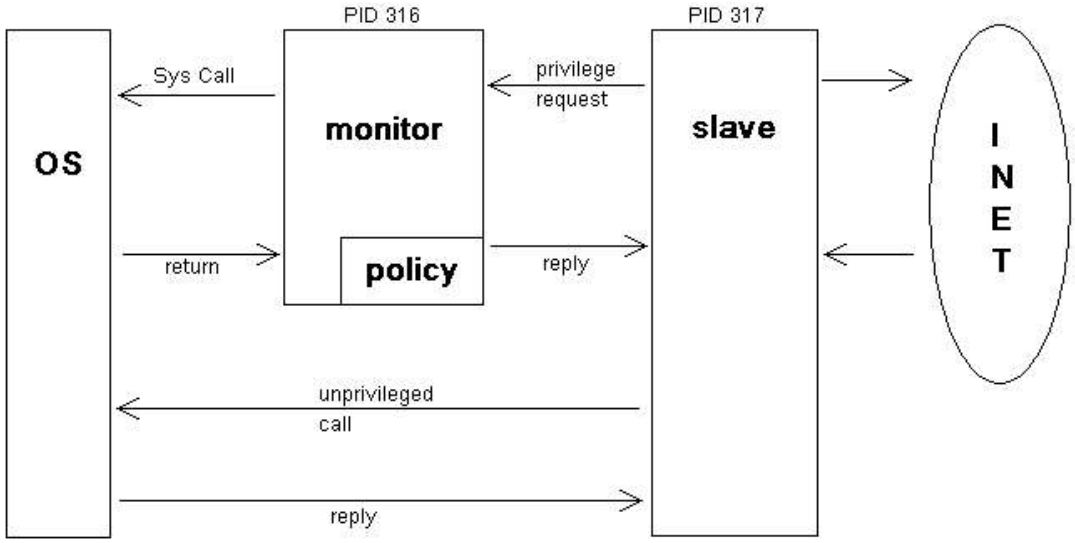
Note: 3/1/2007

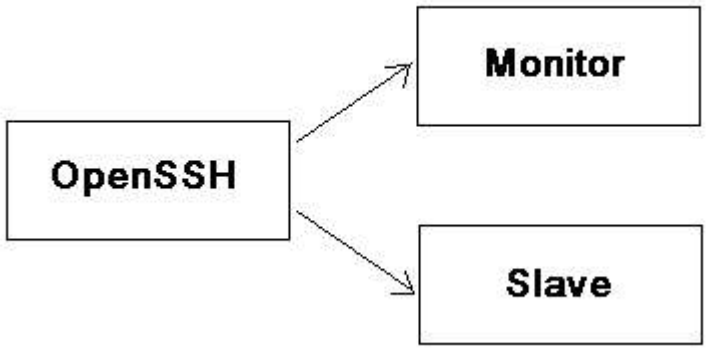
Privilege Separation

- Minimize damage from system compromise
- Easier to reason about overall system

OpenSSH (daemon)

- Open hosts' private key
  - Perform digital sigs of private key
- OS-level privileged operations
  - Opening a pseudo-tty
- Switch its user id
  - After user login





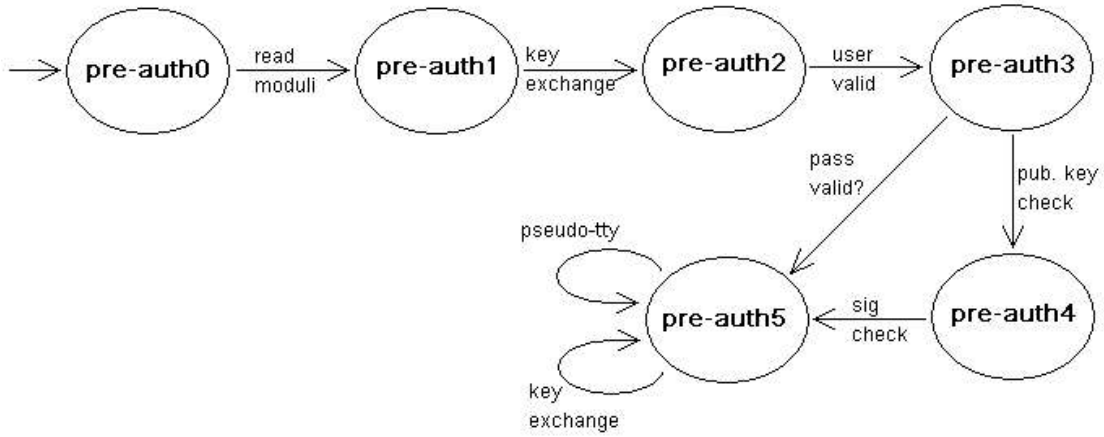
Benefits:

- If slave is compromised, limited damage? (if bug goes in slave only)
- If bug goes to monitor, don't know what will happen
- If monitor is small, we can verify its correctness
  - Also, less likely to contain bugs

Monitor must enforce a policy on its privileged interface

- Must bind privilege and policy

Policy



Privtrans

- Automatically perform privilege separation
  - Author labels "privileged"
    - Functions
    - Data
  - Privtrans generates monitor and slave

Requirements:

- Monitor must be small
- Policy should be in monitor
  - Falls where it may
  - Doing this automatically is very hard
- Should not create new bugs
  - Not a sound transformation
- "It's easy"
  - For author

- Easier than manual

- Should facilitate code audits
  - Automatic okay but not manual