ECS 235B Module 39
Policy Composition I
Policy Composition I

• Assumed: Output function of input
  • Means deterministic (else not function)
  • Means uninterruptability (differences in timings can cause differences in states, hence in outputs)

• This result for deterministic, noninterference-secure systems
Compose Systems

• Louie, Dewey LOW
• Hughie HIGH
• \(b_L\) output buffer
  • Anyone can read it
• \(b_H\) input buffer
  • From HIGH source
• Hughie reads from:
  • \(b_{LH}\) (Louie writes)
  • \(b_{LDH}\) (Louie, Dewey write)
  • \(b_{DH}\) (Dewey writes)
Systems Secure

• All noninterference-secure
  • Hughie has no output
    • So inputs don’t interfere with it
  • Louie, Dewey have no input
    • So (nonexistent) inputs don’t interfere with outputs
Security of Composition

• Buffers finite, sends/receives blocking: composition not secure!
  • Example: assume $b_{DH}, b_{LH}$ have capacity 1

• Algorithm:
  1. Louie (Dewey) sends message to $b_{LH} (b_{DH})$
     – Fills buffer
  2. Louie (Dewey) sends second message to $b_{LH} (b_{DH})$
  3. Louie (Dewey) sends a 0 (1) to $b_{L}$
  4. Louie (Dewey) sends message to $b_{LDH}$
     – Signals Hughie that Louie (Dewey) completed a cycle
Hughie

• Reads bit from $b_H$
  • If 0, receive message from $b_{LH}$
  • If 1, receive message from $b_{DH}$

• Receive on $b_{LDH}$
  • To wait for buffer to be filled
Example

• Hughie reads 0 from $b_H$
  • Reads message from $b_{LH}$
• Now Louie’s second message goes into $b_{LH}$
  • Louie completes step 2 and writes 0 into $b_L$
• Dewey blocked at step 1
  • Dewey cannot write to $b_L$
• Symmetric argument shows that Hughie reading 1 produces a 1 in $b_L$
• So, input from $b_H$ copied to output $b_L$