

# Integrity Policies

CSE497b - Spring 2007

Introduction Computer and Network Security

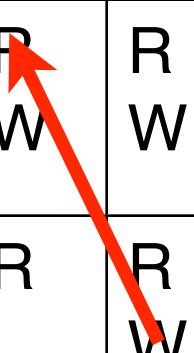
Professor Jaeger

[www.cse.psu.edu/~tjaeger/cse497b-s07/](http://www.cse.psu.edu/~tjaeger/cse497b-s07/)

# Integrity

- Does the following access matrix protect the integrity of J's public key file  $O_2$ ?

	$O_1$	$O_2$	$O_3$
J	R	R W	R W
$S_2$	N	R	R W
$S_3$	N	R	R W

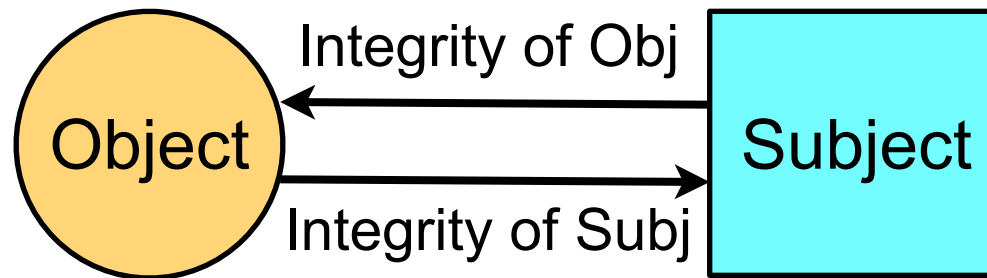


# Integrity

- What determines the integrity of a file or process?
  - The inputs that an object *depends on*
- What does this dependency mean?
  - File: integrity of data written into the file
    - Depends on the integrity of the writers...
  - Process: what the execution of the process depends on
- What concrete actions determine what a process depends on?
  - Read/Execute Code
  - Read/Execute Libraries
  - Read/Write Data

