Nuit de l'info 2018 – Défi « Identifiez vous ! »

Intitulé du défi

La sécurité est un enjeu de plus en plus important dans le développement d'une application, quel que soit le support sur lequel elle est mise à disposition. Un élément central de cette sécurité est la manière dont les utilisateurs vont pouvoir s'authentifier.

L'utilisation d'un couple identifiant/mot de passe est historiquement le moyen de connexion le plus commun, mais il n'est pas pratique du point de vue des utilisateurs. En effet, pour être sécurisé il doit être d'une longueur et/ou d'une complexité importante, et ne doit pas être réutilisé sur plusieurs sites/applications.

Aujourd'hui, de nombreuses entreprises proposent des méthodes d'authentification plus simples mais pas forcément plus sûres (par exemple certaines formes de biométrie qui sont finalement faciles à duper) ou au contraire plus sûres mais moins pratiques (par exemple les authentifications à deux facteurs qui nécessitent de transporter un token physique).

A vous donc d'imaginer une nouvelle méthode (dans les limites du technologiquement réalisable), ou des améliorations à une méthode existante pour la rendre plus sécurisée et/ou plus pratique pour les utilisateurs.

Elle pourra être applicable à un site internet, à une app smartphone, ou au deux, et vous pourrez éventuellement proposer l'utilisation de périphériques externes ou de capteurs spécifiques (en restant toujours dans le domaine du réaliste).

Choix concernant notre réponse au défi

Pour répondre à ce défi, nous avons opté pour faire différentes études de cas plutôt que de développer une méthode précise.

Une méthode précise n'aurait en effet pas été intéressante car soit trop abstraite à spécifier et impossible à implémenter si trop originale ou technique, soit inintéressante à implémenter car trop simple et pas innovante.

Nous avons donc préféré décrire 12 méthodes d'authentification, avec leurs points forts et faibles (listes non exhaustives).

Table des matières

Toute l'équipe Fans2Petru vous souhaite une bonne lecture !

Login et mot de passe

Le login est toujours stocké en clair

Un mot de passe peut se décliner en plusieurs sous catégories :

En clair – Le mot de passe est stocké sans aucune protection dans la base de données

Point fort : Très simple à mettre en place (ne nécessite aucune mesure supplémentaire)

Point faible : Aucune protection, une simple attaque Man In The Middle suffit à compromettre le mot de passe

Chiffrement symétrique – Le mot de passe clair est transformé par une fonction mathématique en une chaîne de caractères n'ayant aucun sens apparent. Cette même fonction mathématique est utilisée sur la chaîne cryptée pour retrouver le mot de passe clair.

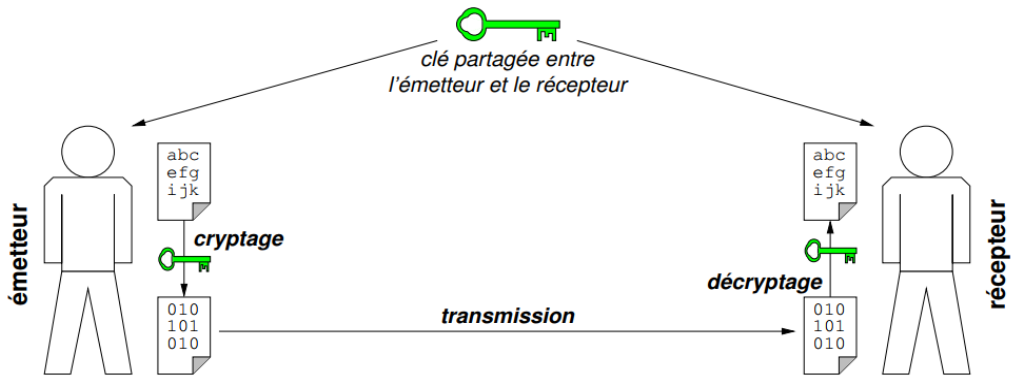

Figure 1 : Chiffrement symétrique (Original : Cyril Pain-Barre)

Point fort : Sécurisé car n'apparaissant pas en clair et protégé contre les attaques MITM récupérant le mot de passe.

