CIS551: Computer and Network Security

Jonathan M. Smith

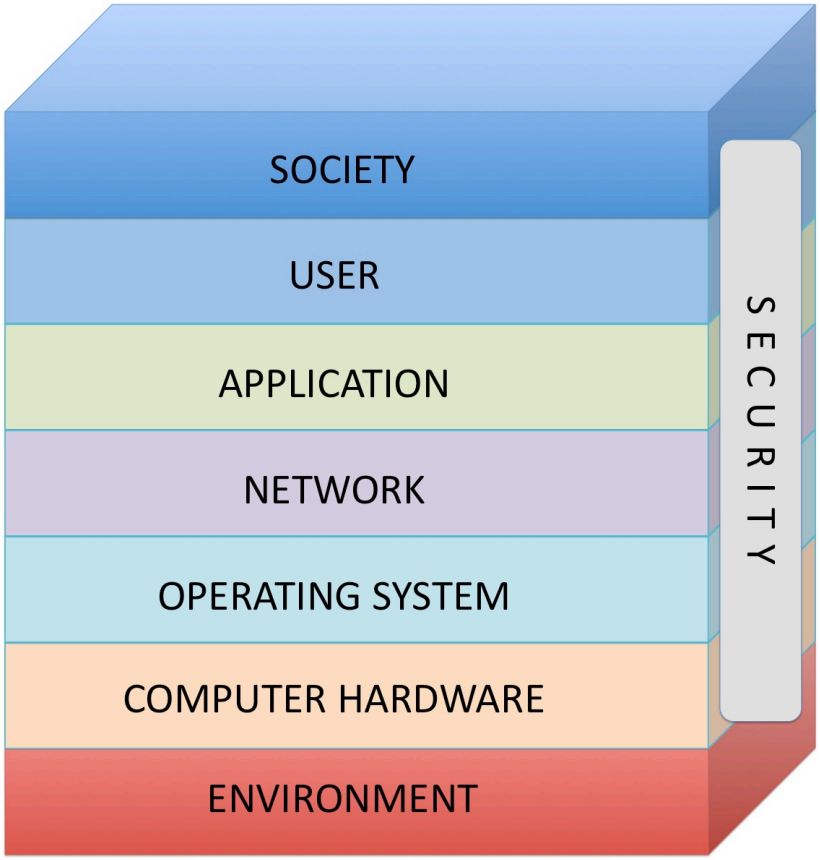
jms@cis.upenn.edu

04/21/2014

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)

Big tech trends

- Big Data / Data Centers
- Parallelism (Multicore, GPUs)
- Smartphones
- Crowdsourcing
- Social Networks
- Computer security
- Reemergence of privacy as a concern

The Future

- Logical problems with security logics
- Continuous “ecosystem” model?
  - Fuzzing – evolving software
- OODA Loop as a design tool
- Cyberinfrastructure threat example
- Medical Devices
- (bionic) Telepathy?

Our model for “secure”:

- Idea: software can be *proven* correct*
  - **Security** is a correctness property
  - Therefore, we can verify software and obtain secure systems!
- Idea based on the foundations of Computer Science in logic and formal languages
- “Gold Standard” for >40 years (e.g., PSOS)

*Not everyone believed this. For a very interesting read, see De Millo, Lipton and Perlis, “Social Processes and Proofs of Theorems and Programs”, CACM May 1979

Not quite satisfactory

- Secure/NOT Secure model has axiomatic assumptions, used as scaffolding for proofs
  - Proofs are *independent* of the environment
  - But how *could* they be?
- Security failures when assumptions *violated*: interactions w/new environment (including new compositions with other systems)
  - Assumptions are always violated - very secure systems are standalone (“air gapped”)!
  - Standard cracker practice: violate!

