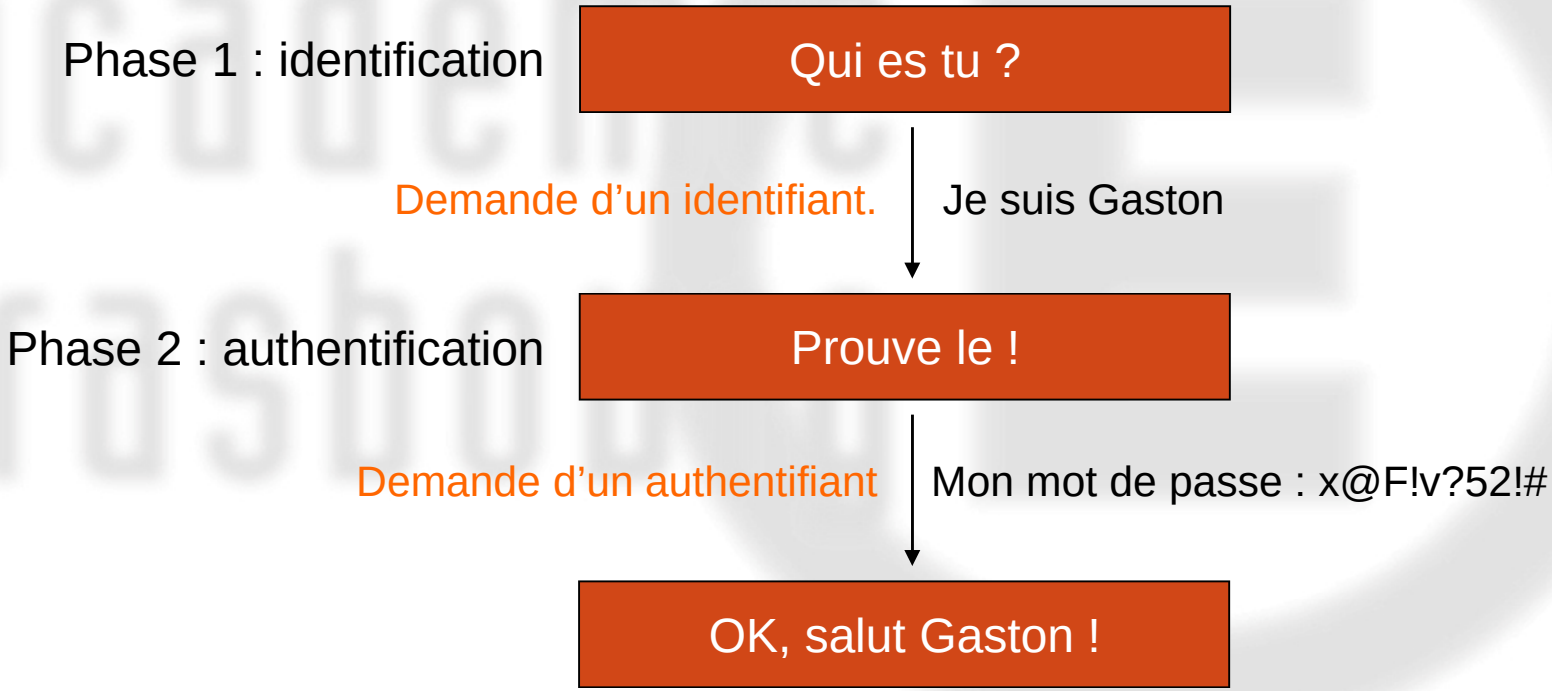
SSI
Identification et authentification

(Sécurité des systèmes d'information)

Sébastien Brière – RSSI

Les notions

« Lorsqu'un utilisateur veut accéder à un système d'information il doit dans un premier temps se confronter à un processus d'authentification »



S'authentifier c'est apporter la preuve de son identité.

Le mot de passe

Le mot de passe permet de réaliser l'authentification.

