Les mots de passe jetables (ou OTP : One Time Password)

Document réalisé par Cyril Labrousse

Présentation

Le but de l'utilisation des OTP est d'accroître la sécurité des accès à distance. En effet, le principe des OTP est simple : chaque mot de passe n'est utilisé qu'une seule fois, un mot de passe différent est donc utilisé a chaque ouverture de session. Ainsi, même si une personne écoute le réseau et intercepte le mot de passe, il sera inutilisable puisqu'il aura déjà été utilisé.

Principe de fonctionnement

Alors que la plupart des authentifications se font de manière simple (login / mot de passe), les OTP se basent sur le couple challenge / réponse. Voici le déroulement d'une authentification utilisant les OTP :

- Le client fait une demande de connexion au serveur à distance (ftp, ssh, telnet, …).
- Le serveur envoie un challenge au client, composé d'un compteur (un nombre plus grand que 1) et d'une graine (2 caractères suivis de 5 chiffres : aa11111).
- Le client calcule alors le mot de passe jetable localement grâce à un programme, en entrant le challenge et une phrase secrète qu'il a choisit auparavant. Une fois le mot de passe calculé, il est envoyé au serveur.
- Le serveur vérifie que le mot de passe correspond bien au challenge envoyé crypté, et permet ou non l'accès.

Le mot de passe jetable est généré en concaténant la graine et la phrase secrète, puis en appliquant une fonction de hachage (MD4 ou MD5) autant de fois qu'indiqué par le compteur. Le résultat est ensuite converti en six courts mots anglais qui constituent le mot de passe non réutilisable.

Le compteur est décrémenté à chaque connexion de l'utilisateur, et lorsque celui-ci arrive à 0, l'utilisateur se voit demander la création d'une nouvelle phrase secrète et d'une nouvelle graine.

Les failles des OTP

Comme tout système, les OTP possèdent des failles, cependant elles restent plus difficile à exploiter qu'avec l'utilisation de mots de passe classiques. Ces failles tournent essentiellement autour de l'attaque brut ou par dictionnaire en récupérant le challenge puis la réponse, et en essayant de retrouver la phrase secrète par exemple. L'utilisation d'un keylogger peut également servir à récupérer la phrase secrète de l'utilisateur lorsqu'il utilise un outil pour générer le mot de passe jetable.

Réalisation

La mise en place des OTP a été réalisée sur un serveur tournant sur la version stable 5.3 de FreeBSD, en installation minimale.

Initialisation :

Après avoir créé un compte utilisateur de test sur le serveur et s'y être connecté, l'utilisateur doit utiliser la commande **opiepasswd**

```
# opiepasswd
Updating Test:
You need the response from an OTP generator.
New secret pass phrase:
        otp-md5 499 fr9088
        Response:
```

Le serveur lance alors un challenge qu'il faut crypter en md5 : otp-md5 499 fr9088. Pour cela, il faut utiliser un générateur localement, **opiekey** sous FreeBSD par exemple, en lui donnant en paramètres le compteur et la graine :

```
# opiekey 499 fr9088
Using the MD5 algorithm to compute response.
Reminder: Don't use opiekey from telnet or dial-in sessions.
Enter secret pass phrase:
HESS OMIT FOIL HULL DOOM TINT
```

Une phrase secrète doit être entrée. Comme il s'agit de l'initialisation des OTP, n'importe quelle phrase de 10 caractères minimum peut être entrée. Le mot de passe jetable ainsi généré doit être donné à la commande **opiepasswd** en réponse au challenge :

```
# opiepasswd
Updating Test:
You need the response from an OTP generator.
New secret pass phrase:
        otp-md5 499 fr9088
        Response: hess omit foil hull doom tint
ID Test OTP key is 499 fr9088
HESS OMIT FOIL HULL DOOM TINT
```

L'initialisation est terminée et les futures connexions de l'utilisateur utiliseront à présent les OTP.

Connexion à distance :

Pour tester les OTP mis en place, nous allons nous connecter en **ssh** au serveur :

```
# ssh Test@192.168.0.40
otp-md5 498 fr9088 ext
Password:
```

La mire de login a changé, il faut résoudre le challenge pour se connecter, en utilisant **opiekey** comme précédemment. On reconnaît bien la graine, et le compteur décrémenté une fois. Une fois le mot de passe jetable généré localement avec **opiekey**, et entré dans la mire de login, la connexion est autorisée.

Notes :

Voici quelques options utiles de la commande **opiepasswd :**
-s graine permet de définir une graine au lieu d'utiliser la graine générée automatiquement.
–n nombre permet de définir l'état initial du compteur, qui est de 499 par défaut sur les tests effectués.
–c permet d'initialiser les OTP en entrant directement la phrase secrète souhaitée au lieu de résoudre un challenge. Cette option ne doit être utilisée que depuis une connexion sécurisée, sans quoi la phrase peut être récupérée en écoutant le réseau.
-d utilisateur permet de supprimer l'utilisation des OTP pour le compte en question.
Enfin, le nom d'un utilisateur peut être donné en argument à la commande, ce qui peut servir à l'administrateur pour initialiser les OTP des utilisateurs.

La commande **opiekey** possède une option très utile, **-n**, à laquelle on peut préciser le nombre de mot de passe à générer. Cela permet de noter les futurs mots de passe jetables, et de se connecter sans avoir besoin de calculer le mot de passe à chaque fois. Ceci peut être intéressent si l'on veut se connecter depuis une machine ne possédant pas de générateur d'OTP.

Sous Windows, le logiciel Winkey peut être utilisé pour calculer des OTP.

Documentation

Manuel français de FreeBSD :
http://www2.ru.freebsd.org/doc/fr_FR.ISO8859-1/books/handbook/one-time-passwords.html

Autres sites :
http://www.securiteinfo.com/crypto/otp.shtml
http://sawww.epfl.ch/SIC/SA/publications/FI96/fi-7-96/7-96-page4.html
http://www.onlamp.com/pub/a/bsd/2003/02/06/FreeBSD_Basics.html