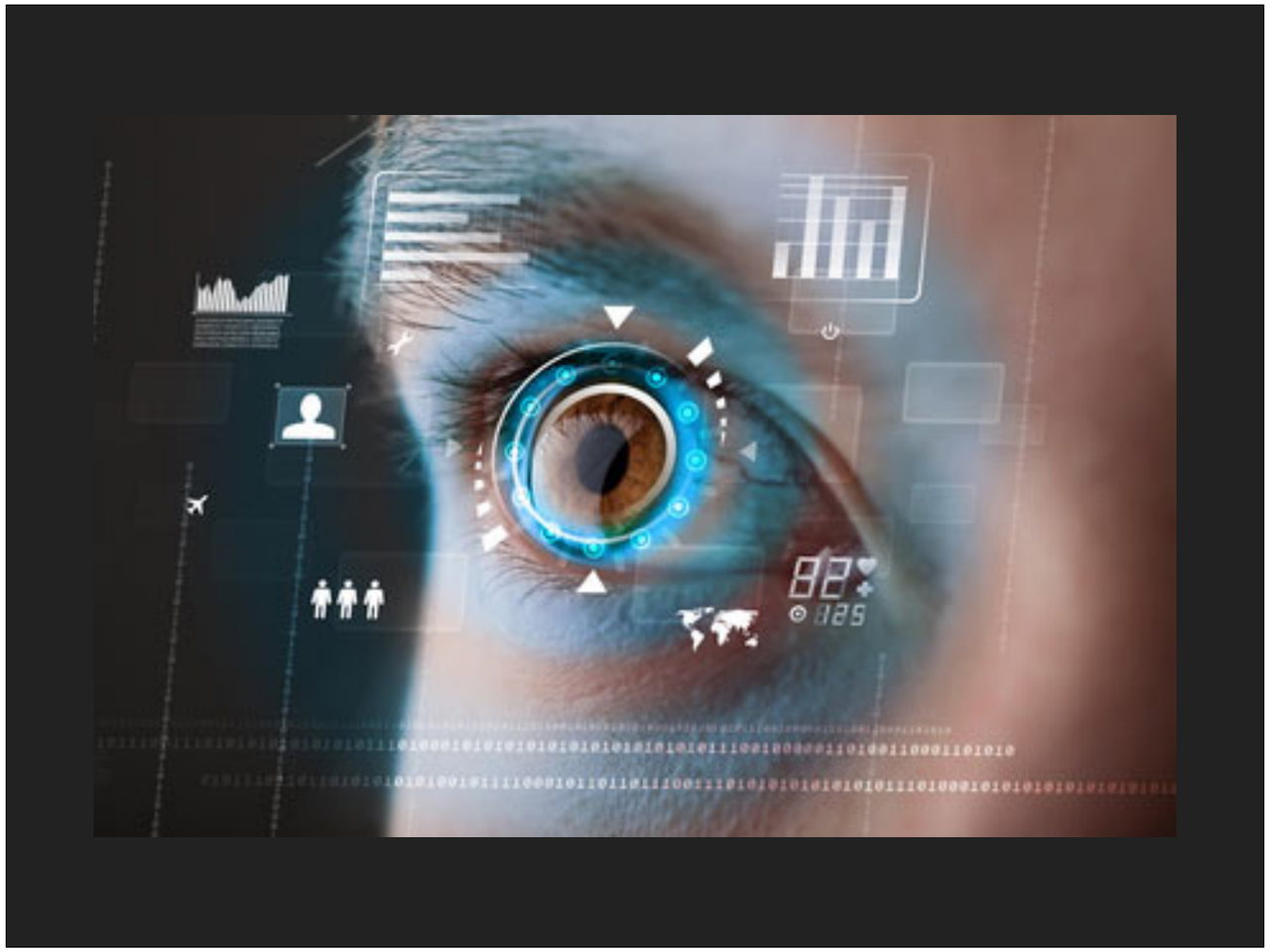
L'AUTHENTIFICATION (PRESQUE) SANS LES MAINS

WEBAUTHN

Bonjour à toutes et à tous !

Merci d'assister à cette présentation sur WebAuthentication, une API qui se propose juste de changer le monde, une partie en tout cas, en supprimant… les mots de passe !



Commençons par définir ce qu’est l’authentification.

L’authentification est le fait de prouver son identité.

Elle diffère de :

- l’identification, qui consiste uniquement à proclamer son identité
- l’autorisation, qui consiste à vérifier qu’une entité authentifiée peut effectuer certaines actions.

Exemple :

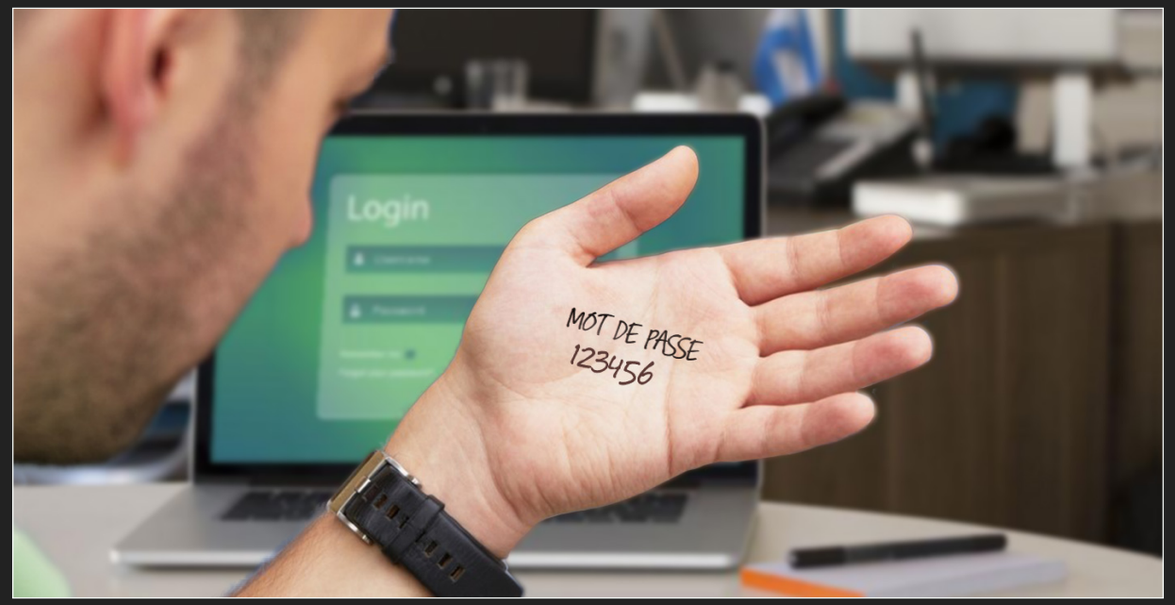
- J’appelle ma mère
- Son téléphone affiche mon prénom, ce qui lui permet de m’identifier avant de décrocher
- Je dis « Allo, c’est moi », à nouveau je m’identifie (heureusement que son téléphone m’a identifié 😆)
- Ma mère m’authentifie à l’aide de ma voix et m’autorise à lui parler

Dans la vie courante nous effectuons souvent implicitement les deux étapes d’identification et d’authentification.
Par exemple lorsque nous croisons quelqu’un que nous connaissons nous l’identifions et l’authentifions en même temps (enfin quasiment).

