# Mesures techniques : Contrôle d'accès

## M231 — Appliquer la protection et la sécurité des données

Jérôme Frosssard

EPAI

2 décembre 2023

# Plan

# Plan

# Protection des données et contrôle d'accès

Nous avons vu que la protection des données implique la mise en œuvre et l'application de :

- **Normes juridiques** : sur le plan national (LPD) et supranational (RGPD)
- **Mesures organisationnelles** : procédures, bonnes pratiques, formation, etc.
- **Mesures techniques** : contrôle d'accès, chiffrement, sauvegardes, etc.

Nous avons déjà abordé la question des normes juridiques et, au moins en partie, la question des mesures organisationnelles imposées par ces normes.

Nous allons maintenant nous concentrer sur les mesures techniques de sécurité informatique, et en particulier sur le **contrôle d'accès**.

# Qu'est-ce que le contrôle d'accès

Dans le cadre de la protection des données, le contrôle d'accès comprend l'ensemble des techniques qui permettent de **prévenir tout accès non autorisé** aux données personnelles. Le contrôle d'accès contribue à assurer la triade CIA de la sécurité informatique :

- **Confidentialité** : les données personnelles et en particulier les données sensibles ne doivent pas pouvoir être consultées par des personnes non autorisées.
- **Intégrité** : l'exactitude des données personnelles est un aspect important de la protection, il est donc important de prévenir toute modification non autorisée.
- **Disponibilité** : les données personnelles doivent pouvoir être consultées lorsque c'est nécessaire, cela n'est pas possible si ces données ont été rendues indisponibles par un acte malveillant, une erreur de manipulation, ou une panne matérielle.

# Contrôle d'accès logique et physique

Pour être en conformité avec le cadre légal de la protection des données (LPD, RGBD, etc.), il est nécessaire de mettre en œuvre un **contrôle des accès** :

- **Physiques :** pour l'accès aux sites, bâtiments, salles, armoires de serveurs, etc.
- **Logique :** pour l'accès aux systèmes informatiques.

Il est important de noter que l'efficacité du contrôle d'accès logique dépend largement du contrôle d'accès physique.

**Aucun contrôle d'accès logique ne résiste longtemps si un attaquant dispose d'un accès physique au matériel (serveur, ordinateur personnel, etc.).**

Même dans le cas d'un système qui verrouille ou détruit les données si une tentative d'effraction est détectée, la sécurité est néanmoins compromise dans le sens où les données ne sont alors plus **disponibles**.

# Contrôle d’accès — Activité

Pensez à la manière dont le contrôle d’accès physique est réalisé dans votre entreprise.

Pensez à d’autre situation dans lesquels il y a un contrôle d’accès.

Identifier les éléments clés du contrôle d’accès.

# Plan

# Composantes du contrôle d'accès

De manière générale, le contrôle d'accès repose sur quatre composantes essentielles :

- **L'identification :** Un individu décline son identité ; il dit qui il est.
- **L'authentification :** L'individu apporte une preuve de son identité, et cette preuve est reconnue comme étant valide.
- **Les autorisations :** L'individu n'a accès qu'aux parties du système pour lesquelles il dispose d'une autorisation.
- **L'audit (journalisation) :** Certaines activités de l'individu sont enregistrées pour la traçabilité, la conformité règlementaire, et l'analyse d'incident.

On peut remarquer que l'audit constitue une collecte de données personnelles et doit donc également se faire de manière conforme à la règlementation.

# Plan

# Utilisateur·rice et session

Un·e utilisateur·rice fait généralement référence à une personne physique qui interagit avec un système informatique. Un·e utilisateur·rice est identifiée dans le système informatique par un **identifiant**.

- Un·e même utilisateur·rice n'a pas nécessairement le même identifiant dans tous les systèmes qu'il ou elle utilise, et peut avoir différents identifiants dans un même système.
- Un identifiant correspond généralement à un **compte d'utilisateur·rice**, parfois appelé **profile**, qui contient souvent des informations pour l'authentification et pour les autorisations.

