Attaques cryptographiques

- Attaques sur l'implémentation souvent causées par la présence d'une des fautes mortelles en crypto :
  - Cryptographie propriétaire ou « maison »
  - Mauvais codage
  - Mauvaise gestion des clés en mémoire ou persistance des clés en mémoire (ex. attaque « cold boot »)
  - Mauvais génération de clé (ex. Debian OpenSSL)
  - Mauvaise source d'entropie dans le système
    - El-Gamal
    - Vecteur d'initialisation pour les algorithmes de flux
    - Challenge-response (à voir dans la section d'authentification)

Principe de gestion de clés

- Générations de clés
  - Nécessité de source de bit parfaitement aléatoire
  - Méthode matériel vs. logiciel vs. "manuel"
  - "Souveraineté" et contrôle sur la génération des clés
  - Difficulté technique pour certains algorithmes
    - RSA : *p* et *q* premier, etc.
    - El-Gamal : *p* t.q. *p*-1a un grand facteur, etc.
- Gestion des clés et réduction de risque
  - Possibilité de révocation
    - Distribution au préalable
    - Contrôle positif (détection de perte ou vol)
  - Mécanisme de protection
    - Contrôle d'accès
    - Chiffrement des clés par mot de passe ou phrase de passe
  - Principe de segmentation
    - Clés de réseaux vs. clés point-à-point
    - Durée de vie limitée des clés
- Distribution de clés
  - Nécessite de canaux privés dédiés
    - Distribution physique
    - Utilisation de KEK (key-encryption keys) ou équivalent

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Réductions de risque et principes de bases (« cheatsheet »)

- Souveraineté de clé
  - Entropie
  - Contrôle d'accès
- Principe de Kerchoff
  - Pas de « sécurité par obscurité »
- Professionalisme
  - Algorithmes
  - Protocoles
  - Implémentations
- Gestion de clés
  - Segmentation
    - Temps,
    - Systèmes/réseaux,
    - Niveau de classification
    - compartiment "verticaux"
  - Mécanismes de confiance (PKI)
    - Hiérarchique
    - Décentralisé
  - Révocation

POLYTECHNIQUE MONTRÉAL

UNIVERSITÉ D'INGÉNIERIE

INF4420: Éléments de Sécurité Informatique

Autorisation, contrôle d'accès

Contenu du cours

- Introduction au contrôle d'accès
- Contrôle d'accès sous LINUX
- Modèles DAC et MAC
- Modèle RBAC
- Modèle ABAC
- Introduction à l'IAM

Contrôle d'accès

- Contrôle d'accès
  - Définition : Fonction permettant de limiter l'accès à des ressources aux individus/machines/entités qui ont le droit d'accéder à ces ressources
  - S'applique autant à des objets physiques qu'à des ressources informatiques

Introduction au contrôle d'accès

- 4 Aspects
  - Identification : Déterminer l'identité du demandeur
  - Authentification : Validation de l'identité du demandeur
  - Autorisation : Validation du droit d'accès au ressources
  - Audit/(« Accounting ») : Attribution d'actions à une identité

  ➔ AAA (Authentication, Authorization and Accounting) ou IAAA
- Dans un système d'exploitation
  - Identification : nom d'usager, identificateur de processus (PID)
  - Authentification : commande d'authentification
  - Autorisation: matrice d'accès, contrôleur de référence
  - Audit : journaux (« logs »)

Introduction au contrôle d'accès

- Contrôleur de référence (« Reference Monitor »)
  - Composant qui s'interpose entre tous les accès de sujets à objets
  - Vérifie chaque demande d'entrée selon une procédure stricte
  - Maintient la sécurité au niveau voulu
  - S'implémente dans la noyau du système d'exploitation (OS)

  - Sujet = Utilisateur ou processus
  - Objet = Processus ou ressource (fichier)
  - Modes d'accès = { R-Read, W-Write, X-Execute }

  - Input: requête d'accès (sujet, objet, mode d'accès)
  - Output: Réponse (oui ou non) selon que l'accès est permis ou pas

Introduction au contrôle d'accès

- Matrice d'accès
  - Matrice qui liste les sujets (lignes) et objets (colonnes) dans un système, et les modes d'accès pour chaque (sujet, objet) (case de la matrice)

Sujet\Objet	File 1	File 2	Process 1	Process 2
Process 1	-	R	R,W,X	-
Process 2	-	X	R	R,W,X
User 1	R,X	W	-	R,X

  - Pour un ordinateur avec A sujets et B objets, la matrice d'access aura une taille de AxB. La majorité de cellules seront vides !

