Time-based One-Time Password

On Mon, Oct 03, 2016 at 06:06:29PM +0000, Lukas Blatter wrote:

> Bei pubkey Auth wird kein Passwort abgefragt?

Den privaten Teil des Schlüssels hast du bei dir auf dem Client. Eine Passwortabfrage passiert dann, wenn du den passwortgeschützt gespeichert hast.

> Funktioniert dies auch mit SCP oder Rsync? Respektive müssten diese

mit pubkey eingesetzt werden, damit der Authenticator umgangen werden kann? Es hängt vom Client ab. Mit den nativen Tools von OpenSSH (ssh, scp, sftp) läuft der Login so ab:

$ ssh host Verification code: 123456 Password for thomasb@host: password

Das heisst, der Benutzer sieht zweimal eine Abfrage nach einem Passwort.

PuTTY handelt das auch so ab. Ob andere Clients (z.B. WinSCP) das können, müsste man testen. Grundsätzlich begrüsse ich die Authenticator Möglichkeit. Allenfalls könnten wir dann die Regelmässigkeit der Passworterneuerung etwas reduzieren. Bei der Konfiguration von PAM könnte man forcieren, dass die Mitglieder einer bestimmten Gruppe nur per Pubkey oder per Authenticator einloggen können.

Wir könnten folgendes anbieten:

1.) Standard: Login mit Passwort, Pubkey und Authenticator und strengem

```
PW-Expiry
```

2.) Token: Login nur mit Authenticator und Pubkey (Benutzer kommt in eine

```
spezielle Unix-Gruppe, die das forciert)
```

3.) kein SSH: Login auf SSH gar nicht möglich (authorizedServices Attribut

```
beim Benutzer wird angepasst)
```

Würde sogar soweit gehen, dass wir uns das PW-Expiry im Fall 2 + 3 nochmals generell überlegen.

Gruss, Thomas.

On Tue, Oct 04, 2016 at 10:06:51AM +0200, Roman Fischer

wrote:

> Meine Ansicht: Wenn wir die Sicherheit des SSH-Zugangs erhöhen wollen, dann müssen wir so umstellen, dass nur Passwort+OTP oder Key-Login erlaubt sind. Solange wir auch „nur Passwort“ zulassen, erhöhen wir nur den Schutz für einzelne User aber nicht des Gesamt-Systems.

Ich würde dies schon primär als Massnahme sehen, mit dem ein einzelner Benutzer sich selber besser schützen kann. Vorallem die Benutzer, die häufig mit fremden Geräten arbeiten.

> Damit man auch einloggen kann, wenn man den Key nicht dabei hat, muss PW+OTP und Key-Login -gleichzeitig- aktiv sein (also kein entweder-oder). Seht ihr das auch so?

Ja, beides aktiv.

> Ich könnte mir noch vorstellen, dass wir im Self-Service eine Option bauen um den Public-Key hochladen zu können… oder ist das eine schlechte Idee?

Würde ich eher nicht machen. Ein mögliches Problem ist, dass man mit einem gestohlenen Passwort im Selfservice dann den Pubkey ersetzen kann.

Von Seite des Selfservice müsste das daher so gelöst sein, dass man das Enforcement von Pubkey + OTP einmalig aktivieren, dann nachher aber nicht mehr abschalten kann.

Gruss, Thomas.

Clients

https://winauth.com/

HW based Solution: Yubico

Auf dem Smartphone gibt es auch
https://play.google.com/store/apps/details?id=org.fedorahosted.freeotp