

RSX112

Sécurité des réseaux

Stéphane LARCHER

A photograph of a sailboat's deck during sunset. The sun is low on the horizon, casting a warm, golden glow over the scene. The sailboat's mast and boom are visible, with white sails partially unfurled. The deck is white, and various pieces of equipment, including a compass and a small electronic device, are visible. The ocean is visible in the background, with a calm surface reflecting the sunset light.

Autorisation
ACL ou capacité

ACL vs Capacité

Les ACL sont des listes qui spécifient les droits d'accès ou les permissions pour chaque utilisateur ou groupe d'utilisateurs par rapport à une ressource particulière, comme un fichier ou un dossier

Chaque entrée dans une ACL spécifie les sujets et leurs droits associés

Lire

Ecrire

Exécuter

Le contrôle d'accès basé sur les capacités utilise des "tokens" ou des "capacités" qui encapsulent les informations d'autorisation

Ces tokens sont attribués aux utilisateurs

Contiennent les droits d'accès que l'utilisateur a sur différentes ressources

Access Control List

Associées aux ressources

Chaque ressource a une ACL qui spécifie qui peut accéder à cette ressource et de quelle manière

Granularité fine

Les permissions peuvent être très détaillées, définissant exactement ce que chaque utilisateur ou groupe peut faire

Gestion centralisée

Dans les systèmes plus complexes, les ACL peuvent être gérées de manière centralisée par des administrateurs de sécurité

Capacité

Associé aux utilisateurs

Contrairement aux ACL où les permissions sont attachées aux ressources

dans les modèles basés sur les capacités

les permissions sont attachées à l'utilisateur ou à l'objet utilisateur

Flexibilité

Les capacités peuvent être facilement transmises entre utilisateurs permettant ainsi des délégations dynamiques des droits

Contrôle décentralisé

Ce modèle peut permettre un contrôle plus décentralisé car chaque utilisateur porte ses propres permissions sous forme de capacités

Systemes d'exploitation et Droits

ACL

Microsoft Windows :

Gérer les permissions détaillées sur les fichiers, les dossiers et les objets du registre

ACL très granulaires, permettant de spécifier des droits spécifiques pour différents utilisateurs et groupes

UNIX et variantes Linux :

Modèle de permission plus simple (propriétaire, groupe, autres)

Toutefois, des extensions comme POSIX ACL sont disponibles sur de nombreux systèmes Linux, comme Red Hat Enterprise Linux et Ubuntu

Contrôles d'accès plus détaillés similaires à ceux de Windows

macOS :

macOS, basé sur UNIX

ACL pour fournir des contrôles d'accès plus fins que le modèle de permission UNIX standard

Systemes d'exploitation et Droits

capacité

Systemes experimentaux et de recherche

CapROS

un descendant de EROS)

seL4 (un microkernel formellement vérifié)

Systemes sont conçus pour fournir une sécurité de haut niveau et une séparation formelle des privilèges

Systemes orientés sécurité

FreeBSD utilise une extension Capsicum.

Etend le noyau UNIX traditionnel avec un modèle de capacité pour permettre la sandboxing des applications

Limite les droits du programme à un ensemble minimal de ressources nécessaires à son fonctionnement

Google Fuchsia

Développé par Google

Modèle basé sur les capacités pour toutes ses interactions entre composants

Isolant les composants les uns des autres et réduisant ainsi la surface d'attaque

Authentication et Autorisation Microsoft



Introduction à la Méthode AGDLP

principe de gestion des droits d'accès aux ressources partagées,

- Basé sur les groupes de sécurité,
- Leurs étendues.
- **A**ccount (utilisateurs)
- **G**lobal (Groupes Globaux),
- **D**omaine **L**ocal (groupes du domaine local),
- **P**ermissions (autorisations attribués aux objets dossiers ou fichiers)

Pourquoi ?

Structurer correctement les accès,

Gestion simple et rapide des permissions à l'aide de groupes ,

Gain de temps pour les administrateurs systèmes,

Sécurité accrue.

