

# Contrôle d'accès



Yannick Chevalier  
Université de Toulouse  
CSA M1, Security



# PLAN

## PRINCIPES

### IDENTIFICATION ET AUTHENTIFICATION

### AUTHENTIFICATION

### CLASSIFICATION DES SUJETS

### CONFORMITÉ DES ACCÈS

### CONCLUSION

# SYSTÈME D'INFORMATION DÉCOMPOSÉ

## BUT

- ▶ recenser les **accès** possibles des sujets sur les objets (lire, écrire, ...)
- ▶ définir les possibilités d'**accès** des sujets aux composants

## CONTRÔLE D'ACCÈS

- ▶ authentifier les sujets pour s'assurer de leur niveau d'habilitation/d'assurance
- ▶ dire quel(s) niveaux d'habilitation/assurance permettent quels accès à quels objets
- ▶ assurer que les accès réels aux données sont conformes

# PLAN

PRINCIPES

IDENTIFICATION ET AUTHENTIFICATION

AUTHENTIFICATION

CLASSIFICATION DES SUJETS

CONFORMITÉ DES ACCÈS

CONCLUSION

# IDENTIFICATION

## RÉSUMÉ

ensemble des attributs définissant un sujet

## PLUSIEURS TYPES D'ATTRIBUTS POSSIBLES :

- ▶ attributs physique : empreintes digitales, de l'œil, de l'oreille, visage, etc.  
→ **biométrie**
- ▶ contexte d'exécution
- ▶ possession d'objets ou de connaissances

# IDENTIFICATION BIOMÉTRIQUE

## AVANTAGES

- ▶ liée à une personne physique
- ▶ pas de “délégation” de l’identité à un objet (clef, carte d’accès)
- ▶ ne nécessite pas de connaissances spéciales
- ▶ ne nécessite pas le consentement du sujet

## INCONVÉNIENTS

- ▶ certaines caractéristiques peuvent être copiées (soit pour tout le monde, soit pour une personne)
- ▶ lorsque c’est le cas, la personne ou le système doivent être désactivés de manière permanente
- ▶ ne nécessite pas le consentement du sujet

## EXEMPLE LIMITE DE BIOMÉTRIE

- ▶ remplacement des captchas par des mesures du mouvement de la souris pour identifier si l’utilisateur d’un site web est humain
- ▶ les paramètres sont gardés secrets pour qu’ils ne puissent pas être simulés par un programme

# IDENTIFICATION PAR LE CONTEXTE

## EN DEHORS DES SI :

- ▶ un homme a assisté gratuitement à plein d'événements en mettant un dossard jaune fluo
- ▶ **The Art of Deception** (K. Mitnick) : ingénierie sociale, source majeure d'attaque sur les SI
- ▶ morale : il faut l'éviter, et pour cela, il faut éduquer les humains utilisant le SI

## DANS LES SI :

- ▶ `/dev/securetty` : possible d'interdire le login de l'administrateur sur certaines consoles
- ▶ sous linux, possible d'ajouter certains groupes (voir plus loin) à des utilisateurs loggués à partir de certaines consoles

# IDENTIFICATION PAR POSSESSION

## PRINCIPE :

- ▶ on suppose que seul un sujet donné possède un certain objet ou une certaine connaissance
- ▶ cet objet ou cette connaissance permet d'identifier le sujet

## POSSESSION D'OBJET

- ▶ carte bleue, numéro **au dos**
- ▶ clef
- ▶ carte RSA (carte qui génère un code unique valable un court moment)

## POSSESSION DE CONNAISSANCE

- ▶ **mot de passe**
- ▶ certificat cryptographique
- ▶ captcha



# PLAN

PRINCIPES

IDENTIFICATION ET AUTHENTIFICATION

**AUTHENTIFICATION**

CLASSIFICATION DES SUJETS

CONFORMITÉ DES ACCÈS

CONCLUSION

# AUTHENTIFICATION

## AUTHENTIFICATION PAR UN COMPOSANT

- ▶ un mot de passe **identifie** un sujet
- ▶ quand un sujet se présente, on veut qu'il **prouve** son identité
- ▶ l'authentification par un composant consiste pour ce logiciel à obtenir une preuve de l'identité du sujet
- ▶ lorsqu'il y a un risque d'écoute, la preuve consiste en général en un protocole challenge/réponse

## CHALLENGE/RÉPONSE

- ▶ au cas où quelqu'un écouterai, ou veut une réponse différente à chaque fois que quelqu'un essaye de s'authentifier (re-jeu)
- ▶ challenge : nombre aléatoire
- ▶ réponse : construite à partir du mdp et du nombre aléatoire

# VARIATIONS SUR L'AUTHENTIFICATION

## AUTHENTIFICATION FÉDÉRÉE

- ▶ plusieurs SI indépendants se font confiance pour identifier leurs utilisateurs (Single Sign-On, OAuth)
- ▶ surtout sur le Web, login *via* Google ou Facebook, eduroam
- ▶ en dehors du Web, pour les réseaux de téléphonie (partage Free/Orange, à l'étranger)

