



# L'Authentification

## dossier

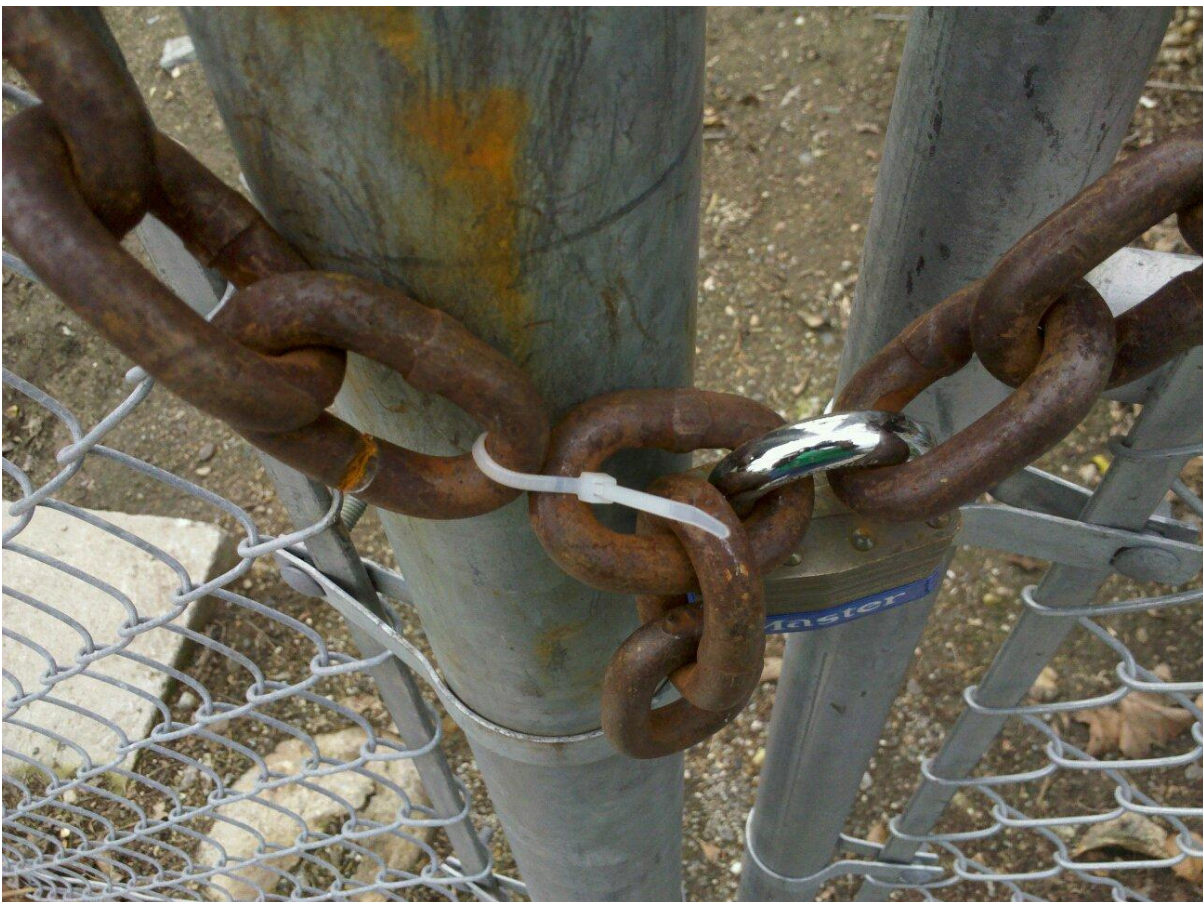
Pour plus de sécurité, adoptez les réflexes CASES !

### Introduction

Les humains ont une capacité innée à reconnaître leurs congénères, une grande partie de notre société repose sur cela. Ils possèdent un système d'identification très évolué à facteurs multiples comme l'apparence, la voix, la manière de parler, la posture, etc.