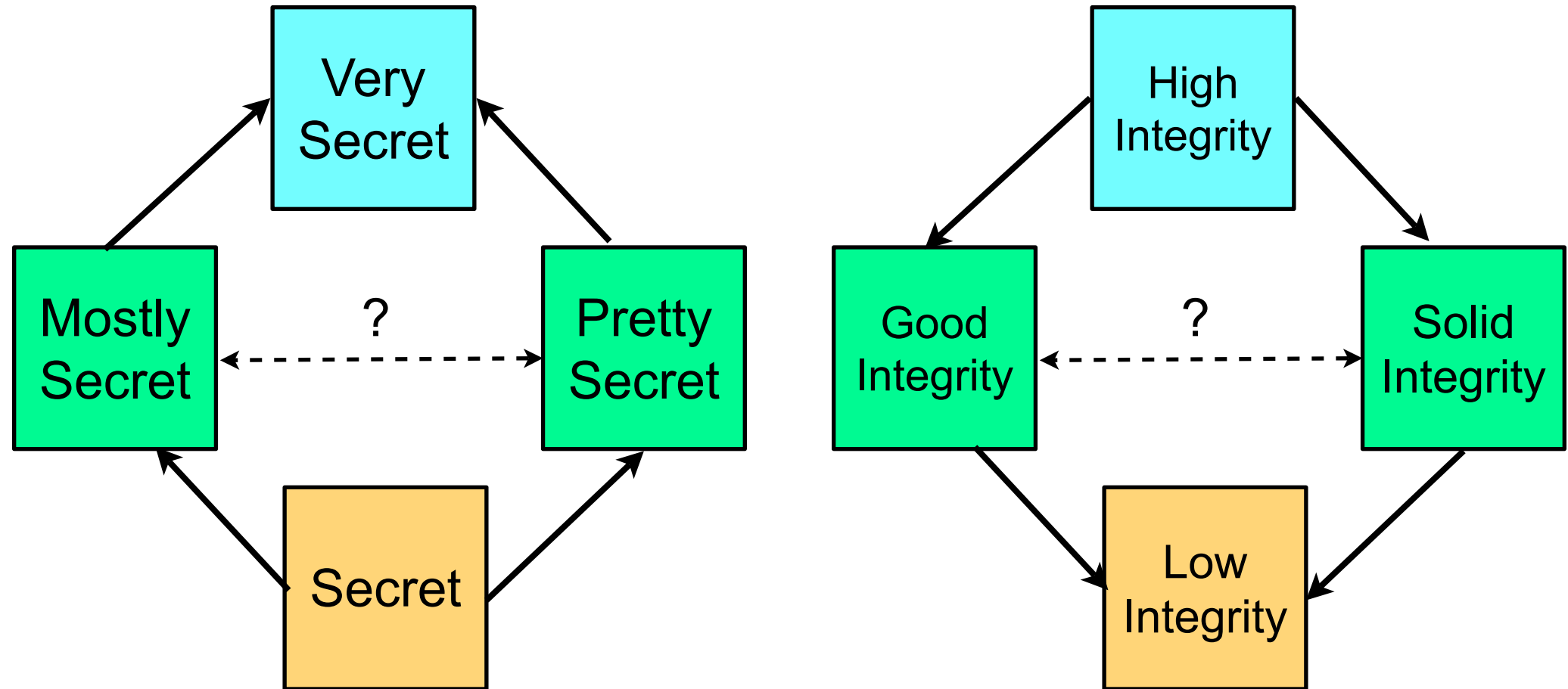
# Integrity Approximation

- Integrity
  - A conservative view
- The *integrity of objects* (data and code) is determined by the integrity of its writers
- The *integrity of a subjects* (processes) is determined by the integrity of the objects it reads