Points faibles :

- Nécessité de protéger la clé de chiffrement
- Si la clé de chiffrement est capturée (par MITM par exemple), l'intégralité des mots de passe chiffrés est compromise.
- Il est possible de retrouver le mot de passe en effectuant une attaque par force brute, dictionnaire ou table arc-en-ciel

Chiffrement asymétrique – Même principe que pour le symétrique : le mot de passe est toujours transformé en une chaîne de caractère sans aucun sens apparent par une fonction mathématique. La principale différence réside justement dans cette clé de chiffrement. Il y en a en fait deux : une publique, permettant de chiffrer le mot de passe, et une privée permettant de déchiffrer la chaîne chiffrée.

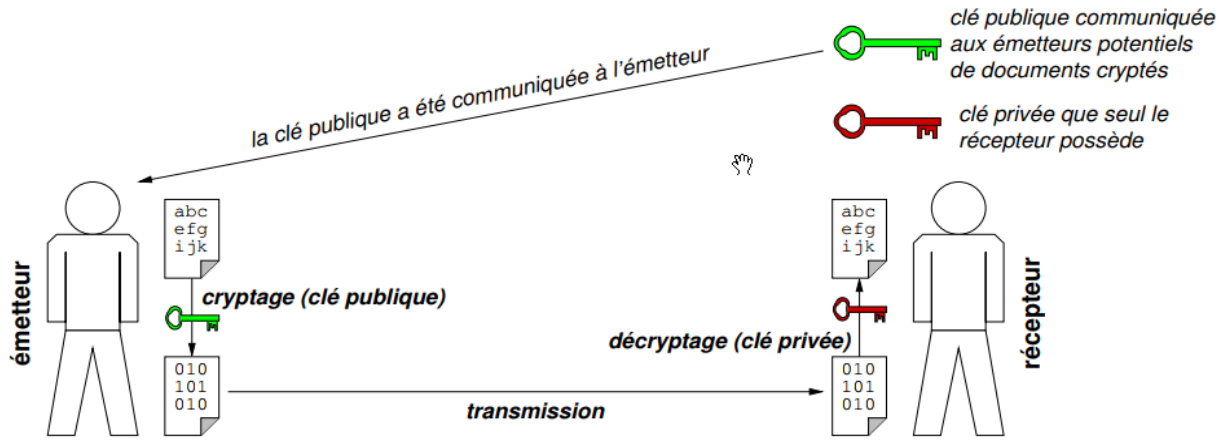

Figure 2 : Chiffrement asymétrique (Original : Cyril Pain-Barre)

Point fort : Sécurisé car n'apparaissant pas en clair et protégé contre les attaques MITM (peu importe ce qu'elle récupère)

Points faibles :

- Nécessité de protéger la clé de chiffrement
- Si la clé de chiffrement est capturée (par MITM par exemple), l'intégralité des mots de passe chiffrés est compromise.
- Il est possible de retrouver le mot de passe en effectuant une attaque par force brute, par dictionnaire ou table arc-en-ciel

Une idée d'amélioration est d'utiliser un chiffrement asymétrique pour établir l'échange de la clé de chiffrement symétrique, puis d'utiliser ladite clé symétrique pour communiquer, puisque l'utilisation d'une méthode symétrique est bien moins coûteuse en calcul. Cette amélioration est déjà implémentée par SSH2 par exemple.

Une autre idée peut être de découper les chaînes chiffrées et de les stocker dans des endroits différents, avec différents niveaux de permission pour accéder aux endroits où sont stockés ces morceaux de chaîne. C'est ce que fait Linux en stockant les mots de passes des utilisateurs : une partie de la chaîne dans un fichier *passwd*, l'autre partie dans le fichier *shadow*.

On peut également appliquer un salt (petit morceau de chaîne fixe) à une chaîne chiffrée pour l'obfusquer un peu plus. Linux applique également cette méthode au mot de passe chiffré de root par exemple.

Authentification à deux facteurs

Variante plus poussée de l'authentification par login/mot de passe, cette méthode nécessite également de posséder un jeton (ou token) sur un autre support, comme une carte électronique physique, une application mobile dédiée ou un SMS.

