

Setting up UUCP over SSH

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

First publication of this article on 28 March 2002. Last update on of 30 August 2006

<http://www.bortzmeyer.org/uucp-over-ssh.html>

UUCP is a very good way to distribute email to a domain (not just a specific individual but an entire domain, with several persons, mailing lists, aliases, etc) when the machine which serves the domain is not always connected or does not have a permanent address (dial-up with POTS or ISDN but also cable modems with dynamic IPs or frequent cut-offs). It was intended that way (unlike many hacks over SMTP) and it works.

UUCP can work over TCP, so you do not need to have the agreement of your access provider (which is great because, unfortunately, very few handle UUCP). Any server on the Internet will work fine for you (if you have trouble finding one, try <<http://www.uucpssh.org/>>).

But, by default, when you connect over TCP, the password is sent in cleartext, with the security problems it triggers.

Therefore, this page is dedicated to the setup of UUCP over SSH. It allows the use of UUCP over an encrypted tunnel. As with any security measure, it does **not** protect you against everything. It just solves the issue of UUCP passwords travelling in clear. Period.

Warning : the actual file names are taken from a Debian machine. On other Unices, the files may be at different places.

First, let us configure the server.

Create an anonymous account for UUCP like that :

```
anonuucp:*:400:400:Anonymous UUCP:/home/anonuucp:/bin/ash
```

Be sure the shell exists : most SSH versions will check that. Also, this user needs the right to run `uucico` (for instance, being member of the `uucp` group).

Make a RSA key without a password :

```
ssh-keygen -C "anonuucp@YOURNAME" -f ~anonuucp/key
```

Hit two returns when it asks the passphrase, so you'll get an empty one.

Authorize bearers of this key to connect (but only to run UUCP), by adding in `anonuucp/.ssh/authorized_keys` the public key (`anonuucp/key.pub`) :

```
no-port-forwarding,no-X11-forwarding,no-agent-forwarding,command="/usr/sbin/uucico -l" 1024 35 121718545783
```

You do not need to have an entry for UUCP in `/etc/inetd.conf`.

Now, let us configure the client.

Copy the private key on your machine, say in `/etc/uucp/anonuucp-YOURPROVIDER`. `chmod 600` it, SSH will check that. But be sure the UUCP user will be able to read it (for instance `chown uucp it`).

Add this in the UUCP `sys` file :

```
system YOURPROVIDER
call-login *
call-password *
time any
chat "" \d\d\r\c ogin: \d\L word: \P
chat-timeout 30
protocol i
port UUCPoverSSH
```

And in the UUCP `port` file :

```
port UUCPoverSSH
type pipe
command /usr/bin/ssh -a -x -q -i /etc/uucp/anonuucp-YOURPROVIDER -l anonuucp uucp.YOURPROVIDER.org
reliable true
protocol etyig
```

You should put the server's fingerprint in `known_hosts` (may be with a command performed by hand first). By default, SSH queries you and UUCP does not run interactively.

That's all : UUCP will be used as usual.

But not everything works the first time. What to do if we need debugging ?

Always check the logfiles (for instance `/var/log/uucp/Log`). You can have more debugging information from software with `'-x 9'`. It will be written in UUCP Debug logfile.

If the problem is an SSH one, running the `ssh` command in the `port` file, replacing `-q` (quiet) by `-v` (verbose) will help you a lot.

To learn more, you can see :

- Free implementations of SSH <<http://www.freessh.org/>>
- OpenSSH <<http://www.openssh.com/>>, the one I use
- Taylor-UUCP <<http://www.airs.com/ian/uucp.html>>, the UUCP I use.
- UUCP over TCP HOWTO <http://jimsun.linxnet.com/jdp/uucp_over_tcp/index.html>
- Plus ou moins le même texte mais in French <<http://linuxfr.org/2001/04/08/3065.html>>
- Alternative : use SSL instead of SSH <<http://taz.net.au/postfix/uucp/>>