Covert Channels

Covert Channel

Def:A covert channel is a path of communication that was not designed to be used for communication.

Confinement Problem

Can we design and implement a service that takes inputs from a customer but provably does not save the inputs or transmit them to the service's owner against the customer's wishes

Total Isolation

A process that cannot be observed and cannot communicate with other processes cannot leak information

Isolation

- How can we isolate a process?

Isolation

- How can we isolate a process?
  - Virtual Machine

Isolation

- How can we isolate a process?
  - Virtual Machine
  - Sandboxing

Isolation

- How can we isolate a process?
  - Virtual Machine
    - A program that simulates the hardware or a computer system
  - Sandboxing

Isolation

- How can we isolate a process?
  - Virtual Machine
    - A program that simulates the hardware or a computer system
  - Sandbox
    - An environment in which the actions of a process are restricted to according according to a security policy

Sandboxes

- Applets
- Jail
  - chroot
- HTML5
  - Has sandbox attribute for iframes

Timing Channels

- What is needed for a covert timing channel?

Timing Channels

- What is needed for a covert timing channel?
  - Shared Limited resource

Timing Channels

- What is needed for a covert timing channel?
  - Shared Limited resource
  - Collusion
  - Clock (sometimes)

Kemmerer

	write	read	create	delete
size()	M	R	M	M
label()	R	R	M	R
exists()	R	R	R,M	R,M

Attributes make up rows
Operations make up columns
The contents of each element of the matrix indicate whether the op references(R) or modifies(M) the attribute.

Wray

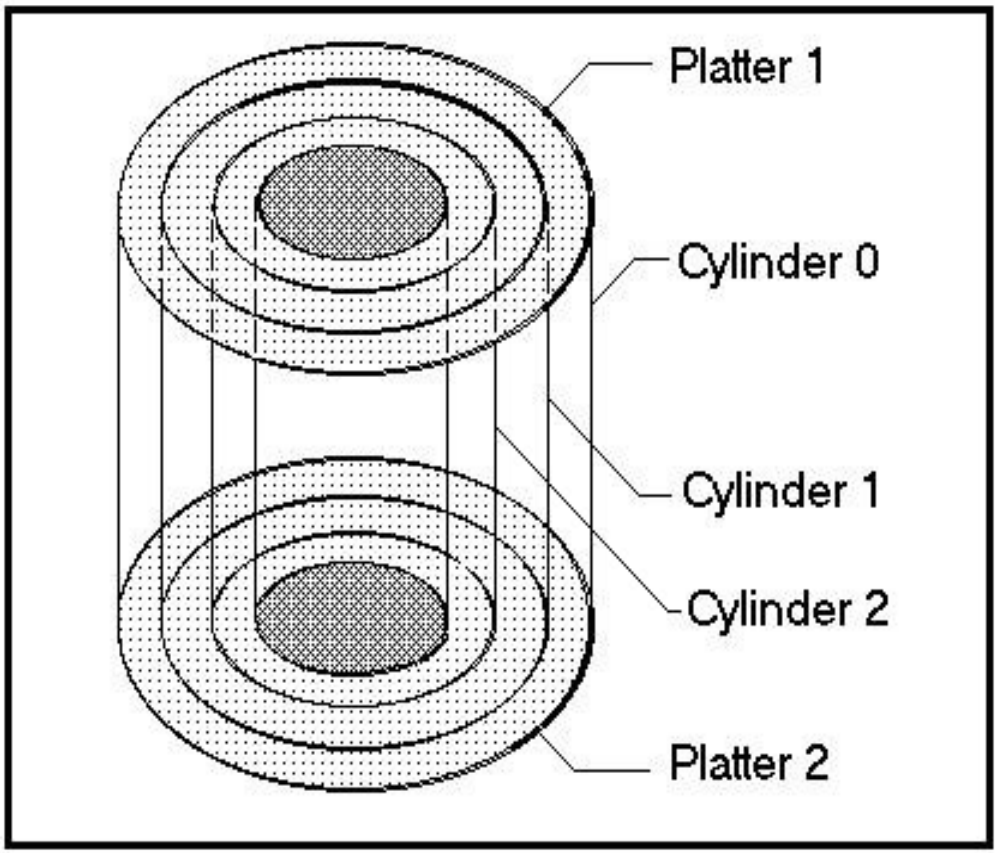
Background:Before Wray covert channels were either storage or timing

- Timing channels info is conveyed by the timing of events(you need an independent clock)
- Storage no external time reference

Wray

In covert channel analysis of VAX it was found that some channels could switch from timing to storage

Wray



How can two process talk to each other if they know the disk access pattern to be shortest seek time first?

Werewolves

Skim:
http://www.cs.unm.edu/~royaen/Papers/CSET2012PaperEnsa

SSH into someone's computer in the lab and try out some of the commands!