Points forts :

- Possède tous les avantages de l'utilisation de la méthode login/mot de passe
- Assure que si un attaquant compromet un support, il ne puisse rien faire s'il ne possède pas l'autre (exemple : si l'attaquant à le contrôle du PC de la cible, il lui faut aussi le contrôle du téléphone de la cible pour usurper son identité)

Points faibles :

- Plus contraignant pour l'utilisateur (une étape de plus, qui plus est sur un support différent)
- Plus compliqué à mettre en place
- Toutes les authentifications à deux facteurs ne sont pas forcément sûres. Par exemple l'utilisation d'un SMS est dépréciée par le National Institute of Standards and Technology (NIST) dans *Special Publication 800-63-3: Digital Authentication Guidelines* car trop vulnérable aux attaques réseau et aux malwares type Eurograbber capable de rediriger les SMS.

Idée d'amélioration : Authentification à trois facteurs, en ajoutant par exemple la localisation du téléphone de l'utilisateur.

Empreinte digitale

Les empreintes digitales d'un individu lui sont propres, et sont un moyen bien plus sûr d'identifier une personne, car si plusieurs personnes peuvent retenir un mot de passe, les empreintes sont uniques.

Le système consiste donc simplement en trois étapes :

- Utilisation d'un capteur pour relever l'empreinte de l'utilisateur
- Une carte de traitement converti l'empreinte en données numériques
- Une base de données stocke les données des empreintes et compare avec l'empreinte lue par le capteur

Points forts :

- Identifie de manière bien plus sûre un utilisateur par rapport à la méthode login/mot de passe
- Aucun effort mémoriel de la part de l'utilisateur
- Système rapide et intuitif

Points faibles :

- Nécessite un périphérique extérieur pour fonctionner
- Plus compliqué à déployer et a généraliser a tous les systèmes nécessitant une authentification
- La précision des capteurs est certes grande, mais génère encore des faux positifs et des faux négatifs
- Les empreintes sont récupérables et falsifiables avec de la silicone par exemple
- Possiblement vulnérable aux attaques MITM si données non chiffrées
- Une fois compromises, impossible de changer des empreintes compromises : cette méthode devient donc non sécurisée et inutile !

Cette méthode tend à se démocratiser puisque les capteurs deviennent de plus en plus précis et abordables (exemple avec les téléphones portables).

Idée d'amélioration : Ajouter un capteur cardiaque lors de la lecture de l'empreinte, ainsi même si l'empreinte est dupliquée elle sera refusée puis que la silicone ne possède pas de pouls.

Iris scan

Comme son nom l'indique, l'iris scan utilise l'iris de l'utilisateur comme moyen d'authentification. En effet, chaque iris est unique (même entre jumeaux ou entre l'œil droit et le gauche), permettant une identification certaine, à l'instar des empreintes digitales. Le système n'analyse pas la couleur (car elle varie au cours de la vie) mais les micro-détails de l'iris (qui eux ne changent pas).

Points forts :

- Identifie de manière bien plus sûre un utilisateur par rapport à la méthode login/mot de passe
- Aucun effort mémoriel de la part de l'utilisateur
- Système rapide et intuitif

Points faibles :

- Nécessite un périphérique extérieur pour fonctionner
- Plus compliqué à déployer et à généraliser à tous les systèmes nécessitant une authentification
- La précision des capteurs n'est pas toujours suffisamment élevée
- Il est possible d'usurper l'identité d'un utilisateur grâce a une simple photo suffisamment précise de son iris
- Possiblement vulnérable aux attaques MITM si données non chiffrées
- Beaucoup de contraintes pour une mesure efficace, par exemple avoir un éclairage restreint et maîtrisé précisément
- Beaucoup de difficultés à authentifier les personnes aveugles ou ayant la cataracte

Idées d'amélioration : Pour éviter l'usage de photos pour contourner le système, il est possible de capter la réactivité de la pupille (sa dilatation ou sa rétractation).

Méthode ADN

A l'instar de la police scientifique, cette méthode utilise l'ADN de l'utilisateur pour l'identifier. L'ADN étant notre « carte d'identité » génétique, il permet une identification assez certaine de l'utilisateur du système.

