Jouons et sécurisons avec une clé FIDO2/WebAuthn

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 29 janvier 2024

https://www.bortzmeyer.org/fido2-webauthn.html

Je viens de me lancer dans l'utilisation d'une clé de sécurité (une Nitrokey) pour les protocoles d'authentification FIDO2 et WebAuthn. Regardons cela.

Un peu de contexte d'abord. Lorsqu'on veut s'authentifier auprès d'un service en ligne (un serveur SSH, un site Web, etc), la solution la plus ancienne est le couple identificateur ("*login*") / mot de passe. Ce système pose plusieurs problèmes :

— La difficulté d'avoir des mots de passe à la fois solides (résistant aux attaques par force brute) et mémorisables par l'utilisateurice.
— Le risque de hameçonnage, lorsque l'utilisateurice se laisse convaincre d'aller sur un service qui n'est pas le vrai, à qui ielle donnera le mot de passe, que le hameçonneur pourra ensuite utiliser.
— Plus généralement, la trop grande facilité avec laquelle un mot de passe se partage, par exemple suite à de l'ingénierie sociale.

Tous ces problèmes ont des solutions. Par exemple, le premier se résout très bien par l'utilisation d'un gestionnaire de mots de passe, solution très recommandée. Mais, évidemment, aucune des solutions n'est parfaite.

On cherche donc à renforcer la sécurité, en ajoutant un deuxième facteur d'authentification, par exemple un code à usage restreint, généré sur une machine distincte, qui peut être un ordinateur (rappel : un ordiphone est un ordinateur) ou un périphérique matériel spécialisé, souvent nommé « clé ». Des protocoles normalisés existent comme HOTP (RFC 4226 [1], le code est alors à usage unique) ou TOTP (RFC 6238, le code étant alors à usage limité dans le temps). Il existe aussi des solutions non normalisées, spécifiques à un seul vendeur, qu'il faut bien sûr fuir. Aujourd'hui, lorsqu'on veut accéder à un service sensible (l'interface de gestion de ses noms de domaine, par exemple), cette authentification à deux facteurs doit être considérée comme impérative.

Je vais essayer ici une technique qui permet, soit de remplacer le couple identificateur / mot de passe par une authentification à un seul facteur, mais plus sûre, soit d'utiliser comme deuxième facteur une méthode plus sûre que HOTP ou TOTP. Il s'agit de FIDO2/WebAuthn. C'est en fait un ensemble de plusieurs protocoles. Pour les expliquer, un peu de terminologie (tout en se rappelant qu'en français, il n'y a souvent pas de terminologie standard et répandue pour une bonne partie du vocabulaire de l'informatique). Il y a quatre entités, humaines et non-humaines, qui interviennent

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4226.txt

— L'**utilisateurice**, M. ou Mme Toutlemonde.
— Le **service** auquel ielle veut se connecter (par exemple un site Web).
— Le **logiciel client** de l'utilisateurice (par exemple un navigateur Web).
— L'**authentificateur**, qui est un dispositif à la disposition de l'utilisateurice (par exemple une clé physique comme ma Nitrokey).

Le protocole entre l'authentificateur (relayé par le logiciel client) et le service utilise la classique cryptographie asymétrique. Le service génère des données à usage unique qu'il chiffre avec la clé publique de l'authentificateur, celui-ci les déchiffrera et les enverra, prouvant ainsi qu'il connait la clé privée. Le service n'apprend donc jamais aucun secret (contrairement à ce qui se passe avec le mot de passe), ce qui protège contre le hameçonnage. Les clés privées ne quittent pas l'authentificateur, le logiciel client ne les voit jamais. FIDO2 désigne la communication avec l'authentificateur, WebAuthn l'API JavaScript exposée aux services.

Voyons en pratique ce que cela donne, avec le service de test . Je visite le site Web avec Firefox, j'indique mon identificateur puis je clique sur "*Authenticate*" :

Je sors ensuite ma clé, une Nitrokey 3A NFC :

Je la mets dans le port USB de la machine et j'appuie sur le bouton de la clé (une lumière sur la clé clignote pour vous le rappeler) et je suis authentifié. Ici, on n'a qu'un seul facteur (la possession de la clé). Avec la version de Firefox sur mon système, on ne peut pas ajouter de code PIN à la clé <https://support.nitrokey.com/t/ubuntu-20-04-nitrokey3a-nfc-and-chrome-firefox/4637> (mais ça marche avec Chrome, sur la même machine ; dans le monde FIDO2 / WebAuthn, vous rencontrerez souvent ce genre de problèmes d'interopérabilité ; sur Android, Fennec n'a tout simplement pas WebAuthn). Notez aussi que, la première fois, il faudra s'enregistrer auprès du service pour être reconnu par la suite.

