

---

# OneTimePassword

**By rac**

Published: 07.01.2008 - 12:04

OTP wurde mithilfe folgender Anleitung installiert: [1](#)

1.  
aptitude install opie-client opie-server

2.  
pico /etc/pam.d/ssh

Folgende abänderung in ssh

1.  
# Standard Un\*x authentication.

2.  
#@include common-auth

3.  
auth sufficient pam\_unix.so

4.

---

auth sufficient pam\_opie.so

5.  
auth required pam\_deny.so

1.  
pico /etc/ssh/sshd\_config

Changed from no to yes

1.  
# Change to yes to enable challenge-response passwords (beware issues with

2.  
# some PAM modules and threads)

3.  
ChallengeResponseAuthentication yes

---

1.  
/etc/init.d/ssh restart

2.  
\* Restarting OpenBSD Secure Shell server... [ ok ]

Zum Anmelden mit OTPs ist eine Initialisierung des OPIE-Dienstes mit dem Befehl `opiepasswd -c` (`opiepasswd -fc`) notwendig. Dabei wird das Konto mit dem man gerade arbeitet, hinzugefügt. Zudem fragt der Generator nach einer mindestens 10-stelligen Passphrase, die als Parameter in die Erzeugung der Einmalpasswörter eingeht. Als Antwort wirft das Tool beispielsweise aus:

1.  
ID dab OTP key ist 499 wl3899

2.  
BUG KEEN SMOG MAP MOON TIDY

Die erste Zeile enthält die Sequenznummer (499) und das so genannte Seed (hier wl3899). Die zweite Zeile zeigt das dazugehörige, aus sechs Teilen bestehende OTP. Letzteres ist nur für Sonderfälle notwendig, da bei der nächsten Anmeldung am Server bereits das OTP mit der Sequenznummer mit der nächst niedrigeren Nummer abgefragt wird, in unserem Fall 498. Loggt man sich nun per SSH auf dem Server ein, zeigt der Login die Sequenznummer und das Seed an. Damit muss man nun einen OTP-Generator füttern, beispielsweise das in OPIE enthaltenen `opiekey`-Tool:

---

1.  
opiekey 498 wl3899

Leider gibt es dabei ein Problem: Ohne Zugriff auf einen Rechner mit opiekey sind wahrscheinlich nur Stephen Hawking und Bruce Schneier in der Lage, das Einmalpasswort auszurechnen. Der Rest der Menschheit muss weiter auf Hilfsmittel zurückgreifen. Am einfachsten ist die Zettelmethode. Dazu lässt man sich von opiekey mehrere OTPs im voraus berechnen, druckt die Liste aus und steckt sie sich in das Portemonnaie. Zwanzig solcher OTPs erzeugt etwa der Befehl, für die oben initialisierte Reihe:

1.  
dab@server:/etc/pam.d\$ opiekey -n 20 499 wl3899

2.  
Using the MD5 algorithm to compute response.

3.  
Enter secret pass phrase:

4.  
480: HILL ELK AMOK NOOK CITY FIRM

5.  
481: MOOR BELT LYE JOB AHM END

6.  
...

7.  
499: ROIL PEG LUKE RUSE DAWN ADD

---

Eleganter als eine OTP-Liste ist, auf einem Java-fähigen Handy die Java-Implementierung eines OTP-Rechners zu installieren und zu jeder abgefragten Sequenznummer und dem dazugehörigen Seed das OTP einzeln zu berechnen. Eine davon ist jotp, die als abgespeckte Version selbst auf einfachen Handys mit der Java Micro Edition (JME) läuft [2](#).

1. [1. http://www.heise.de/security/artikel/87555/0](http://www.heise.de/security/artikel/87555/0)
2. [2. http://tanso.net/j2me-otp](http://tanso.net/j2me-otp)

-->

**Trackback URL for this post:**

<http://www.2030.tk/trackback/32>