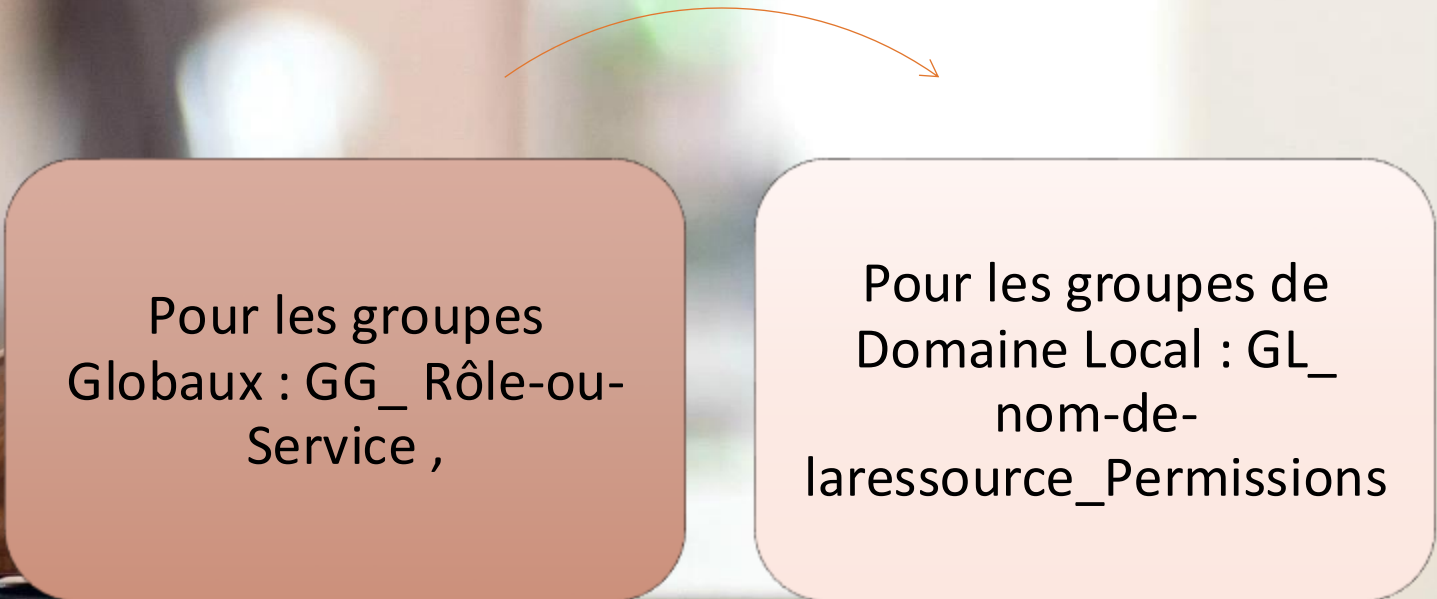
Etendues de groupes

Groupe de domaine local (GL)

Groupe global (GG)

Groupe universel (GU)

Dénomination des groupes



Pour les groupes
Globaux : GG_ Rôle-ou-
Service ,

Pour les groupes de
Domaine Local : GL_
nom-de-
laressource_Permissions

Exemple

Dans une entreprise, il existe un partage pour le service,

Direction qui contient des fichiers / dossiers sensibles. Il est bien évident que toute l'entreprise ne doit pas avoir accès à cette ressource mais seulement les membres de la Direction.

En revanche, il arrive fréquemment que le directeur, Mr Alain DUPONT, demande à une secrétaire, Mme Laura MARTIN, de relire certains de ses documents. Elle a donc aussi besoin d'un accès à ce partage mais seulement en lecture car le directeur ne veut pas que ses documents soient modifiés.

