Prof. Dr. Christian Schindelhauer
Julius Holderer, Dirk Kienle

Freiburg, 2009-12-07

Practical Exercises

Communication Systems (Rechnernetze II)

Topic 16: SSH

Exercise 1:

Create an RSA key pair for SSH. This allows to autologin on an remote machine without a password or run a command remotely without password interaction. Work together with your neighbor! One of you as server and one as client.

- CLIENT only:
  Create an RSA-key pair: *ssh-keygen -t rsa*. The default filename is ok. Do not insert a password. The created files are in */root/.ssh/*. There should be two files: The public key file *id_rsa.pub* and the private key file *id_rsa* .
  Now copy the public key file to directory */root/.ssh/* on the Server. The directory *.ssh* may not exist.
- SERVER only:
  Create the file */root/.ssh/authorized_keys2* and insert the public-key:
  cat id_rsa.pub » /root/.ssh/authorized_keys2
  Then start the SSH deamon: */etc/init.d/ssh start*
- Now establish a ssh connection using the *ssh* command.

Exercise 2:

Tunneling TCP Data over SSH:
Sometimes it is useful to secure services via a secure channel (e.g. if no TLS implementation is available). To do so you can use a SSH tunnel. In this example you should tunnel cleartext data from a telnet session over a secure ssh connection.

- Open the ssh tunnel: *ssh -N -L 4321:localhost:23 root@192.168.10.1*
  This will forward the local port 4321 on your machine to the port 23 on the Server 192.168.10.1.
- Open a telnet session: *telnet localhost 4321*
  Because of the ssh tunnel all data send to your local port 4321 is send to the port 23 of the remote machine.

Take a look at the generated packets via wireshark. Compare the generated packets to the packets from a unencrypted telnet session.