

# SSH - informacje ogólne

Położenie: (nie dotyczy)

© Imagine Studio 2005, <http://myGentoo.tk>

## Wstęp

Korzystanie z FTP ma wady:

1. Połączenie nie jest szyfrowane i można podsłuchać hasło.
2. Domyślnie korzystanie z konta roota jest wyłączone (opcja *RootLogin* w pliku *proftpd.conf* lub wpis w */etc/ftpusers*).
3. Nie obsługuje wielu poleceń systemowych.

SSH szyfruje połączenie, i to jeszcze przed autoryzacją hasłem (hasło nie jest nigdy przesyłane czystym tekstem). Zaleca się jednak używać autoryzacji w oparciu o klucze i tzw. przepustki, a nie o hasła systemowe. W pliku */etc/ssh/sshd\_config* ustawiamy opcje:

*PasswordAuthentication no*

*PubkeyAuthentication yes*

Należy pamiętać, iż pliki konfiguracyjne użytkownika (*\$home/.ssh/config*) nadpisują ustawienia zawarte w */etc/ssh/ssh\_config*, ale jeszcze większy priorytet mają opcje w linii komend. Oczywiście nie wszystkie opcje można nadpisać.

## Tworzenie klucza ogólnego

W czasie pierwszego uruchomienia serwera SSH (*/etc/init.d/sshd start*) generuje on następujące klucze:

Hostkey:

*/etc/ssh/ssh\_host\_key* (-rw-----) - identyfikacja serwera

*/etc/ssh/ssh\_host\_key.pub* (-rw-r--r--) - klucz publiczny serwera

DSA-Hostkey:

*/etc/ssh/ssh\_host\_dsa\_key* (-rw-----) - identyfikacja serwera DSA

*/etc/ssh/ssh\_host\_dsa\_key.pub* (-rw-r--r--) - klucz publiczny serwera DSA

RSA-Hostkey:

*/etc/ssh/ssh\_host\_rsa\_key* (-rw-----) - identyfikacja serwera RSA

*/etc/ssh/ssh\_host\_rsa\_key.pub* (-rw-r--r--) - klucz publiczny serwera RSA

Opis kluczy:

**RSA1** - algorytm stworzony w 1978, nazwa pochodzi od pierwszych liter nazwisk twórców; dotychczas udało się złamać 500-bitowy klucz; wszystkie klucze 700-bitowe i większe uważane są za bezpieczne; używa protokołu SSH1.

**RSA2** - używa protokołu SSH2.

**DSA** (*Digital Signature Algorithm*) - algorytm asymetryczny, amerykański standard narodowy uważany przez niektórych (Schneier) za bardziej bezpieczny, używa protokołu SSH2.

## Tworzenie kluczy indywidualnych

Po skonfigurowaniu serwera ssh (*/etc/ssh/sshd\_config*) oraz klienta ssh (*/etc/ssh/ssh\_config*), należy utworzyć klucze indywidualne (każdy użytkownik tworzy je na swoim koncie):

**ssh-keygen -t dsa**

W czasie tworzenia kluczy pada pytanie o tzw. przepustkę (*passpharese*). Nie jest ona tożsama z hasłem systemowym i powinna różnić się od niego. Akceptowane są spacje. Możliwe jest także ustanowienie "pustej przepustki" na potrzeby skryptów inicjowanych przez crona (zob. *BatchMode* w konfiguracji klienta ssh). Przepustki mogą być cachowane (tzw. *Agent SSH*, polecenie *ssh-add*) i wtedy nie trzeba podawać ich przy każdej operacji kopiowania (nie zaleca się jednak korzystania z tego).

Klucze zostaną utworzone w:

*\$home/.ssh/id\_dsa* (rw-----) - klucz prywatny (nie udostępniamy nikomu!)