Exemple

2 utilisateurs

Alain DUPONT
Laura MARTIN

2 services différents

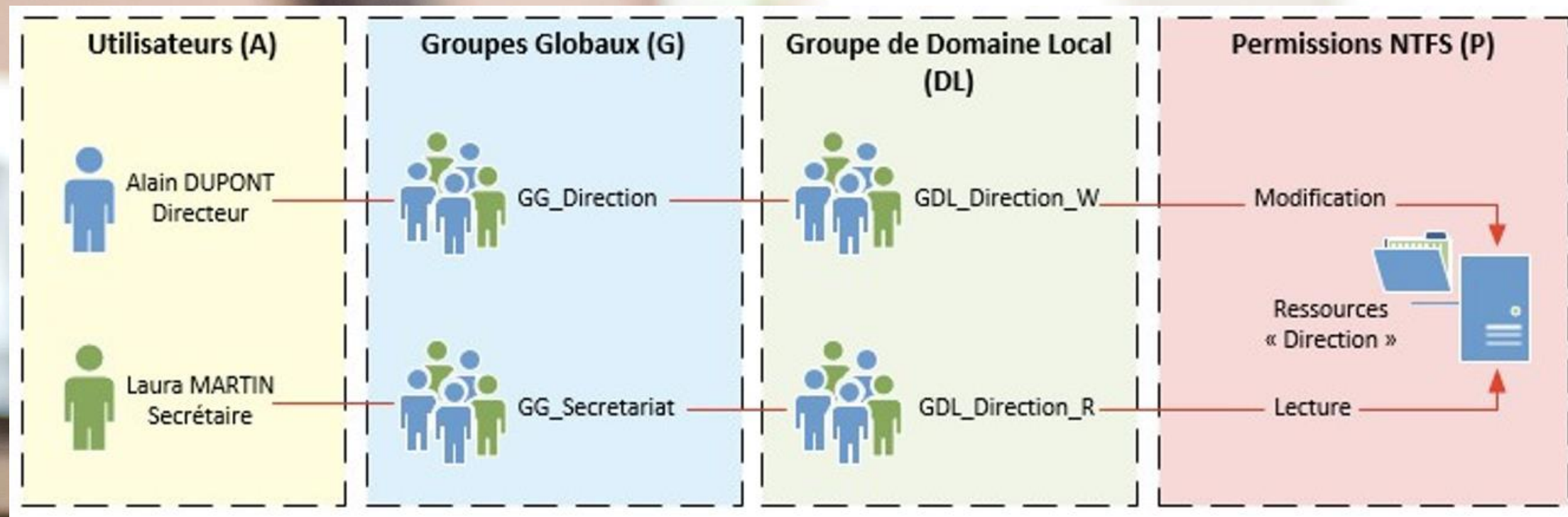
Direction et Secrétariat

1 répertoire accessible pour
les 2 services

partage « Direction »

1 accès en lecture/écriture
pour le service Direction

1 accès en lecture pour le
service Secrétariat



Exemple


Créer un (ou plusieurs) groupe de Domaine Local selon les droits (Lecture ou Ecriture)

Créer un (ou plusieurs) groupe Global (ou utilisé un groupe GG_x déjà existant) et l'ajouter au groupe de Domaine Local précédemment créé selon les droits nécessaires toujours


Créer la ressource sur le serveur de fichiers

Exemple

Attribuer les droits nécessaires au(x) groupe(s) de Domaine Local précédemment créé(s) correspondant à cette ressource



Aller dans l'onglet Partage et faire un partage « Avancé » de la ressource

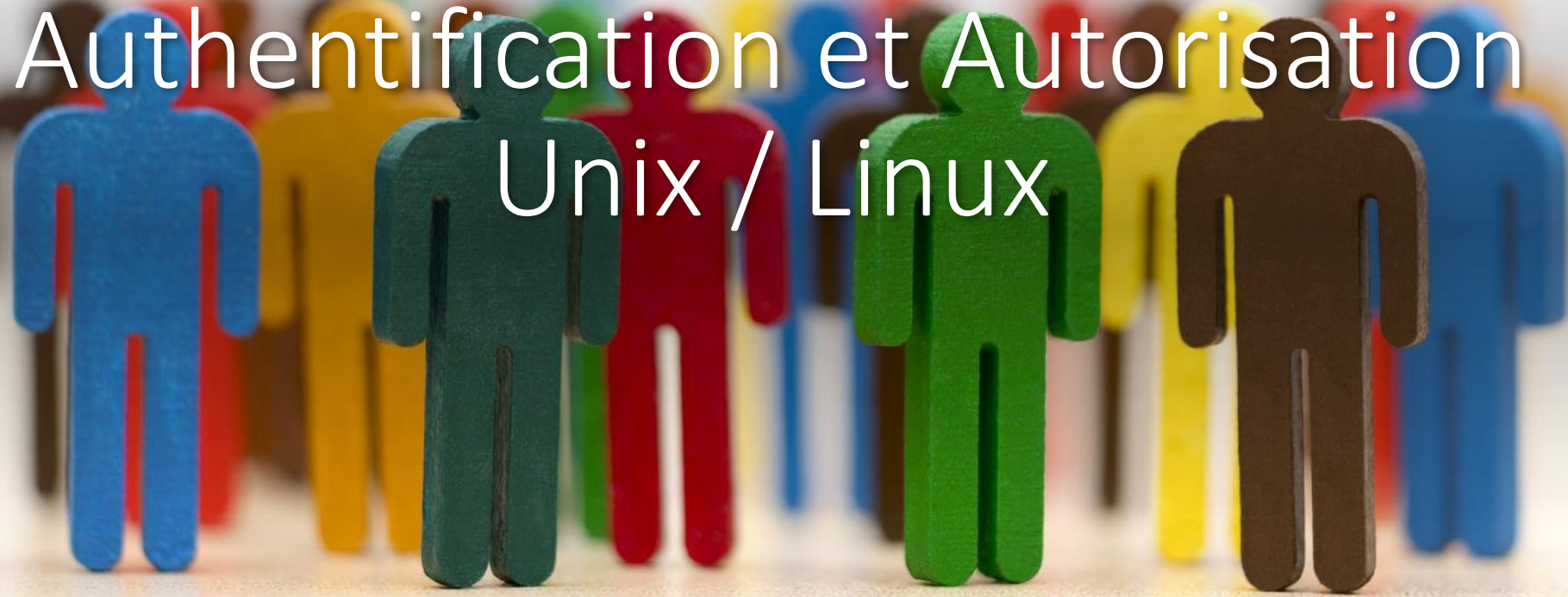


Aller dans « Autorisations » et donner les droits de Lecture et de Modification au groupe « Tout le monde » puis Valider pour terminer