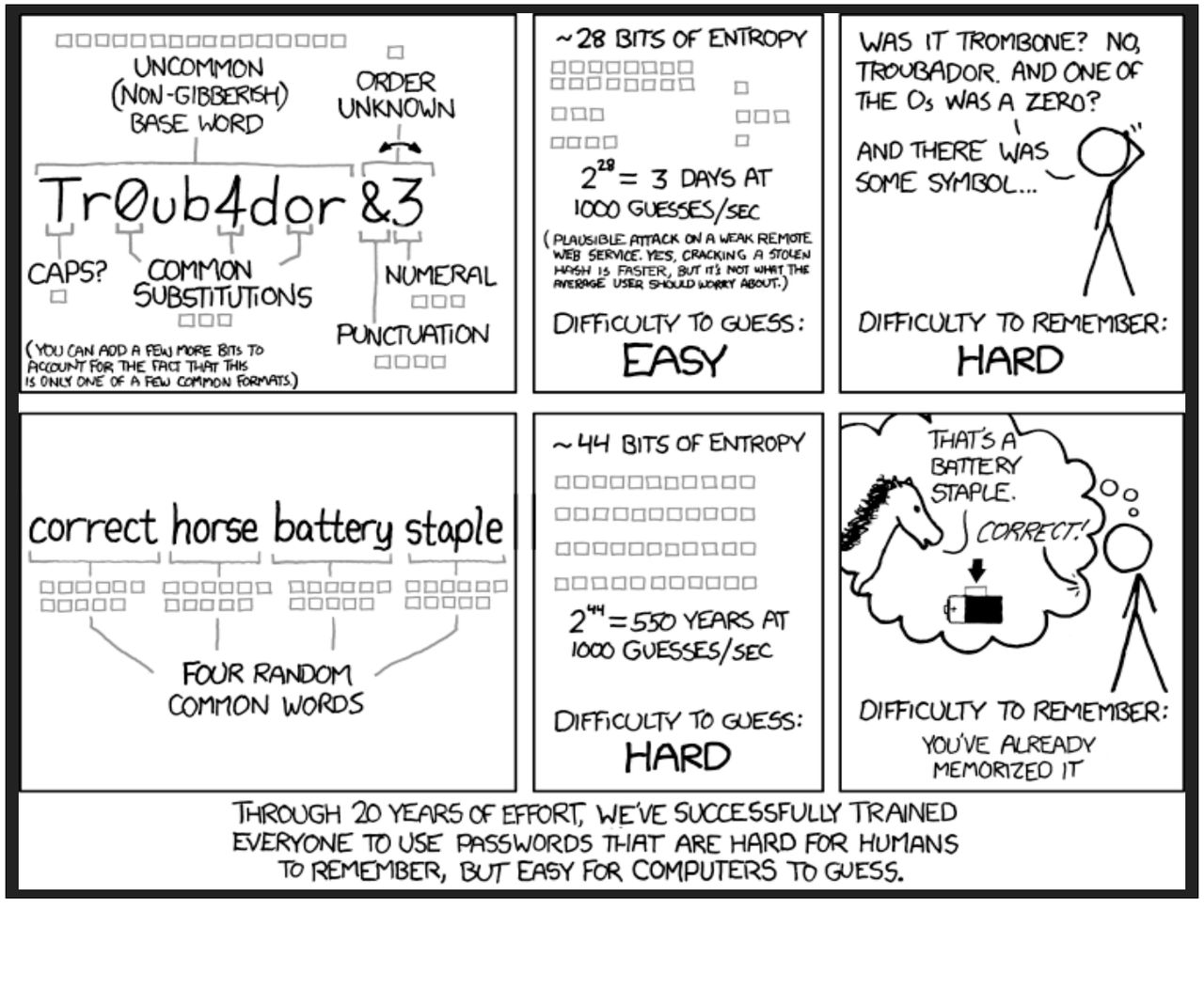
IDENTIFICATION

- Benoît Giraudou
- Développeur depuis 15 ans
- Actuellement chez Zenika Bordeaux
- Intéressé par la sécurité depuis tout petit…

Dans les temps anciens de l’informatique les choses étaient simples, vous aviez deux chaînes de caractères, un nom d’utilisateur et un mot de passe pour vous authentifier.
L’environnement était simple aussi, un seul gros ordinateur partagé par beaucoup de gens. On pouvait vous voler votre mot de passe mais il fallait accéder également à ce gros ordinateur !



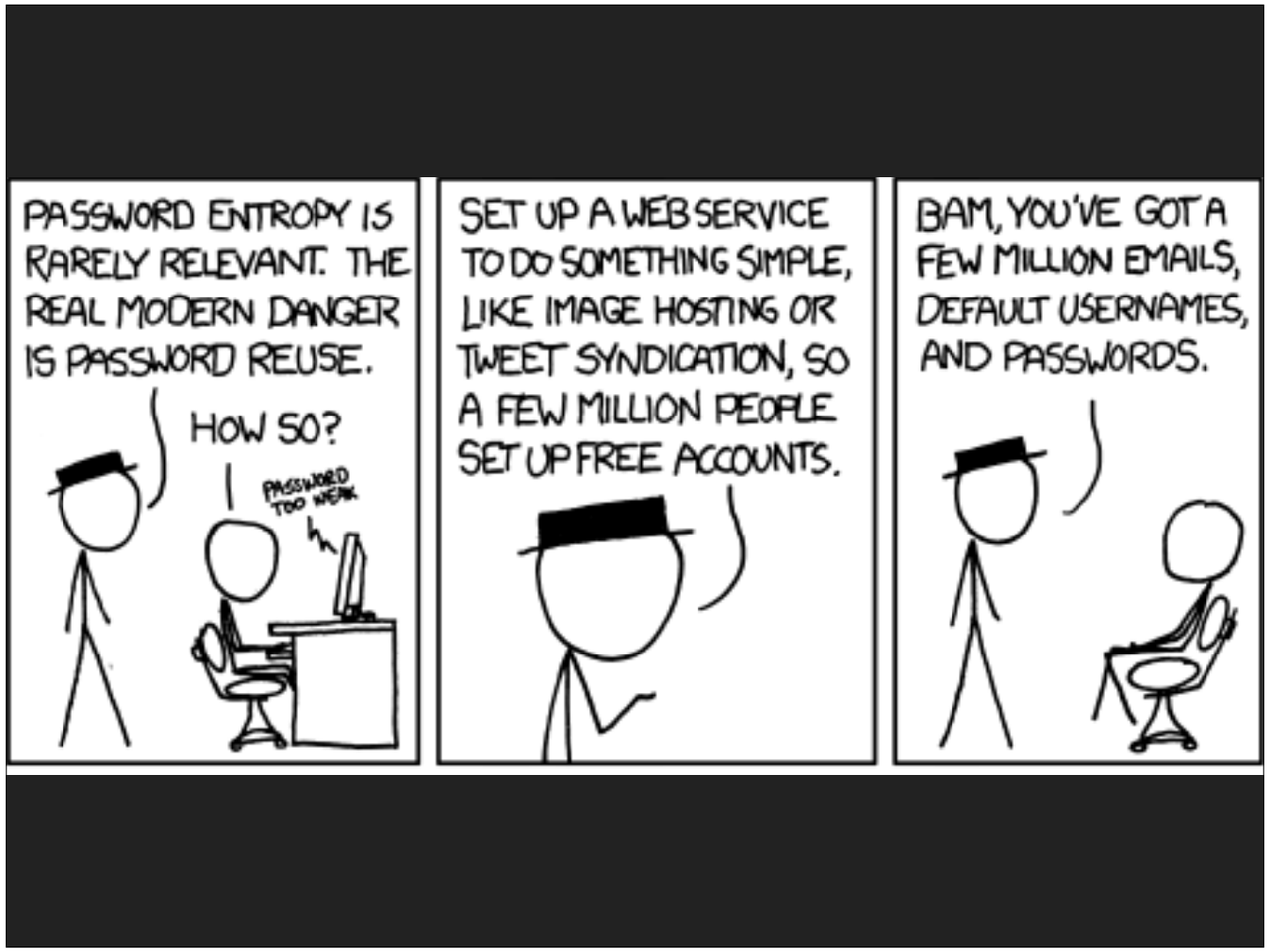
De plus les machines n’étaient pas systématiquement connectées à un réseau et il fallait donc un accès physique à la machine en plus des identifiants de l’utilisateur pour s’y connecter.
Puis est arrivé Internet, avec une connexion de plus en plus en grande des différentes machines (aujourd’hui tout objet dit connecté est connecté directement ou indirectement à Internet).
Combiné à cela une explosion des services et donc du besoin de créer des comptes (alors qu’auparavant un seul compte pour accéder au SI de votre société).



