CIS551: Computer and Network Security

Jonathan M. Smith

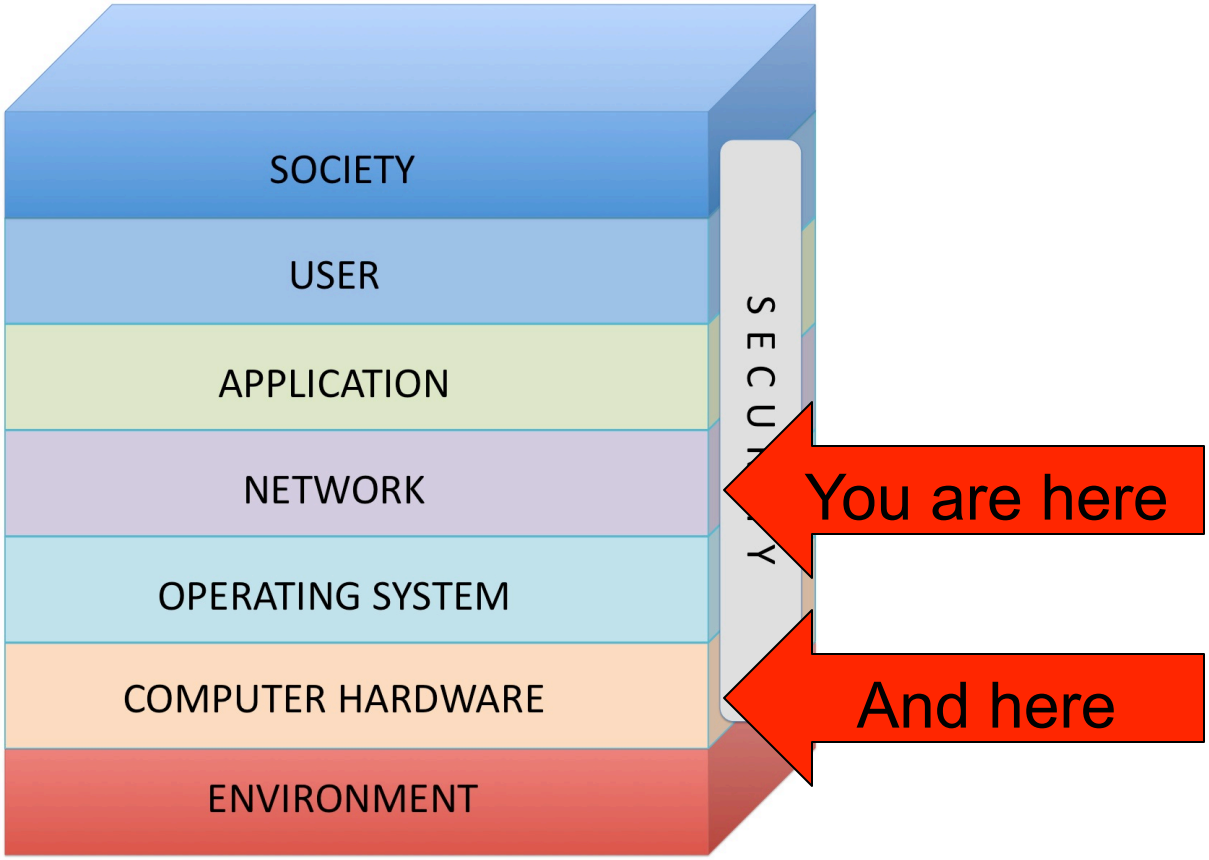
jms@cis.upenn.edu

02/03/2014

CIS551 Topics

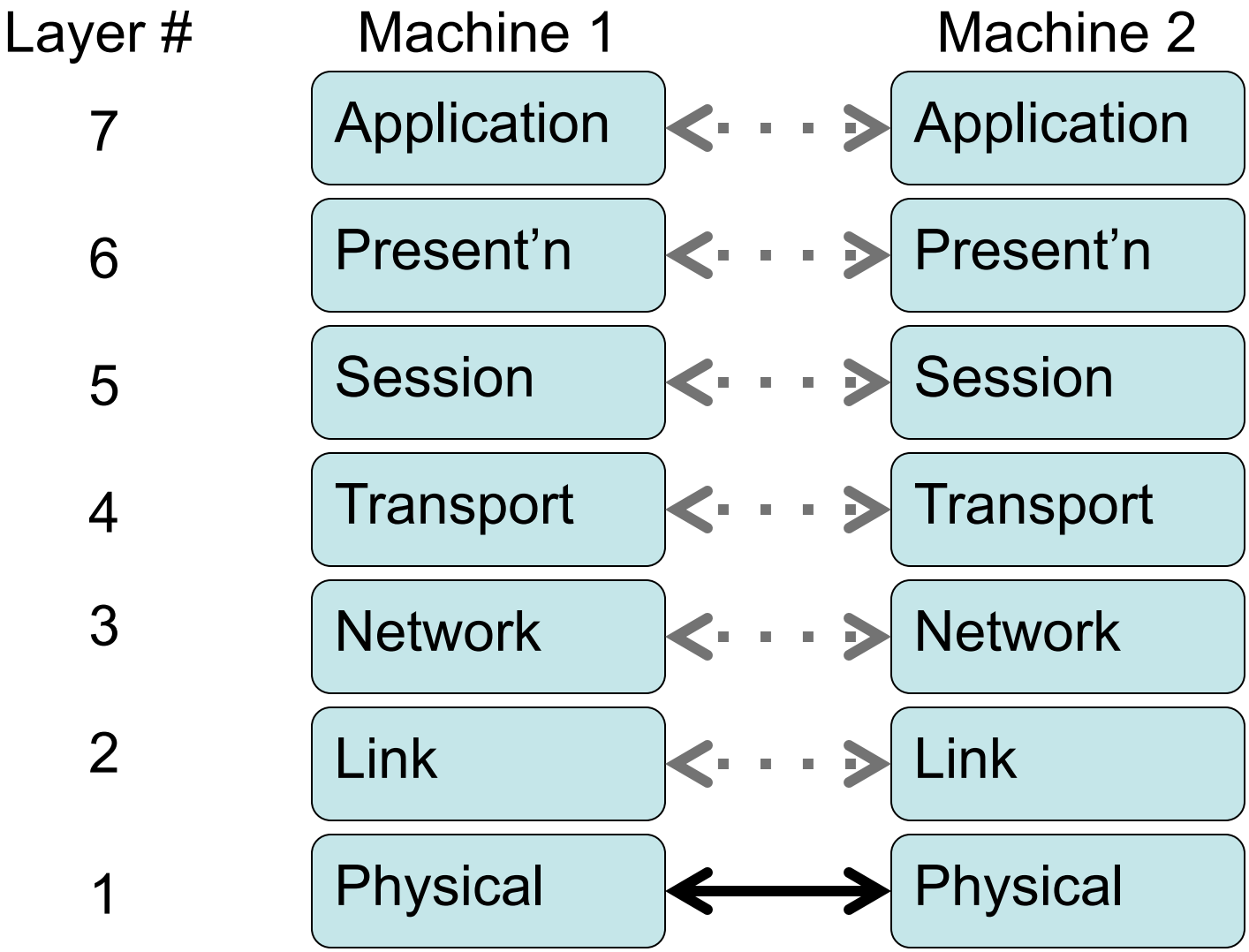
- Computer Security
  - Software/Languages, Computer Arch.
  - Access Control, Operating Systems
  - Threats: Vulnerabilities, Viruses
- Computer Networks
  - Physical layers, Internet, WWW, Applications
  - Cryptography in several forms
  - Threats: Confidentiality, Integrity, Availability
- Systems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



Physical layers

- Wires (electrical)
- Fibers (optical)
- Wireless (radio, free-space optical, IR)
- Provide means of sending signal
- Hardware, coding determine binary digits (“bits”)
  - E.g., voltage threshold for “1”

