Intro. to discussion on Interactive sessions and password security

A.J.Flavell
Glasgow PPE Group

UK HEP SYSMAN @ UCL,
30 Sept 1998

Some problem areas:

- r-series commands (rsh etc) risky,
- .rhosts and .netrc abuses
- X Windows security problems
- plain text passwords vulnerable to sniffers
- trusted-host compromises

BUT:

- Users still reasonably want to do their work!
- And from sometimes strange places
- And run unattended batch work.

Aspects of security

It's a *compromise* (like locking your house)...

Primary security:

- Keep hackers out as far as possible
  - Turn off services you don't need
  - Keep abreast of security alerts
  - Cultivate user mindsets (some hope?)

Secondary security:

- Limit the damage they can do when in, remembering that they'll be using:
  - "Exploits" whereby user can get root
  - Sniffers, trojan horses etc.

Some approaches

- One Time Passwords
- Kerberos
- SRP http://srp.stanford.edu/srp/
- **ssh**

Others?

Legal problems:

- North American munitions legislation
- French crypto legislation -
- - and its impact on CERN policy
- ..then there’s Russia, India etc.

ssh is:

- a network protocol
- one implementation of that protocol
  http://www.cs.hut.fi/ssh/

Well, actually two of both:

- v1 is experimental and we can use it free
- v2 protocol is standards-track and incompatible, but the available implementation would not be free to us.

So we go with v1 for the moment, OK?

Other products, platforms

- AFS patch http://www.monkey.org/~dugsong/ssh-afs-kerberos.html (can be used with KTH KRB4)
- ttssh for w95/NT http://www.zip.com.au/~roca/ttssh.html
- ssh 1.2.26 ported to Cygwin (not tried yet)
- ssh 1.2.14 ftp.cs.hut.fi/pub/ssh/contrib/
- http://www.lysator.liu.se/~jonasw/freeware.html for the Mac
- DataFellows (commercial, rec. by SLAC)

ssh usage

- Secure shell (user interface similar to rsh)
- Many authentication options
- Use as replacement rsh, rlogin, **telnet**
- Port forwarding - use for many things (X, IMAP, POP etc.) FTP is messy.
- scp has other problems cross-platform
- Compression option sometimes useful.

To make some things palatable to users, we need nice recipes...

AFS interactions

- ssh+AFS can pass an AFS token
- sshd gets confused by unix permissions/ACLs
  - and so do users!
  - sshd gets upset by permissions settings on home directory and on .ssh: setting them to what sshd wants doesn’t seem to cause any harm(?)
  - but in AFS the permissions don’t do anything, the ACLs are what matters, and they are per-directory not per-file
  - when public and private files have to share the same directory, move the relevant files into public or private subdirectories and symlink to them.

ssh configuration options

- Wide range of server configuration choices
  - Some obviously unacceptable (.rhosts, .shosts)
  - A wide grey area
- User-baffling range of authentication options
  - teach them to use `-v` when things seem to be going wrong
- Keypair management is an issue
  - batch/cron/unattended jobs seem to haunt us
  - no “crack-style” check for passphrases?
- use of ssh-agent

X Windows

- To some extent ssh simplifies X Windows
- …but it also adds some complications of its own?
- Dealing with unix workstations is easy enough:
  `ssh -f remotehost xcommand`
- best way to handle exceed etc.?
- best way to handle X terminals?
- window manager? - session manager? HEPiX?

Miscellany

building ssh:

- KTH KRB4 libraries in wrong place
- r-series substitutes (optional)
- making the version details show up
- one person’s configuration recipe

Options for FTP (passive or not)

Misc. 2

- Harvesting host keys, and the mysteries of clusters
  - careless harvesting sets off security alarms
  - clusters like HPPLUS are interpreted as a single host with many interfaces, causing mayhem