Points forts :

- Identifie de manière bien plus sûre un utilisateur par rapport à la méthode login/mot de passe
- Aucun effort mémoriel de la part de l'utilisateur

Points faibles :

- Nécessite un périphérique extérieur pour fonctionner
- Obligation de récupérer l'ADN d'une quelconque manière (racine de cheveu, salive, sang, etc.), ce qui soulève un gros problème d'hygiène.

- Problème des jumeaux ! En effet, ils possèdent le même ADN et il est donc impossible de les différencier par ce biais
- Plus compliqué à déployer et à généraliser à tous les systèmes nécessitant une authentification
- Possiblement vulnérable aux attaques MITM si données non chiffrées (elles peuvent être récupérées et possiblement « injectées » dans le périphérique externe pour usurper l'identité de l'utilisateur)

Dynamique des frappes de clavier

Bien que le nom puisse faire sourire, cette méthode est assez originale et intéressante. Elle consiste a analyser la manière propre qu'à un utilisateur de taper son mot de passe : ainsi, les caractères ne sont plus la seule chose évaluée pour être authentifié, car la manière de taper les caractères l'est également. Lors de la première connexion, l'utilisateur est invité à saisir son mot de passe une dizaine de fois pour déterminer sa manière de le taper, puis cette manière est stockée comme « Profil de frappe ». On vérifie ensuite a chaque tentative de connexion si la manière de saisir correspond au profil de frappe.

Points forts :

- Très simple à mettre en place + pas de hardware
- Simple à déployer
- Fausses acceptations inférieures à 0.5% avec un mot de passe de 8 caractères

Points faibles :

- Si l'utilisateur utilise plusieurs claviers différents (exemple, AZERTY et QWERTY) il faut un profil de frappe par clavier
- Il ne faut pas être dérangé lors de la frappe, car cela peut provoquer un refus de son propre mot de passe !

Puce physique

Méthode qui peut sembler futuriste mais qui est tout de même applicable, elle consiste à implanter sous la peau de l'utilisateur une puce contenant un code/identifiant qui lui est propre. Cette puce pourrait ensuite être lue par un dispositif approprié.

Points forts :

- Si la puce n'est pas falsifiable/duplicable, alors le système est tout à fait sécurisé
- Identifie de manière bien plus sûre un utilisateur par rapport à la méthode login/mot de passe
- Aucun effort mémoriel de la part de l'utilisateur
- Très simple d'utilisation

Points faibles :

- L'éthique de poser un implant a chaque utilisateur est discutable, surtout si la puce possède des fonctionnalités supplémentaires (géolocalisation par exemple) …

- Possibles problèmes de santé liés à l'implant (le rejet de celui-ci par exemple)
- Nécessite un périphérique extérieur pour fonctionner (lecteur de puce)
- Coût de déploiement très élevé
- La nécessité de changer la puce si on veut changer de code d'authentification

Question(s) secrète(s)

Méthode qui possède des failles assez évidentes mais dont nous allons parler quand même. Elle consiste à poser une ou plusieurs questions personnelles à l'utilisateur et considérer que s'il y répond bien, c'est bien lui (de manière certaine)

Points forts :

- Très facile à mettre en place
- Adapté à tous les utilisateurs (enfants, personnes âgées, etc.)
- Effort mémoriel très faible (retenir des réponses a des questions concernant directement l'utilisateur)

Points faibles :

- Nul besoin d'une quelconque technique avancée pour usurper l'identité ! Il suffit de bien connaître l'utilisateur ou de rassembler un maximum d'informations sur lui
- Possiblement vulnérable aux attaques MITM si réponses non chiffrées

Code barre

Tel un produit au supermarché, l'utilisateur pourrait être identifié par un code barre unique tatoué sur son corps par exemple. Cette méthode est très similaire à celle de l'implant de puce, à la différence près qu'elle remplace les problèmes de santé lié à l'implant par des problèmes d'allergie à l'encre et d'infection de la zone tatouée.