Les interactions entre un·e utilisateur·rice et un système informatique ont lieu durant une **session**. Une session **commence souvent par l'authentification** de l'utilisateur·rice par le système, mais ce n'est pas toujours le cas.

# Identification

L'identification consiste à décliner son **identité**, à dire qui l'on est à l'aide d'un **identifiant**.

Par exemple :

- À la réception d'un bâtiment sécurisé, on décline généralement son nom et prénom, et peut-être une adresse et un numéro de téléphone.
- Dans un système informatique, l'identifiant est souvent l'identifiant d'un compte utilisateur·rice ou une adresse de courriel.

**Un identifiant doit être unique**. Si deux individus ont le même identifiant, ils ne sont plus identifiables. Cela peut arriver dans le cas d'une **usurpation d'identité** ou d'une fâcheuse coïncidence.

L'identification est déclarative. Il ne suffit pas de prétendre être une personne autorisée pour avoir accès à des locaux sécurisés ou à un système informatique. **Il faut encore le prouver**.

# Authentification d'un individu inconnu du système

L'authentification consiste à fournir une **preuve** de son identité qui peut être **reconnue comme valide** par le système. L'authentification diffère selon que l'individu est déjà reconnu par le système ou non.

Pour les nouveaux utilisateurs, l'authentification nécessite généralement l'implication d'un **tiers de confiance** ; une tierce partie à laquelle tout le monde accorde sa confiance. Par exemple :

- Les **documents d'identité** (passeport, carte d'identité, etc.) sont délivrés par des instances officielles reconnues. Ces instances sont autant de tiers de confiance.
- Dans le monde numérique, le tiers de confiance peut être le fournisseur de notre **adresse de courriel**, ou l'**autorité de certification** du certificat qui l'accompagne.

La validité d'une preuve délivrée par un tiers de confiance repose sur le fait qu'elle soit **difficilement falsifiable**. Plus les enjeux sont grands, plus l'authenticité de la preuve nécessite un examen minutieux.

# Authentification d'un individu connu du système

Lorsque l'individu est connu du système, l'authentification est généralement réalisée à l'aide de preuves définies lors de son inscription dans le système.

Par exemple :

- Dans le monde physique, il peut s'agir, par exemple, d'une carte d'employé·e, d'un **badge d'accès**, d'un PIN, ou simplement d'une clé.
- Dans le monde numérique, il s'agit le plus souvent d'un **mot de passe** dont l'empreinte est stockée dans le système, d'une clé privée, d'un certificat, ou encore d'une carte à puce (p. ex. une carte SIM).

En cas de compromission, il est important que les preuves inscrites dans le système soient **faciles à révoquer**. Pour renforcer la sécurité, l'**authentification multifacteur** (MFA) exige la présentation de plusieurs preuves de types différents, réduisant ainsi le risque d'accès non autorisé si l'une des preuves est compromise.

# Authentification multifacteur — Activité

Lorsque vous vous connectez à moodle avec votre identifiant et votre mot de passe, vous êtes en principe invité à confirmer que vous êtes bien l'auteur de cette tentative de connexion à d'une application sur votre smartphone.

D'abord, seul·e durant 5 min, puis par groupe de trois ou quatre durant 10 min, cherchez à répondre aux questions suivantes :

- Quelles sont les preuves que vous avez fournies au système ?
- Qu'est-ce qui fait que ces preuves sont effectivement des preuves de votre identité ?
- Qu'est-ce qui caractérise chacune d'elles ?
- Existe-t-il d'autres sortes de preuves que ces deux-là ?
- Quels sont leurs avantages et inconvénients ?
- Pourquoi est-ce que l'utilisation de plusieurs sortes de preuve augmente la sécurité ?

