CIS551: Computer and Network Security

Jonathan M. Smith

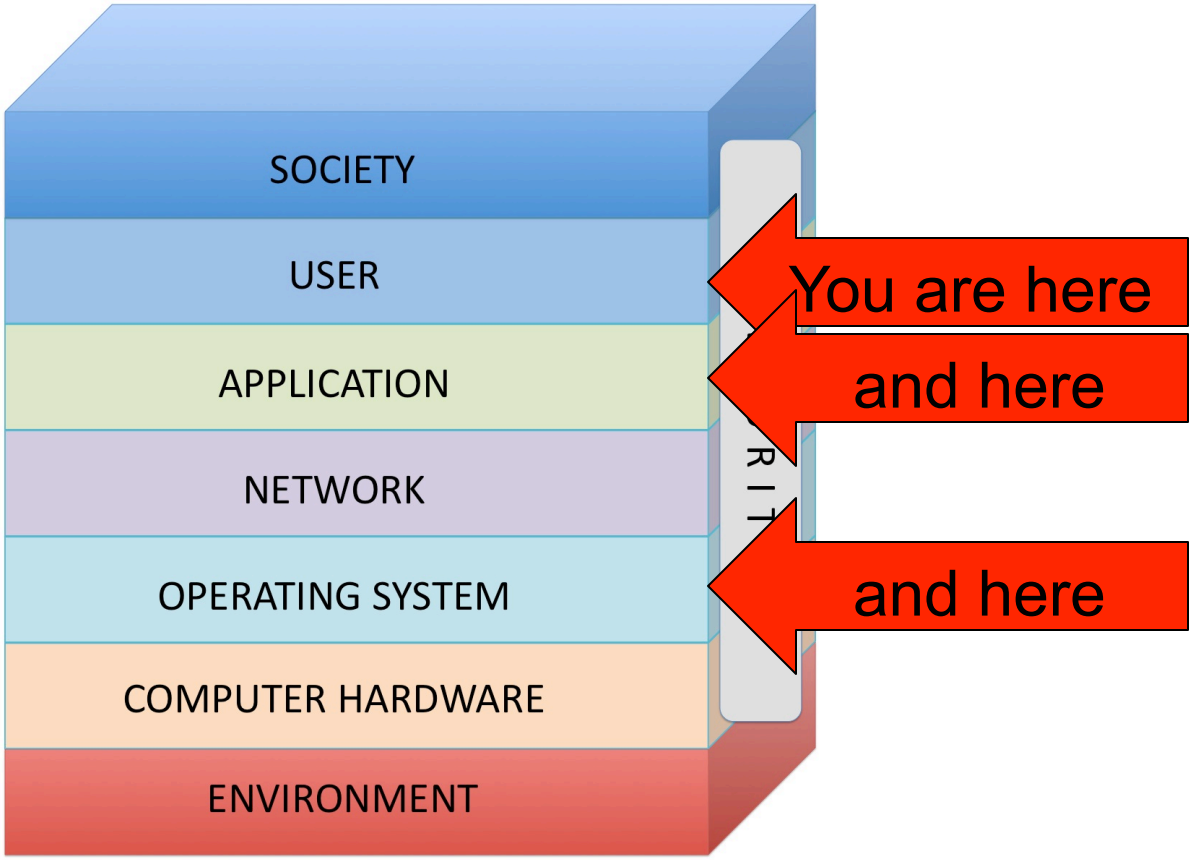
jms@cis.upenn.edu

02/19/2014

CIS551 Topics

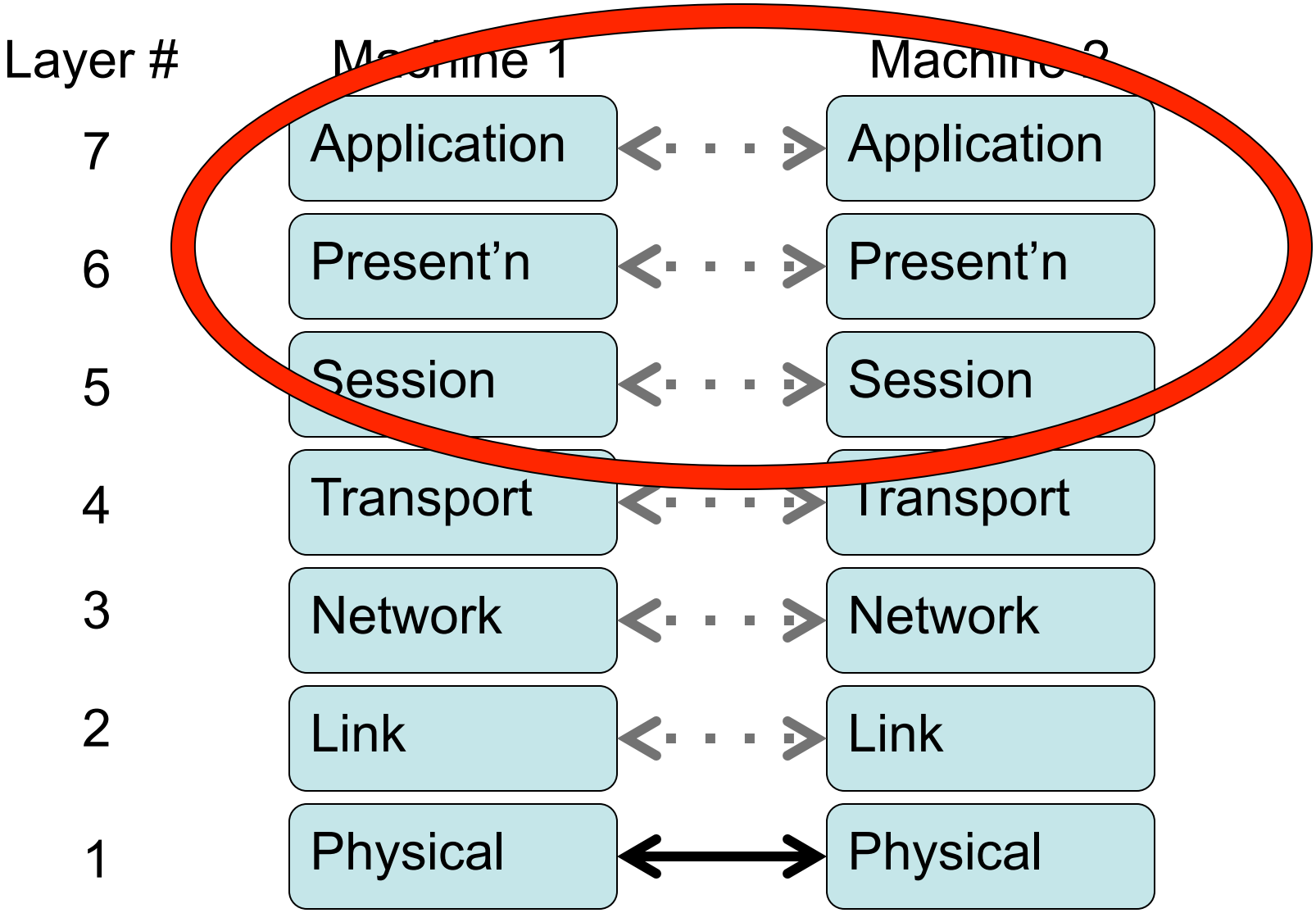
- Computer Security
  - Software/Languages, Computer Arch.
  - Access Control, Operating Systems
  - Threats: Vulnerabilities, Viruses
- Computer Networks
  - Physical layers, Internet, WWW, Applications
  - Cryptography in several forms
  - Threats: Confidentiality, Integrity, Availability
- Systems Viewpoint
  - Users, social engineering, insider threats

Sincoskie NIS model



W.D. Sincoskie, *et al.* “Layer Dissonance and Closure in Networked Information Security” (white paper)

7-layer OSI network model



Cyber-Ecosystem

User

Application Vendor

Browser Vendor

App

Web Browser

Client Computer

E-mail client

Host Software Vendor

Gateway

Network Vendor (ISP)

DPI

Gateway

Content Vendor

Enterprise Manage-ment

Web Server

Server

E-mail service

Service Vendor

Trust

- **Trust** is the *expectation* that the right thing will happen for the right person at the right time and at the right place
- Various factors can increase or decrease this expectation
  - Unknowns (and unknowables?)
  - Adversaries
- 100% and 0% not achievable, but how close?

Reasoning about Trust

- Trust is often based on *transitive* trust
  - I trust Alice since I trust Bob and Bob trusts Alice
- But *degree* of trust is more subtle
  - I trust Alice less than Bob, with whom I vacation (*i.e.*, my knowledge of Bob is better, and direct)
- Trust is dynamic
  - More experience with Alice, Bob cheats me, …
  - As examples show, increases *and* decreases

Dependencies and Independence

- Trust is often based on *assumptions* of trust
  - This creates a chain of dependencies
  - See Thompson, “Reflections on Trusting Trust”
- Most SW systems assume HW trusted
  - “FPGA Viruses”, Hazdic, Udani, Smith, FPL ‘99
  - “Overcoming an untrusted TCB”, Hicks, Finnicum, King, Martin, Smith, S&P ’10
- Desiderata: Independent attestation
  - Thinking Bayes: Pr(good) = 1-Pr(bad_1)*Pr(bad_2)*…