Tek-Kullanımlık Şifreler

Uzun ve sözlükte bulunmayacak, sayı ve karakterlerden oluşan en az 8 haneli şifre kullanımı tabiki güvenliğinizi arttırmakta.Şifre güvenliği hakkında bu tur şifreler seçmekten başka bir yol yok mu? İşte bu yazıda bu konuyu tartışacağız.

Normalde FreeBSD sisteminize girdiğinizde size kullanıcı adiniz ve şifreniz sorulur.Bu tur şifrelere, sisteme her girdiğinizde aynisini kullandığınız ve kendi başınıza değiştirebileceğiniz için, "Tekrar kullanıla bilinir şifre" adini veriyoruz.Bu da tabiki güvenlik olarak şifrenizi bilmeyen kimsenin sisteminize girmeyeceği ve sizin belgelerinize ulaşamayacağı anlamına gelmekte.Sisteminizde bulunan başka bir kullanıcı sizin şifrenizi bulması ise bu tur bir yöntemin sonunu getirmekte.

Sistem güvenliği için bunun yanında kullanabileceğimiz yöntem ise OTP (Tek kullanımlık şifreler." İsminden de anlaşılabileceği gibi, tek şifreyi sadece bir kere kullanabiliyor ve ayni şifreyi bir daha kullanamıyorsunuz.Böylece başka bir kullanıcı sizin şifrenizi öğrense bile kullanamıyor.Güvenlik açısından şifre kırıcılar, paket yakalayıcılar ve keylogger şeklinde adlandırdığımız klavyedeki tuşlamaları izleyen programlara karşı harika bir yöntem olarak kabul edilebilir.OTP sistemi hakkındaki RFC`lere Ietf sayfasindan[1] ulaşabilirsiniz.

OTP`ye giriş

OTP şu anda Telcordia olarak adlandırılan Bellcore`da S/Key adıyla anılan ve basta bedava olarak dağıtılan bir program olarak geliştirilmişti.Eğer bu konuda daha fazla bilgi almak isterseniz hakkındaki yaziyi[2] adresinden okuyabilirsiniz.

Bellcore daha sonra S/Key ismini onaylatıp ticari urun olarak geliştirmeye başladı.Yazılım başka bir yerde OPIE (Her şeyde tek kullanımlık şifre) adıyla devam etti.Daha sonra ise OTP donanım ürünlerinde de kullanılır hale geldi.Yazılım ve donanım olarak gelişimini daha detaylı şekilde bu[3] sayfadan okuyabilirsiniz.

Benim gibi sizin de FreeBSD sisteminize OTP`yi donanımsal olarak ekleyebilmek için gerekli parçaları alabilecek kadar zengin olmadığınızı varsayıp size sadece yazılımsal eklemeyi göstereceğim.

OTP FreeBSD sisteminizle beraber gelmekte.Eğer FreeBSD 4.x veya daha aşağı versiyonunu kullanıyorsanız muhtemelen hem `s/key` hem de `opie` sisteminizde yüklüdür. Bunlardan `Opie` MD5 kullanırken `s/key` MD4 kullanmakta.Bu yüzden FreeBSD 5.0`dan itibaren artık `s/key` yerini `Opie`ye bırakmakta.Bu yazıda da size `opie`nin konfigürasyonunu göreceğiz.

OTP`nın Başlatılması

`Opie`yi kullanmaya başlamadan önce kendinizi `/etc/opiekeys` altında bulunan veritabanına eklemeniz gerekiyor.Bunun için `opiepasswd` komutunu kullanacağız:

```
$ opiepasswd -c
Adding dlavigne6:
Only use this method from the console; NEVER from remote. If you are
using
telnet, xterm, or a dial-in, type ^C now or exit with no password.
Then run opiepasswd without the -c parameter.
Using MD5 to compute responses.
Enter new secret pass phrase:
Secret pass phrases must be between 10 and 127 characters long.
Enter new secret pass phrase:
Again new secret pass phrase:

ID dlavigne6 OTP key is 499 dh0391
CHUG ROSA HIRE MALT DEBT EBEN
```

Bu komutu çalıştırdığımda neler olduğuna yakından bakalım. `opiepasswd -c` komutunu ancak sistemimizin başında ya fiziksel olarak otururken veya `ssh` ile bağlı iken kullanmalısınız.Eğer buna uymaz ve örneğin telnet ile bağlı iken bu komutu kullanırsanız kullanacağınız şifre ve bunun sonucunda oluşturulacak tek kullanımlık anahtar ağ üzerinden açık olarak gönderilecek ve ağınızı dinleyen herhangi birisi bu şifreyi alıp OTP kullanmanıza rağmen hesabinizi kullanabilecektir.