# Facteur d'authentification

Un **facteur d'authentification** est une **sorte de preuve** qui peut être utilisée dans le processus d'authentification.

On peut distinguer au moins trois facteurs d'authentification :

- Quelque chose que l'on sait : un mot de passe, un PIN, un pattern, etc.
- Quelque chose que l'on a : un téléphone portable, un tocken OTP, une carte à puce, etc.
- Quelque chose que l'on est : une empreinte digitale, palmaire, rétinienne, etc.

Il en existe d'autres. Par exemple, « quelque chose que l'on sait faire » comme une signature

# Authentification multifacteur (MFA)

L'authentification multifacteur consiste à combiner plusieurs facteur d'authentification.

La combinaison la plus fréquente est :

- Quelque chose que l'on sait : un mot de passe
- Quelque chose que l'on a : un smartphone

Il est important qu'il ait deux facteurs d'authentification bien distincts.

Si toutes les preuves sont du même type (p. ex. quelque chose que l'on sait), un événement qui mène à la compromission de l'une a de forte chance de mener à la compromission des autres.

# Facteur biométrique

Un facteur biométrique n'est jamais le premier facteur d'authentification. Il est utilisé lorsqu'un haut niveau de sécurité est requis ou, de plus en plus, par commodité, par exemple, pour déverrouiller un téléphone portable.

Parmi les désavantages des facteurs biométriques, on peut mentionner :

- Impossible à changer : ils ne peuvent pas être changés s'ils sont compromis. Les facteurs biométriques qui laissent des traces comme les empreintes digitales ou la reconnaissance faciale ont plus de chance d'être compromis.
- Fiabilité : la reconnaissance faciale des personnes racisées est notoirement défaillante.
- Données sensibles : les empreintes biométriques sont des **données sensibles** qui doivent être traitées en conformité avec la réglementation.

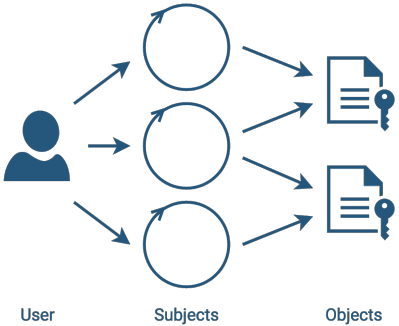
# Plan

# Utilsateur·rice, sujet et objet

Dans le contexte du contrôle d'accès, un **sujet (*subject*)** est un processus qui exécute un traitement pour un·e utilisateur·rice.

Un **objet (*object*)** est une ressource sur laquelle le traitement est appliqué. Par exemple, un fichier, une table dans une base de données, une imprimante, etc.

De manière générale, un·e utilisateur·rice agit toujours sur un objet par l'intermédiaire d'un sujet. Dans un système, il peut y avoir un grand nombre de sujets pour un·e même utilisateur·rice.



# Opération et permission

À la demande d'un·e utilisateur·rice, un sujet effectue des **opérations** telles que lire ou écrire sur un ou plusieurs objets.

Une opération réuissit si l'utilisateur·rice a la **permission** (ou le **privilège**) d'effectuer cette opération sur l'objet.

Parmi les techniques les plus commune de spécifier les permissions, on trouve notamment :

- Les **permissions POSIX** : permettent de définir les permissions *read*, *write*, et *execute* pour le propriétaire, le group propriétaire, et tous les autres utilisateur·rice·s.
- Les **listes de contrôle d'accès (ACL)** : permettent de définir une liste d'entité de sécurité (*principals*) telle que des utilisateur·rice·s, des groupes ou des ordinateurs avec, pour chacune d'elles, une liste de permissions.

Avec ces techniques, les permissions sont attachées aux l'objets.

# Problème de la modification des permissions

Avec des ACL ou des permissions POSIX, il est très facile de déterminer quelles utilisateur·rice·s ont accès à un objet particulier et avec quelles permissions.