*\$home/.ssh/id\_dsa.pub* (rw-r--r--) - klucz publiczny

Klucz publiczny należy przenieść (skopiować/wysłać dyskietkę) na komputer, z którym zamierzamy się łączyć, na konto o tej samej nazwie. Nazwę klucza zamieniamy przy tym na:

*\$homeZdalne/.ssh/authorized\_keys* (r-----)

Jeśli zamierzamy dodać kilka kluczy (wygenerowanych na różnych komputerach) wtedy dodajemy je po prostu za pomocą komendy:

```
cat id_dsa.pub >> $homeZdalne/.ssh/authorized_keys (r-----)
```

W pliku `$home/.ssh/authorized_keys` można umieścić linie z opcjami, np.:

```
command="JakiśSkrypt" (wykonywany po połączeniu użytkownika)
```

```
from="nazwa.dozwolonego.klienta"
```

## Ustanowienie połączenia

Wykaz możliwych komend (uwaga: nazwy komputerów muszą być zawarte w `/etc/hosts`, a po każdej zmianie nazwy naszego hosta, np. z `host` na `host.domena`, należy zmienić opcję `AllowUsers` w pliku konfiguracyjnym serwera):

```
ssh nazwaKomputera
```

```
ssh -l użytkownik nazwaKomputera [lub:]
```

**ssh użytkownik@nazwaKomputera** (logowanie się jako inny użytkownik, przy autoryzacji kluczami, nie będzie możliwe, gdyż nie mamy dostępu do klucza umieszczonego na innym koncie)

```
ssh -f użytkownik@nazwaKomputera aplikacja (uruchamia zdalną aplikację w tle, co umożliwia zamknięcie terminala)
```

## Transmisja plików

```
scp /home/użytkownik/plik.txt użytkownik@zdalnyKomputer:/home/użytkownik/
```

Możliwe jest także wydanie komendy odwrotnej, powodującej skopiowanie pliku ze zdalnego komputera na nasz dysk lokalny.

Innym narzędziem jest `sftp` (posiada takie funkcje jak `ftp`, ale jest szyfrowane).

## Zdalne uruchamianie programów

```
ssh użytkownik@zdalny.komputer "echo testowyList | mail adresat@domena.pl"
```

## Tunelowanie

Tunelowanie to łączenie naszego lokalnego portu z portem zdalnym. W efekcie użytkownicy obu sieci lokalnych mają wrażenie, że pracują w jednej sieci lokalnej bez pośrednictwa Internetu. Taki tunel może służyć do transportu mniej bezpiecznych protokołów, np. POP3. Najpierw łączymy się z naszym portem lokalnym (wybieramy pomiędzy 1024-65535):

```
ssh -L 10110:localhost:110 zdalnyKomputer (lokalny port to 10110, a zdalny to 110, czyli POP3)
```

Aby odebrać pocztę przez ten tunel, trzeba ją odebrać łącząc się po prostu na lokalny port 10110, a nie na zdalny 110. Tunel jest zamykany wraz z zamknięciem shella. Wykaz nasłuchujących portów można sprawdzić poleceniem:

```
netstat -l --tcp -p | grep ssh
```

Istnieje możliwość obejścia zabezpieczeń firewalla, np. tunelując usługę ftp przez port przeznaczony dla www.

## Problemy

Jeśli pojawia się komunikat "*Permission denied (publickey,keyboard-interactive)*", serwer SSHd nie rozpoznaje nazw NetBIOS we wpisie `AllowUsers`. Wydaje się, że nie korzysta on z pliku `/etc/hosts`, ale z pliku `/etc/nsswitch.conf` (na maszynie była kiedyś instalacja `ybind`) i gdy go brakuje lub gdy są nieodpowiednie wpisy, to nie rozpoznaje nazw hostów. (Niestety, nie wiem dlaczego tak jest i gdzie to zmienia się).

## Darmowe klienty SSH dla Windows

**SSH Secure Shell** (<http://osusls.osu.edu>)

**Tera Term** (<http://www.zip.com.au/~roca/ttssh.html>)

**Putty** (<http://www.chiark.greenend.org.uk/~sgtatham/putty>)

Więcej na temat SSH:

- "CHIP Special. Linux" 2001, wiosna, s. 58;
- <http://gorzow-wlkp.pl/linux/ssh2.html>