Cette habileté humaine est quelque chose qui manque cruellement aux ordinateurs. Bien qu'il existe certains systèmes automatisés de reconnaissance faciale, ceux-ci sont loin d'être au point et le secret partagé, c'est-à-dire le mot de passe, reste le facteur d'authentification prépondérant. C'est parce que les facteurs d'authentification sur machine sont si éloignés de nos facultés naturelles à reconnaître les personnes, qu'ils représentent souvent le maillon faible de la sécurité de l'information.

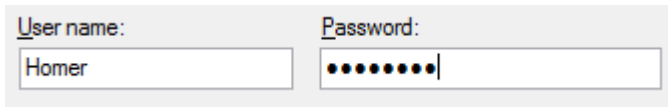
L'authentification est loin d'être une procédure prise au sérieux, elle est plutôt considérée par la plupart des gens comme un mal nécessaire. Pourtant, c'est souvent la seule protection que les utilisateurs ont face à l'utilisation frauduleuse de leur identité en ligne.



## Facteurs d'une authentification

Pour les authentifications sur ordinateur, différents facteurs d'identification ont été imaginés. Ces facteurs peuvent être classés en quatre catégories :

- quelque chose que vous savez (le mot de passe par exemple) ;



A screenshot of a login form. It has two input fields: 'User name' containing the text 'Homer' and 'Password' containing a series of black dots. The labels 'User name:' and 'Password:' are positioned above their respective fields.

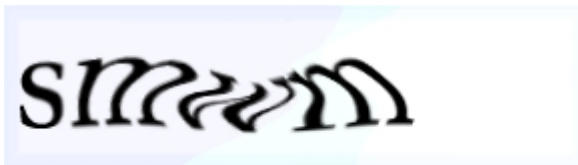
- quelque chose que vous possédez (une carte cryptographique dans votre porte-monnaie par exemple) ;



- quelque chose que vous êtes (votre empreinte digitale par exemple) ;



- quelque chose que vous savez faire (lire un mot déformé par exemple).



La quatrième catégorie n'est souvent prise en compte que pour différencier les humains des ordinateurs (les fameux champs « captcha », où l'on vous demande de recopier un mot), car la plupart des compétences humaines sont partagées par de larges groupes de la population et l'identification ne serait de ce fait pas univoque.

Si une authentification utilise au moins deux des trois premiers facteurs, on dit que c'est une authentification à facteur multiples. Plus il y a de facteurs supplémentaires, plus la sécurité de l'authentification devient grande. Plus l'intérêt d'attaquer un bien ou un service est grand, plus importants seront les efforts qui seront mis en œuvre pour y arriver. Pour cette raison, les différents services en ligne sont différemment sécurisés.

L'idéal serait évidemment de toujours utiliser des authentifications à facteurs multiples lors de tout accès identifié ; le facteur limitant ici est malheureusement le coût, l'accessibilité à la technologie et la mobilité de la solution. Peu de gens possèdent un lecteur d'empreintes digitales et moins encore sont prêts à le transporter pour pouvoir accéder à leur compte de n'importe où. Si Facebook avait utilisé ce genre d'authentification, Mark Zuckerberg, son fondateur, roulerait aujourd'hui en petite voiture et habiterait dans un minuscule studio.

C'est pour cette raison que la forme la plus répandue d'authentification se fait seulement à l'aide d'un mot de passe, c'est-à-dire un secret commun partagé entre l'utilisateur et l'ordinateur.

## Notion de risque

Vous l'avez compris, plus le service dispose d'une politique de sécurité sévère, plus il a du mal à être adopté. C'est pour ça que les authentifications à facteurs multiples sont réservées à des applications critiques, comme l'accès à votre compte en banque par exemple.

Pour les gestionnaires d'applications, comme pour l'utilisateur, il est nécessaire de procéder par analyse de risques (Quelle est la menace, quelle est la vulnérabilité et quel est l'impact potentiel lors d'une exploitation réussie).

