Comprendre le pourquoi pour améliorer le comment

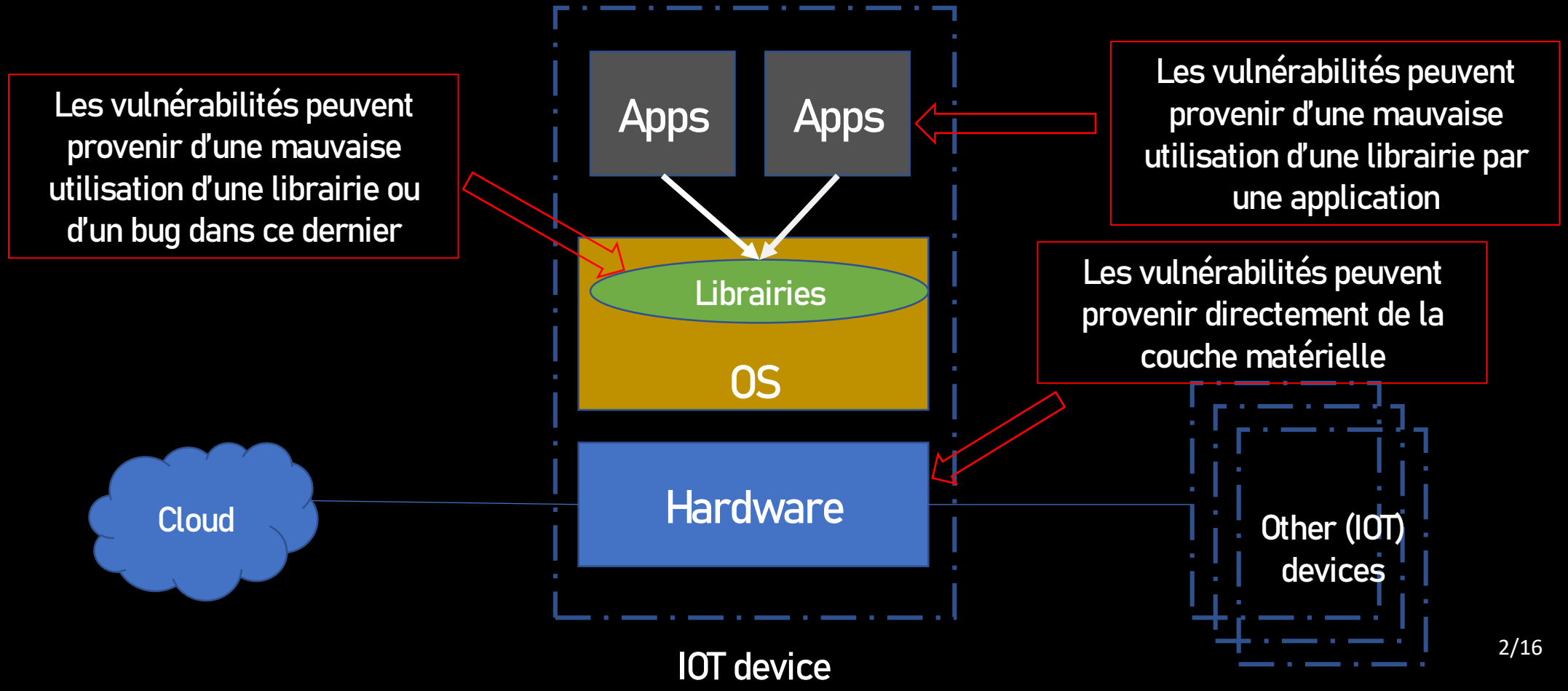
ESIR 2 – SRIO

Djob Mvondo

Rappel

Les failles peuvent intervenir à toutes les couches.

On le sait et vous aussi maintenant, mais **pourquoi y'a-t-il toujours autant de failles/attaques ?**



across the network and gained control over a super-admin account. From there, they were able to hijack control of the cameras to launch future attacks and access video footage stored on the cloud of Verkada's more than 24,000 client list.