xkcd obligatoire 😀

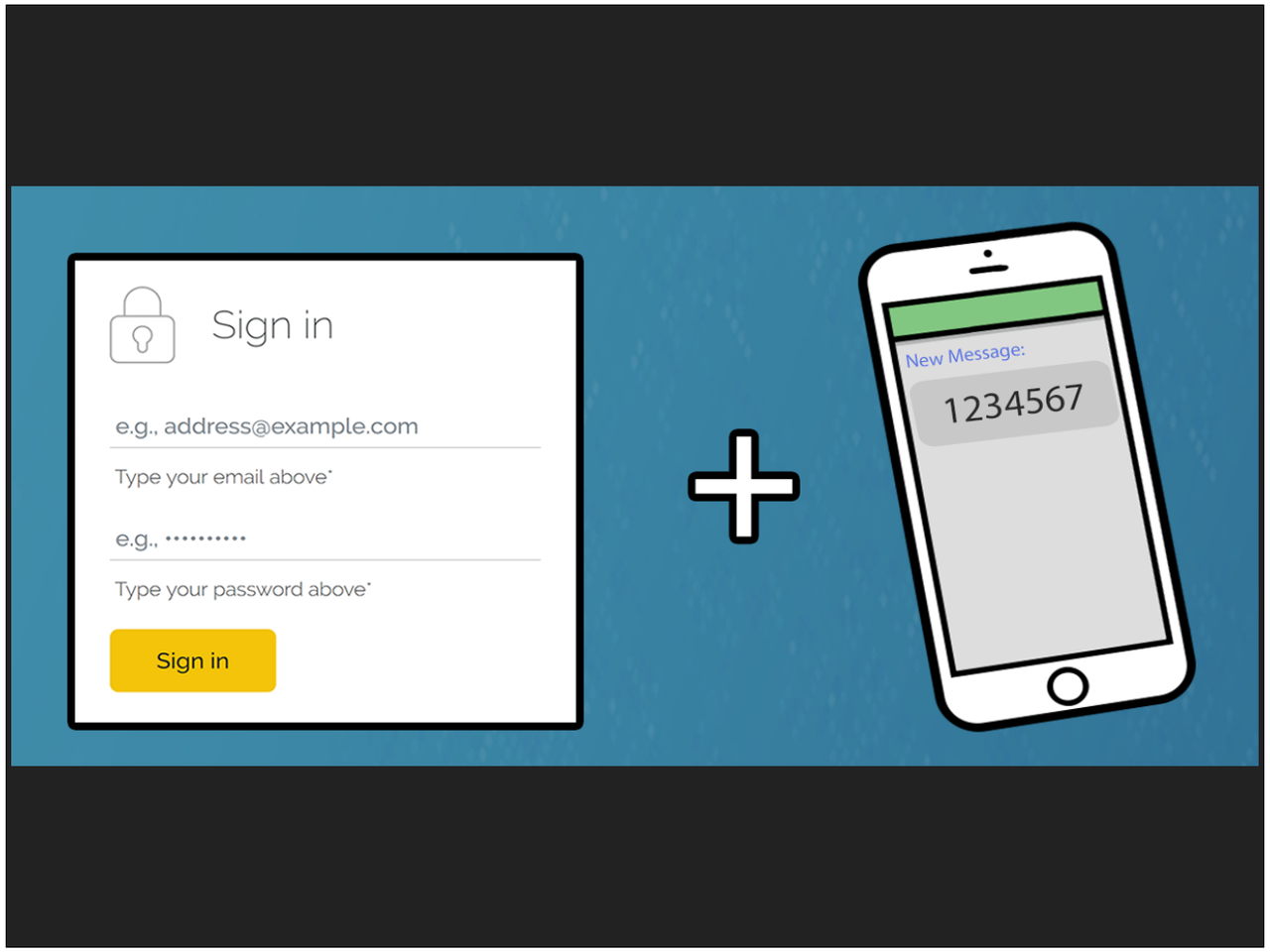
Un conseil souvent donné aux gens est d'utiliser un mot de passe « fort », long, avec certains caractères spéciaux… bref quelque chose d'impossible à retenir.
Personnellement je dois avoir trois cents comptes différents.
En particulier les substitutions de lettre « classiques » (3 à la place de E, 1 à la place de L…) sont inutiles, si vous y avez pensé les pirates y ont aussi pensé.

Explication du xkcd : https://security.stackexchange.com/questions/6095/xkcd-936-short-complex-password-or-long-dictionary-passphrase/6096#6096



Un problème souvent rencontré est la réutilisation des mots de passe.
Une étude de Google a montré qu'en moyenne sur 50 sites un utilisateur réutilise le même mot de passe pour 10 sites en moyennes.
La sécurité d'une chaîne étant égale à son maillon le plus faible cela signifie que les sites sont vulnérables si l'un des 10 sites stocke les mots de passe en clair ou d'une manière insuffisamment sécurisée.
Sur une année plus de 2 milliards d'identifiants (nom d'utilisateur et mot de passe) ont fuité.
En tant que concepteur de site Web même si l'on respecte les dernières règles de l'état de l'art pour le stockage des mots de passe (Argon2id pour le chiffrement des mots de passe, base de données différente…) nous sommes à la merci des autres sites également 😢.

Une étude récente menée par des chercheurs allemands a par exemple montré que beaucoup de professionnels stockaient les mots de passe en clair si la sécurité n'était pas explicitement mentionné dans les exigences.
La moitié ont utilisé md5 ou base64 (!) pour stocker les mots de passe de manière « sécurisée » (https://net.cs.uni-bonn.de/fileadmin/user_upload/naiakshi/Naiakshina_Password_Study.pdf).