## SAME SIGN-ON

plusieurs couples login/mot de passe permettent de se connecter au même compte (*e.g.*, Office 365)

## IMPACT SUR LA SÉCURITÉ

- ▶ Single Sign-On : les organisations ne sont plus les uniques responsables de leurs sujets
- ▶ Same Sign-On : identité partagée, donc ressources partagées dans le cloud

## NON-RÉPUDIATION

- ▶ pour l'authentification, le composant se fait confiance
- ▶ la preuve ne peut en général pas être présentée à un tiers qui n'a pas confiance en le composant
- ▶ lorsqu'il faut pouvoir garder la preuve d'un accès (pour des raisons légales) indépendante du composant, on parle de non-répudiation

# PLAN

PRINCIPES

IDENTIFICATION ET AUTHENTIFICATION

AUTHENTIFICATION

CLASSIFICATION DES SUJETS

CONFORMITÉ DES ACCÈS

CONCLUSION

# GROUPES

## DÉFINITION

un **groupe** est un ensemble de sujets.

## EXEMPLES (LINUX)

- ▶ groupes administratifs : root, sys, adm, etc.
- ▶ groupes liés à du matériel : video, audio cdrom, etc.
- ▶ groupes liés à une application :www-data, irc, mail, etc.

# RÔLES

## DÉFINITION

Un rôle est un sujet ou un ensemble de rôles

## CAS D'UTILISATIONS

- ▶ bases de données SQL
- ▶ applications Web

## INTÉRÊT

- ▶ permet de hiérarchiser les permissions
- ▶ adapter pour les systèmes complexes

# ATTRIBUTS

## DÉFINITION

Caractéristiques affectées à un sujet

## INTÉRÊT

- ▶ permet d'être plus agile qu'avec des rôles
- ▶ avec des attributs correspond à des permissions précises, il est plus facile de modifier ces permissions
- ▶ les capacités sous linux sont aussi utilisées pour réduire les permissions à celles réellement utiles (voir plus bas)



# PLAN

PRINCIPES

IDENTIFICATION ET AUTHENTIFICATION

AUTHENTIFICATION

CLASSIFICATION DES SUJETS

CONFORMITÉ DES ACCÈS

CONCLUSION

# PERMISSIONS SOUS UNIX

## CODAGE

- ▶ entier sur 4 chiffres en base 8
- ▶ convention C/Unix : les entiers en base 8 commencent par un 0
- ▶ donc une permission est un entier  $< 07777$
- ▶ les 0 en tête peuvent être enlevés
- ▶ les autres chiffres se lisent sous la forme  $1 + 2 + 4$
- ▶ ex : 5 contient 1 et 4, 3 contient 1 et 2, 0 ne contient rien, etc.

# 3 DERNIERS CHIFFRES

## LECTURE DES PERMISSIONS

- ▶ possesseur-groupe-autre
- ▶ lors d'un accès, on regarde les chiffre le plus précis, **pas le plus avantageux**

|       | fichier                   | répertoire   |
|-------|---------------------------|--|
| 4 (r) | lecture                   | lecture du contenu                                     |
| 2 (w) | écriture                  | ajout, suppression, ou renommage des fichiers contenus |
| 1 (x) | exécution comme programme | cd et recherche dans le répertoire                     |

# PREMIER CHIFFRE

NE PEUT ÊTRE ENLEVÉ QU'AVEC -

## 1/ $\pm$ T

- ▶ le droit d'écriture sur un répertoire permet d'ajouter ou d'enlever des fichiers dans ce répertoire
- ▶ `sticky bit` : un utilisateur ne peut enlever que les fichiers qu'il possède

## 2/ $G\pm S$

- ▶ quand un programme est lancé, il effectue des accès en ayant le même groupe que l'utilisateur ayant lancé le programme
- ▶ `setgid` : si le fichier est exécutable, lors du lancement, le programme fera des accès en ayant le groupe du fichier (pas du lanceur)

## 4/ $U\pm S$

- ▶ quand un programme est lancé, il effectue des accès en étant le même sujet que l'utilisateur ayant lancé le programme
- ▶ `setuid` si le fichier est exécutable, lors du lancement, le programme fera des accès en étant le possesseur du fichier (pas le lanceur)

# PLAN

PRINCIPES

IDENTIFICATION ET AUTHENTIFICATION

AUTHENTIFICATION

CLASSIFICATION DES SUJETS

CONFORMITÉ DES ACCÈS

CONCLUSION

# AU-DELÀ DES PERMISSIONS CLASSIQUES

- ▶ utilisation des ACL : plusieurs utilisateurs et groupes par fichier
- ▶ capacités : donner certaines permissions de root à des programmes sans `set(g,u)id root`
- ▶ attributs de fichiers (trusted) : plus de précisions sur les actions possibles sur un fichier