# CIS551: Computer and Network Security

Jonathan M. Smith

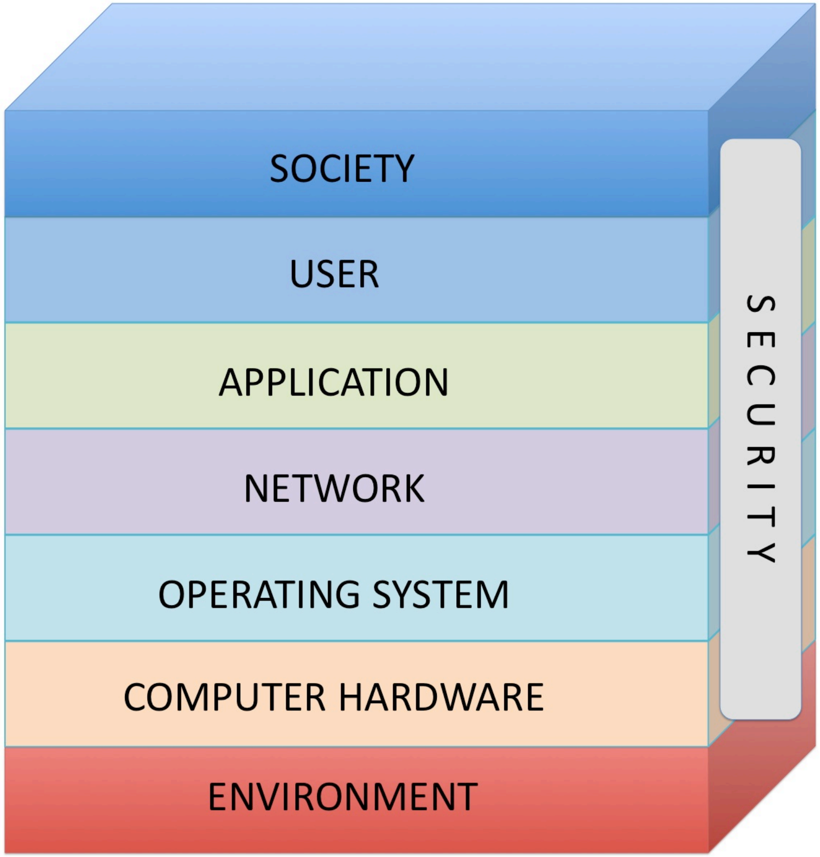
jms@cis.upenn.edu

04/23/2014

# CIS551 Topics

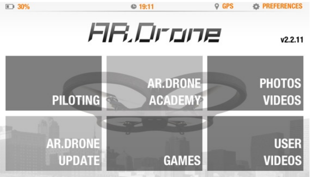
- Computer Security
  - Software/Languages, Computer Arch.
  - Access Control, Operating Systems
  - Threats: Vulnerabilities, Viruses
- Computer Networks
  - Physical layers, Internet, WWW, Applications
  - Cryptography in several forms
  - Threats: Confidentiality, Integrity, Availability
- Systems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

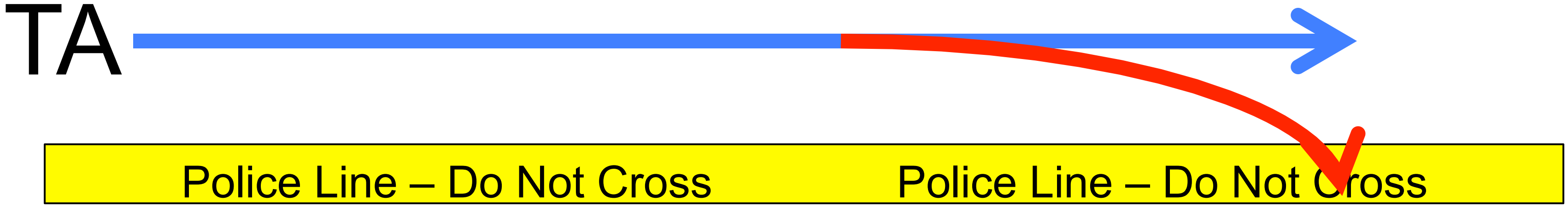
# Sincoskie NIS model



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

# Demo setup for 4/28 and 4/30:





TA

Police Line – Do Not Cross Police Line – Do Not Cross

# Demo

- Three tries, 15 minute window
  - TA will fly using app
  - Once control demoed, you are done!
- At least 1 TA and I will be present
  - Some CIS Ph.D. students may also come
- Your whole group must be present for your slot

# A few rules for demos:

- If anything can go wrong, it will
- No matter how perfect things are made to appear, Murphy's law will take effect and screw it up
- If there is a possibility of several things going wrong, the one that will cause the most damage will be the FIRST to go wrong
- Field experience is something you don't get until just after you need it

# Final exam topics

- Up to 1st midterm: *ca*. 25%
- Between 1st and 2nd midterm: *ca*. 25%
- Since 2nd midterm: *ca*. 50%
- Several slides of example topics follow
- Will try to get out sample next week

# Software

- Vulnerabilities, exploits
- Buffer overflows
- Input checking
- Language effects (C, *vs*. new langs.)
- Architecture/Stack Model
- Defenses

# Networking

- Links: Wired (Ethernet), Wireless
  - Packet switching
- Internet Protocol (IP)
  - Encapsulation
  - Addressing
  - Routing
- TCP/IP
  - Flow and Congestion Control

# Network Applications

- Web
  - HTTP
  - Client/Server architecture
  - Threats to servers
  - Browsers/Javascript on client
- E-mail
  - Network properties
  - MIME

# Privacy

- Extensive data collections
- IP + queries visible
- Face recognition
- Defenses
  - Proxies, Tor
  - Disguises

# Network defenses

- Firewalls:
  - – Packet filters
  - – Application gateways
  - – Uses in a network architecture
  - – Limitations
- Intrusion detection systems
  - – Uses and limitations
  - – Combinations with firewalls (IPS)

# Crypto

- History and purposes (C,I, but not A)
- Cryptography
  - Shared/Symmetric
  - Public-Key
- Cryptanalysis
  - Algorithmic & implementation bugs
- Cryptographic Protocols
  - Dolev-Yao

# Trust

- Trust Assumptions
  - Dependencies
- Trusted Computing Base
  - Components
  - Minimization
- Trusted Hardware
  - Attacks

# The Human Element: Social Engineering / Insider Threat

- Goals of social engineer
  - Mitnick “rules of thumb”
- Increasing trust – verifying claims
- Insider: already trusted
- Personnel security
- Walker spy incident