AGDLP

« best practice »
lors de la mise en
place d'une
structure Active
Directory

Authentification et Autorisation Unix / Linux



Environnement Linux

Les droits d'accès

`rwX rwX rwX`

user

group

other

R

lecture

W

écriture

X

exécute

Environnement Linux

Les droits d'accès

Définition des permissions sur 3 bits en binaire

user
r(100) 4
w(010) 2
x(001) 1

group
r(100) 4
w(010) 2
x(001) 1

Other
r(100) 4
w(010) 2
x(001) 1

Environnement Linux

Les droits d'accès

- `r` (read) = 4
- `w` (write) = 2
- `x` (execute) = 1
- no permissions = 0

```
stephanelarcher@stephanelarcher-virtual-machine: ~  
stephanelarcher@stephanelarcher-virtual-machine:~$ ls -l  
total 16172  
drwxr-xr-x 2 stephanelarcher stephanelarcher 4096 nov. 4 22:55 Desktop  
drwxr-xr-x 3 stephanelarcher stephanelarcher 4096 nov. 4 23:17 Documents  
drwxr-xr-x 2 stephanelarcher stephanelarcher 4096 nov. 4 23:12 Downloads  
drwxr-xr-x 2 stephanelarcher stephanelarcher 4096 nov. 4 22:55 Music  
drwxr-xr-x 2 stephanelarcher stephanelarcher 4096 nov. 4 22:55 Pictures  
drwxr-xr-x 2 stephanelarcher stephanelarcher 4096 nov. 4 22:55 Public  
drwx----- 5 stephanelarcher stephanelarcher 4096 nov. 5 17:15 snap  
drwxr-xr-x 2 stephanelarcher stephanelarcher 4096 nov. 4 22:55 Templates  
-rw-rw-r-- 1 stephanelarcher stephanelarcher 16522081 mai 9 2022 terraform_0.12.24_linux_amd64.zip  
drwxr-xr-x 2 stephanelarcher stephanelarcher 4096 nov. 4 22:55 Videos  
stephanelarcher@stephanelarcher-virtual-machine:~$
```


Environnement Linux

Les droits d'accès

```
-rw-r--r-- 12 linuxize users 12.0K Apr  8 20:51 filename.txt
|[-][-][-]-  [-----] [---]
| | | | | | | |
| | | | | | | +-----> 7. Group
| | | | | | | +-----> 6. Owner
| | | | | | +-----> 5. Alternate Access Method
| | | | | +-----> 4. Others Permissions
| | | +-----> 3. Group Permissions
| | +-----> 2. Owner Permissions
| +-----> 1. File Type
```


```
login:password:UID:GID:comment:homedir:shell
```

- Champ 1 : le login ou nom d'utilisateur.
- Champ 2 : sur les vieilles versions, le mot de passe crypté. Actuellement, si un x est présent, le mot de passe est placé dans **/etc/shadow**. Si c'est un point d'exclamation, le compte est verrouillé.
- Champ 3 : le User ID.
- Champ 4 : le GID, c'est-à-dire le groupe principal.
- Champ 5 : un commentaire ou descriptif. C'est un champ d'information qui contient souvent le prénom et le nom de l'utilisateur, mais qui peut contenir autre chose.
- Champ 6 : le répertoire de travail, personnel, de l'utilisateur. C'est le répertoire dans lequel il arrive lorsqu'il se connecte.
- Champ 7 : le shell par défaut de l'utilisateur. Mais ce peut être toute autre commande, y compris une commande interdisant la connexion.

Le fichier **/etc/passwd** contient la liste des utilisateurs du système local. Il est lisible par tout le monde. Les informations qu'il contient sont publiques et utiles tant pour le système que pour les utilisateurs.

```
group:password:GID:user1,user2,...
```

- Champ 1 : le nom du groupe.
- Champ 2 : le mot de passe associé. Voyez l'explication ci-après.
- Champ 3 : le Group ID.
- Champ 4 : la liste des utilisateurs appartenant à ce groupe.