Grand Theft Auto VI footage leaks, hacker threatens to spill more

St Ju

Even more t … to the FDA

found that S … ld deplete the

batte

Ma,

devi

enal

hacl

However, these systems are not exempt from IoT security breaches. In May 2019 research by **Applied Risk** (a cyber security firm) identif… 10 vulnerabilities in the Nortek Linear eMerge E3 devices that would allow hackers to hijack credentials, take control of devices (opening/locking doors), install malware, and launch DoS (Denial of Service) attacks all whilst circumventing the security measures in pl…

USA Today

Uber data breach: Employee apparently tricked into sharing credentials

La réalité

« Un système 100% sécurisé est un système fermé avec aucune **intervention humaine**. En gros, aucun système ☺ »

Djob Mvondo

Ceux qu’ils faudraient avoir en tête

Hacker

- White hat

Ceux qu’ils faudraient avoir en tête

Hacker

- White hat

- **Professionnelle**
- **Estime personnelle/communauté**
- **Bug Bounty**

Ceux qu'ils faudraient avoir en tête

Hacker

- White hat

- Black hat

Phisher

- Hameçonneur

Phreaker

- Telephonie

- Professionnelle
- Estime personnelle/communauté
- Bug Bounty

- Raisons économiques
- Politiques/idéologistes
- Désir personnelle (vengeance, contrôle)

Raisons des failles de sécurités

Bugs

- **Application mal developpé**
- **Design pas conforme aux cas d'utilisation**

Erreur humaine

- **Ingénieurie sociale**
- **Pas éduqué**

Prix

- **La sécurité coûte cher**
- **On préfère prendre le risque**

La sécurité utilisable

- Trop souvent, la sécurité **arrive en second plan** dans la conception alors qu'elle devrait faire partie de tout le processus.

- Les politiques de sécurité doivent considérer les **propriétés cognitives** de l'être humain.

- La politique de sécurité ne doit pas **reposer sur la bonne volonté des utilisateurs** et ne devrait pas demander un **effort** spéciale de leur part.

Carolyn Brodie et al. Usable security and privacy: a case study of developing privacy management tools. SOUPS'05

Y. Acar et al. A Research Agenda for Usable Security and Privacy Research Beyond End Users. SecDev'16

La sécurité utilisable

- Trop souvent, la sécurité **arriv** **se** **lan** dans la conception alors qu **devrai** processus.
- Les politiques **riétés cogniti**
- La politique de **se** pas **eposer sur la bonne volonté des utilisa** **urs** et ne devrait pas demander un **effort** spéciale de leur part.

Un vaste domaine de **recherche** très intéressant sur **l'intéraction homme machine**

Carolyn Brodie et al. Usable security and privacy: a case study of developing privacy management tools. SOUPS'05

Y. Acar et al. A Research Agenda for Usable Security and Privacy Research Beyond End Users. SecDev'16

La sécurité utilisable

Cas pratique: Les mots de passes

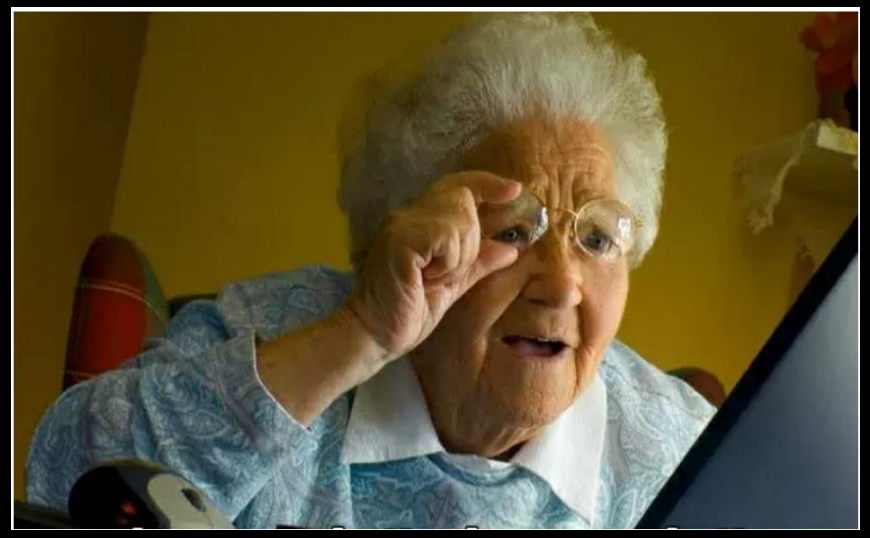
Recommandation classiques

Plus un mot de passe est long, plus il est sécurisé : visez 12 caractères ou plus. Pensez « phrase de passe » plutôt que « mot de passe » !

