

ECS 235B Module 55

Confinement Problem

Example Problem

- Server balances bank accounts for clients
- Server security issues:
 - Record correctly who used it
 - Send *only* balancing info to client
- Client security issues:
 - Log use correctly
 - Do not save or retransmit data client sends

Generalization

- Client sends request, data to server
- Server performs some function on data
- Server returns result to client
- Access controls:
 - Server must ensure the resources it accesses on behalf of client include *only* resources client is authorized to access
 - Server must ensure it does not reveal client's data to any entity not authorized to see the client's data

Confinement Problem

- Problem of preventing a server from leaking information that the user of the service considers confidential

Total Isolation

- Process cannot communicate with any other process
- Process cannot be observed

Impossible for this process to leak information

- Not practical as process uses observable resources such as CPU, secondary storage, networks, etc.

Example

- 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

Covert Channel

- A path of communication not designed to be used for communication
- In example, file system is a (storage) covert channel

Rule of Transitive Confinement

- If p is confined to prevent leaking, and it invokes q , then q must be similarly confined to prevent leaking
- Rule: if a confined process invokes a second process, the second process must be as confined as the first

Lipner's Notes

- All processes can obtain rough idea of time
 - Read system clock or wall clock time
 - Determine number of instructions executed
- All processes can manipulate time
 - Wait some interval of wall clock time
 - Execute a set number of instructions, then block

Quiz

What is the difference between a side channel and a covert channel?

1. A side channel uses an observable outside the system; a covert channel uses an observable within the system
2. A covert channel requires an active sender and receiver; a side channel requires simply observing some aspect of system computation
3. Access controls can close a covert channel, but not a side channel
4. A side channel is just another term for a covert channel