En revanche, déterminer la liste des objets auxquels un·e utilisateur·rice a accès est une opération dont l'exécution peut prendre beaucoup de temps. En effet, elle implique de **parcourir la totalité des objets du système** et de lire les permissions de chacun d'eux.

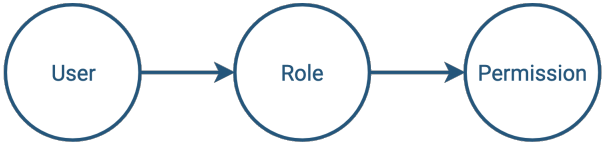
Dans le cadre de la protection des données, cela pose un sérieux problème lorsqu'il s'agit de modifier ou de supprimer les privilèges d'un·e utilisateur·rice.

# Utilisateur·rice et rôle

Une manière simple de résoudre ce problème est de partir du constat que même si les utilisateur·rice·s changent souvent, les permissions associées aux différents rôles que peuvent exercer ces utilisateur·rice·s dans l'organisation sont, elles, plutôt stables.

Dans une entreprise ou de manière générale dans une organisation, il y a bien des créations et des suppressions de postes (des rôles), celles-ci sont sans commune mesure avec les arrivées et les départs d'employé·e·s ou de membres.

L'idée est donc d'**associer les utilisateur·rice·s à des rôles** et les rôle aux objects avec des permissions appropriées. C'est le principe de base du **RBAC (*role based access control*)**.



# Attribution de permission par le propriétaire de l'objet

Par défaut, dans les systèmes Windows et POSIX, un objet a un·e propriétaire. Le ou la propriétaire d'un objet a généralement tous les privilèges sur cet objet et peut en attribuer à d'autres utilisateur·rice·s. C'est ce que l'on appelle contrôle d'accès discrétionnaire (***discretionary access control* ou DAC**).

Dans un contexte professionnel ou gouvernemental, le propriétaire d'un l'objet est en général l'organisation elle-même et pas l'utilisateur·rice, même s'il ou elle en est l'auteur. Si une réglementation impose l'application de ce principe, il est nécessaire d'implémenter un contrôle d'accès obligatoire (***madatory access contrôl* ou MAC**).

Pour cela, on doit généralement avoir recours à des systèmes tiers. Dans sa version standard, Windows Server ne permet pas ce type de contrôle d'accès. Sous Linux, des extensions de sécurité comme **Linux SE** ou **AppArmor** permettent de le faire, au moins dans une certaine mesure.

# Exemple de MAC

La forme originale du MAC définie pour les services de renseignement des USA dans les années 1970 est très restrictive. Chaque utilisateur·rice à un niveau d'accréditation, comparable à un rôle, et toutes les transactions doivent respecter deux règles :

- ***No read up*** : Pas d'accès en lecture à un objet dont le niveau d'accréditation est supérieur. Il n'est pas possible de lire un document « top secret » si votre niveau d'accréditation est « confidentiel ».
- ***No write down*** : Pas d'accès en écriture dans un objet dont le niveau d'accréditation est inférieur. Si vous écrivez ou modifiez un document, son niveau d'accréditation est automatiquement modifié pour correspondre au vôtre. Si votre niveau d'accréditation est « secret » et que vous modifiez un document confidentiel, alors le document devient « secret » et les utilisateurs·rice·s dont le niveau est « confidentiel » n'y ont plus accès.

Il faut des privilèges spéciaux pour modifier le niveau d'accréditation d'un document.

# Accès physique à un ordinateur — Activité

Un contrôle d'accès correctement implémenté permet d'éviter des accès non autorisé au données personnelles.

Est-ce que ces systèmes de contrôle d'accès peuvent protéger les données si un attaquant a un accès physique à la machine qui héberge les données ?

Que faut-il faire pour assurer la confidentialité des données dans un ordinateur personnel ?

À quel prix cette confidentialité est-elle préservée ?