Environment Canada Environnement Canada

Canada

THE TRICKS OF THE SSH MASTER

Michel Valin
CIOB / HPCS

What is ssh ?

- SSH (Secure Shell) is a network protocol allowing safe exchange of data
  - remote shell (instead of rsh/rlogin)
  - file transfer utilities (scp/sftp instead of rcp/ftp)
- Uses a client-server model
- Uses public-key criptography
- Identification credentials are always strongly encrypted
- Data encryption is optional

SSH client control

- $HOME/.ssh directory
  - must not be group or world accessible (700 permissions)
- Files in $HOME/.ssh directory
  - config (optional user configuration)
  - id_dsa id_dsa.pub (private and public keys)
  - authorized_keys2 (optional authorization file)
  - known_hosts
    - host keys for known and trusted machines
    - These keys may change when ssh software is reinstalled / reinitialized on a host, thereby triggering messages like

ssh ssh-server.example.com
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

SSH client control

- ls -al $HOME/.ssh

```
drwx------  2 asphmfv hpcs  4096 Feb 11  2009 .
drwxr-xr-x 50 asphmfv cidu  8192 Nov 23 11:42 ..
-rw-r--r--  1 asphmfv hpcs  6150 Jan 28  2009 authorized_keys2
-rw-------  1 asphmfv hpcs    84 Jan 28  2009 config
-rw-------  1 asphmfv hpcs   668 Jan 28  2009 id_dsa
-rw-r--r--  1 asphmfv hpcs   617 Jan 28  2009 id_dsa.pub
-rw-r--r--  1 asphmfv hpcs 17505 Sep 29 15:15 known_hosts
```

SSH client setup

- mkdir $HOME/.ssh ; chmod 700 $HOME/.ssh
- create a key pair
  - ssh-keygen -t dsa (and answer questions)
- validate your own credentials
  - cat id_dsa.pub >> authorized_keys2
- test with a remote command
  - ssh localhost hostname
- some useful config file options
  - ForwardX11 no
  - StrictHostKeyChecking no

SSH client setup

- cd $HOME/.ssh
- ssh-keygen -t dsa

```
averroes 510% ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/users/dor/asph/mfv/.ssh/id_dsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /users/dor/asph/mfv/.ssh/id_dsa.
Your public key has been saved in /users/dor/asph/mfv/.ssh/id_dsa.pub.
The key fingerprint is:
03:2b:c2:74:d7:92:d4:48:f8:f3:6a:0a:cc:08:6b:dc asphmfv@averroes
```

All questions were answered with a carriage return

SSH client setup

- cat id_dsa.pub >>authorized_keys2
- echo StrictHostKeyChecking no >>config
- ssh localhost hostname

```
averroes 512% cat  id_dsa.pub >>authorized_keys2
averroes 514% echo StrictHostKeyChecking no >>config
averroes 515% ls -al
total 24
drwxr-xr-x  2 asphmfv hpcs 4096 Nov 24 13:09 .
drwxr-xr-x 51 asphmfv cidu 8192 Nov 24 13:01 ..
-rw-r--r--  1 asphmfv hpcs  606 Nov 24 13:07 authorized_keys2
-rw-r--r--  1 asphmfv hpcs   25 Nov 24 13:09 config
-rw-------  1 asphmfv hpcs  668 Nov 24 13:02 id_dsa
-rw-r--r--  1 asphmfv hpcs  606 Nov 24 13:02 id_dsa.pub
averroes 516% ssh localhost hostname
Warning: Permanently added 'localhost' (RSA) to the list of known hosts.
averroes
```

All set now !!

SSH client setup

- cd $HOME/.ssh
- cat config

```
averroes 504% cat config
BatchMode yes
StrictHostKeyChecking no
ForwardX11 no
Protocol 2,1
```

