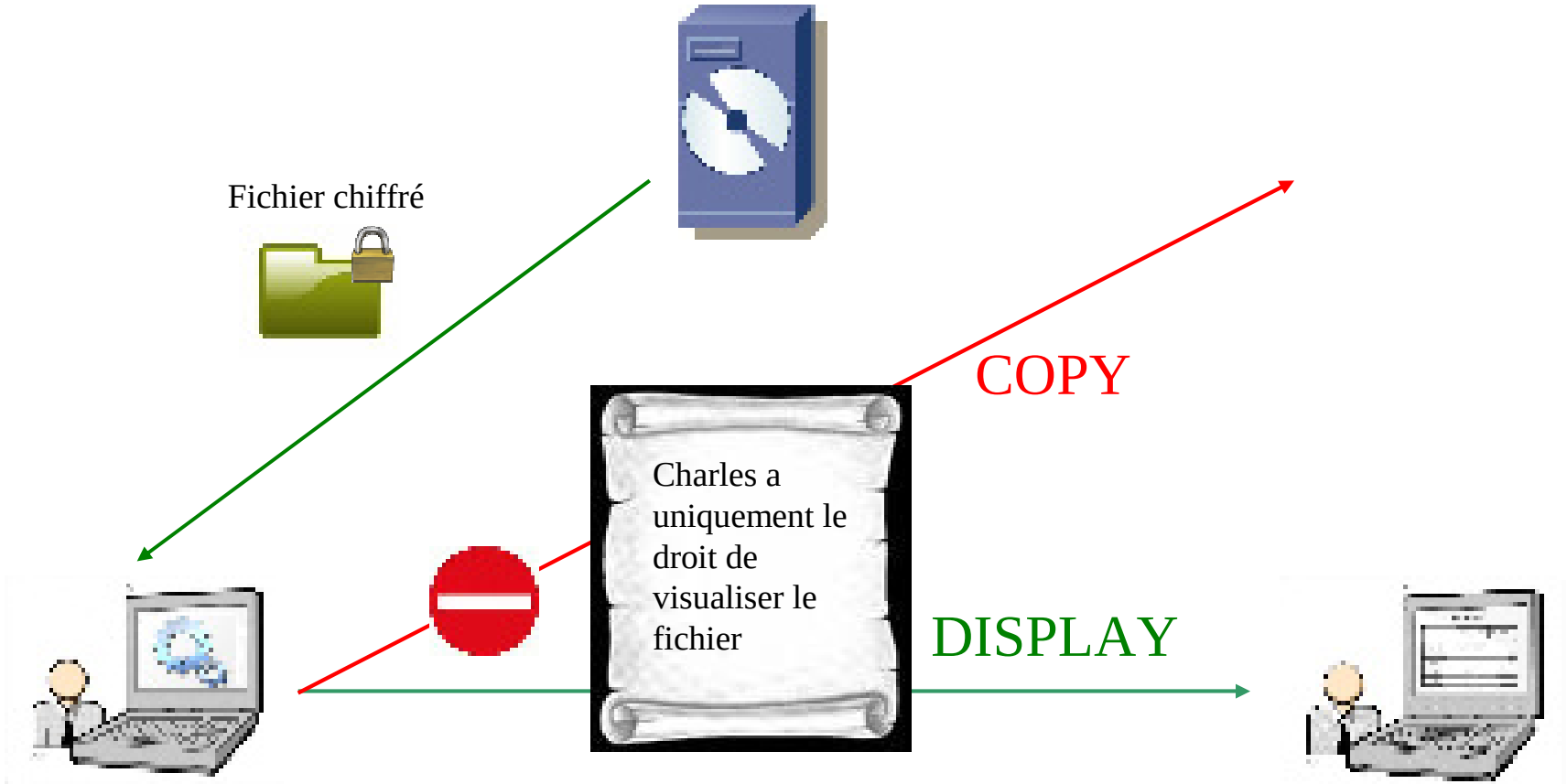
Modèle de Contrôle d'Usage

- La partie du logiciel client qui effectue les contrôles de sécurité (noyau de sécurité) est de confiance
  - Par définition, le noyau de sécurité ne peut être contourné et est dépourvu de
    - failles,
    - vulnérabilité,
    - cheval de Troie

Modèle de Contrôle d'Usage

- Les applications des DRM sont de plusieurs ordres
  - Protection des droits d'auteurs et des intérêts commerciaux des distributeurs de contenus multimédia (films, musique)
  - Cependant, de plus en plus, les DRM sont utilisées dans des applications dont l'objectif est de contrôler la distribution de contenus sensibles (Entreprise-DRM)

Modèle de Contrôle d'Usage



Le noyau de sécurité du client est de confiance et déchiffre le fichier

Le noyau de sécurité du client vérifie et implante le règlement d'usage

Le projet ANR FLUOR

- FLUOR (2007 – 2010)
  - convergence du contrôle de FLux et d'Usage dans les Organisations
  - Projet ANR SESUR 2007
    - ENST-Bretagne
    - UPF
    - Université de Pau
    - INRIA
    - CNRS

Le projet ANR FLUOR

- Financement pour l'UPF
  - 37000 euros / an sur 3 ans
  - 1 bourse de thèse sur 3 ans
    - Bénéficiaire: Léo Letouzey

Le projet ANR FLUOR

- Dans le cadre de FLUOR, nous travaillons sur deux thématiques:
  - La protection de l'information géographique
    - Voir présentation Patrick
  - Etude des signatures numériques déléguées – Application au modèle DRM
    - Voir présentation Léo