



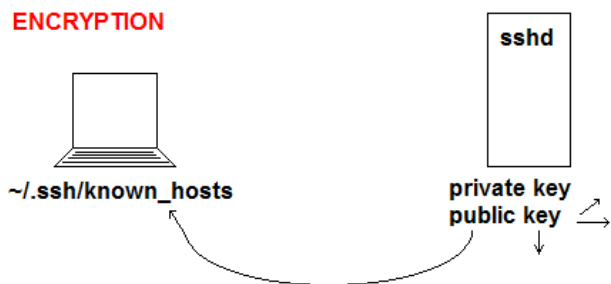
Requirements

- During the labs: use connections from SuSE to SuSE or from RedHat to RedHat to prevent version incompatibility.

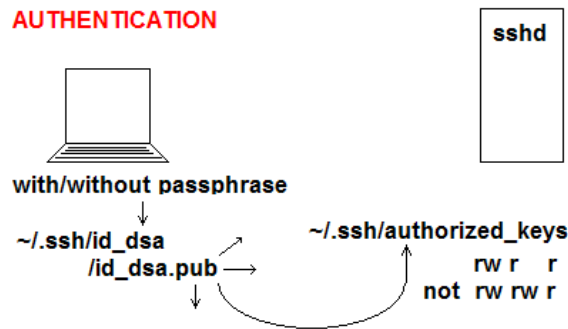
To Do

1. Ask your neighbor for an IP address of his server with the distribution of your choice.
2. Create a user on the neighbor's computer including a home directory using *ssh* and *useradd*.
3. Create a dsa key for automatic ssh logon (without a passphrase password) and put the public key on the remote host. Test the remote ssh logon (without a password).
4. Create a new private key with a passphrase and put the public key on the remote host.
5. Test the new key. Use '*ssh-agent bash*' and '*ssh-add*' to remember the ssh password during the life of the shell.
6. Start a remote X client with a local X server, e.g.:
`ssh -XC usr@remhost /sbin/yast2`

ENCRYPTION



AUTHENTICATION



Quick Reference Objectives to learn

```
Secure Teleworking #Execute next commands at local host:
scp file usr@remhost:/dir #Secure copy to remote host (ip or name)
sftp -C user@host #Secure ftp using ssh and compression
ssh usr@remhost #Secure telnet terminal
xhost [+remhost] #Enable a remote host to use the X server
#"unable to open display" error?: #Use: sux - or graphical login as root and
#the .Xauthority file will be created

#Create rsa|dsa keys for automatic logon:
ssh-keygen -t dsa -b 2048

#Put public key on the managed hosts:
scp ~/.ssh/id_dsa.pub usr@remhost:/tmp

ssh usr@remhost mkdir .ssh

ssh usr@remhost cat /tmp/id_dsa.pub >> ~/.ssh/authorized_keys #rw r r

#To make life easier after every reboot:
ssh-agent bash #Add passphrase interception
ssh-add #Add passphrase to running ssh-agent

#Start remote X-client and display locally
ssh -XC usr@remhost /sbin/yast2

#putty.exe and e.g. wiki.freedesktop.org/wiki/Xming for Windows

#Terminal Server client #See also ltsp.org. Enable remote access:
vi /etc/sysconfig/displaymanager #Tip: Use YaST or other GUI-tool on rem.host
DISPLAYMANAGER_REMOTE_ACCESS="yes"
X-query 172.28.24.24 #Gives local <alt-f7> for remhost (from init 3)
X-query 172.28.24.25 :1.0 & #Gives local <ctrl-alt-f8> for remhost
```

Theory Modules

- LPIC 1 Certification Bible, isbn 0-7645-4772-0
- p. 705-717 Using SSH
 - p. 371-375 Running X and clients remotely
- Downloadable manual(www.novell.com/documentation)
SUSE LINUX Enterprise Server – Install. and Admin.
- p. 652-656 SSH – Secure Shell, the Safe Alternative

Extra References

- www.tldp.org
- www.ltsp.org the Linux Terminal Server Project