Points forts :

- Si le code est bien unique, on est bien certain d'authentifier la bonne personne
- Identifie de manière bien plus sûre un utilisateur par rapport à la méthode login/mot de passe
- Aucun effort mémoriel de la part de l'utilisateur
- Très simple d'utilisation

Points faibles :

- L'éthique de tatouer un code barre à chaque utilisateur est discutable, qui plus est sur les raisons esthétiques, symboliques et religieuses par exemple.
- Possibles problèmes de santé liés au tatouage (infections, mauvaise cicatrisation, allergies)
- Nécessite un périphérique extérieur pour fonctionner (lecteur de code barre)
- Coût de déploiement élevé
- La nécessité d'un nouveau tatouage si on veut changer de code d'authentification

Scanner cérébral

Chaque cerveau est différent dans les détails de sa structure, et permet donc, théoriquement, d'identifier de manière certaine quelqu'un. Ainsi, si on effectue un scanner du cerveau de l'utilisateur pour le mettre en place comme mot de passe, il suffit de scanner à nouveau le cerveau de l'utilisateur lors qu'il tente une connexion pour l'identifier si les scanners sont les mêmes.

Points forts :

- Théoriquement très sécurisé et non falsifiable

Points faibles :

- Très contraignant niveau matériel
- Très contraignant pour l'utilisateur (un scan par authentification, c'est très lourd)
- Extrêmement coûteux à mettre en place
- Impossible à déployer chez des particuliers
- Le fait de faire beaucoup de scanner peut, au final, avoir des effets négatifs sur la santé

Signaux cérébraux

Cette méthode ressemble à de la science-fiction, mais a pourtant été déjà testée avec succès par des scientifiques de l'Université de Binghamton à New York, avec un taux de réussite de 100%. Cette méthode consiste à fournir un stimulus visuel (une image) et à enregistrer l'activité cérébrale « répondant » à ce stimulus. Il a été montré que la manière de réagir à une image est propre à l'individu, même si l'image est la même pour toutes les personnes. Cette activité cérébrale est mesurable par un simple électro encéphalogramme (EEG) de précision.

Points forts :

- Théoriquement très sécurisé et non falsifiable
- Peu de matériel à mettre en place
- **Aucun** effort demandé à l'utilisateur

Points faibles :

- Cette méthode est encore expérimentale et n'est pas directement implémentable à l'heure actuelle
- Nécessite d'avoir un appareil à EEG connecté, technologie peu répandue
- La réaction à un stimulus visuel peut évoluer à force d'y être exposé, ce qui implique la mise à jour de l'activité nécessaire à l'authentification.

Idée d'amélioration : Périodiquement mettre à jour l'activité nécessaire à l'authentification pour coller avec les changements de réaction

Composition et pigmentation du cheveu

L'eumélanine et la phéomélanine sont les molécules responsables de la pigmentation des cheveux. La proportion de chacune des deux molécules, couplées à d'autres caractéristiques du cheveu (épaisseur, résistance, etc.) permettent d'identifier sans erreur un individu précis. Il est intéressant de noter que ni l'impact du soleil ni les colorations « artificielles » n'altèrent la proportion de ces deux molécules. Nous pouvons donc nous servir de cela comme méthode d'authentification.

Points forts :

- Méthode très difficile à falsifier de part la complexité de la structure d'un cheveu
- Pas d'effort mémoriel pour l'utilisateur

Points faibles :

- Même chose que pour l'ADN, cette méthode ne résout pas le problème des jumeaux ! Partageant le même code génétique, il y a de grandes chances que le système ne fasse pas de différence entre leurs cheveux respectifs
- Exclu les utilisateurs chauves
- Nécessite beaucoup de tests pour rendre un résultat fiable et certain
- Matériel très coûteux (excluant les particuliers)
- Méthode toujours considérée expérimentale, donc incertaine

Conclusion

Voilà qui conclut les différentes études de sécurité que nous avons effectué sur les douze méthodes qui composent ce dossier.

Nous vous remercions de l'avoir lu jusqu'au bout, et nous vous remercions également pour avoir proposé ce défi pour cette Nuit de l'Info 2018.

Nous avons pris beaucoup de plaisir à effectuer toutes les recherches qui ont été nécessaires, et nous espérons que ce dossier vous a intéressé.

Nous restons à votre disposition à l'adresse : adrien.mollet@etu.univ-amu.fr