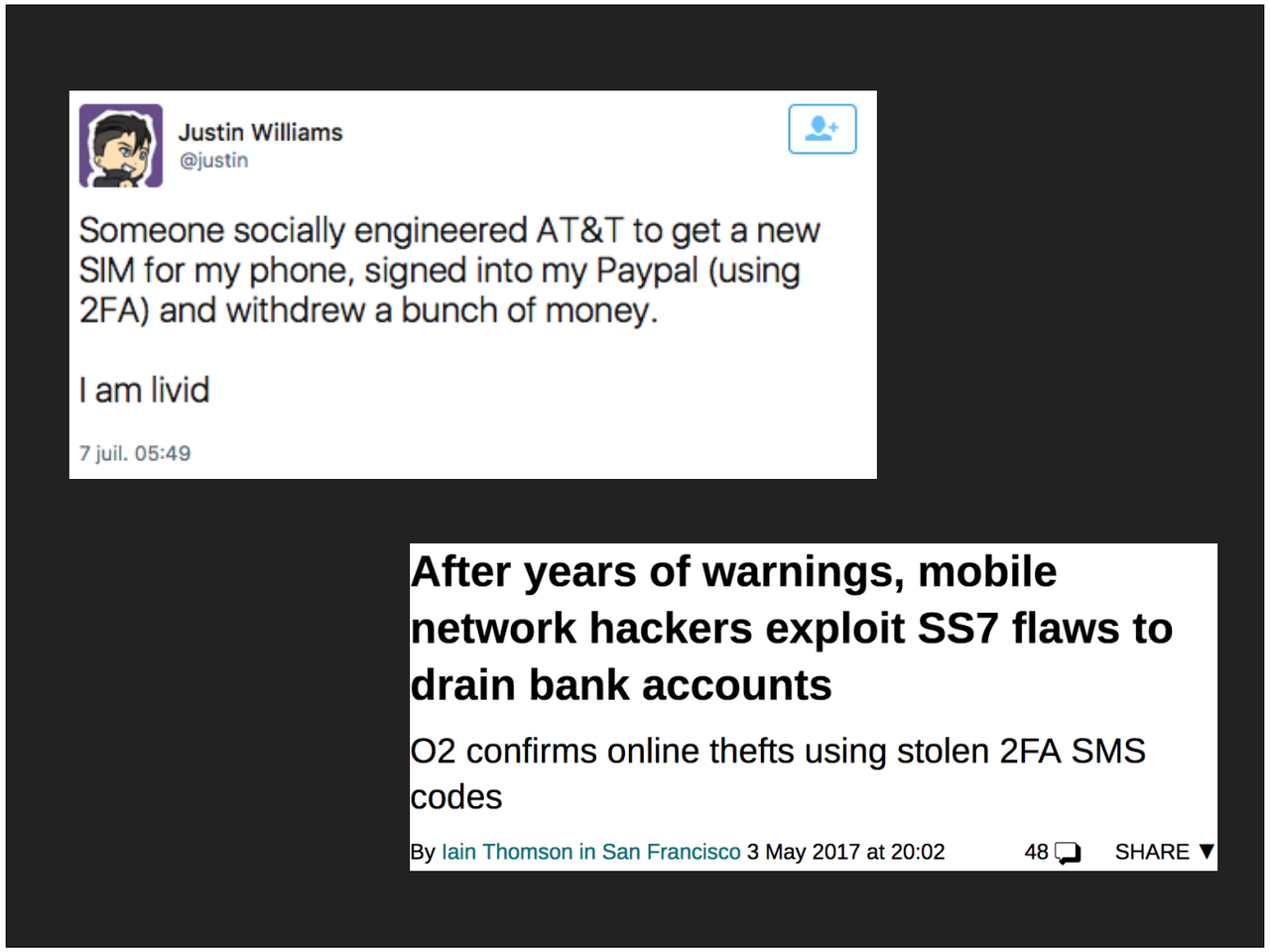


Pour pallier au problème des mots de passe faible et réutilisés il a été petit à petit conseillé d'ajouter un second facteur d'authentification.
Le mot de passe est quelque chose que vous connaissez, le second facteur étant quelque chose que vous possédez (un téléphone pour recevoir un SMS, une application pour générer un code).
Il existe plusieurs types de facteur :

- connaissance (ce que l'on sait), par exemple un code PIN, un mot de passe, la réponse à une question personnelle
- possession (ce que l'on a), par exemple un téléphone (ou plutôt la carte SIM liée au numéro de téléphone) pour recevoir un SMS, une application pour générer un code OTP (on possède le code d'initialisation) ou encore une clé de sécurité
- appartenance (ce que l'on est), empreinte digitale ou rétinienne, voix, ADN…

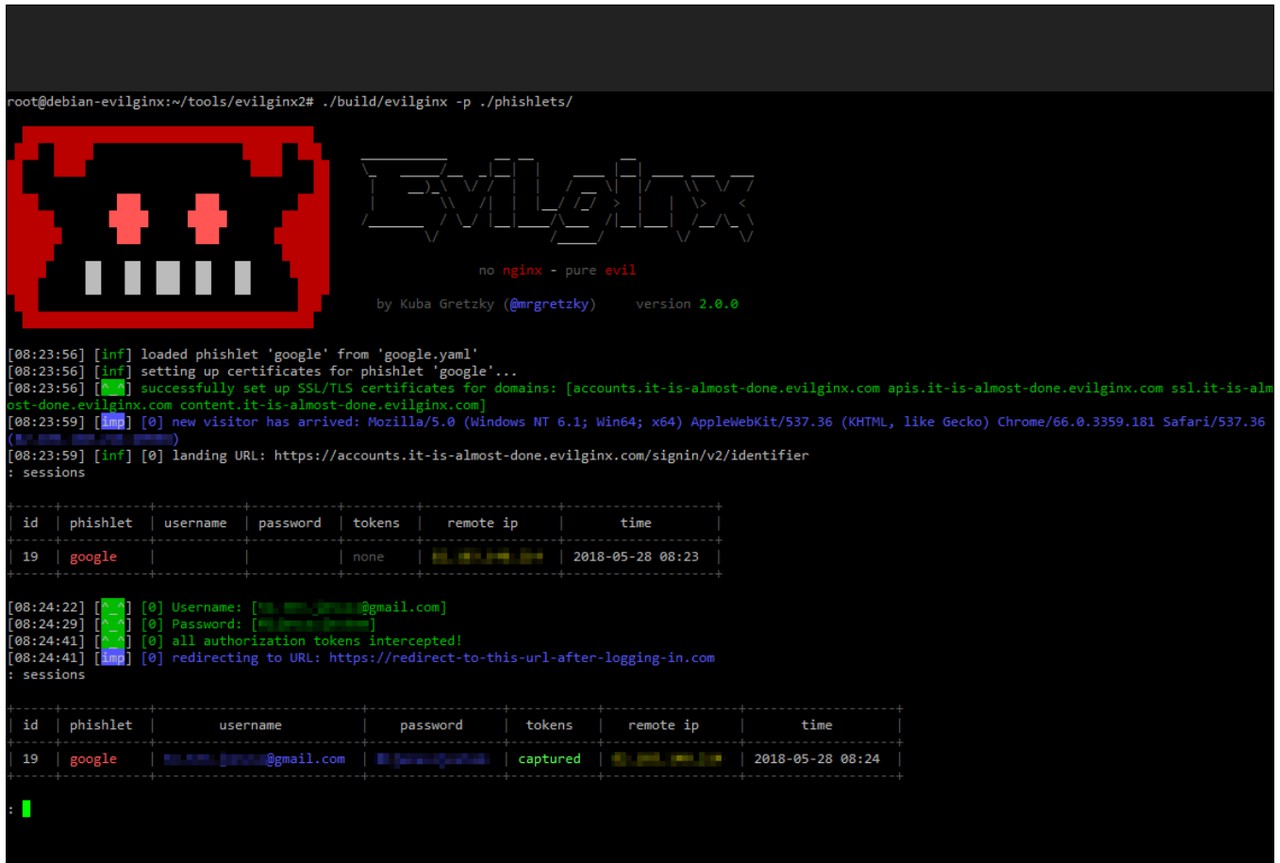
Ce dernier type de facteur peut poser certains problèmes ; c'est un facteur fixe impossible à révoquer et il peut porter atteinte à la vie privée.
C'est néanmoins le facteur qui intéresse le plus en ce moment, pour des raisons pratiques, l'authentification ayant deux objectifs parfois entrant en conflit :

