AUTHENTIFICATION FORTE VIA OTP

LUCAS THITEUX
BLOC 1 - 2019-2020
INFORMATIQUE & TECHNIQUE
BACHELIER EN SECURITE DES SYSTEMES

Table des matières

0. Introduction 2
1. Du hard-token au soft-token 2
2. Fonctionnement des One-Time Password (OTP)..... 4
3. HOTP 4
4. TOTP 5
5. Risques d'utilisations d'OTP 5
5.1. Générateur d'OTP hard-token : 5
5.2. Générateur d'OTP soft-token : 6
6. Conclusion.....6

0. Introduction

Les risques de l'authentification par couple login et mot de passe ne sont plus à prouver. Les principaux risques de cette méthode sont la divulgation de ceux-ci (piratage et publication massifs de base donnée en ligne) et par leurs faiblesses qui permettent aux personnes mal intentionnées d'utiliser des techniques afin de deviner ceux-ci (craquage, ingénieries sociales, …).

L'authentification forte est apparue pour résoudre ces problèmes : elle consiste à combiner divers facteurs, de nature distincte.

Parmi ceux-ci, les plus souvent représentés sont :

1. Ce que l'entité connait (mot de passe, code pin, …).
2. Ce que l'entité possède (carte à puce, clé USB, …).
3. Ce que l'entité est (reconnaissance faciale, empreinte digitale, …).
4. Ce que l'entité sait faire ou fait (reconnaissance vocale, signature manuscrite, …).
5. Où l'entité se trouve (localisation).

Ce document a pour but de se concentrer sur le deuxième facteur d'authentification, c'est-à-dire sur ce que l'entité possède et plus précisément sur les générateurs d'OTP. Il développera les sections suivantes : leur évolution dans le temps, leur fonctionnement, les avantages et inconvénients d'implémentation ainsi qu'une conclusion qui évoquera les futures technologies et les menaces qu'impliquent ces dernières.

1. Du hard-token au soft-token

L'authentification forte est apparue dans les entreprises sous forme de token physique. Celui-ci générait un mot de passe unique d'une durée de vie limitée (OTP) qu'il fallait introduire en plus du couple login / mot de passe.

Ces tokens physiques se présentaient sous la forme de petits boitiers que l'on pouvait accrocher à son porte-clés ou sous forme de carte magnétique que l'on pouvait conserver dans son portefeuille (voir figure 1.1 et 1.2).

Figure 1.1

Figure 1.2

Cette technologie n'était pas seulement présente dans le monde de l'entreprise, elle était aussi présente dans le monde du jeu vidéo. De 2010 à 2015, les utilisateurs de la plateforme battle.net (Blizzard Entertainment) pouvaient augmenter la sécurité de leur compte en achetant un « Battle.net authenticator » (voir figure 1.3) qui leur procurait un OTP nécessaire lors de chaque utilisation de la plateforme.

Figure 1.3

Toutefois, la mise en place et la gestion de ces « hard-tokens » impliquait un certain coût pour les entreprises. La démocratisation des smartphones a permis aux entreprises de fournir une alternative robuste par l'installation d'applications génératrices d'OTP équivalentes aux solutions apportées par les hard-tokens. Ces applications se nomment « soft-token ». Leurs coûts de déploiement et de gestion sont bien inférieurs.

Pour reprendre l'exemple précédemment cité, la plateforme battle.net a elle aussi changé de stratégie pour une application soft-token appelée « Blizzard Authenticator ».

2. Fonctionnement des One-Time Password (OTP)

Le site *idento.fr* désigne un « One-time Password » (mot de passe à usage unique) comme un *« mot de passe généré pour être utilisé lors d'une unique session, transaction sur un système informatique ou autre appareil numérique ».*

Les OTP présentent plusieurs avantages :

- Ils sont faciles à implémenter car ils sont open-source.
- Ils génèrent des codes à usage unique ce qui leur permet d'éviter les attaques « par rejoué ».
- Ils ne nécessitent pas forcément l'utilisation d'internet.

Ils fonctionnent grâce à deux composants : un générateur d'OTP et un serveur d'authentification.

1. Le serveur commence par générer et envoyer un « seed » au générateur.
2. Le générateur génère un OTP à travers plusieurs itérations sur base d'un secret connu par l'utilisateur et sur base du « seed » fourni par le serveur. Il le transmet ensuite au serveur d'authentification.
3. Le serveur génère l'OTP attendu et le compare à celui envoyé précédemment par le générateur.
4. Enfin, le serveur valide ou refuse l'authentification.

3. HOTP

HMAC-Based One-Time Password (*Hash-based message authentification codes*) est un algorithme qui est apparu en 2005 et qui est basé sur les évènements.

L'Initiative for Open AuTHentication (OATH) est un groupe de collaboration internationale qui a pour but de promouvoir l'authentification forte open-source. L'HOTP fait partie des standards développés par l'OATH.

Cet algorithme génère des OTP à partir du seed et d'un compteur. Le serveur commence par générer le seed et le transmet au générateur. Le générateur effectue ensuite une fonction de hachage SHA1 sur le seed mixé à la valeur du compteur. Après cette opération, il incrémente la valeur du compteur et transmet l'OTP au serveur pour validation.

Le serveur, lui aussi, génère l'OTP et le compare à celui reçu. Si et seulement si l'OTP généré et celui transmis par le générateur sont équivalents, la valeur du compteur du serveur est incrémentée.

