Dossier documentaire MFA et OTP

Les mots de passe à usage unique basé sur le temps (HOTP / TOTP)

HOTP

HOTP (pour HMAC One Time Password) est un mécanisme d'authentification reposant sur l'utilisation d'une **clé secrète** et d'un **compteur commun** entre le **client** et le **serveur**.

> **HOTP** ne nécessite donc pas l'utilisation d'une horloge.

HOTP se base sur **HMAC**. HMAC est un type de code d'authentification de message qui combine l'utilisation d'une **fonction de hachage** (SHA-256) avec une **clé secrète** dans le but de vérifier simultanément l'intégrité des données et l'authenticité du message.

Toutefois, HOTP est susceptible de **perdre la synchronisation du compteur** entre le client et le serveur. Il peut ainsi s'avérer difficile de maintenir un compteur commun.

TOTP

Un mot de passe à usage unique **basé sur le temps** (TOTP, Time based One Time Password en anglais) est un algorithme permettant de générer un mot de passe à **usage unique**. TOTP permet la **génération d'une séquence de caractères** valable seulement pendant un **intervalle de temps limité** afin de constituer un mécanisme de double authentification. C'est une extension du mot de passe à usage unique basé sur HMAC.

> Contrairement à HOTP qui nécessite un compteur incrémental partagé entre les deux entités pour garantir l'utilisation unique, TOTP utilise l'heure et un secret partagé.

Un intervalle de temps de validité est défini pour tolérer une désynchronisation des horloges. Source : Wikipédia

Phase d'enregistrement

Phase d'authentification

Dans le schéma ci-dessus, nous constatons que la clé secrète est commune et qu'elle a été transmise au client lors de la phase d'enregistrement. L'avantage de passer par une clé de sécurité est de pouvoir stocker cette clé secrète sur un matériel spécifique et non directement sur le smartphone ou sur l'ordinateur client.

•

> **Attention !** TOTP ne protège pas d'un certain nombre d'attaques (phishing, fuite du secret commun sur le serveur). Cette méthode d'authentification ne respecte pas l'état de l'art.

Rappel concernant les facteurs d'authentificaiton)

Voici les catégories de facteur d'authentification :

- **facteur de connaissance** : « ce que je sais », il s'agit d'une connaissance mémorisée ;
- **facteur de possession** : « ce que je possède », il s'agit d'un élément secret non mémorisable contenu dans un objet physique qui protège cet élément de toute extraction ;
- **facteur inhérent** : « ce que je suis », il s'agit d'une caractéristique physique indissociable d'une personne (ADN, empreinte

digitale, empreinte rétinienne).

> Selon l'ANSSI, le **facteur inhérent** n'est recommandé qu'avec l'usage d'un facteur de possession dans le but du déverrouillage d'un élément permettant l'authentification forte.

Rappel concernant la différence entre authentification multifacteur et authentification forte

En langue française, l'authentification **multifacteur** est souvent **confondue** avec l'appellation authentification **forte** (ou robuste), ce qui laisserait entendre qu'une authentification multifacteur est nécessairement plus robuste qu'une authentification avec un unique facteur.

Il convient ainsi de différencier authentification multifacteur et authentification forte. D'une part, une authentification multifacteur est une authentification faisant intervenir plusieurs catégories de facteurs. Néanmoins, **ces facteurs, pris indépendamment ou ensemble, ne sont pas forcément considérés comme étant forts** (un exemple typique étant un mot de passe associé à un code temporaire reçu par SMS).

D'autre part, une **authentification forte** (qui repose généralement sur un facteur unique) est une **authentification reposant sur un mécanisme cryptographique** dont les paramètres et la sécurité sont jugés robustes (l'élément secret est alors généralement une clé cryptographique).

Source : Guide de « Recommandations relatives à l'authentification multifacteur et aux mots de passe » publié par l'ANSSI