# Biba Integrity

- Information Flow Works for Secrecy
  - Try Integrity Too

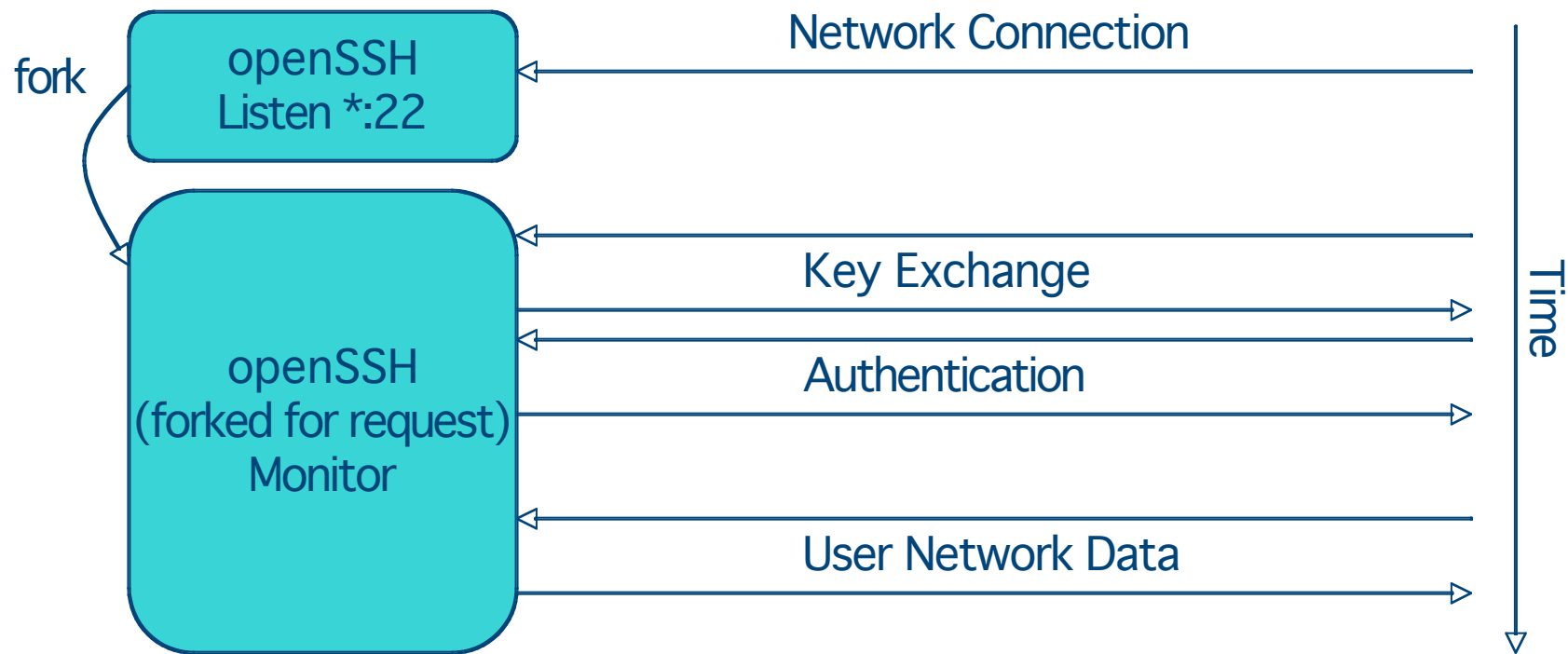


# Biba Integrity Levels

- High and Low
  - System and users
- Other levels?

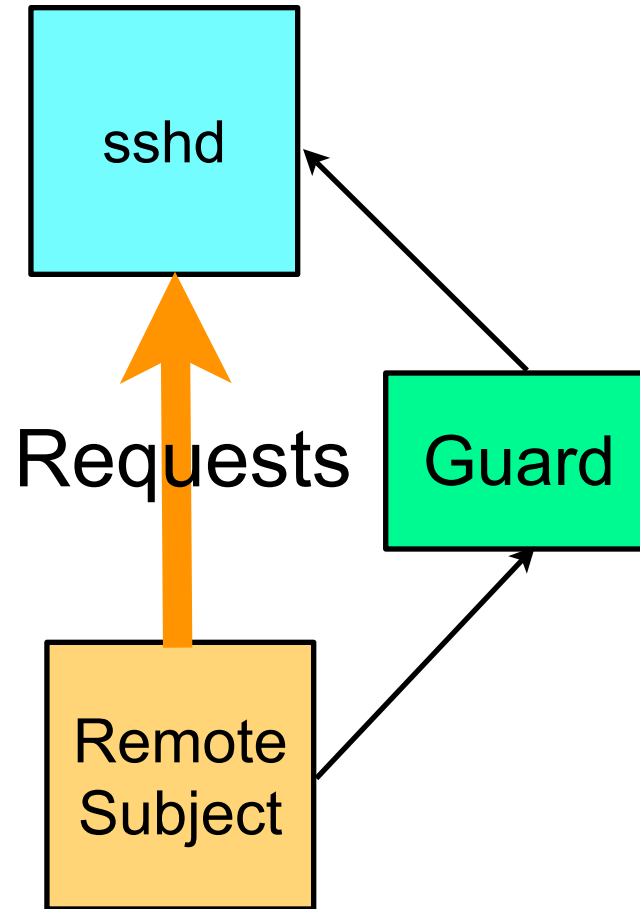
# Integrity Example

- SSH Daemon (sshd)



