Outline for May 17, 2013

Reading: §17.2–17.3, 33, [SMB06][1] **Assignments due:** Homework #4, due May 24, 2013

1. Isolation: virtual machines
   a. What it is
   b. Example: KVM/370
   c. Example: VAX/VMM
2. Isolation: sandboxes
   a. What it is
   b. Adding mechanisms to libraries or kernel
   c. Modify program or process to be executed
   d. Example: Janus
3. Covert channels
   a. Storage vs. timing
   b. Noise vs. noiseless
   c. Existence
   d. Bandwidth
4. Covert channel detection
   a. Noninterference
   b. Shared Resource Matrix Model
   c. Information flow analysis
   d. Covert flow trees
5. Noninterference
   a. Version of the Unwinding Theorem
   b. Specifications of SAT
   c. Example analysis for SAT
6. Shared resource matrix methodology
   a. Identify shared resources, attributes
   b. Operations accessing those attributes
   c. Building the matrix
   d. Issues about the methodology
7. 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
8. Capacity and noninterference
   a. When is bandwidth of covert channel 0?
   b. Noninterference sufficient but not necessary
   c. Analysis
   d. Measuring capacity
9. Mitigating covert channels
   a. Preallocation and hold until process terminates
   b. Impose uniformity

[1] This is available in the Resources area of SmartSite; look in the folder "Handouts"

c. Randomize resource allocation
d. Efficiency/performance vs. security