authorized_keys2 play by play

- from="142.135.1?.*,142.135.?.*",no-port-forwarding,no-X11-forwarding,no-agent-forwarding,no-pty,command="bin/command2" ssh-dss AAAAB3NzaC1kc3MAAACBALF1Eg6rF/mcyW9zkioKm3CcVxl/10j5twQGnSKAU8ukbIbkQdFuahD74XVefCoxMe26h0jMpgIYroriy7PDmcpZOn2+kiWNnkgy0sqn21HPVJqJJTPazdy6ng7NwJ9qFtrGq252u4+m8UWWLkwIRPxG87nahuXkUv36WljnHvHBAAAAFQCf+r8sk/vWECWN69lgpkmJkmfkPQAAAIEAqj06DHYMpjiIKKfWQC8h6ETZz+qYJxn9JKlGpsRNXjAmdfb5sF9a4hlbt6AHNaCFdtGXSSz39h9kH0m66x8Zt8B8uhwjg3XsUNOhQs/yKdubV2nkDDVqdYQlZAw1jkKX4fkQr5rFsjlE5mLGpXN3K9HIedCvvHiYjKnCnR3R1yEAAACBAK+qnOxWKrWHBEF9Oiaf4VNqjNeO8OTD4OmSzMMZe9z95bV59U2Kot/2w+KXpL8zoxU6MaCXZrShgQxEEiPnA85hbAwxra28K70POQ9MT8aFTkfi7RhbYduBbwAxH4tyMxwYZlK2hprrPJCwr87qJkO4lkPdRGMAAqg+xumptcu0 armnmfv@rossby

authorized_keys2 play by play

- from="142.135.1?.*,142.135.?.*",no-port-forwarding,no-X11-forwarding,no-agent-forwarding,no-pty,command="bin/command2" ssh-dss AAAAB3NzaC1kc3MAAACBALF1Eg6rF/mcyW9zkioKm3CcVxl/10j5twQGnSKAU8ukbIbkQdFuahD74XVefCoxMe26h0jMpgIYroriy7PDmcpZOn2+kiWNnkgy0sqn21HPVJqJJTPazdy6ng7NwJ9qFtrGq252u4+m8UWWLkwIRPxG87nahuXkUv36WljnHvHBAAAAFQCf+r8sk/vWECWN69lgpkmJkmfkPQAAAIEAqj06DHYMpjiIKKfWQC8h6ETZz+qYJxn9JKlGpsRNXjAmdfb5sF9a4hlbt6AHNaCFdtGXSSz39h9kH0m66x8Zt8B8uhwjg3XsUNOhQs/yKdubV2nkDDVqdYQlZAw1jkKX4fkQr5rFsjlE5mLGpXN3K9HIedCvvHiYjKnCnR3R1yEAAACBAK+qnOxWKrWHBEF9Oiaf4VNqjNeO8OTD4OmSzMMZe9z95bV59U2Kot/2w+KXpL8zoxU6MaCXZrShgQxEEiPnA85hbAwxra28K70POQ9MT8aFTkfi7RhbYduBbwAxH4tyMxwYZlK2hprrPJCwr87qJkO4lkPdRGMAAqg+xumptcu0 armnmfv@rossby
- Only accept connections from network addresses
  - 142.135.[0 through 19].[0 through 255]

authorized_keys2 play by play

- from="142.135.1?.*,142.135.?.*",no-port-forwarding,no-X11-forwarding,no-agent-forwarding,no-pty,command="bin/command2" ssh-dss AAAAB3NzaC1kc3MAAACBALF1Eg6rF/mcyW9zkioKm3CcVxl/10j5twQGnSKAU8ukbIbkQdFuahD74XVefCoxMe26h0jMpgIYroriy7PDmcpZOn2+kiWNnkgy0sqn21HPVJqJJTPazdy6ng7NwJ9qFtrGq252u4+m8UWWLkwIRPxG87nahuXkUv36WljnHvHBAAAAFQCf+r8sk/vWECWN69lgpkmJkmfkPQAAAIEAqj06DHYMpjiIKKfWQC8h6ETZz+qYJxn9JKlGpsRNXjAmdfb5sF9a4hlbt6AHNaCFdtGXSSz39h9kH0m66x8Zt8B8uhwjg3XsUNOhQs/yKdubV2nkDDVqdYQlZAw1jkKX4fkQr5rFsjlE5mLGpXN3K9HIedCvvHiYjKnCnR3R1yEAAACBAK+qnOxWKrWHBEF9Oiaf4VNqjNeO8OTD4OmSzMMZe9z95bV59U2Kot/2w+KXpL8zoxU6MaCXZrShgQxEEiPnA85hbAwxra28K70POQ9MT8aFTkfi7RhbYduBbwAxH4tyMxwYZlK2hprrPJCwr87qJkO4lkPdRGMAAqg+xumptcu0 armnmfv@rossby
- No port will be forwarded in any direction