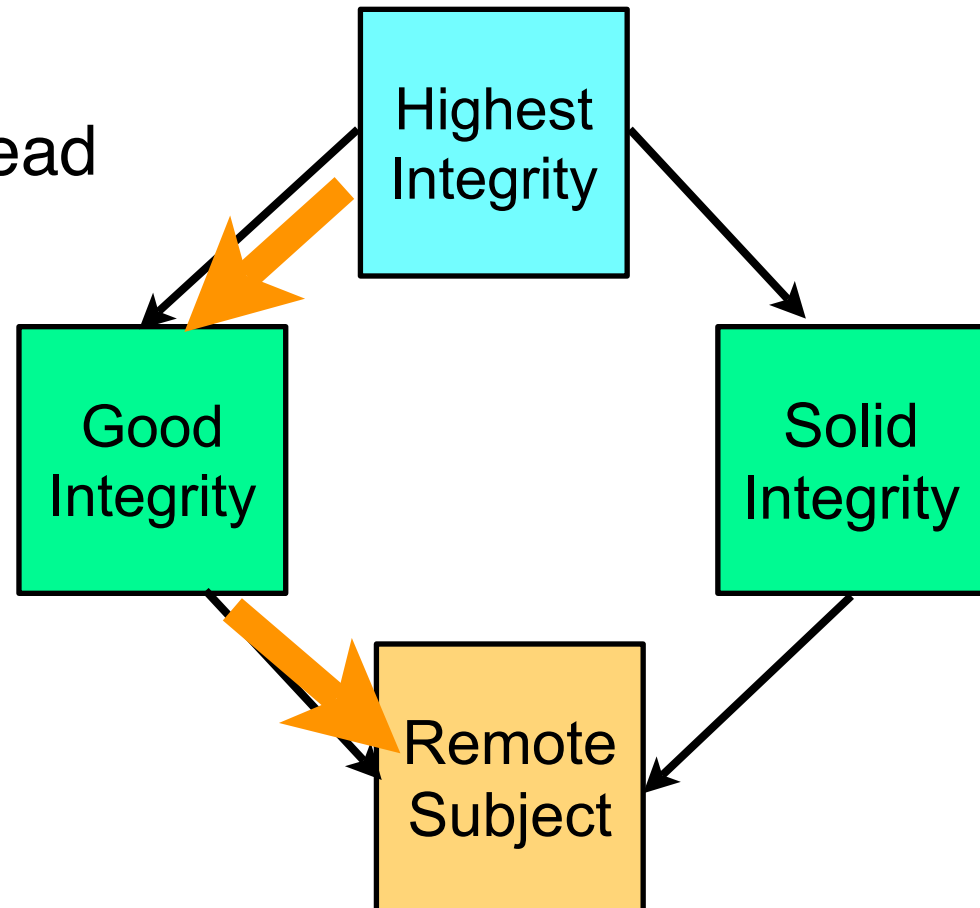
# Biba and SSH

- Does it work?



# Low Water Mark (LOMAC) Integrity

- Subject Integrity Level
  - Highest integrity level initially
- Object Integrity Level
  - Based on level of subjects that have written (lowest)
- Subject Integrity Level
  - Changes as objects are read
  - Minimum of object levels



# Self-Revocation Problem

- Self-Revocation Problem

- Process starts with high integrity
- Open high integrity object o1
- Read from low integrity object o2
- LOMAC semantics reduce process's integrity to low
- No longer can write to o1
- Inconsistent with UNIX