Signalling

- Distance constrained by medium
  - Fiber – long distance
  - Copper/wires – depends on cabling
  - Wireless – depends on frequency/power
- Power, baud rate, signal to noise ratio
- These limits are designed in
  - E.g., “campus” for 10 and 100 Mbps ether

Data formats

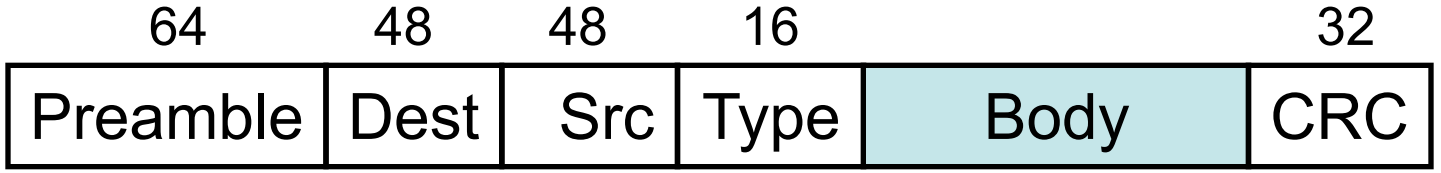
- Bits are *framed* – organized into groups
- Data often coded with error-correction
  - E.g., wireless
  - Try to emulate a 100% reliable channel
  - Coding can overcome SOME errors
- The data format at this layer is done by hardware, devices exchange frames

Link layers

- Could have a simple point-point topology
  - E.g., two tin cans and a string
- Much more interesting to have addresses
  - Phone numbers
  - Ethernet addresses (more on this later)
  - Allows, e.g., for broadcast networks

Example link layer

- Ethernet packet network
- Packets have 48-bit source and destination addresses
- Also, preamble (to recognize frame)
- Also, CRC (to protect frame)



Addressing

- Source address of adapter from manufacturer (medium access control or “MAC” address)
- 48 bits, so 281,474,976,710,656 addrs.
- Unlikely to run out soon…
- Node can recognize its own address as destination

Ethernet is a *broadcast* net

- Logically connected to a common wire
- A network adapter uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) to share bus
- Broadcasts to all listeners
- Enables (logically) promiscuous mode
- CSMA/CD requires a minimum frame size (why?)

Data Rates (Ethernet)

- Original Ethernet (Xerox PARC) 3 Mbps
- DIX Ethernet 10 Mbps
- 100 Mbps
- 1 Gbps
- 10 Gbps (optical or heavy cable)
- 100 Gbps (coming)

CSMA/CD Ethernet

- There are also distance limitations (why?)
- Some can be overcome with a repeater
- Scaling requires bridges
  - Modern: switched ethernet
  - Above 100 Mbps – all switched
- Bridges – spanning tree (why?)

Topology issues

- Could use remote bridges
  - LANs connected by point-to-point
  - Problem of broadcast storms from STP
- Generally resolved by interconnecting LANs at Layer 3 (Internet Protocol) layer (more on this later)

Ethernet security questions

- How can *broadcast* information be kept confidential?
- Can a private *channel* be established?
- Can we prevent packets from reaching a destination?
- Can we prevent misconfiguration?

Other (now uncommon) LANs

- Token Ring (token for MAC)
  - Ring topology
  - Lost to Ethernet
- Asynchronous Transfer Mode (ATM)
  - Very sophisticated signalling
  - Blend of packet and circuit model
  - Completely switched
  - Lost to Ethernet (but lives on: ADsl/MPLS)

“Wireless Ethernet” - WiFi

- More on this Wednesday 2/5, but preview:
  - Radio transmission / reception
  - Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) MAC
  - Ethernet-like to ease adoption (it worked!)
  - Originally 915 Mhz, later 2.4 Ghz Ghz
    - Klystron effects at 2.4 Ghz… ☺
    - now ~5 Ghz