Bu işlemden sonra, şifremin çok kısa olduğuna dair bir uyarı ile birlikte, ikinci kez şifremi girmem istendi.Oluşturulan bu şifre ayni ssh şifreleme yönteminde kullanılan anahtar ile ayni şekilde çalışmakta.Bu her kullanım açılısında kullanılacak ayni şifre olarak değil, benim bu veri tabanına `dlavigne6` hesabini ekleyen kişi olduğum ve sonucunda tek kullanımlık şifrenin sahibi olduğumu gösterir anahtar olarak kullanılmaktadır.

Bu noktada `opie` veri tabanında olduğumu doğrulayabilirim:

```
$ more /etc/opiekeys
dlavigne6 0499 dh0391           669a4a62db6714f3  Jan 18,2003 15:25:44
```

Bu çıktıda görebileceğiniz gibi ismim tek satırda; bir sayaç (499), bir kod (dh0391) ile bunu izleyen anahtar (669a4a62db6714f3) ve tarihten oluşmakta.Burada kullanılan sayaç ve kod her şifre yaratılısında kullanılacağından önemlidirler.

Kod ve sayaç değerlerinizi su şekilde kontrol edebilirsiniz:

```
$ opieinfo
498 dh0391
```

`opieinfo` komutu sisteme bir sonraki girişimde kullanılacak olan sayaç numarasını göstermekte.Burada giriş numarası ”498” ile ilişkilendirilmiş kodu beklediğine dikkat

edin.Ben ise sadece “499” ile ilişkilendirilmiş kodu bilmekteyim.Bir sonraki girişte kullanılacak kodu bulabilmek için bir hesaplayıcı kullanmam gerekecek, burada ise hesaplama görevini üstlenen program `opiekey` komutu olmakta.

Sisteme giriş

Bu noktada iki seçeneğim var: Ya her terminale girişimde başka bir terminal üzerinde `opiekey` komutunu kullanır ve çıktıyı girmek istediğim terminale yazarım veya kendime bütün kodların çıktısını alır ve bunlar bittiğinde yenilerini yaratırım.Her ikisini de deneyelim:

```
login: dlavigne6
otp-md5 498 dh0391 ext
Password:
```

Sisteme girdiğimde OTP sistemi beni karşılıyor. `opie` 498 numarası ile ilişkilendirilmiş tek kullanımlık şifreyi beklemekte.Normalde kullanıcıların sistem girişlerinde OTP kullanıp kullanmamak arasında secim yapabilmek gibi bir şansı bulunmaktadır.Bu yüzden eğer her zaman kullandığım şifremi girersem yine Kabul edilip sisteme girebilirim.

Eğer OTP kullanarak giriş yapmak istersem gerekli olan anahtarı hesaplamam gerekmekte.Nerde hesapladığım, şifrelenmemiş bir ağ bağlantısı üzerinde kullanmadıktan sonra fark etmiyor.Bunun için Alt-F3 kullanarak diğer bir terminale geçip oradan hesaplayıcıyı çalıştırabilirim.Hesaplayıcıyı kullanabilmek için üç şeyi bilmem gerekiyor:

- kullanılacak sayaç
- sayaç numarası ile ilişkilendirilmiş kod
- şifre

Burada önem verilmesi gereken şey her zamanki gibi şifremin bilinmemesidir.şifremi bilen tek kişi olarak sadece ben tek kullanımlık şifreyi üretebilmeli ve sisteme girebilmeliyim.

`Opiekey` komutunu kullanırken, giriş yapacağım sayacın numarasını da giriyorum:

```
$ opiekey 498 dh0391
Using the MD5 algorithm to compute response.
Reminder: Don't use opiekey from telnet or dial-in sessions.
Enter secret pass phrase:
MASK BALM COL HER RIFT TERM
```

İşlem sırasında şifremin de sorulduğuna dikkat edin.Bunun sonucunda 498 sayacıyla ilişkilendirilen şifre: `MASK BALM COL HER RIFT TERM` olarak gözükmekte.

Şimdi artik dogru şifreyi bildigime göre geri dönüp diğer terminalden girebilirim:

```
login: dlavigne6
otp-md5 498 dh0391 ext
Password: (here I pressed enter)
otp-md5 498 dh0391 ext
Password [echo on]: mask balm col her rift term
```

Bu sefer ise tekrar kullanılabilir şifremi girmek yerine, Enter tuşuna basıp echo`yu açıyorum.Tekrar kullanıla bilinen şifrelerin girilmesi sırasında her zaman kapalı olan bu özellik ben çıktı olarak aldığım şifreyi girerken birisi beni görse bile ayni şifreyi kullanarak sisteme giremeyeceği için OTP kullanımı sırasında açık kalabiliyor.Ayrıca tekrar kullanılabilir şifrelerin aksine büyük/ küçük harf ayrımı önemli olmuyor.