Utilisez un mélange aléatoire de lettres minuscules et majuscules, de chiffres et de caractères spéciaux.

Évitez : les informations personnelles (date de naissance, identifiant, nom d'une proche…), les suites de caractères du clavier (azerty, 12345), des mots du dictionnaire ou des paroles de chanson.

Une astuce est de créer des règles dont vous pourrez vous souvenir facilement. Par exemple, vous pouvez remplacer les caractères simples par des caractères spéciaux (remplacer a par @, s par $, o par 0…) ou soustraire 1 à chaque chiffre d'une date (ex : 20/06/1990 donne 19/95/0889), etc.



A votre avis, qu'est-ce qu'elle fera ?

La sécurité utilisable

Cas pratique: Les mots de passes --- quelques alternatives

Choisir une phrase que vous retiendrez facilement

Exemples :

Mon mot de passe est un secret bien gardé depuis 25 ans !
Le rire seul échappe à notre surveillance. Natalie Cliffort-Barney, 1920.
Le carré de l'hypoténuse est égal à la somme des carrés des 2 autres côtés.

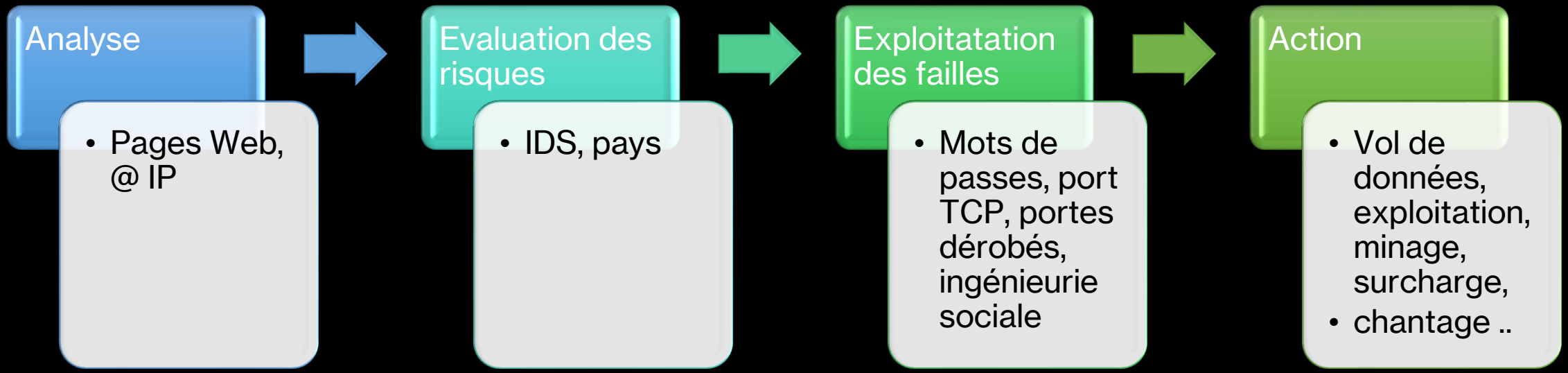
https://www.cnil.fr/

3D Ultra Violet Face authentification

Ultrasonic fingerprint authentification

Les étapes d'une attaque de sécurité

Quelles étapes si vous deviez vous introduire chez quelqu'un.e ?



Les principes de sécurité

Confidentialité

Un système ne doit pas être accessible par quelqu'un non-autorisé.

LLP --- Least Level Privilege --- Une entité ne doit posséder que les droits minimales pour ses opérations.