Les principaux risques liés au mot de passe sont :

Sa faiblesse

et

Sa divulgation

Le mot de passe

La faiblesse d'un mot de passe est une faille sérieuse.

La divulgation d'un mot de passe est considéré comme un incident grave de sécurité.

Elle est causée :

Par un acte de malveillance (hameçonnage, craquage, keylogueur, etc.).

Par action volontaire : « je prête mon mot de passe à mon collègue ou à mon responsable »

Le mot de passe

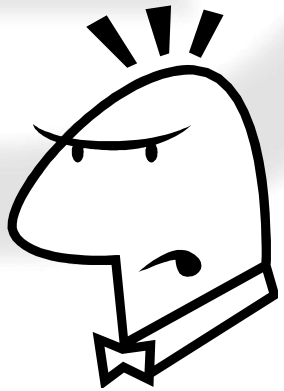
« Je prête mon mot de passe à mon collègue ou à mon responsable »

C’est illégal !!! Lorsque deux personnes ou plus connaissent le mot de passe correspondant à une identité d'utilisateur, il s'agit d'une infraction à la sécurité.

Pourquoi les utilisateurs communiquent sciemment leur mot de passe ?

Par méconnaissance des règles ou parce qu’on leur a mal expliqué.

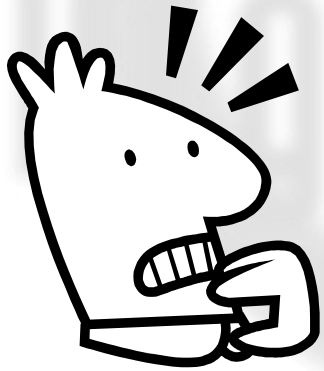
~~« Le mot de passe sert à donner un droit d’accès »~~



Le mot de passe

Le mot de passe ne permet pas de donner un droit d'accès.

Il permet uniquement d'assurer l'imputabilité dans l'usage de ces droits d'accès.



Il s’agit donc d’une donnée personnelle qui ne peut en aucun cas être partagée

Le mot de passe (conclusions)

La sécurité de l'accès s'appuie sur la robustesse du mot de passe et sur notre capacité à le garder secret.

Le mot de passe engage la responsabilité de son utilisateur.

Le prêt d'un authentifiant est strictement interdit.

Pour assimiler cela, les utilisateurs doivent être sensibilisés et formés.

La politique des mots de passe

L'administration remet à chaque utilisateur un identifiant et un authentifiant afin que chacun puisse engager ou désengager sa responsabilité.

L'authentifiant doit :

- **rester confidentiel et ne pas être accessible à proximité du poste de travail (post-it par exemple). L'utilisateur s'engage à le rendre inaccessible**
- **être changé dès la première utilisation**
- **être saisi par l'utilisateur lors de l'authentification et ne pas être préenregistré (comme cela est parfois proposé par les navigateurs internet)**
- **être renouvelé régulièrement (tous les 4 à 6 mois),**
- **comporter au moins 8 caractères formant une combinaison de caractères spéciaux et de lettres alphanumériques**

La politique des mots de passe

Les consignes et bonnes pratiques :

- **modifier son mot de passe en cas de doute sur sa confidentialité (après une attaque de type "Phishing" par exemple).**
- **signaler obligatoirement toutes difficultés ou risques éventuels liés à ces mots de passe à l'administrateur informatique local ou directement au RSSI.**
- **ne jamais communiquer ses mots de passe à quiconque, ni même aux administrateurs ou au RSSI.**
- **chercher à exploiter le même mot de passe par domaine restreint.**

Le mot de passe

Le mot de passe est t'il suffisant pour apporter la preuve d'une identité ?

Si j'annonce mon identité par téléphone et que mon interlocuteur me demande ma date de naissance pour m'authentifier, le suis-je vraiment si c'est la seule information utilisée et qu'elle est aisément récupérable (réseaux sociaux, etc.) ?