Prof. Dr. Christian Schindelhauer
Hoor Al-Hasani, Elmar Haussmann,
Julius Holderer, Dirk Kienle

Freiburg, 2010-01-13

Practical Exercises
Communication Systems (Rechnernetze II)
Topic 20: IPsec

IPsec is the extension of Internet Protocol, for a purpose of establishing a secure communication.
In order to do so, a Pre shared Key (Internet exchange keys)+ Authentication Header (AH) + Encapsulating Security Payload (ESP) must be introduced in each part of the communication.
For this Exercise sheet, the communication will be between two laptops.

Exercise 1:
One laptop should generate the AH and the ESP, for the keys must be identical in both laptops.

- For AH use this command: `dd if=/dev/random count=16 bs=1| xxd -ps`
- For ESP use the same command but with 192 bit: `dd if=/dev/random count=24 bs=1| xxd -ps`

The configuraton for two laptops **A** 10.0.2.5, **B** 10.0.2.6:

- **In laptop A:**

```
/etc/setkey.conf
flush;
spdflush;
add 10.0.2.5 10.0.2.6 ah 0x200 -A hmac-md5 ADD HERE THE AH KEY;
add 10.0.2.6 10.0.2.5 ah 0x300 -A hmac-md5 ADD HERE THE AH KEY;
add 10.0.2.5 10.0.2.6 esp 0x201 -E 3des-cbc ADD HERE THE ESP KEY;
add 10.0.2.6 10.0.2.5 esp 0x301 -E 3des-cbc ADD HERE THE ESP KEY;
spdadd 10.0.2.5 10.0.2.6 any -P out ipsec
esp/transport//require
ah/transport//require;
spdadd 10.0.2.6 10.0.2.5 any -P in ipsec
esp/transport//require
ah/transport//require;
```

- **In laptop B:** Use the same configuration in A, reverse the ”Out” to ”In” and vise virsa in B.
- Use the command `setkey -f /etc/setkey.conf` after these changes.
- Ping each other, check the packets being exchanged in wireshark.

Exercise 2:
In this exercise, the tool racoon will be used for Pre Shared Keys:

- **In laptop A:**

1. Configure the file setkey.sh `/etc/racoon/setkey.sh`

   ```
   flush;
   spdflush;
   spdadd 10.0.2.5 10.0.2.6 any -P out ipsec ipcomp/transport//use
   esp/transport//require;
   spdadd 10.0.2.6 10.0.2.5 any -P in ipsec ipcomp/transport//use
   esp/transport//require;
   ```

2. Configure the file psk.txt `/etc/racoon/psk.txt`

   ```
   10.0.2.5 ADD HERE THE PASSWORD
   10.0.2.6 ADD HERE THE PASSWORD
   ```

3. Configure the file racoon.conf `/etc/racoon/racoon.conf`

   ```
   path include ”/etc/racoon”;
   path pre_shared_key ”/etc/racoon/psk.txt”;
   remote 10.0.2.6
   { exchange_mode main;
   proposal
   {
   encryption_algorithm 3des;
   hash_algorithm md5;
   authentication_method pre_shared_key;
   dh_group 2; }
   }
   sainfo anonymous
   {
   pfs_group 2;
   encryption_algorithm 3des, blowfish 448, rijndael ;
   authentication_algorithm hmac_sha1, hmac_md5 ;
   compression_algorithm deflate ;
   }
   ```

- **In laptop B:**

  1. Configure the file setkey.sh `/etc/racoon/setkey.sh`
     change ”Out” to ”In”, and visa virsa!
  2. Configure the file psk.txt `/etc/racoon/psk.txt`
     Psk should be the same for both laptops.
  3. Configure the file racoon.conf `/etc/racoon/racoon.conf`
     change the remote address to your partner’s address.

- Use the following command to find the racoon’s process ID and kill it!
  ps −ef | grep racoon (to kill: *kill pid*)

- Now ping each other after excuting on both laptops the following commands:

  ```
  setkey -f /etc/racoon/setkey.sh
  racoon -f /etc/racoon/racoon.conf
  ```