Authentifications et autorisations

Table des matières

1 Identification

S'identifier est simplement fournir son nom. Ici aucune preuve que le nom que j'annonce est bien le mien et quelqu'un peut facilement usurper l'identité d'une autre personne.
Une carte de fidélité sans photo par exemple ne fait qu'identifier son porteur, mais techniquement il n'est pas possible d'authentifier la personne.
Une carte d'identité ou un passeport permettent dans certaines limites d'authentifier la personne car la carte doit avoir certaines propriétés, notamment la présence de tous les dispositifs de sécurité empêchant sa reproduction par n'importe qui, et la photo du propriétaire de la carte d'identité ou du passeport.

2 Authentification

L'authentification est ce qui permet de s'assurer de l'identité d'un utilisateur. Pour cela il doit prouver qui il est. Pour cela plusieurs catégories de challenges existent : ce que je connais, ce que je possède ou ce que je suis.

2.1 Ce que je connais

La méthode la plus simple pour s'authentifier est l'utilisation d'un mot de passe. Ce mot de passe est stocké de façon sécurisée par le serveur quand l'utilisateur le choisi. L'empreinte sauvegardée est utilisée pour vérifier que l'utilisateur connaît le bon mot de passe.
Ce mot de passe peut être deviné s'il est trop simple, par exemple s'il s'agit d'une informations à propos de la personne, en relation avec son métier, ses occupations, ses proches… ou simplement dérivé d'un mot d'un dictionnaire.
Une extension est l'utilisation de mots de passe à usage unique. Le serveur donne à l'utilisateur une liste de mots de passe. L'utilisateur utilise à chaque fois le premier mot de passe de la liste qui n'a pas encore été utilisé. Même si un voleur capture un mot de passe sur le réseau, il ne pourra pas l'utiliser pour s'authentifier à la place de l'utilisateur.

2.2 Ce que je possède

Rapidement ont été utilisés des « tokens ». Les premiers se connectaient à un ordinateur et au moment de l'authentification un programme vérifiait la présence d'un token.
Ces tokens simples ne se distinguent pas les uns des autres et un tel token peut être utilisé par n'importe qui et notamment en cas de vol peut être utilisé par le voleur.
Sont ensuite apparus des token dynamiques nécessitant une interaction entre l'utilisateur et le token.
Sur les plus simples, lors de l'authentification l'utilisateur appuie sur un bouton du token qui affiche une valeur. Cette valeur est généralement calculée par le token à partir d'un secret qui a été configuré dans le token et de l'heure courante. L'utilisateur envoie au serveur la valeur affichée. Le serveur effectue le même calcul que le token et vérifie donc que le token utilisé correspond à celui confié à l'utilisateur identifié.
Avec ce token un voleur peut se faire passer pour l'utilisateur associé au token. Des tokens plus évolués sont apparus où l'utilisateur rentre un code pin (ce que je connais) via un clavier sur le token. Ici aussi le token génère une réponse en fonction secret configuré dans le token et de l'heure courante. Cette double authentification permet également d'authentifier simultanément l'utilisateur qui est le seul à connaître le code pin du token.

2.3 Ce que je suis

Un dernier type d'authentification correspond à toutes les authentifications biométriques. L'utilisateur est authentifié via les propriétés de certaines parties de son corps. La première a été les empreintes digitales, aujourd'hui relativement répandues notamment sur les ordinateurs portables et les smartphones. Malheureusement il a été montré que de nombreuses implémentations sont vulnérables à des faux positifs, par exemple dans une entreprise de plusieurs centaines de personnes quand l'empreinte est utilisée seule sans l'identité de son propriétaire, une personne non autorisée peut avoir une chance sur deux d'être reconnu comme une personne de l'entreprise. De plus certaines implémentations permettent facilement la

contrefaçon, une photo pouvant suffire à s'authentifier.
Une autre authentification biométrique est l'iris de l'oeil. Celle-ci possède une complexité accrue par rapport aux empreintes et sont beaucoup plus difficilement victimes de contrefaçons.
Dans le secteur de la recherche, d'autres possibilités sont les lobes des oreilles, la voix, les rythmes cardiaque et cérébral, etc.

2.4 Authentifications multiples

Il est possible de combiner plusieurs types d'authentification afin de minimiser les risques de faux positifs. Par exemple coupler la connaissance d'un mot de passe à la possession d'un token ou d'une caractéristique biométrique.

3 Autorisations

L'autorisation est l'opération consistant à vérifier que l'utilisateur précédemment authentifié est bien autorisé à effectuer la fonction demandée.
Un exemple simple est l'accès à un fichier. Lors de la demande d'accès, le système récupère l'identité de la personnes authentifiée et la liste des accès configurés sur le fichier. Si l'utilisateur est autorisé à accéder au fichier de la façon demandée (lecture et/ou écriture) alors la demande est acceptée, sinon elle est refusée.
La vérification des autorisations doit être systématique. Par exemple lors de l'accès à une fonction d'un programme, le programme doit vérifier que l'utilisateur est autorisé à accéder à cette fonction. Lors de l'accès à des données gérées par le programme, il doit vérifier que l'utilisateur a l'autorisation d'accéder à ces données.
L'autorisation et l'authentification sont des fonctionnalités complémentaires et aucune des deux ne peut être négligée pour assurer la sécurité d'un programme ou d'un système.