Des problèmes de synchronisation entre les compteurs peuvent survenir si le serveur ne valide pas l'OTP du générateur. C'est pourquoi le serveur

essayera des OTP avec des valeurs compteur proches de celle du compteur jusqu'à une limite définie.

Cette limite est appelée « look-ahead window » et sa valeur recommandée est entre 80 et 100. Si le compteur du générateur dépasse cette limite, les compteurs du générateur et du serveur doivent être resynchronisés.

De plus, un OTP généré n'a pas de durée de vie tant que l'on ne l'utilise pas ou que l'OTP suivant n'est pas utilisé.

4. TOTP

Time-based One Time password est un algorithme apparu en 2011 basé sur le temps et fait également partie des standards développés par l'*OATH*. Il est basé sur le HOTP mais utilise l'heure Unix (ou Posix) plutôt qu'un compteur.

Cet algorithme évite donc le problème de synchronisation car tous les processeurs possèdent une horloge interne basée sur l'heure Posix (nombre de seconde depuis le 1er janvier 1970 à minuit pile). Donc le générateur et le serveur possèdent la même valeur.

De plus, toutes les x secondes, un nouvel OTP est généré. Par conséquent, l'OTP précédemment généré ne sera valide que pendant cet intervalle.

5. Risques d'utilisation d'OTP

Les OTP permettent de combler certaines lacunes associées aux mots de passe statiques (attaques par rejoué, faiblesses des mots de passe, …). Cependant, certaines de leurs utilisations peuvent présenter des failles dont il faut tenir compte.

5.1. Générateur d'OTP hard-token :

Les hard-tokens constituent une alternative assez coûteuse mais qui présente quelques avantages par rapport aux soft-tokens. La majorité de ces appareils sont conçus pour être « tamper-résistant », c'est-à-dire qu'ils offrent des sécurités contre les techniques de reverse engineering ayant pour but de découvrir le seed du générateur.

Cette sécurité nécessite cependant l'utilisation d'une pile interne non remplaçable, ce qui ne permet qu'une durée de vie limitée pour l'appareil.

Une gestion des cycles de vie des tokens doit donc être mise en place lors de l'implémentation de ces appareils.

5.2. Générateur d'OTP soft-token :

L'utilisation de soft-tokens a beaucoup d'avantages par rapport aux hard-tokens. Parmi ceux-ci, on trouve leur coût et le fait qu'ils puissent être installés sur plusieurs types de systèmes (ordinateur, smartphone, …). Cependant, ils sont vulnérables à plusieurs types de techniques telles que « man in the middle » utilisée lorsque les OTP sont transmis via un réseau. Ils sont aussi vulnérables aux techniques de reverse engineering.

6. Conclusion

L'authentification forte via OTP était, par le passé, réservée uniquement aux grandes entreprises en raison de son coût et de sa gestion compliquée. Désormais, grâce aux générateurs de soft-tokens, cette solution s'est démocratisée et est accessible à tous.

Cependant, l'utilisation de soft-tokens lors de l'authentification doit être réfléchie et correctement implémentée car leur utilisation entraine en effet des contraintes sécuritaires.

Un des impératifs à prendre en compte lors de l'implémentation des OTP est malheureusement souvent oublié : un OTP doit être à usage unique et limité temporellement.

Les utilisateurs rechignent à utiliser des mots de passe ou des codes pin. Dans un futur proche, pour améliorer l'expérience utilisateur et la sécurité de ceux-ci, les entreprises pourraient se tourner vers la technologie biométrique.

Désormais, de plus en plus de plateformes recommandent ou nécessitent l'utilisation d'applications de génération d'OTP. Cette tendance augmente fortement la sécurité des comptes des utilisateurs et il est désormais commun d'avoir plusieurs applications d'authentification forte installées dans son smartphone.

Il existe même une application développée par Google qui permet de centraliser tous les OTP d'un utilisateur pour les différentes plateformes qu'il utilise. Cette application se nomme « *Google Authenticator ».*

Cependant, cette externalisation rend notre smartphone indispensable pour l'utilisation des différentes plateformes. Par conséquent, en cas de vol ou d'oubli de celui-ci, l'accès aux plateformes devient impossible.

Il est donc préférable soit d'externaliser les moyens d'authentification sur différents appareils pour ne pas dépendre exclusivement de l'un d'eux, soit d'utiliser d'autres techniques d'authentification forte (localisation, reconnaissance faciale…).

7. Bibliographie

- https://connect.ed-diamond.com/MISC/MISC-098/Tour-d-horizon-de-l-authentification-forte-MFA
- https://ssi.ac-strasbourg.fr/bonnes-pratiques/recommandations/lidentification-et-lauthentification/
- https://fr.wikipedia.org/wiki/Authentification_forte
- https://fr.wikipedia.org/wiki/Mot_de_passe_%C3%A0_usage_unique
- https://wowwiki.fandom.com/wiki/Battle.net_Authenticator
- https://www.securiteinfo.com/cryptographie/otp.shtml
- https://idento.fr/one-time-password-otp/
- https://www.protectimus.com/blog/hotp-algorithm/#What%20is%20HMAC
- https://fr.slideshare.net/Pronetis/pronetis-livre-blancotp
- https://blog.identityautomation.com/two-factor-authentication-2fa-explained-one-time-password-hard-tokens
- https://doubleoctopus.com/blog/tokens-hard-soft-and-whats-in-between/
- https://en.wikipedia.org/wiki/Tamperproofing
- https://www.sciencedirect.com/topics/computer-science/software-token
- https://www.silicon.fr/avis-expert/nouvelles-normes-et-biometrie-cles-du-futur-de-la-securite-digitale