Le fichier **/etc/group** contient la définition des groupes d'utilisateurs et pour chacun, la liste des utilisateurs dont il est le groupe secondaire.


```
bean:$2a$10$AjADxPEfE5iUJcltzYA4w0Z0.f2UZ0qP/8En0FY.P.m10HifS7J8i:  
15141:0:99999:7:::
```

- Champ 1 : le login.
- Champ 2 : le mot de passé crypté. Le \$xx\$ initial indique le type de cryptage.
- Champ 3 : nombre de jours depuis le 1er janvier 1970 du dernier changement de mot de passe.
- Champ 4 : nombre de jours avant lesquels le mot de passe ne peut pas être changé (0 : il peut être changé n'importe quand).
- Champ 5 : nombre de jours après lesquels le mot de passe doit être changé.
- Champ 6 : nombre de jours avant l'expiration du mot de passe durant lesquels l'utilisateur doit être prévenu.
- Champ 7 : nombre de jours, après l'expiration du mot de passe, après lesquels le compte est désactivé.
- Champ 8 : nombre de jours depuis le 1er janvier 1970 à partir du moment où le compte a été désactivé.
- Champ 9 : réservé.

/etc/shadow :stockage, entre autres, des mots de passe cryptés des utilisateurs. Il contient toutes les informations sur les mots de passe et leur validité dans le temps.



```
groupe:password:admins:members
```

- Le mot de passe fonctionne comme ceux de shadow.
- Les administrateurs sont une liste d'utilisateurs (séparés par des virgules) qui ont le droit d'ajouter des membres au groupe ou de changer le mot de passe du groupe.
- Les membres sont les utilisateurs qui ont le droit d'utiliser ce groupe sans mot de passe.



Le fichier **/etc/gshadow** est le pendant du fichier précédent mais pour les groupes.

Droits Utilisateurs

- Identification d'un utilisateur :

- Le propriétaire du fichier, noté **user**.
- Le groupe d'appartenance du propriétaire, noté **group**.
- Les autres ou le reste du monde, noté **other**.

```
stephanelarcher@stephanelarcher-virtual-machine:~$ w
18:04:14 up 8 min,  1 user,  load average: 0,00, 0,16, 0,14
USER      TTY      FROM          LOGIN@  IDLE   JCPU   PCPU WHAT
stephane  tty2     tty2          17:56   8:01   0.05s  0.05s /usr/libexec/gnome-session-binary --session=ubuntu
stephanelarcher@stephanelarcher-virtual-machine:~$
```



Droits Utilisateurs

- Changement de propriétaire d'un fichier :

```
stephanelarcher@stephanelarcher-virtual-machine:~$ touch test.txt
stephanelarcher@stephanelarcher-virtual-machine:~$ ls -l
total 16172
drwxr-xr-x 2 stphanelarcher stphanelarcher 4096 nov. 4 22:55 Desktop
drwxr-xr-x 3 stphanelarcher stphanelarcher 4096 nov. 4 23:17 Documents
drwxr-xr-x 2 stphanelarcher stphanelarcher 4096 nov. 4 23:12 Downloads
drwxr-xr-x 2 stphanelarcher stphanelarcher 4096 nov. 4 22:55 Music
drwxr-xr-x 2 stphanelarcher stphanelarcher 4096 nov. 4 22:55 Pictures
drwxr-xr-x 2 stphanelarcher stphanelarcher 4096 nov. 4 22:55 Public
drwx----- 5 stphanelarcher stphanelarcher 4096 nov. 5 17:15 snap
drwxr-xr-x 2 stphanelarcher stphanelarcher 4096 nov. 4 22:55 Templates
-rw-rw-r-- 1 stphanelarcher stphanelarcher 16522081 mai 9 2022 terraform_0.12.24_linux_amd64.zip
-rw-rw-r-- 1 stphanelarcher stphanelarcher 0 nov. 23 18:00 test.txt
drwxr-xr-x 2 stphanelarcher stphanelarcher 4096 nov. 4 22:55 Videos
stephanelarcher@stephanelarcher-virtual-machine:~$
```