Introduction au contrôle d'accès

- Listes de contrôle d'accès (ACL)
  - Prendre chaque colonne de la matrice d'accès pour chaque sujet non-vide
  - Stocker la liste d'accès avec l'objet
  - Pour chaque accès à l'objet, le contrôleur de référence vérifie si le sujet a les droit requis

Sujet\Objet	File 1	File 2	Process 1	Process 2
Process 1	-	R	R,W,X	-
Process 2	-	X	R	R,W,X
User 1	R,X	W	-	R,X

Contrôle d'accès Linux

- Modèle de sécurité Linux
  - Toutes les ressources sont des objets (fichier, répertoire, mémoire, IO)
  - Chaque objet a un propriétaire
  - L'administrateur peut ajouter de nouveaux utilisateurs, lire et changer tous les objets, et changer les droit d'accès de tous les objets.
  - Les utilisateurs peuvent seulement accéder aux objets pour lesquels ils ont la permission, et peuvent seulement changer les droits d'accès des objets dont ils sont propriétaires
  - Les logiciels s'exécutent avec les droits de l'utilisateur qui a lancé le programme

Contrôle d'accès Linux

- Utilisateurs
  - User ID (UID) pour chaque utilisateur
  - UID 0 est réservé pour l'administrateur (root)
  - Les fichiers ont l'ID de l'utilisateur qui a créé le fichier
- Groupes
  - Group ID (GID)
  - Les utilisateurs ont un groupe principal
  - Les utilisateurs peuvent joindre d'autres groupes
  - Les fichiers ont le groupe principal de l'utilisateur qui a créé le fichier
- Utilisateurs et groupes ne sont pas des objets

Contrôle d'accès Linux

- Chaque fichier a un UID et GID assigné
- Chaque programme a un UID et GID assigné
- Avant d'exécuter un appel de fonction du système (« system call »), le contrôleur de référence vérifie :
  - Si UID = 0, permettre l'accès
  - Sinon, lire la liste de contrôle d'accès de l'objet et vérifier si l'accès est permis

Contrôle d'accès Linux

- Permissions de fichiers
  - R (lire)
  - W (écrire/changer)
  - X (Exécuter)
- Pour
  - U (Propriétaire)
  - G (Groupe)
  - O (Autres utilisateurs)

```
-rw-r----- 1 Emilie profs 7627  Oct 1 12:50 exam
-rw-rw-rw- 1 root   root  12987 Sep 7 19:34 /etc/passwd
```

Contrôle d'accès Linux

- Changement du propriétaire d'un objet
  - Commande chown
  - Exemple : chown patrick exam
    - Patrick devient le nouveau propriétaire du fichier exam
  - Seul l'administrateur root pour exécuter un chown

Contrôle d'accès Linux

- Changement des droits sur un objet
  - Commande chmod
  - Seul le propriétaire et l'administrateur peuvent changer les droits

  - Exemple : chmod u=rwx, g=rx, o=r myfile
  - Commande équivalente à : chmod 754 myfile
    - read = 4
    - write = 2
    - execute = 1
    - pas de permission = 0