Step 1: initial state



Step 2: ps reads low file



Step 3: demotion

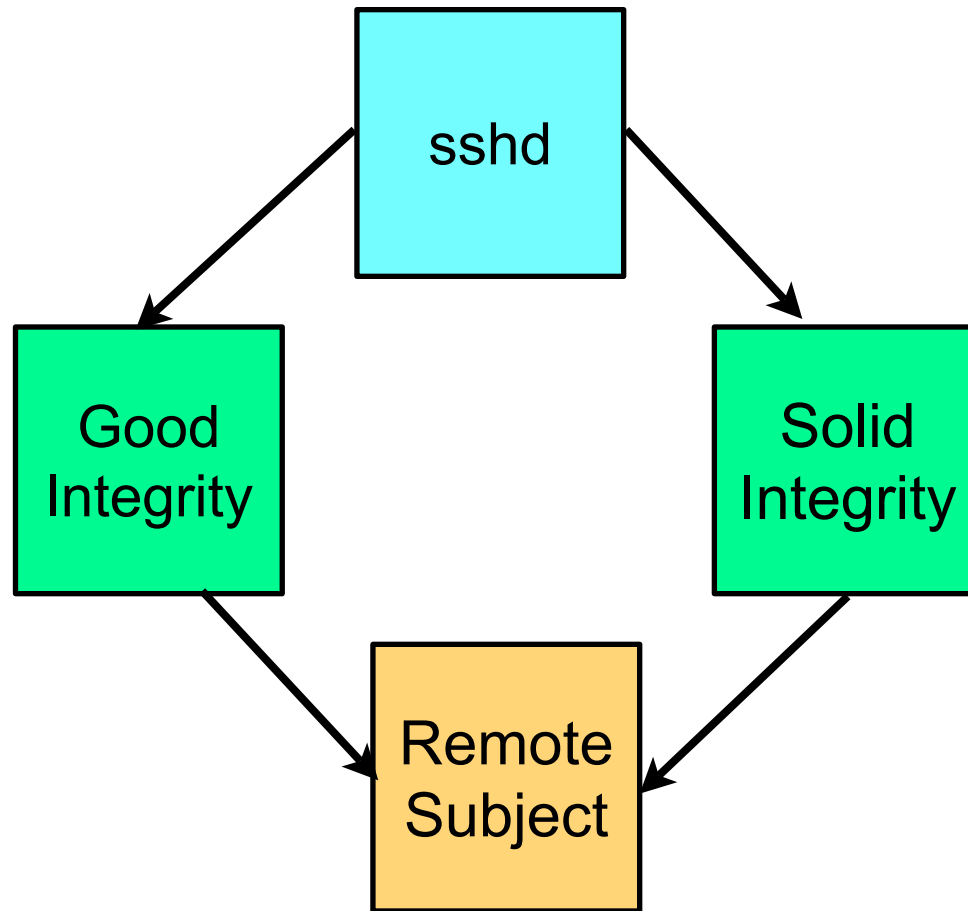


Step 4: pipe write denied



# SSH and LOMAC

- Does SSH work with LOMAC?