Droits Utilisateurs

- Changement de propriétaire d'un fichier :
 - Seul le propriétaire du fichier peut le faire.



```
stephanelarcher@stephanelarcher-virtual-machine:~$ sudo chown francksharko test.txt
[sudo] password for stephanelarcher:
stephanelarcher@stephanelarcher-virtual-machine:~$ ls -l
total 16172
drwxr-xr-x 2 stephanelarcher stephanelarcher 4096 nov. 4 22:55 Desktop
drwxr-xr-x 3 stephanelarcher stephanelarcher 4096 nov. 4 23:17 Documents
drwxr-xr-x 2 stephanelarcher stephanelarcher 4096 nov. 4 23:12 Downloads
drwxr-xr-x 2 stephanelarcher stephanelarcher 4096 nov. 4 22:55 Music
drwxr-xr-x 2 stephanelarcher stephanelarcher 4096 nov. 4 22:55 Pictures
drwxr-xr-x 2 stephanelarcher stephanelarcher 4096 nov. 4 22:55 Public
drwx----- 5 stephanelarcher stephanelarcher 4096 nov. 5 17:15 snap
drwxr-xr-x 2 stephanelarcher stephanelarcher 4096 nov. 4 22:55 Templates
-rw-rw-r-- 1 stephanelarcher stephanelarcher 16522081 mai 9 2022 terraform_0.12.24_linux_amd64.zip
-rw-rw-r-- 1 francksharko stephanelarcher 0 nov. 23 18:00 test.txt
drwxr-xr-x 2 stephanelarcher stephanelarcher 4096 nov. 4 22:55 Videos
stephanelarcher@stephanelarcher-virtual-machine:~$ sudo chgrp francksharko test.txt
stephanelarcher@stephanelarcher-virtual-machine:~$ ls -l
total 16172
drwxr-xr-x 2 stephanelarcher stephanelarcher 4096 nov. 4 22:55 Desktop
drwxr-xr-x 3 stephanelarcher stephanelarcher 4096 nov. 4 23:17 Documents
drwxr-xr-x 2 stephanelarcher stephanelarcher 4096 nov. 4 23:12 Downloads
drwxr-xr-x 2 stephanelarcher stephanelarcher 4096 nov. 4 22:55 Music
drwxr-xr-x 2 stephanelarcher stephanelarcher 4096 nov. 4 22:55 Pictures
drwxr-xr-x 2 stephanelarcher stephanelarcher 4096 nov. 4 22:55 Public
drwx----- 5 stephanelarcher stephanelarcher 4096 nov. 5 17:15 snap
drwxr-xr-x 2 stephanelarcher stephanelarcher 4096 nov. 4 22:55 Templates
-rw-rw-r-- 1 stephanelarcher stephanelarcher 16522081 mai 9 2022 terraform_0.12.24_linux_amd64.zip
-rw-rw-r-- 1 francksharko francksharko 0 nov. 23 18:00 test.txt
drwxr-xr-x 2 stephanelarcher stephanelarcher 4096 nov. 4 22:55 Videos
```

- /etc/default/useradd : règles par défaut



```
## Default values for useradd(8)
#
# The SHELL variable specifies the default login shell on your
# system.
# Similar to DSHELL in adduser. However, we use "sh" here because
# useradd is a low level utility and should be as general
# as possible
SHELL=/bin/sh
#
# The default group for users
# 100=users on Debian systems
# Same as USERS_GID in adduser
# This argument is used when the -n flag is specified.
# The default behavior (when -n and -g are not specified) is to create a
# primary user group with the same name as the user being added to the
# system.
# GROUP=100
#
# The default home directory. Same as DHOME for adduser
# HOME=/home
#
# The number of days after a password expires until the account
# is permanently disabled
# INACTIVE=-1
#
# The default expire date
# EXPIRE=
#
# The SKEL variable specifies the directory containing "skeletal" user
# files; in other words, files such as a sample .profile that will be
# copied to the new user's home directory when it is created.
# SKEL=/etc/skel
#
# Defines whether the mail spool should be created while
# creating the account
# CREATE_MAIL_SPOOL=yes
```


A close-up, grayscale image of a fingerprint. The ridges and valleys of the skin are clearly visible, creating a complex, wavy pattern. A red crosshair is overlaid on the center of the fingerprint, consisting of a vertical line and a horizontal line intersecting at the middle. The word "Authentication" is written in white, sans-serif font across the center of the image, partially overlapping the fingerprint and the crosshair.

Authentication

Authentification par mot de passe

Techniques de stockage : Hachage et Sel

Hachage

Pour sécuriser les mots de passe, on utilise des fonctions de hachage cryptographiques qui transforment le mot de passe en une chaîne de caractères fixe, appelée "hash"

Les fonctions de hachage sont conçues pour être à sens unique, ce qui signifie qu'il est pratiquement impossible de retrouver le mot de passe original à partir du hash

Sel

Un "sel" est une donnée aléatoire ajoutée au mot de passe avant son hachage

Ceci assure que même si deux utilisateurs ont le même mot de passe, leurs hash seront différents

Le sel aide à protéger contre les attaques par tables de hachage pré-calculées, appelées attaques par table arc-en-ciel

Authentification biométrique

Empreintes digitales

Utilise les motifs uniques des empreintes digitales pour identifier un utilisateur

Les capteurs d'empreintes digitales analysent les crêtes et les vallées des empreintes pour créer une image ou un modèle numérique

Reconnaissance de l'iris

Analyse les caractéristiques uniques de l'iris de l'œil

Les caméras spéciales captent les motifs complexes de l'iris pour les comparer à ceux enregistrés dans une base de données

Authentification par objet transporté

Jeton

Un jeton est un dispositif physique que l'utilisateur doit posséder pour s'authentifier

Il peut générer un mot de passe à usage unique ou contenir une clé cryptographique

Carte à puce

C'est une carte plastique avec une puce intégrée qui stocke et traite des données