- le plus invisible possible pour l'utilisateur
- le plus sécurisé possible



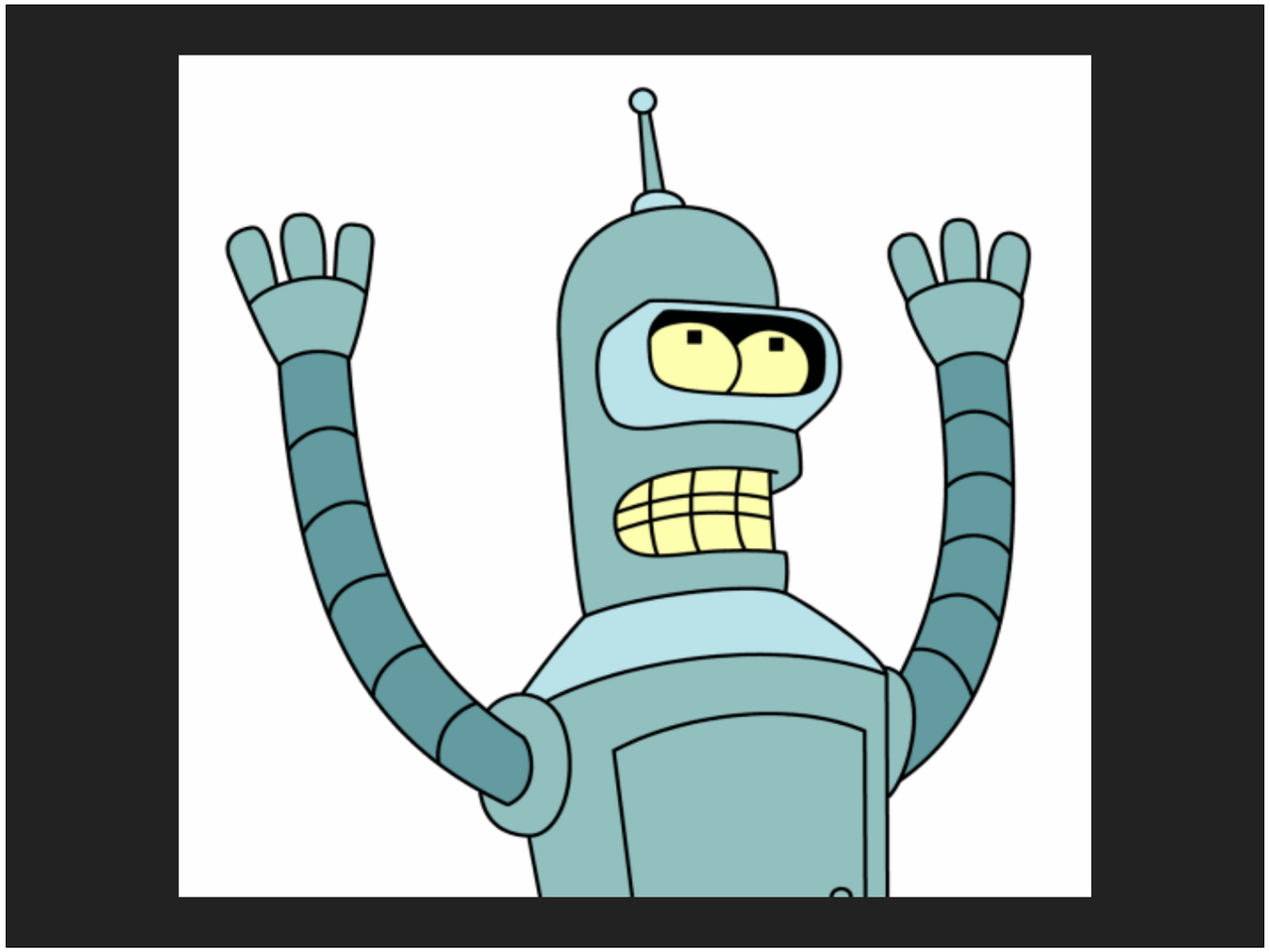
Revenons au second facteur d’authentification par SMS…
Malheureusement, cette méthode a assez rapidement montré ses limites.
Ingénierie sociale pour obtenir une carte SIM, faille réseau téléphonique (permettant l’interception des communications vocales et textuelles, des entreprises américaines proposant même ce genre de services à leurs clients).
Le NIST (National Institute of Standards and Technology) a rendu obsolète l’usage du SMS pour le 2FA dans ses dernières recommandations.
D’ailleurs le code envoyé par SMS pour valider ces achats en ligne doit être remplacé d’ici la fin d’année.

Les codes OTP offrent un niveau de protection supplémentaires mais ils sont également vulnérables aux attaques par hameçonnage.
Il y a 12 millions d’attaques par phishing sur une seule année !
Ils peuvent également poser certains problèmes pour être correctement sécurisés, au niveau de leur sauvegarde (la clé initiale devant être sauvegardée).



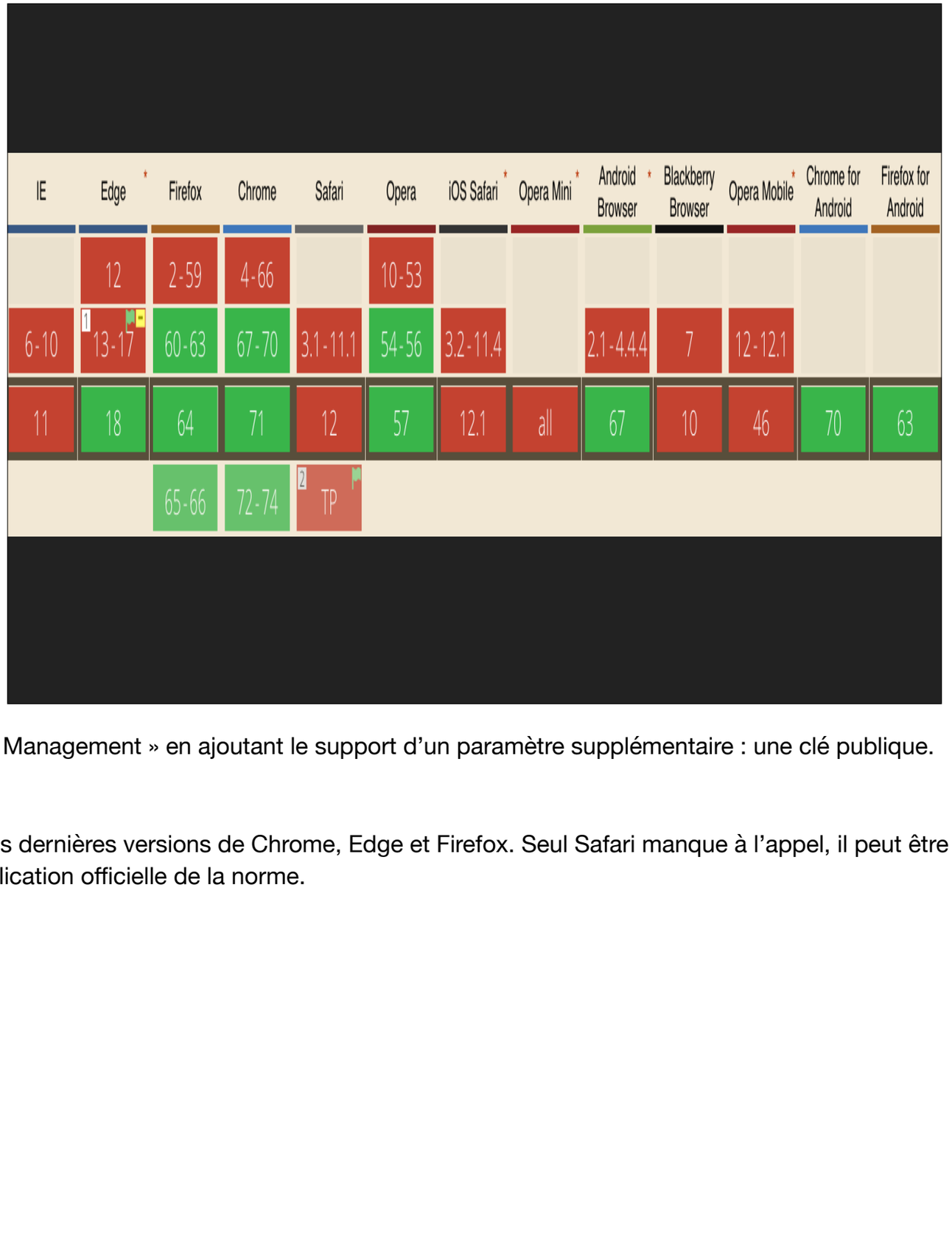
On peut également parler de Evilginx2 qui permet de mettre en place des sites de phishing de manière simple.
En gros il duplique le site cible et le présente à l'utilisateur, le tout de manière automatisée.
Il peut être utilisé pour faire des campagnes de sensibilisation au hameçonnage.

Une autre possibilité promue par l’alliance FIDO (Fast IDentity Online, un consortium d’industriels dont le seul but est de développer des standards interopérables pour l’authentification sécurisée) est l’utilisation de périphériques de sécurité.
Le standard U2F (Universal Second Factor) permet de simplifier l’utilisation de périphériques USB ou NFC comme facteur d’authentification supplémentaire.
Malheureusement uniquement géré en standard par Chrome (on peut néanmoins l’activer dans Firefox), ce qui peut expliquer un succès mitigé en dehors du monde de l’entreprise.
Utilisé par exemple par les 85000 employés de Google depuis début 2017, 0 attaques par phishing depuis ont été déplorés par Google.