Şu anda eğer `opieinfo` komutunu verirsem 497 sayacıyla kullanılacak şifreyi görebilirim.Fark edebileceginiz gibi her tek kullanımlık şifre kullanılışında sayaç bir azalmakta bu yüzden 0 a yaklaştığımda yeni anahtarlar oluşturmam gerekecek.

Çoklu Anahtar Üretimi

Her giriş yapmaya çalıştığınızda yeni bir anahtar üretmek sıkıcı bir durum halini alabilir.Bu yüzden tüm kodları listelememize izin veren ikinci giriş yolumuza göz atalım.

Bu sefer `opiekey` komutu ile kaç tane kod üretmek istediğime göre bir numara veya `n` parametresini kullanacağım.Örneğin 497 ile başlayan bundan sonraki 10 kodun çıktısını almayı deneyelim:

```
$ opiekey -n 10 497 dh0391

Using the MD5 algorithm to compute response.
Reminder: Don't use opiekey from telnet or dial-in sessions.
Enter secret pass phrase:
488: COIN LO DOG GOLF ACTA FULL
489: SOD STUN SINK DRAW LAWN TILT
490: MALT STAY MASH CAR DEBT WAST
491: HOWE DRY WALL TOO BUDD SWIM
492: ROOT SPY BOND JEST HAIL SCAR
493: MEAN ADD NEON CAIN LION LAUD
494: LYLE HOLD HIGH HOME ITEM MEL
495: WICK BALI MAY EGO INK TOOK
496: RENT ARM WARN ARC LICE DOME
497: LEAD JAG MUCH MADE NONE WRIT
```

Bundan sonra kullanacağım 10 şifreyi bildiğime göre artık bunları ya bir kağıda yazıp cüzdanıma koyabilir veya komut sonucunda aldığım çıktıyı sistem üzerinde bir dosya olarak yazabilirim.çıktıyı başka bir dosya olarak kullanmak için şu komutu kullanabilir:

```
$ opiekey -n 10 497 dh0391 > secretlist
```

ve daha sonra yazıcıdan çıktısını alabilirim.çıktısını aldıktan sonra sisteminizdeki bu dosyayı sildiğinizden emin olun.Zira eğer sistemde bırakırsanız güvenlik açısından yaptığınız bunca şey boşa gidebilir.

Eğer sayacım artık sonlara geldiyse tekrar yeni şifreler üretmem gerekecektir.Bunu da `opiepasswd` komutuyla yapabilirim.Şifre veritabanında olduğum için artık `c` parametresi yerine `n` parametresini ve `s` parametresini beraber kullanabilirim.Sayacımı 499`a ayarlayıp kodumu dh1357 olarak belirlemek için su anda kullandığım için geçerli olan kodu girmem gerekecek:

```
$ opiepasswd -n 499 -s dh1357
Updating dlavigne6:
You need the response from an OTP generator.
Old secret pass phrase:
        otp-md5 8 dh0391 ext
        Response: loot omit safe eric jolt dark
New secret pass phrase:
        otp-md5 499 dh1357
        Response: hewn as dot mel mali mann
```

Sonuç

Peki OTP`yi ne zamanlarda kullanmalıyız?Uzaktaki bir bilgisayara girdiğinizde ssh kullanıyor olacağınızdan ve zaten ssh sizin için şifreleme işini halledip tüm iletişiminizin bu şifreleme ile güvenli hale getirildiğinden emin olduğu için OTP kullanmak pek iyi bir fikir değildir.OTP daha çok bir terminale girdiğinizde arkanızdan şifrenizi görebilecek olan kişiler olduğunda iyi bir yöntem olarak adlandırıla bilinir.İlk bakışta biraz saçma da gelse lap topunuzla kalabalık bir yerde olduğunuzu farz ederseniz çok yerinde bir yöntem olduğunu anlayabilirsiniz.

Sisteminize giren diğer kullanıcıları OTP kullanmak ve kullanmamak konusunda serbest bırakmak iyi bir fikir olacaktır.Tabi bunun yanında her zaman FreeBSD sisteminizin kullanıcılarınızı OTP kullanmaya zorlamasını da, `/etc/opieaccess` dosyasını yaratarak sağlayabilirsiniz. Fakat bunun çok güvenli bir yöntem olduğunu söyleyemeyiz.Eğer `man opieaccess` metnine bir göz atarsanız bunun bir güvenlik açığı olarak kabul edildiğini görebilirsiniz.

İyi çalışmalar.

1 http://www.ietf.org/html.charters/otp-charter.html
2 http://citeseer.nj.nec.com/haller94skey.html
3 http://www.deer-run.com/~hal/ns2000/otp.pdf

Özgür Özdemircili
http://www.enderunix.org
http://news.enderunix.org
http://haber.enderunix.org

Sorularınız için : dionypheles@gmx.net

Kaynaklar

Dru Lavigne “One-time passwords”

FreeBSD Handbook