Ces cartes peuvent nécessiter un code PIN pour l'accès et sont souvent utilisées pour l'authentification dans les systèmes bancaires ou les bâtiments sécurisés

Authentification forte à plusieurs facteur

L'authentification forte à plusieurs facteurs (MFA) combine deux ou plus des catégories suivantes pour sécuriser l'accès :

Quelque chose que vous connaissez

un mot de passe ou un code PIN

Quelque chose que vous avez

comme un jeton sécurisé ou une carte à puce

Quelque chose que vous êtes

identification biométrique comme les empreintes digitales ou la reconnaissance de l'iris

Modèles de sécurité hiérarchique



Modèles de Sécurité hiérarchique

Confidentialité

- Cryptage
- Contrôle d'accès
- Politiques de confidentialité
- Authentification multi-facteurs

Intégrité

- Contrôles d'intégrité
- Signatures numériques
- Journaux d'audit
- Hachage

Disponibilité

- Redondance
- Sauvegardes régulières
- Plan de reprise après sinistre
- Systèmes de détection et de prévention des intrusions

Modèles de Sécurité hiérarchique

Principes Fondamentaux du Modèle Bell-LaPadula

Principe du non-déclassement ("No read up" ou simple security property)

Un sujet à un certain niveau de sécurité ne peut pas lire des données classifiées à un niveau de sécurité supérieur
Par exemple, un utilisateur avec une autorisation de niveau "Confidentiel" ne peut pas lire des informations de niveau "Secret"

Principe du non-déclassification ("No write down" ou star property)

Un sujet à un certain niveau de sécurité ne peut pas écrire des données à un niveau de sécurité inférieur
Cela évite que des informations sensibles ne soient accidentellement ou malveillamment divulguées à des niveaux de sécurité inférieurs
Par exemple, un utilisateur avec une autorisation de niveau "Secret" ne peut pas écrire des informations dans un document de niveau "Confidentiel"

Propriété discrétionnaire de sécurité (Discretionary Security Property) :

Règles de contrôle d'accès discrétionnaires, comme des listes de contrôle d'accès (ACL), en complément des politiques de sécurité obligatoire

Confidentialité des données

Domaine militaire

Modèles de Sécurité hiérarchique

Modèle Bell-LaPadula

Structure Hiérarchique

Le modèle Bell-LaPadula est basé sur une hiérarchie de niveaux de classification de sécurité, tels que :

Non classifié
Confidentiel
Secret
Très Secret

Chaque utilisateur (sujet) et chaque donnée (objet) dans le système se voient attribuer un niveau de classification

Les sujets et les objets peuvent également avoir des ensembles de catégories (ou compartiments) qui définissent des domaines spécifiques de sensibilité des informations

Les décisions d'accès prennent en compte à la fois les niveaux de classification et les catégories

Modèles de Sécurité hiérarchique

Modèle Bell-LaPadula

Assignation des niveaux de sécurité :

Chaque utilisateur et chaque objet est étiqueté avec un niveau de sécurité et éventuellement des compartiments.
Par exemple, un document pourrait être étiqueté comme "Secret" et appartenir aux compartiments "Projet A" et "Projet B".

Contrôles d'accès :

Lorsque qu'un utilisateur (sujet) tente d'accéder à une ressource (objet), le système vérifie les niveaux de classification et les compartiments pour déterminer si l'accès est autorisé.
Par exemple, si un utilisateur avec une autorisation "Confidentiel" et les compartiments "Projet A" et "Projet C" tente d'accéder à un document "Secret" avec les compartiments "Projet A" et "Projet B", l'accès sera refusé en raison du principe "No read up".

Exécution des principes :

Les systèmes de sécurité mettent en œuvre des mécanismes pour garantir que les principes du modèle Bell-LaPadula sont respectés. Cela inclut des vérifications automatiques lors des tentatives d'accès et des politiques qui empêchent les utilisateurs de violer les règles "No read up" et "No write down".

Modèles de Sécurité hiérarchique

Modèle Bell-LaPadula

Avantages

Confidentialité renforcée

Assure que les informations sensibles ne peuvent être lues ou écrites par des utilisateurs non autorisés

Simplicité

Les règles sont claires et simples à comprendre et à implémenter.

Limites

Focus sur la confidentialité uniquement

Ne prend pas en compte d'autres aspects de la sécurité comme l'intégrité et la disponibilité

Rigidité

Peut être trop rigide pour des environnements non militaires où les flux d'information sont plus dynamiques

Complexité dans la gestion des catégories

Les catégories multiples et les compartiments peuvent devenir complexes à gérer.