La Nitrokey 3A NFC que je possède peut aussi, comme son nom l'indique, être « connectée » en NFC (testé avec succès sur mon Fairphone, bien qu'il faille un peu chercher où la placer sur l'ordiphone, et avec un Samsung, même problème).

Une fois que vous avez testé votre clé sur ce service et que tout marche, vous pouvez commencer à activer son utilisation sur divers services réels (mais lisez cet article jusqu'au bout : il y a des pièges). Ici, par exemple, sur Proton Mail :

Sans la configuration d'un code PIN sur la clé, le vol de la clé permet au voleur de se faire passer pour vous. Il ne faut donc l'utiliser qu'en combinaison avec un autre facteur. Certaines clés, plus coûteuses, peuvent reconnaitre leur utilisateurice par biométrie mais ne vous fiez pas aux promesses des commerciaux : la biométrie est très loin d'être la solution miracle. Non seulement un attaquant peut reproduire des caractéristiques biométriques (vous laissez vos empreintes digitales un peu partout) mais inversement, vos propres doigts ne sont pas forcément reconnus (les empreintes s'usent avec l'âge et vous aurez de plus en plus de problèmes).

Quand à la perte de la clé, elle doit être anticipée. Sans la clé, vous ne pourrez plus vous connecter. Comme le dit la FAQ <https://docs.nitrokey.com/nitrokey3/faq>, il faut avoir un plan B. Par exemple, lorsqu'on active la sécurité FIDO2/WebAuthn sur Cloudflare, le service fournit une longue série de chiffres secrets qui permettront de récupérer son compte, et suggère très fortement de les stocker dans un endroit sécurisé (à la fois contre le vol et contre la perte). Il n'y a pas de mécanisme de sauvegarde de la clé (c'est délicat à concevoir pour un dispositif dont le but est d'empêcher les clés privées de sortir). La solution la plus simple semble être d'avoir deux clés et d'enregistrer les deux auprès des services qui le permettent.

Pour gérer ma clé, j'utilise l'utilitaire en ligne de commande nitropy <https://docs.nitrokey.com/software/nitropy/>. La documentation en ligne n'est pas terrible (sauf pour la partie sur l'installation sur une machine Linux, où il faut configurer udev <https://docs.nitrokey.com/software/nitropy/linux/udev>). Mais le logiciel a une aide avec `--help`. Voici quelques exemples d'utilisation :

```
% nitropy list
Command line tool to interact with Nitrokey devices 0.4.45
:: 'Nitrokey FIDO2' keys
:: 'Nitrokey Start' keys:
:: 'Nitrokey 3' keys
/dev/hidraw3: Nitrokey 3 522A...

% nitropy nk3 status
Command line tool to interact with Nitrokey devices 0.4.45
UUID:               522A...
Firmware version:   v1.5.0
Init status:        ok
Free blocks (int):  60
Free blocks (ext):  478
Variant:            LPC55
```

Pour finir, des liens utiles :

— Les documentations officielles de Nitrokey <https://docs.nitrokey.com/>.
— Une des raisons de mon choix pour la Nitrokey est son caractère ouvert <https://github.com/Nitrokey/>.
— Un autre service de test <https://www.token2.com/tools/fido2-demo> et un troisième <https://demo.yubico.com/webauthn-technical/> (bien qu'il soit fait par la société Yubi, il marche avec la Nitrokey).
— Plusieurs services ont la possibilité de s'authentifier via FIDO2 / WebAuthn : outre Proton Mail <https://proton.me/support/two-factor-authentication-2fa> et Cloudflare, déjà cités, il y a GitHub <https://docs.github.com/en/authentication/securing-your-account-with-t
configuring-two-factor-authentication#configuring-two-factor-authentication-using-a-
PyPi <https://pypi.org/manage/account/webauthn-provision> et bien d'autres <https://hideez.com/pages/supported-services> (cf. aussi cette seconde liste <https://www.dongleauth.com/>).
— Les autres modèles de clé similaires à la Nitrokey : Yubikey <https://www.yubico.com/>, Thetis, Google Titan <https://store.google.com/fr/product/titan_security_key>, Winkeo Fido2 de Néowave <https://neowave.fr/fr/produits/gamme-fido-2/winkeo-a-fido-2/>...