Secure communication

Using SSH, openssl and stunnel on OS/2

Peter Verweij

@ junk@molen.xs4all.nl

Content of this presentation

- Installing and using SSH (with demo)
- Installing openssl
- Installing and using stunnel (with demo)
- Installing and using gnu pg / with pmmail and thunderbird

The problem I had

- Wanted to access my mail-server
- Didn't want to have standard port 25 for smtp open
- If possible gain access to the whole server

Installing SSH (1)

- Download the required files at:
  http://users.socis.ca/~ataylo00/os2/utils
  The homepage of Alex Taylor
  openssh-5_3p1.wpi
  ssesinst.wpi
  tnpipe.wpi (not needed, vioroute is better)
  vioroute.wpi
- Installing openssh-5_3p1.wpi will install all the needed
- Don't forget to reboot

Installing SSH (2)

- Create a user key with:
  ssh-keygen.exe -b 1024 -t dsa
  It will store the key id_rsa and id_rsa.pub in the os2/.ssh by default (at the client)
- On the server make a user directory beneath c:\home
- Copy the id_rsa.pub file to the newly created user directory, and rename the file to authorized_keys

Installing SSH3

- Create a server key-pair with:
  ssh-keygen -b 1024 -t dsa -f /etc/ssh-host_dsa_key -N “”
- Create a user account with:
  user -a <name of user>
- In the directory c:\security\etc there is a file passwd
  edit the home directory of the user, and change CMD.EXE: to viostart.exe (with appropriate directory structure)

Installing SSH4

- In the directory c:\security\etc there's also a file acl, if you want you can restrict the access of the user.
- If you want you can now use SSH, but it uses simple user and password restriction.

Changing SSHD_config

- Change the port number!
- LoginGraceTime 300
- StrictModes yes
- RSAAuthentication no
- PubkeyAuthentication yes
- AuthorizedKeysFile .ssh/authorized_keys
- HostbasedAuthentication no
- IgnoreUserKnownHosts yes
- PasswordAuthentication no
- PermitEmptyPasswords no
- ClientAliveInterval 600
- ClientAliveCountMax 3
- Subsystem sftp c:\usr\bin\sftp-server.exe

Changing ssh_config

- Change to port to the server port

Adding icons

- Added icon for ssh-pop and ssh-vnc connection

```
/* start secure channel for POP client */
parse arg host user
if host = '' then do Say
Say 'Please specify the name of your POP server'
parse pull host
Say 'Please specify your SSH username'
parse pull user
end
Say 'Do not close this window when you using email'
'ssh -l 'user' -2 -N -L 25:127.0.0.1:25 -L 110:127.0.0.1:110
'host' '
'pause'
```

The vnc client

- The same as pop client, after the end statement change the lines to:
  ```
  'ssh -l 'user' -2 -N -L 5900:127.0.0.1:5900 'host
  'pause'
  ```
- Start regedit2, ad stringvalue allowloopback=1 at hini_user_profile, er_pmvncd

SSH a little demonstration

- Just for fun, you can use sftp plugin from netdrive to connect to your server, using ssh
- If you want to log your accounts or possible break-ins start syslogd in the tcpip\bin directory. The log file is in \mptn\etc directory

Using stunnel

- Pmmail has an integrated stunnel, client, so using stunnel should be user friendlier
- You have to install openssl first, at hobbes you will find: openssl-0.9.8n-os2knix-20100325-runtime.zip
- Put the openssl bin and dll directory in the path and libpath statement of config.sys
- Optionally perl can be used.

Create the needed certificates 1

- This is the hard part of using stunnel :-)
- Create a directory myca, with the following subdirectores:
- Private (for the keys)
- Certs (the certificates)
- Newcerts (unencrypted pem files)
- Crl (revokation directory)
- Create a file index.txt (empty, just 1 space)
- Create a file serial (with value 01 in it)

Create your CA certificate

- Go the the created directory and type:
  (you will be creating your ca certificate, beware to remember your passphrase)

  ```
  openssl req -new -x509 -extensions v3_ca
  -keyout private/myca.key -out certs/myca.crt
  -days 1825
  ```

- Change the openssl.conf

  ```
  dir      = .
  certificate = $dir/certs/myca.crt
  private_key = $dir/private/myca.key
  ```

Create your server certificate

- Create your server certificate request:
  ```
  openssl req -new -nodes -keyout private/server.key -out server.csr -days 365
  ```
- Sign your certificate request:
  ```
  openssl ca  -policy policy_anything -out certs/server.crt -infiles server.csr
  ```
- Put your server key in your certificate:
  ```
  cat certs/server.crt private/server.key > private/server-key-cert.pem
  ```

Create your client certificate

- It's the same as creating a server certificate. It makes it simple to change server into client, everything else keeps the same.

You should now have

- The following files:
  - myca.crt
  - server.crt
  - server.key
  - server-key-cert.pem
  - client-key-cert.pem
  - client.crt
  - client.key
- For further readings see: http://www.g-loaded.eu/2005/11/10/be-your-own-ca/

Install stunnel

- Download it from http://smedley.info
- Unzip it in a directory
- Change the stunnel.conf

```
cert = F:\tools\stunnel\server-key-cert.pem
key = F:\tools\stunnel\server-key-cert.pem
verify = 3
CApath = f:\tools\stunnel
CAfile = f:\tools\stunnel\myca.crt
debug = 7
output = stunnel.log
```

(see next page)

Changing stunnel.conf

```
[pop3s]
accept  = 995
connect = 110
[imaps]
accept  = 993
connect = 143
[ssmtp]
accept  = 465
connect = 25
[https]
accept  = 443
connect = 80
```

Just 1 thing for starting

- Copy the files:
  myca.crt
  server-key-cert.pem
  into the stunnel directory.
- Don't forget to add the contents of the client.crt file into the myca.crt file which is in the stunnel directory.
- Start stunnel with stunnel stunnel.conf

Stunnel and pmmail

- Copy the following files to pmmail\bin or other directory:
  - myca.crt (the original one, without the client.crt contents)
  - client-key-cert.pem
- In the settings of pmmail, put the needed information in the secure transfer tab.
- Verification level must be 2, with 3 I get problems

Thunderbird and stunnel

- In order to get thunderbird working you have to convert your client certificate to the p12 format:

  ```
  openssl pkcs12 -export -out client.p12 -inkey client-key-cert.pem -in client-key-cert.pem -certfile myca.crt
  ```

- Choose options, advanced, certificates, view certificates, your certificates to install the client certificate.

A little demonstration again

- Showing, stunnel with pmmail, thunderbird, but also with web/2 which now has https thanks to stunnel !!

Is everything now secure

- Until now only the connection to the (mail)server is secure.
- Everything from your mailserver to all other mailservers is insecure.
- If you also want to secure this, encrypt your messages! Use gnuPG

Installing gnu pg

- Download gnu pg from: http://www.tobiashuerlimann.de/software/gnupg
- Download enigmail from: http://enigmail.mozdev.org/home/index.php choose save as for the xpi package, otherwise you will install it in firefox.

- Install the gnu pg wpi package.
- Start thunderbird and install the xpi package, add-ons, install

Using gnu pg

- Create a new key-pair, using setup wizard.
- Sign or encrypt your messages, only encrypted ones are save.
- Attachments are not encrypted, thunderbird does do it, but pmmail can't

A little demonstration

- Keys in thunderbird

Thanks for your attention