ECS 235B Module 52
Covert Channels

ECS 235B, Foundations of Computer and Information Security

Covert Channels

- Shared resources as communication paths

- *Covert storage channel* uses attribute of shared resource
  - Disk space, message size, etc.

- *Covert timing channel* uses temporal or ordering relationship among accesses to shared resource
  - Regulating CPU usage, order of reads on disk

Example Storage Channel

- Processes *p, q* not allowed to communicate
  - But they share a file system!

- Communications protocol:
  - *p* sends a bit by creating a file called *0* or *1*, then a second file called *send*
    - *p* waits until *send* is deleted before repeating to send another bit
  - *q* waits until file *send* exists, then looks for file *0* or *1*; whichever exists is the bit
    - *q* then deletes *0, 1*, and *send* and waits until *send* is recreated before repeating to read another bit

Example Timing Channel

- System has two VMs
  - Sending machine S, receiving machine R

- To send:
  - For 0, S immediately relinquishes CPU
    - For example, run a process that instantly blocks
  - For 1, S uses full quantum
    - For example, run a CPU-intensive process

- R measures how quickly it gets CPU
  - Uses real-time clock to measure intervals between access to shared resource (CPU)

Example Covert Channel

- Uses ordering of events; does not use clock

- Two VMs sharing disk cylinders 100 to 200
  - SCAN algorithm schedules disk accesses
  - One VM is *High* (*H*), other is *Low* (*L*)

- Idea: *L* will issue requests for blocks on cylinders 139 and 161 to be read
  - If read as 139, then 161, it's a 1 bit
  - If read as 161, then 139, it's a 0 bit

How It Works

- *L* issues read for data on cylinder 150
    - Relinquishes CPU when done; arm now at 150
- *H* runs, issues read for data on cylinder 140
    - Relinquishes CPU when done; arm now at 140
- *L* runs, issues read for data on cylinders 139 and 161
    - Due to SCAN, reads 139 first, then 161
    - This corresponds to a 1
- To send a 0, *H* would have issued read for data on cylinder 162

Analysis

- Timing or storage?
  - Usual definition $\Rightarrow$ storage (no timer, clock)

- Modify example to include timer
  - *L* uses this to determine how long requests take to complete
  - Time to seek to 139 < time to seek to 161 $\Rightarrow$ 1; otherwise, 0

- Channel works same way
  - Suggests it's a timing channel; hence our definition

Noisy vs. Noiseless

- Noiseless: covert channel uses resource available only to sender, receiver

- Noisy: covert channel uses resource available to others as well as to sender, receiver
  - Idea is that others can contribute extraneous information that receiver must filter out to "read" sender's communication

Key Properties

- *Existence*: the covert channel can be used to send/receive information

- *Bandwidth*: the rate at which information can be sent along the channel

- Goal of analysis: establish these properties for each channel
  - If you can eliminate the channel, great!
  - If not, reduce bandwidth as much as possible