### Premier cas : Services non critiques avec de nombreuses alternatives

Pour des applications non critiques ou dont les alternatives sont nombreuses (Facebook, Twitter, etc.) une authentification à facteurs multiples intimiderait les gens. Souvent ces applications sont des plateformes publicitaires et elles ont des revenus proportionnels à leur nombre d'utilisateurs. De ce fait, il faut instaurer une authentification minimale qui ne soit pas perçue comme une gêne par les usagers qui seraient, de fait, poussés à aller chez le concurrent. Les authentifications à facteurs multiples seraient même peu souhaitables, car souvent elles réduisent l'anonymat recherché (imaginez une entreprise posséder les empreintes digitales de ses millions d'utilisateurs).

Un vol d'identité dans le cas présent n'est généralement pas considéré comme une tragédie et ne représente pas de perte de renommée pour le gestionnaire. Les utilisateurs touchés, décident avec fatalité de changer leur mot de passe et continuent à utiliser le service.

Pour ces applications, la sécurité doit en partie être gérée par l'utilisateur. Il ne tient qu'à vous de choisir un mot de passe complexe, difficile à deviner, que vous changerez de temps à autre. Il est très important que vous ne réutilisez pas ce mot de passe pour d'autres sites, car vous ne pouvez pas faire confiance à la sécurité ou honnêteté du service en question.

Faites également attention à utiliser des communications chiffrées (Facebook et Twitter proposent ces services dans leurs options ; ajoutez le « s » à « http » pour en faire un « https »). Sans communication chiffrée votre mot de passe, aussi bon soit-il, n'est pas en sécurité puis qu'il est envoyé en clair.

### Deuxième cas : Services Critiques avec beaucoup ou peu d'alternatives

Nous nous retrouvons presque dans la même situation que précédemment, mais cette fois-ci le risque encouru est plus grand. Nous parlons ici de messageries électroniques par exemple. Les gens n'ont pas envie que d'autres personnes lisent leur courrier électronique. La perception de risque est ici bien moindre que la réalité du danger que représente un vol d'identité. Peu de gens prêtent attention au fait qu'ils s'inscrivent à tous les services en ligne à l'aide de leur adresse e-mail et que les liens d'oubli de mot de passe donnent un accès illimité à toutes les identités associées à une adresse.

Malheureusement peu de gestionnaires de messagerie vous donnent la possibilité d'une communication chiffrée et moins encore d'une authentification à deux facteurs (Gmail en est un exemple, mais l'option est bien cachée). Une amélioration de la sécurité dans cette catégorie serait la bienvenue. De fait, une simple carte contenant des codes à usages uniques, bien que facilement copiable, améliorerait significativement la sécurité et serait la bienvenue.