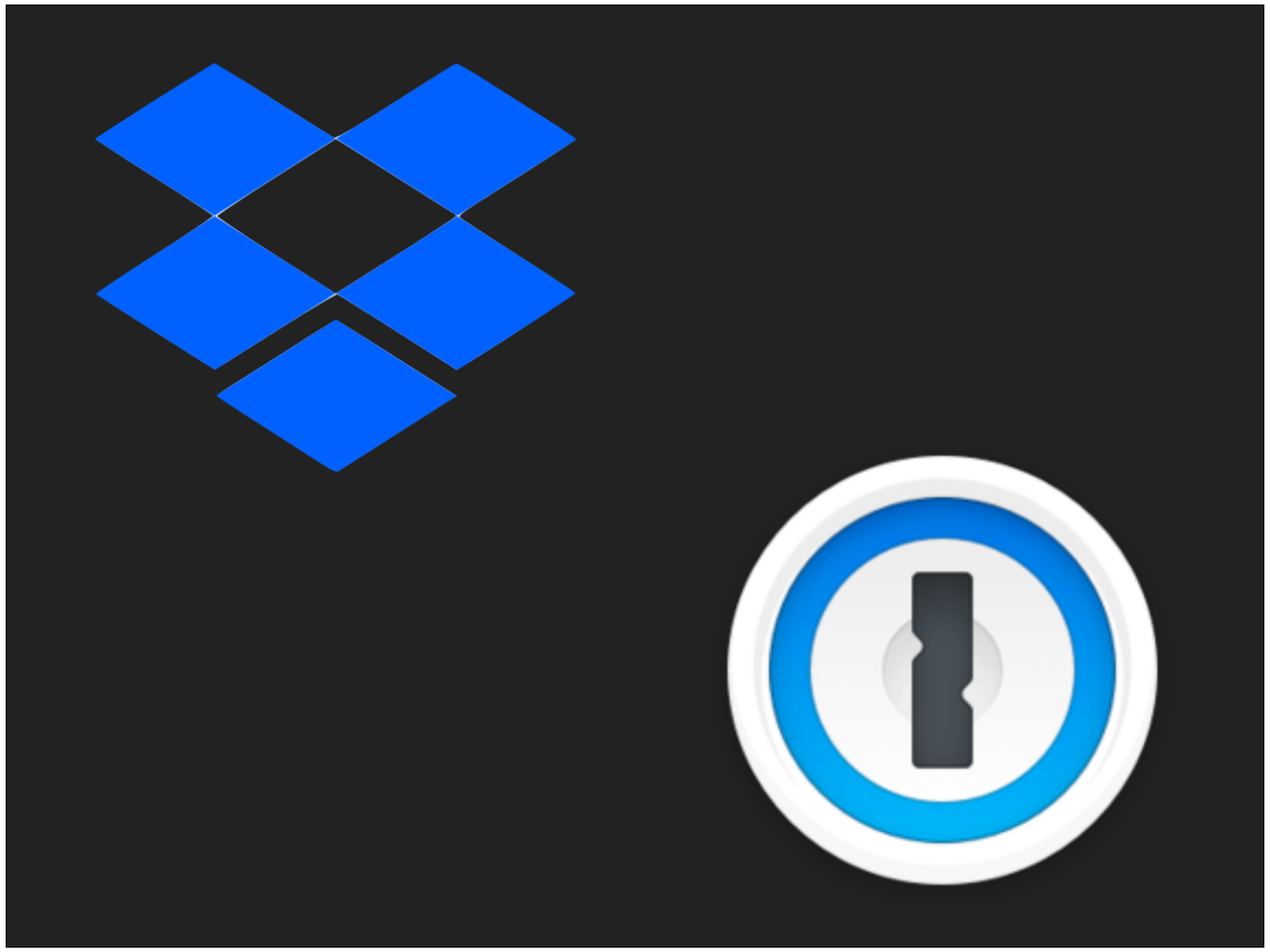
Heureusement WebAuthentication, WebAuthn de son petit nom, arrive pour nous sauver !
Il s’agit d’un travail conjoint du W3C et de l’alliance FIDO (Fast IDentity Online).
L’API a été publiée le 4 mars 2019 par le W3C.
Peut être utilisé comme unique facteur d'authentification ou en complément d'autres moyens (empreinte digitale, reconnaissance faciale, code PIN).

C’est une partie du standard FIDO2, l’autre partie étant CTAP (Client-to-Authenticator Protocol) qui définit comment utiliser des périphériques externes comme authentificateur (ordiphone, clé de sécurité).
Presque rétro-compatible avec le standard U2F (même si la plupart des périphériques certifiés U2F ne sont pas capables de stocker l’identité de l’utilisateur et donc de pouvoir utiliser une même clé pour plusieurs identités sur un même service).

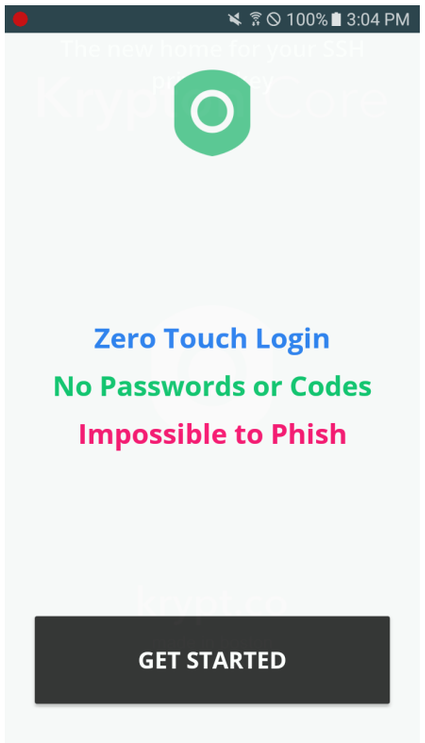


WebAuthn étend l’API Web « Credential Management » en ajoutant le support d’un paramètre supplémentaire : une clé publique.

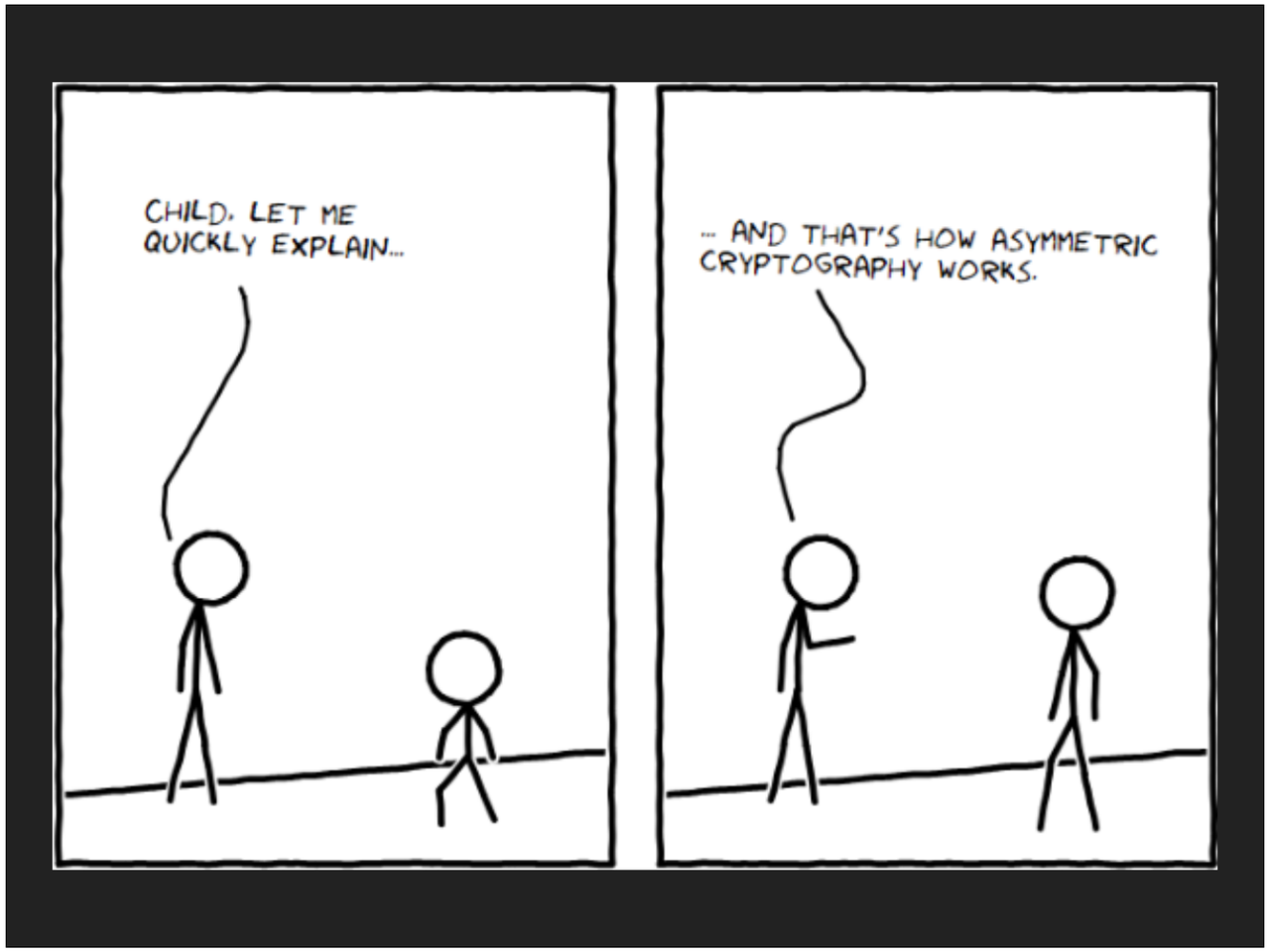
Est-ce que l’on peut l’utiliser ?
Bien sûr ! WebAuthn est supporté par les dernières versions de Chrome, Edge et Firefox. Seul Safari manque à l’appel, il peut être utilisé dans la version TP 12.1 et devrait rapidement arriver suite à la publication officielle de la norme.