Intégrité

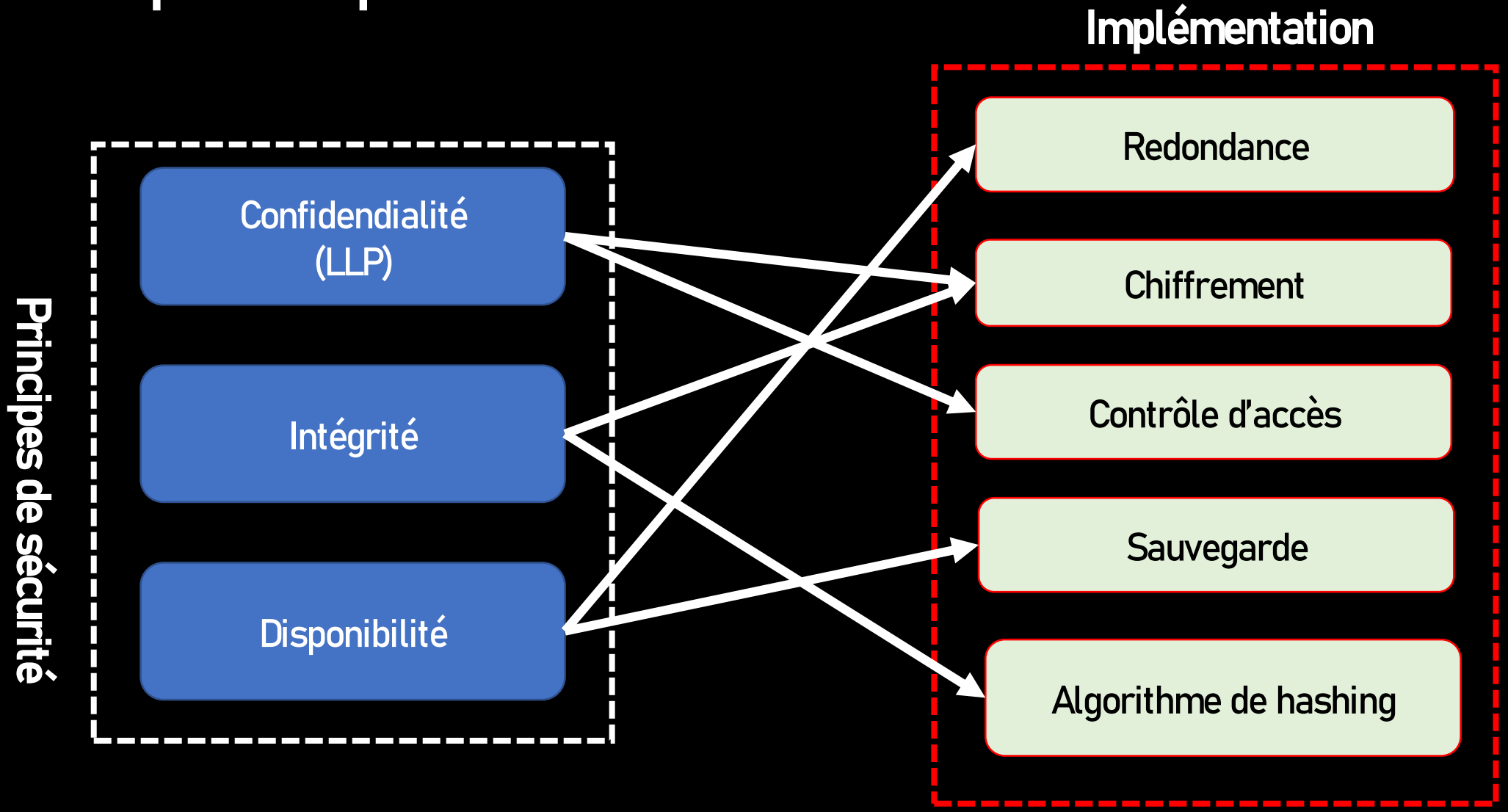
Lorsqu'on accède à une donnée, on doit avoir la certitude qu'elle n'a pas été altérée.

Disponibilité

Un système doit être disponible lorsqu'on en a besoin.

Aussi bien physiquement que virtuellement.