### Troisième cas : Indispensables et critiques avec peu d'alternatives

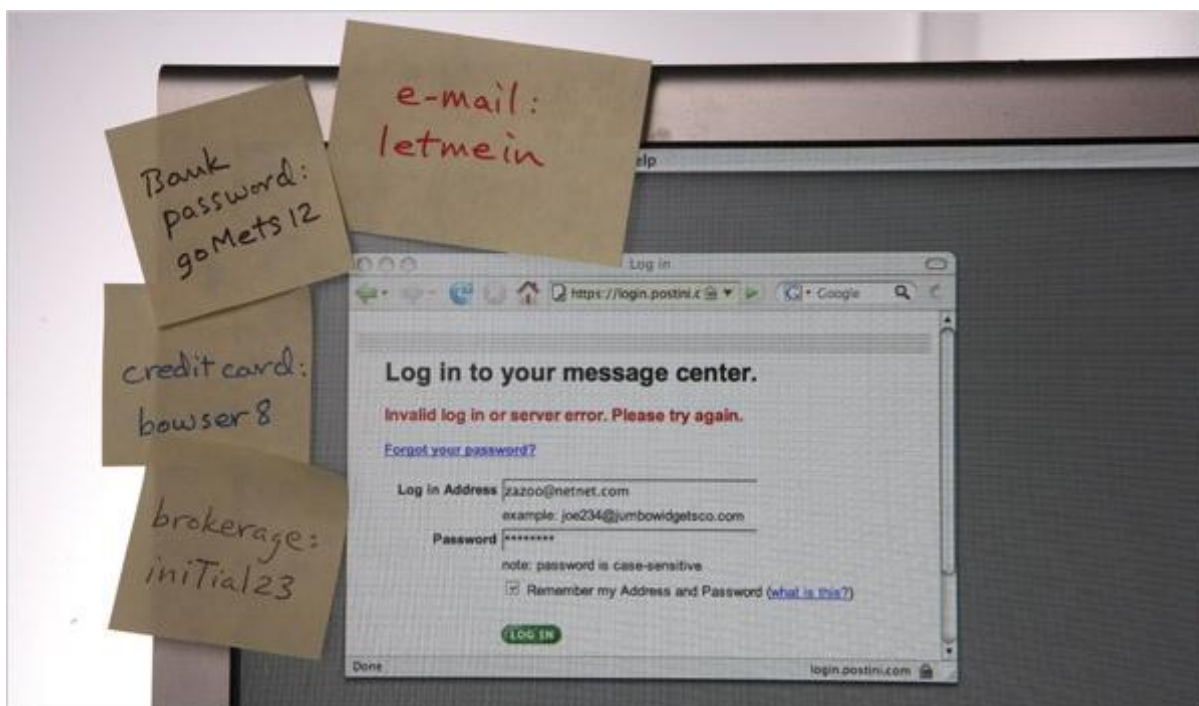
L'accès à votre compte en banque entre dans cette catégorie. Une vol d'identité serait ici désastreux et représenterait une perte de renommée pour le gestionnaire. Vu que les clients choisissent en premier leur banque et s'adaptent ensuite aux services en ligne qu'elle offre, le gestionnaire peut imposer des solutions

mieux adaptées aux risques qui se présentent. Le facteur limitant pour une institution comme une banque est que l'argent investi dans la solution de sécurité ne doit pas être supérieur à l'argent économisé en l'appliquant. Parmi les frais d'une solution de sécurité nous retrouvons non seulement le coût de la solution elle-même mais aussi les frais du support au client et les remboursements en cas de vol entre autres. Ce calcul ne prend malheureusement que rarement en compte la perte de renommée et la perte de confiance voire carrément le choc subi par le client. En effet, même si la probabilité d'un risque est infime, il peut quand-même survenir.

Toutes les banques luxembourgeoises utilisent heureusement une authentification à deux facteurs. Malheureusement le deuxième facteur est très souvent une tancard (carte à codes), qui peut être très facilement copiée (par une personne ou logiciel malveillant). Les solutions LuxTrust, qui sont des solutions sur base de procédés cryptographiques, dans l'état actuel de la science incassables, sont bien supérieures et devraient être privilégiées.

## Conclusion

La sécurité de vos données dépend principalement de la force de l'authentification nécessaire pour les protéger. Il faut que chacun décide du coût qu'il est prêt à payer pour cette sécurité. En général, ce coût sera le plus souvent une gêne supplémentaire pour l'utilisateur et si vous êtes assez soucieux de votre sécurité pour avoir lu ce document jusqu'au bout vous devriez être prêt à supporter cette gêne supplémentaire. Dans beaucoup d'autres domaines les humains sont prêts à subir ces gênes, comme par exemple l'attente à un feu avant de traverser la route. Tant que la sécurité de l'information ne sera pas ancrée dans nos us et coutumes nous serons condamnés à ceci :



Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

[www.cases.lu](http://www.cases.lu)