Lecture 14 Outline

Reading: *text*, §16.5, 17

1. Examples
    - a. Security pipeline interface
    - b. Secure network server mail guard
2. Confinement problem
    - a. What it is
    - b. Covert channels
    - c. Rule of transitive confinement
    - d. Difficulty of preventing leaking
3. Isolation: virtual machines
    - a. What it is
    - b. Example: KVM/370
    - c. Example: VAX/VMM
4. Isolation: sandboxes
    - a. What it is
    - b. Adding mechanisms to libraries or kernel
    - c. Modify program or process to be executed
    - d. Example: Janus
5. Covert channels
    - a. Storage vs. timing
    - b. Noise vs. noiseless
    - c. Existence
    - d. Bandwidth
6. Covert channel detection
    - a. Noninterference
    - b. Shared Resource Matrix Model
    - c. Information flow analysis
    - d. Covert flow trees
7. Noninterference
    - a. Version of the Unwinding Theorem
    - b. Specifications of SAT
    - c. Example analysis for SAT
8. Shared resource matrix methodology
    - a. Identify shared resources, attributes
    - b. Operations accessing those attributes
    - c. Building the matrix
    - d. Issues about the methodology
9. Covert flow trees
    - a. What it is
    - b. Node types
    - c. Construction
        - i. Determine what attributes primitive operations reference, modify, return
        - ii. Locate covert storage channel that uses some attribute
        - iii. Construct lists: sequences of operations that modify, recognize modifications
    - d. Analysis
10. Capacity and noninterference
    - a. When is bandwidth of covert channel 0?

   b. Noninterference sufficient but not necessary
   c. Analysis
   d. Measuring capacity

11. Mitigating covert channels
    a. Preallocation and hold until process terminates
    b. Impose uniformity
    c. Randomize resource allocation
    d. Efficiency/performance vs. security