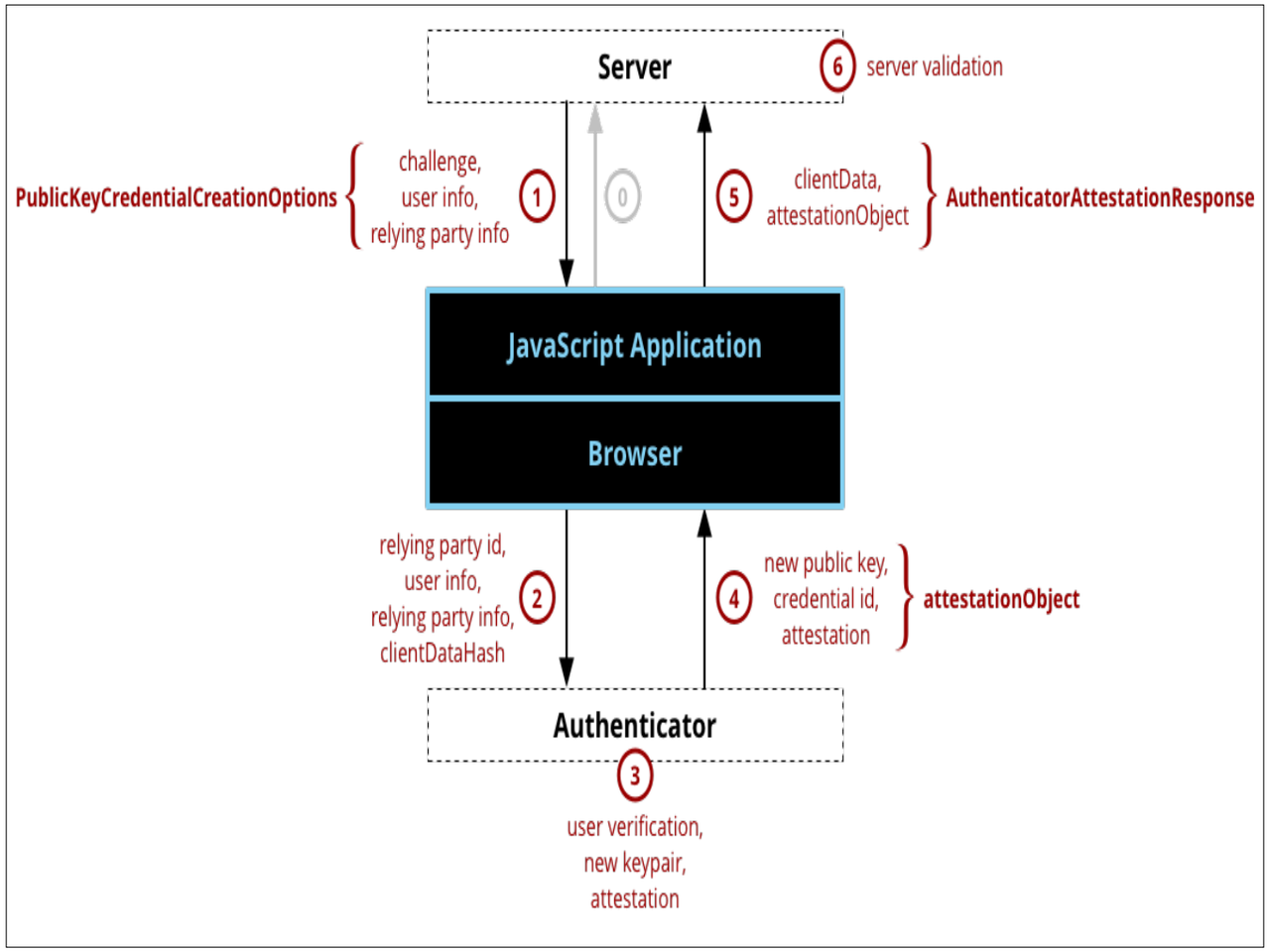
Et côté sites web ?
Pour l’instant c’est un peu calme, Dropbox a été le premier a annoncé le support de WebAuthn en mai 2018 (comme second facteur).
1Password a ajouté le support d’un second facteur d’authentification physique en utilisant WebAuthn en juin 2019.
On peut également parler de Windows Hello qui supporte le standard FIDO2 (dont WebAuthn est une partie).
Ceci dit il faut garder à l’esprit que c’est une nouveauté et que suite à la publication en mars 2019 du standard par le W3C le déploiement devrait accélerer.



Les périphériques compatibles ?
Clé YubiKey 5, clé Solo (financement participatif qui se termine demain !) ou application Krypton (que je n’arrive pas à faire fonctionner sur mon téléphone malheureusement).
Les clés Titan proposées par Google ne sont pas compatibles actuellement avec FIDO2 (et elles ne semblent pas être vendues en France).

