Covert Channels

CSCI283/172 Fall 2006
GWU

Draws extensively from Memon's notes, Brooklyn Poly
And book by Pfleeger, Chapters 3 and 4

Covert Channels

- A covert channel is a path of communication that was not designed to be used for communication.
- Say p is a Trojan horse watching Poorvi write the T/F answers in the test. q is the student who wrote the Trojan horse and has an account on seas. To send message p creates a file named *outputs* in q's directory on seas. In this file, the number of spaces between two words reveals a bit of information: 2 spaces is True, one space is False. q can deny everything if accused.
- Different from traditional crypto in the sense that not only is message encrypted, but an opponent cannot even determine if it is present.

Storage channel

- A covert storage channel uses an attribute of the shared resource, like whether a file is locked or not. This attribute can be checked at pre-determined time intervals.
- The Trojan horse p can create and erase a directory in q's account, with a pre-determined name at pre-determined intervals.
- If p does not have such access to the same a/c as q, p can signal 1's by creating a large file so that q cannot if he tries to as well.
- Observe p and q need to share a resource and a time cycle.