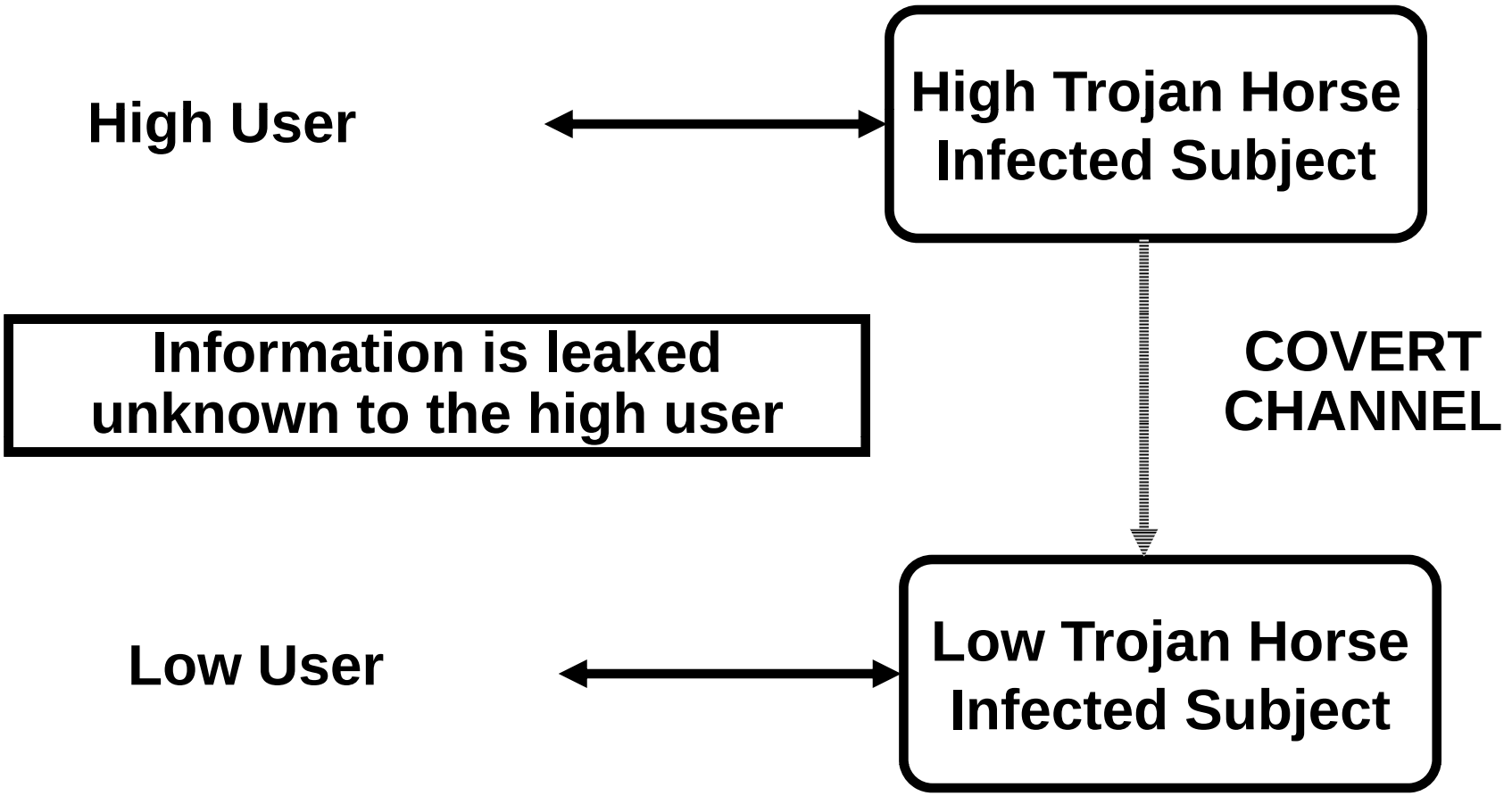
COVERT CHANNELS

Ravi Sandhu

COVERT CHANNELS

- **A covert channel is a communication channel based on the use of system resources not normally intended for communication between the subjects (processes) in the system**

COVERT CHANNELS



COVERT CHANNELS

- **The concern is with subjects not users**
  - **users are trusted (must be trusted) not to disclose secret information outside of the computer system**
  - **subjects are not trusted because they may have Trojan Horses embedded in the code they execute**
- **star-property prevents overt leakage of information and does not address the covert channel problem**

RESOURCE EXHAUSTION CHANNEL (STORAGE CHANNELS)

Given 5GB pool of dynamically allocated memory

HIGH PROCESS

bit = 1 $\Rightarrow$ request 5GB of memory

bit = 0 $\Rightarrow$ request 0GB of memory

LOW PROCESS

request 5GB of memory

if allocated then bit = 0 otherwise bit = 1

LOAD SENSING CHANNEL (TIMING CHANNEL)

HIGH PROCESS

bit = 1 $\Rightarrow$ enter computation intensive loop

bit = 0 $\Rightarrow$ go to sleep

LOW PROCESS

perform a task with known computational requirements

if completed quickly then bit = 0 otherwise bit = 1

COPING WITH COVERT CHANNELS

- **identification**
  - **close the channel or slow it down**
  - **detect attempts to use the channel**
  - **tolerate its existence**

SIDE CHANNELS VS COVERT CHANNELS

- **Covert channels require a cooperating sender and receiver**
- **Side channels do not require a sender but nevertheless information is leaked**