Modèles de Sécurité hiérarchique

Modèle Biba

l'intégrité des données

Principe de non-lecture en bas ("No read down" ou simple integrity property)

Un sujet à un certain niveau d'intégrité ne peut pas lire des données à un niveau d'intégrité inférieur
Cela empêche la contamination de données intégrées par des données potentiellement moins fiables
Par exemple, un utilisateur avec un niveau d'intégrité "Haute" ne peut pas lire des informations à un niveau d'intégrité "Basse"

Principe de non-écriture en haut ("No write up" ou star integrity property)

Un sujet à un certain niveau d'intégrité ne peut pas écrire des données à un niveau d'intégrité supérieur
Cela empêche qu'un sujet à un niveau inférieur de compromettre l'intégrité des données à un niveau supérieur
Par exemple, un utilisateur avec un niveau d'intégrité "Basse" ne peut pas écrire des informations à un niveau d'intégrité "Haute"

Principe de non-invocation en bas ("No invocation down" ou invocation property)

Un sujet à un certain niveau d'intégrité ne peut pas invoquer (demander les services de) un sujet à un niveau d'intégrité inférieur
Cela garantit que les sujets à des niveaux plus élevés ne dépendent pas de sujets à des niveaux inférieurs, réduisant ainsi les risques de contamination

Modèles de Sécurité hiérarchique

Avantages et Limites

Avantages

Protection de l'intégrité

Le modèle est spécifiquement conçu pour protéger l'intégrité des données, ce qui est crucial pour les systèmes où la précision et la fiabilité des données sont essentielles

Simplicité conceptuelle

Les règles sont claires et directes, facilitant leur implémentation et compréhension

Limites

Focus unique

Le modèle Biba ne prend pas en compte la confidentialité, ce qui peut être une limitation dans des environnements nécessitant des protections multiples

Rigidité

Comme pour Bell-LaPadula, le modèle peut être trop rigide pour certains environnements dynamiques où les niveaux de sécurité et d'intégrité doivent être plus flexibles

Modèles de Sécurité hiérarchique

Comparaison avec Bell-LaPadula

Focus

Bell-LaPadula se concentre sur la confidentialité
protéger les informations sensibles contre la
lecture non autorisée

Biba se concentre sur l'intégrité
protéger les informations sensibles contre la
modification non autorisée

Règles d'accès

Bell-LaPadula

No read up (Simple security property)
No write down (Star property)

Biba

No read down (Simple integrity property)
No write up (Star integrity property)

Modèles de Sécurité hiérarchique

Modèle à Compartiments

- Pour la classification et la gestion des informations en fonction de leur sensibilité et de leur besoin de savoir
- Chaque compartiment représente un domaine de sensibilité distinct
- Sujets doivent avoir les autorisations nécessaires pour accéder à ces compartiments

Modèles de Sécurité hiérarchique

Exemple avec SELinux

Security-Enhanced Linux

Implémentation de la sécurité obligatoire (Mandatory Access Control, MAC) pour Linux. SELinux utilise des politiques de sécurité

Définir comment les processus et les utilisateurs peuvent interagir avec les objets du système

Les politiques peuvent être configurées pour implémenter des modèles comme Bell-LaPadula ou Biba

Exemple de Bell-LaPadula

Dans SELinux, une politique pourrait être configurée pour empêcher un utilisateur avec un niveau de confidentialité inférieur de lire des fichiers classifiés à un niveau supérieur

Exemple de Biba

Une politique pourrait empêcher un processus avec un niveau d'intégrité bas d'écrire dans des fichiers à un niveau d'intégrité supérieur

Modèles de Sécurité hiérarchique

Exemple avec Windows 10

Utilise des fonctionnalités de sécurité
Mandatory Integrity Control (MIC)
User Account Control (UAC)

MIC

Modèle Biba en empêchant les processus à faible intégrité de modifier des objets à haute intégrité

UAC

Ajoute une couche de sécurité en demandant des autorisations élevées pour certaines actions aidant à prévenir l'escalade de privilèges

Modèles de Sécurité hiérarchique

Politiques de Sécurité Discretionnaires

Discretionary Access Control, DAC

Propriétaire de l'objet (fichier, dossier, etc.) a le contrôle discrétionnaire sur qui peut accéder à l'objet

Les permissions peuvent être accordées ou révoquées par le propriétaire

Modèles de Sécurité hiérarchique

Politiques de Sécurité Obligatoires

Mandatory Access Control MAC

Contrôles d'accès sont gérés par des politiques de sécurité définies par l'administrateur du système non par les propriétaires des objets

Politiques basées sur des niveaux de sensibilité et des étiquettes de sécurité

Exemples :

SELinux

Utilise des politiques MAC pour contrôler l'accès aux objets du système en fonction de règles strictes définies par l'administrateur

Windows MIC

Utilise des niveaux d'intégrité pour appliquer des contrôles d'accès qui ne peuvent pas être modifiés par les utilisateurs ordinaires