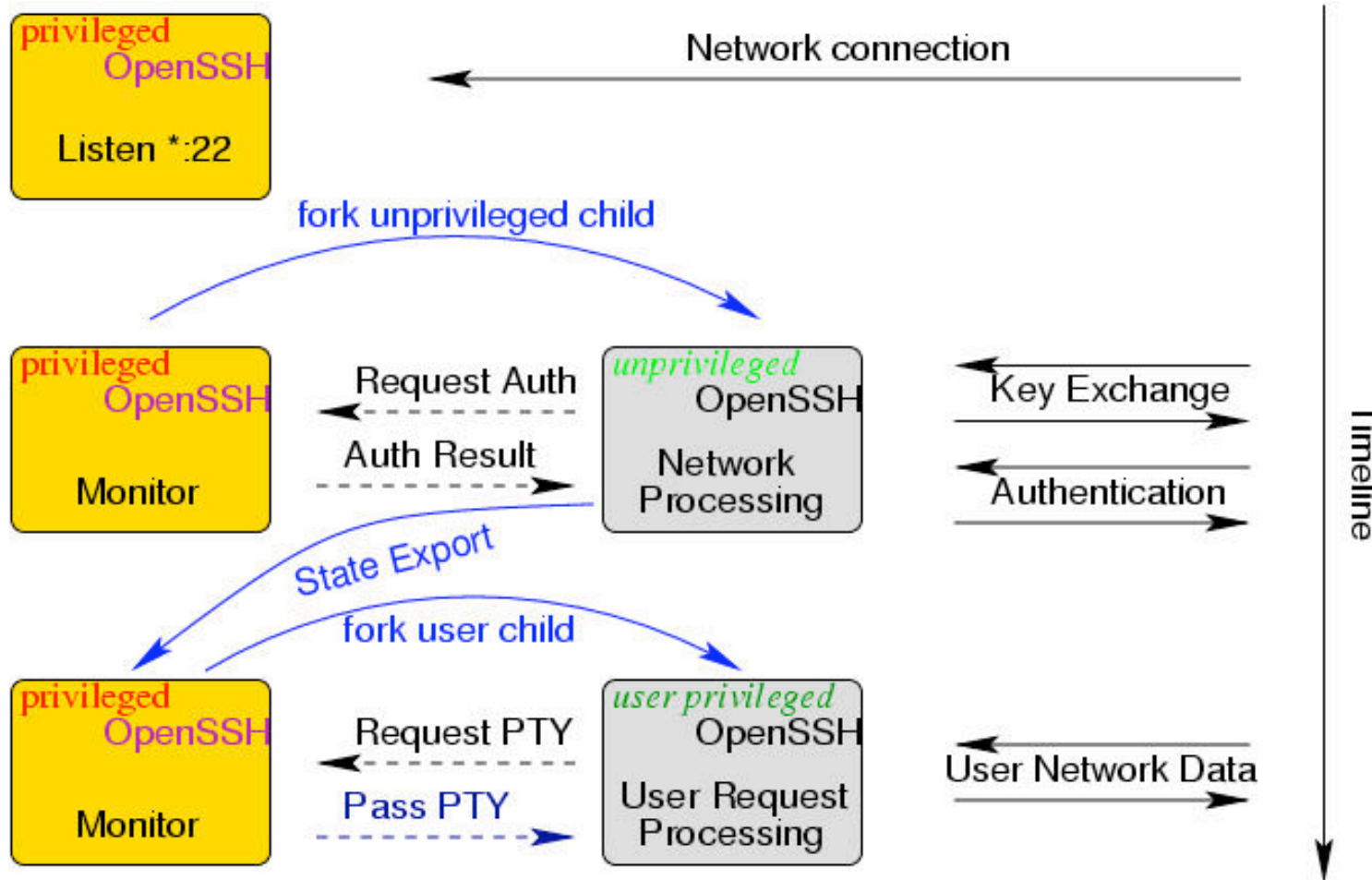


# Privilege Separation

- Limit the amount of code that runs with privilege
  - Decompose program
    - Privileged component
    - Unprivileged component
    - Interface between the two
- Each component is designed to minimize the amount of code with privilege!
- Build secure application
  - Postfix mail system
  - SSH daemon
  - Not too many others

# Privilege Separated OpenSSH

- Current version of OpenSSH



# Integrity and Privilege Separated OpenSSH

- Should this improve integrity?
  - Fewer commands
  - Filter inputs
  - Limit legal command orders
  - Remove direct access to network input
- Does this enable Biba integrity?
  - Are low integrity inputs made to privileged component?
  - Are they upgraded?
- Does this enable LOMAC integrity?
  - How do the inputs to the privileged component impact its integrity level?

# Clark-Wilson Integrity

- Propose that high integrity programs can protect themselves from low integrity inputs!
- How are low integrity inputs processed?
  - Upgrade: turn them into high integrity data
  - Discard: drop them immediately
- How do we know that the high integrity program did this correctly?
  - Need complete program assurance
- Still working on this...
  - Discuss later in Linux and Virtual Machine Systems

# Take Away

- Integrity has to do with dependence
  - Harder to pin down than secrecy
- If dependence is based on reading
  - Integrity is the dual of secrecy
- Integrity models
  - Biba, LOMAC, Clark-Wilson
  - Don't exactly correspond to real-world
- What do we do?
  - Protect the integrity of high secrecy data and code