Lecture 15 Outline

Reading: *text*, §17.3, 18

1. Shared resource matrix methodology
   a. Identify shared resources, attributes
   b. Operations accessing those attributes
   c. Building the matrix
   d. Issues about the methodology
2. 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
3. Capacity and noninterference
   a. When is bandwidth of covert channel 0?
   b. Noninterference sufficient but not necessary
   c. Analysis
   d. Measuring capacity
4. Mitigating covert channels
   a. Preallocation and hold until process terminates
   b. Impose uniformity
   c. Randomize resource allocation
   d. Efficiency/performance vs. security
5. Assurance
   a. Trustworthy entities
   b. Security assurance
   c. Trusted system
   d. Why assurance is needed
   e. Requirements
   f. Assurance and software life cycle