MouSSH

der Mouse
BSDCan 2006
2006-05-12/13

- What is moussh?
- What prompted it?
- How is it distinctive?
    - What advantages?
    - What disadvantages?

What is moussh?

- An implementation of ssh2

What prompted it?

- Learning the protocol
- NetBSD dropping ssh1 access
  - ssh.com
  - OpenSSH
  - others

Advantages

- Under active development
- Completely independent implementation
- Fully open code (almost entirely PD)
- Connection sharing, notably auto-share mode
- TCP forwarding revocation works
- Very flexible config file language
- Improved known-hosts management
  - lookup key
  - more actions
- Additional crypto
  - non-AES Rijndael
  - ssh1-like kex from Ben Harris
  - fixed arcfour
- Missing pty modes
  - ECHOPRT, ALTWERASE, NOKERNINFO, CS*
- Connection-sharing-friendly forwarding
- Low encryption exponent RSA attack
- Client CLI
- Must-work command-line forwarding
- Comparatively small

Disadvantages

- Under active development
- Completely independent implementation
- Relatively new and un-beaten-on
  - password and keyboard-interactive auth
- No easy way to import known-hosts files
- No easy way to import private keys
- Nothing scp/sftp/etc-like
- No stock X forwarding
- No fallback to ssh1
- No compression
- Agent is single-threaded
- No privsep
- No sensitive-data memory separation
- Client CLI quit slightly broken
- Connection sharing loss handled badly
- Dependent on things like gcc and Torek stdio
- Deleting a key from the agent requires a file
- UTF-8 protocol conformance issues

Future work

- Fix disadvantages
- Interactive agent
- Check against RFCs
- Better internals doc