Les principes de sécurité



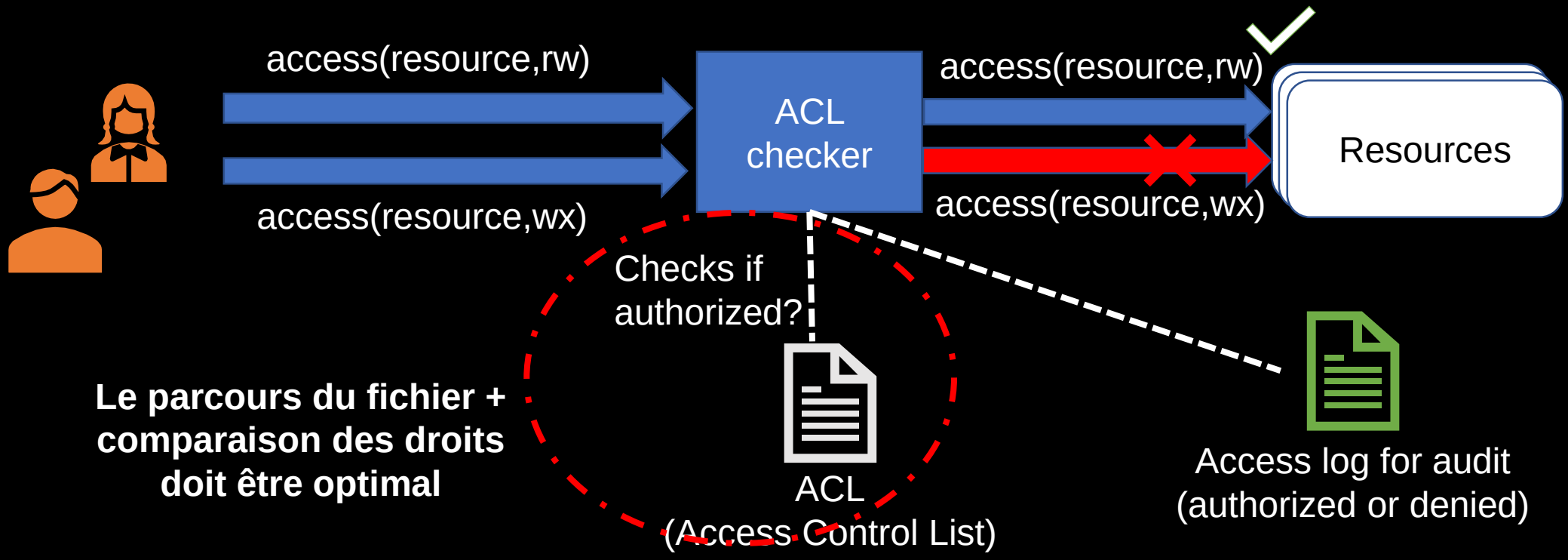
Essayons de faire correspondre

Contrôle d’accès

Le contrôle d’accès est un mécanisme qui permet de limiter l’accès à des ressources ou un système à des personnes autorisés. Elle est très efficace avec le principe du LLP.

Contrôle d’accès

Le contrôle d’accès est un mécanisme qui permet de limiter l’accès à des ressources ou un système à des personnes autorisés. Elle est très efficace avec le principe du LLP.



Le parcours du fichier + comparaison des droits doit être optimal

Contrôle d’accès

Le contrôle d’accès est un mécanisme qui permet de limiter l’accès à des ressources ou un système à des personnes autorisés. Elle est très efficace avec le principe du LLP.

Les noyaux des systèmes d’exploitations ex: Linux, offrent un socle solide pour la gestion du contrôle d’accès.

Devoir 3

1. Faîtes des recherches des failles et attaques subient par des entreprises/particuliers dû à l'ingénierie sociale. Choisissez en 3 où vous expliquez le procédé et donner votre avis sur comment cela aurait pu être éviter si possible.
2. D'après vous, quelle principe de sécurité vu en cours est le plus difficile à mettre en œuvre ? (Pas plus de 2000 mots).
3. Documenter vous sur la gestion des droits du noyau Linux et faîtes un résumé basique de ce qu'il permet de faire (Pas plus de 2000 mots).