authorized_keys2 play by play

- from="142.135.1?.*,142.135.?.*",no-port-forwarding,no-X11-forwarding,no-agent-forwarding,no-pty,command="bin/command2" ssh-dss AAAAB3NzaC1kc3MAAACBALF1Eg6rF/mcyW9zkioKm3CcVxl/10j5twQGnSKAU8ukbIbkQdFuahD74XVefCoxMe26h0jMpgIYroriy7PDmcpZOn2+kiWNnkgy0sqn21HPVJqJJTPazdy6ng7NwJ9qFtrGq252u4+m8UWWLkwIRPxG87nahuXkUv36WljnHvHBAAAAFQCf+r8sk/vWECWN69lgpkmJkmfkPQAAAIEAqj06DHYMpjiIKKfWQC8h6ETZz+qYJxn9JKlGpsRNXjAmdfb5sF9a4hlbt6AHNaCFdtGXSSz39h9kH0m66x8Zt8B8uhwjg3XsUNOhQs/yKdubV2nkDDVqdYQlZAw1jkKX4fkQr5rFsjlE5mLGpXN3K9HIedCvvHiYjKnCnR3R1yEAAACBAK+qnOxWKrWHBEF9Oiaf4VNqjNeO8OTD4OmSzMMZe9z95bV59U2Kot/2w+KXpL8zoxU6MaCXZrShgQxEEiPnA85hbAwxra28K70POQ9MT8aFTkfi7RhbYduBbwAxH4tyMxwYZlK2hprrPJCwr87qJkO4lkPdRGMAAqg+xumptcu0 armnmfv@rossby
- NO MATTER what was specified on the remote ssh command, the command that will be executed as myself will be
  - $HOME/bin/command2

authorized_keys2 play by play

- from="142.135.1?.*,142.135.?.*",no-port-forwarding,no-X11-forwarding,no-agent-forwarding,no-pty,command="bin/command2" ssh-dss AAAAB3NzaC1kc3MAAACBALF1Eg6rF/mcyW9zkioKm3CcVxl/10j5twQGnSKAU8ukbIbkQdFuahD74XVefCoxMe26h0jMpgIYroriy7PDmcpZOn2+kiWNnkgy0sqn21HPVJqJJTPazdy6ng7NwJ9qFtrGq252u4+m8UWWLkwIRPxG87nahuXkUv36WljnHvHBAAAAFQCf+r8sk/vWECWN69lgpkmJkmfkPQAAAIEAqj06DHYMpjiIKKfWQC8h6ETZz+qYJxn9JKIGpsRNXjAmdfb5sF9a4hIbt6AHNaCFdtGXSSz39h9kH0m66x8Zt8B8uhwjg3XsUNOhQs/yKdubV2nkDDVqdYQlZAw1jkKX4fkQr5rFsjlE5mLGpXN3K9HIedCvvHiYjKnCnR3R1yEAAACBAK+qnOxWKrWHBEF9Oiaf4VNqjNeO8OTD4OmSzMMZe9z95bV59U2Kot/2w+KXpL8zoxU6MaCXZrShgQxEEiPnA85hbAwxra28K70POQ9MT8aFTkfi7RhbYduBbwAxH4tyMxwYZlK2hprrPJCwr87qJkO4IkPdRGMAAqg+xumptcu0 armnmfv@rossby
- This is the public key that must match the private key used by the remote command
  - ssh -i private_key_file .....

authorized_keys2 play by play

- from="142.135.1?.*,142.135.?.*",no-port-forwarding,no-X11-forwarding,no-agent-forwarding,no-pty,command="bin/command2" ssh-dss AAAAB3NzaC1kc3MAAACBALF1Eg6rF/mcyW9zkioKm3CcVxl/10j5twQGnSKAU8ukbIbkQdFuahD74XVefCoxMe26h0jMpgIYroriy7PDmcpZOn2+kiWNnkgy0sqn21HPVJqJJTPazdy6ng7NwJ9qFtrGq252u4+m8UWWLkwIRPxG87nahuXkUv36WljnHvHBAAAAFQCf+r8sk/vWECWN69lgpkmJkmfkPQAAAIEAqj06DHYMpjiIKKfWQC8h6ETZz+qYJxn9JKlGpsRNXjAmdfb5sF9a4hlbt6AHNaCFdtGXSSz39h9kH0m66x8Zt8B8uhwjg3XsUNOhQs/yKdubV2nkDDVqdYQlZAw1jkKX4fkQr5rFsjlE5mLGpXN3K9HIedCvvHiYjKnCnR3R1yEAAACBAK+qnOxWKrWHBEF9Oiaf4VNqjNeO8OTD4OmSzMMZe9z95bV59U2Kot/2w+KXpL8zoxU6MaCXZrShgQxEEiPnA85hbAwxra28K70POQ9MT8aFTkfi7RhbYduBbwAxH4tyMxwYZlK2hprrPJCwr87qJkO4lkPdRGMAAqg+xumptcu0 armnmfv@rossby
- Comments about the origin of the key