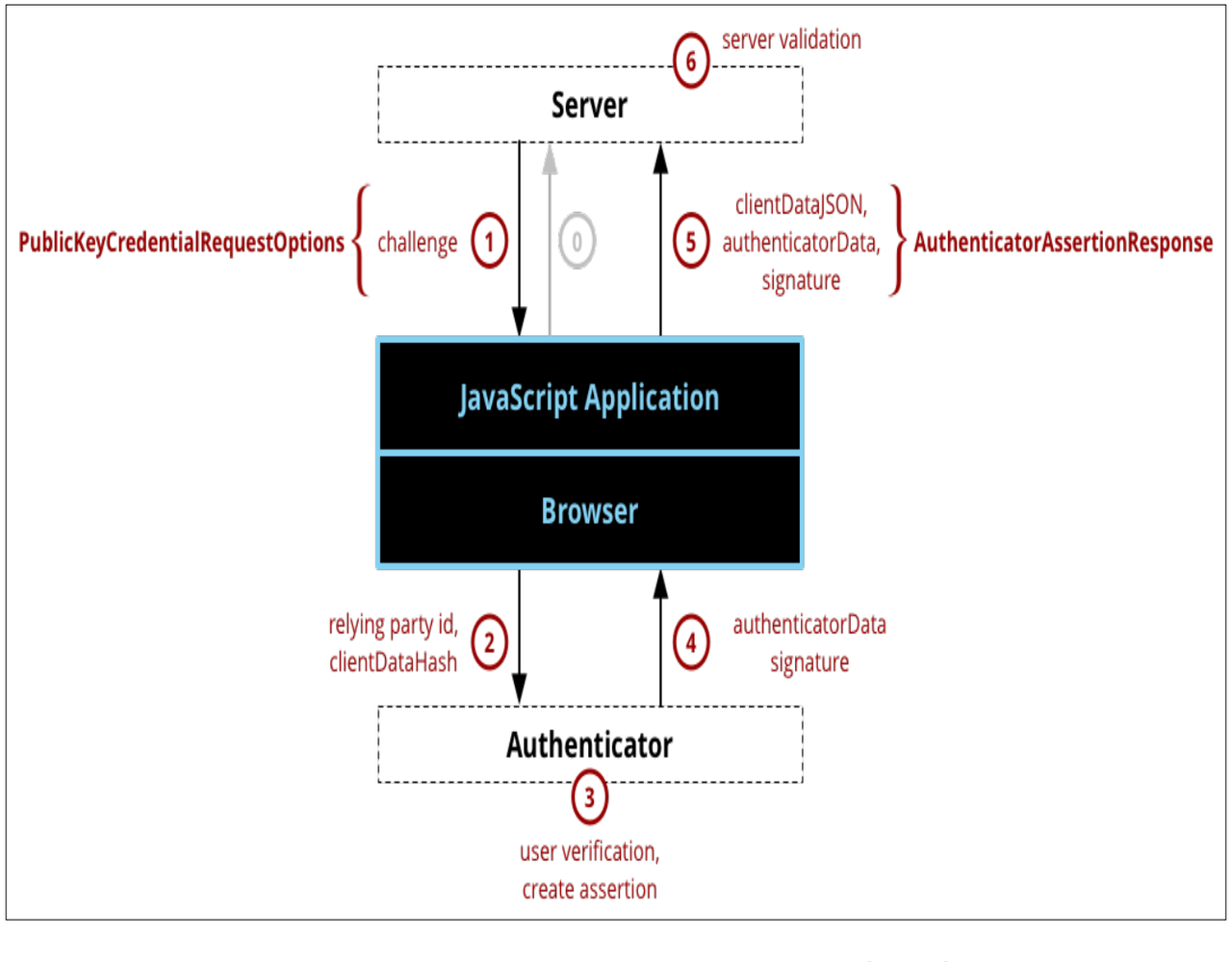


Parlons de cryptographie asymétrique, aussi connue sous le nom de cryptographie à clé publique.
Chaque utilisateur possède deux clés, une clé privée et une clé publique.
Comme son nom l'indique la clé privée doit rester secrète, la clé publique peut être diffusée sur Internet.
Je peux utiliser la clé publique d'Alice pour lui envoyer un message, elle seule sera en mesure de le déchiffrer.
Il est possible également d'utiliser la clé privée pour signer un message et n'importe qui peut vérifier avec ma clé publique que j'ai bien signé le message.
On peut aussi utiliser la cryptographie à clé publique pour s'authentifier (SSH par exemple).



Tout ceci nous amène au fonctionnement de WebAuthn.

Lors de l'enregistrement d'un nouveau compte, le serveur (dénommé « Relying Party » dans la spécification de WebAuthn) envoie un challenge à l'authentificateur par le biais du navigateur.
Celui-ci génère une clé privée qu'il garde localement et renvoie la clé publique et la réponse au challenge.
Le serveur stocke la clé publique de l'utilisateur.

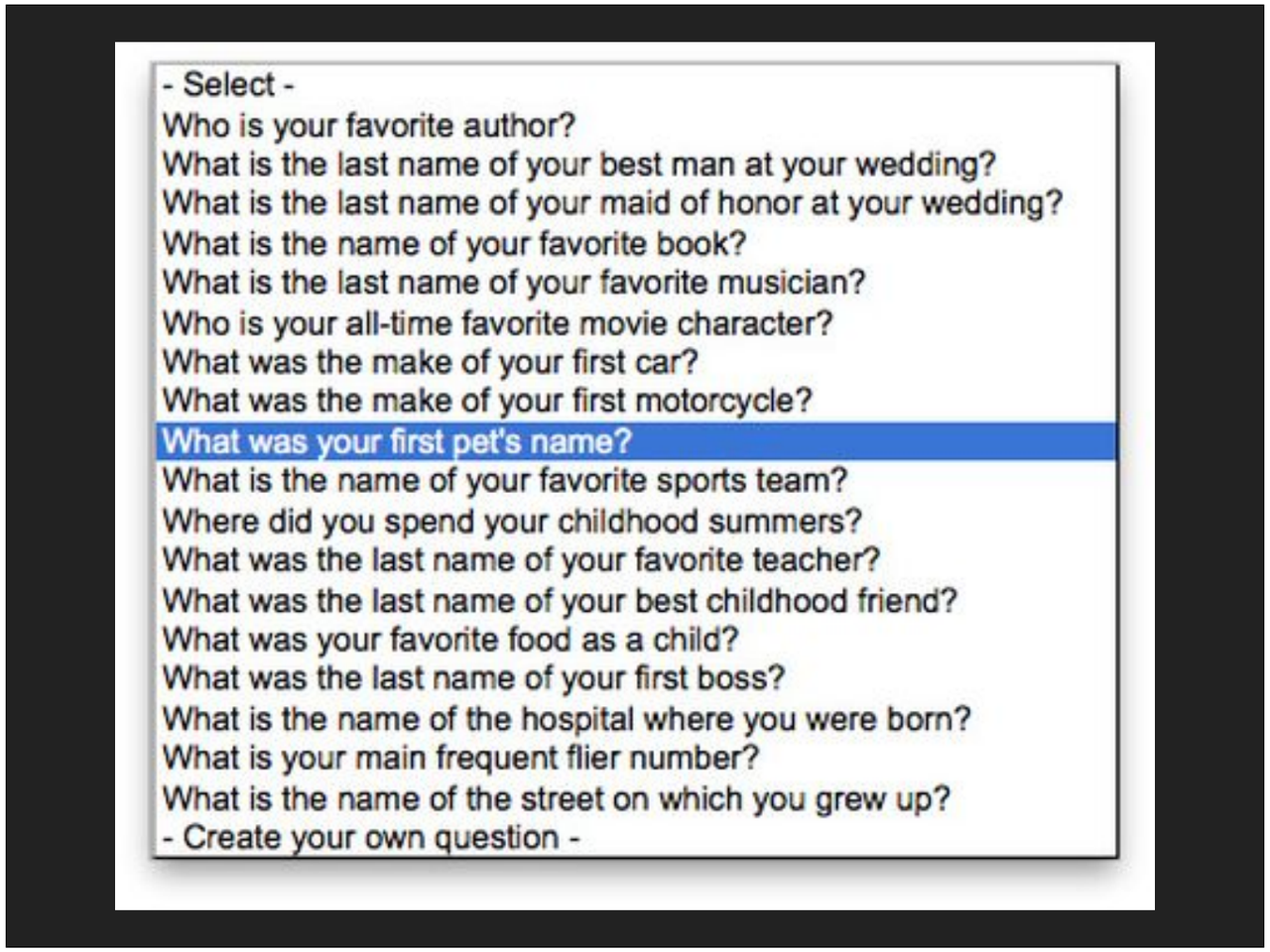


Lors d’une future connexion, le « serveur » envoie un challenge que l’authentificateur signera avec la clé privée correspondant au site et renverra la réponse au serveur (challenge signé).

Démo !

PASSWORDS ?

Pour conclure, les mots de passe :
KILL IT WITH FIRE !


- Select -
Who is your favorite author?
What is the last name of your best man at your wedding?
What is the last name of your maid of honor at your wedding?
What is the name of your favorite book?
What is the last name of your favorite musician?
Who is your all-time favorite movie character?
What was the make of your first car?
What was the make of your first motorcycle?
What was your first pet's name?
What is the name of your favorite sports team?
Where did you spend your childhood summers?
What was the last name of your favorite teacher?
What was the last name of your best childhood friend?
What was your favorite food as a child?
What was the last name of your first boss?
What is the name of the hospital where you were born?
What is your main frequent flier number?
What is the name of the street on which you grew up?
- Create your own question -

Questions ?

RÉFÉRENCES

- Spécification => https://www.w3.org/TR/webauthn/
- MDN => https://developer.mozilla.org/en-US/docs/Web/API/Web_Authentication_API
- Chrome => https://developers.google.com/web/updates/2018/05/webauthn
- Détails => https://www.imperialviolet.org/2018/03/27/webauthn.html
- Code => https://github.com/joow/webauthn-demo
- Stockage mots de passe : https://net.cs.uni-bonn.de/fileadmin/user_upload/naiakshi/Naiakshina_Password_Study.pdf