**Privilege Separation**
- minimize damage from system compromise
- easier to reason about overall system

**OpenSSH (daemon)**
- open host’s private key
  - perform digital signatures with private key
- OS-level privilege operations
  - Opening a pseudo tty
- Switch it user id
  - After user logs in

![Diagram]

**Benefits**
- If slave is compromised
  - Limits damage (if bugs go to slave)
- If bugs go to monitor
  - Don’t know?
- If monitor is small, can verify its correctness
  - Also less likely to contain bugs
- Monitor must enforce a policy on its privileged interface
  - Must bind privilege and policy
**Privilege-separated OpenSSH**

**Privtrans**
- Automatically perform privilege separation
  - Author labels “privileged” functions and data
  - Privtrans generates monitor and slave

**Requirements:**
- monitor should be small
- policy should go in monitor
- should not create new bugs
- its easy
- should facilitate code audits
Privtrans

- Its easy – for author
  o Easier than manual
- Facilitate audits
  o Automatic? Ok
  o Manual? Not yet
- No new bugs
  o Not a sound transformation
- Small monitor
  o Yes
- Policy
  o Falls where it may.
  o But doing this automatically is very hard.