  - Ajout de droit : chmod g+w myfile
  - Retrait de droit : chmod o-r myfile

Contrôle d'accès Linux

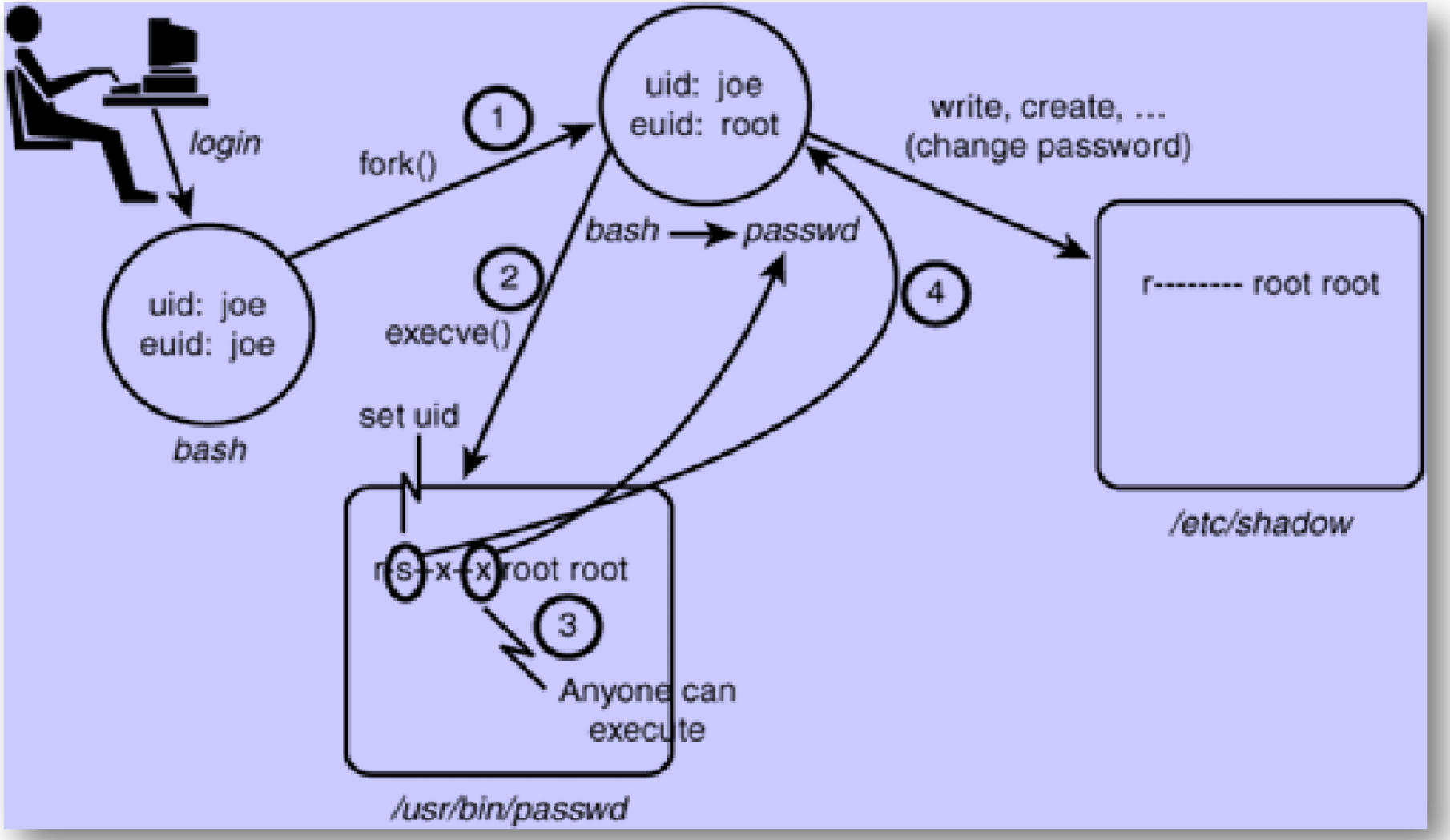
- Sticky bit
  - Pas d'effaçage du fichier
- setuid
  - Le programme s'exécute avec les permissions du propriétaire
  -
- setgid
  - Le programme s'exécute avec les permissions d'un utilisateur dans le groupe du propriétaire

Contrôle d'accès Linux

- Les mots de passe sur Linux se changent en utilisant la commande /usr/bin/passwd
- Les utilisateurs peuvent changer leur mot de passe
- Root peut changer le mot de passe de tous les utilisateurs

- Comment est-ce qu'un utilisateur peut changer son mot de passe sans permission d'écriture à /etc/shadow ?

Exemple setuid



Limites de DAC

- Linux utilise le Contrôle d'accès discrétionnaire (DAC)
  - Les utilisateurs peuvent changer les permissions de leur fichiers

  chmod 655 /home/david/declaration_impot_16

- DAC représente les droits sous forme de matrice

	Jean	Paul	Marie
File1	rw	r	w
File2	r	-	rw
File3	r	w	-

- DAC fonctionne correctement sous 2 conditions
  - **Si les usagers ne font pas d'erreurs**
  - **Si on peut faire confiance à tous les programmes**

  ➔ **Impossible !!!**

Limites du modèle DAC

- Exemple de matrice

	Dossier médical	Ordonnance
Médecin	RW	RW
Patient (Attaquant)	-	R