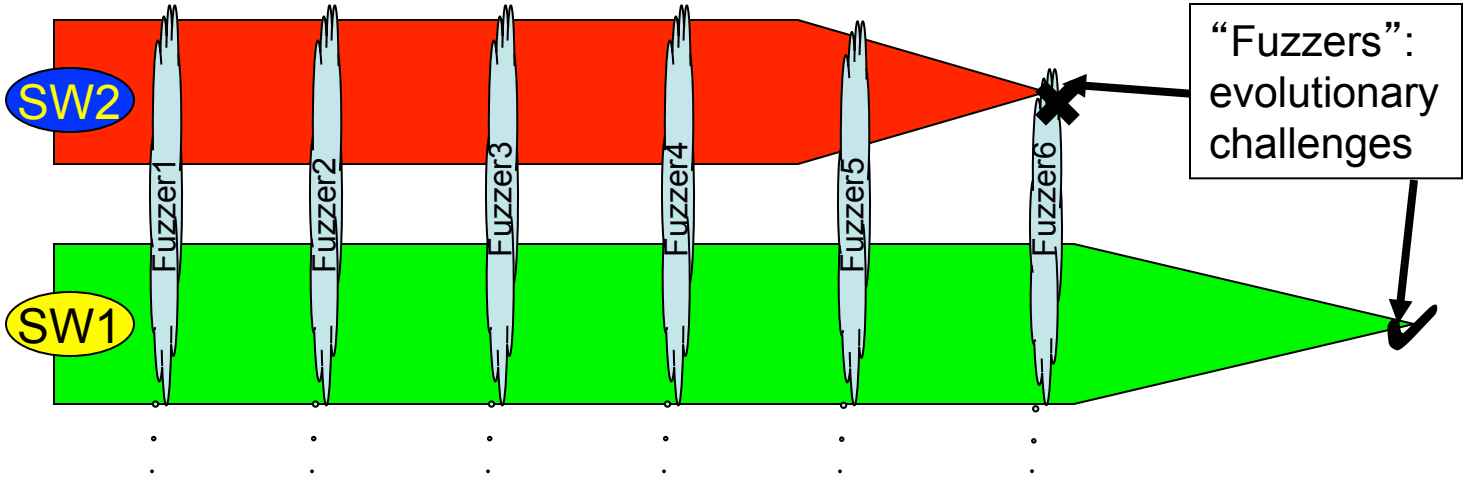
“Continuous” security models

- The environment is continuous and evolving
  - Software has to live in a cyber “ecosystem”
- Can we develop a model that models:
  - New compositions (e.g., Service Oriented Arch)
  - Evolving environments (e.g., cellphones)
  - Evolving threats (e.g., evolving botnets)
  - Response to a range of unknown threats?

Software Evolution?

- T. S. Ray, ``Software Evolution.'' *Systems, Control and Information* 40(8): 337-343, 1996.
  - Tierra system
- P. McKinley, *et al*., “Harnessing Digital Evolution”, *IEEE Computer*, Jan. 2008.
  - Avida system
- Great idea – will need to overcome “farmed” versus “natural” environment issues…

Can we measure evolutionary fitness for software?



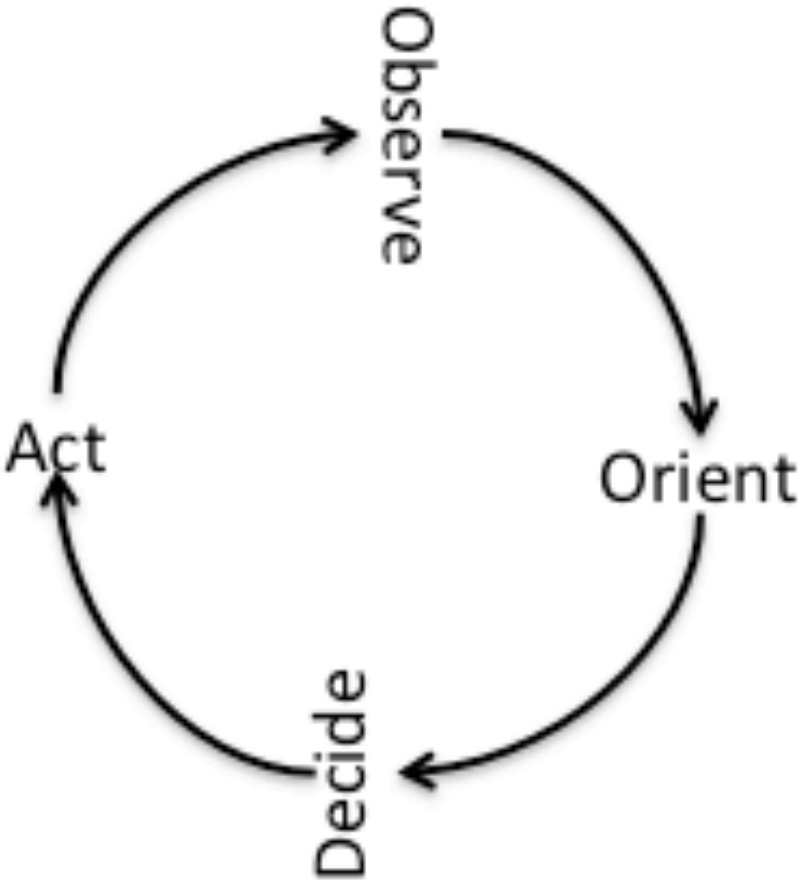
Notional Metric S(SW1)>S(SW2)

Maybe Software Evolution versus Software Creationism?

- Preserve good components
- Composition / inheritance
- Embrace complexity* - the environment is complex!
- Save *everything* that worked in the past
- Cognitive: sense, compute, actuate

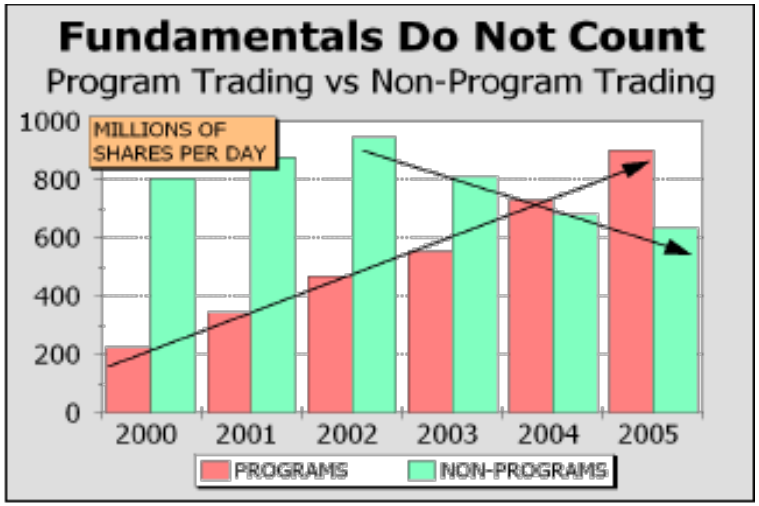
* The best essay I have read on scale is J.B.S. Haldane's "On being the right size". All engineers should read it!

John Boyd's OODA Loop



- Faster cycles than adversary: wins
- Technologies should therefore focus on accelerating OODA loop cycles

Cyberinfrastructure & Markets



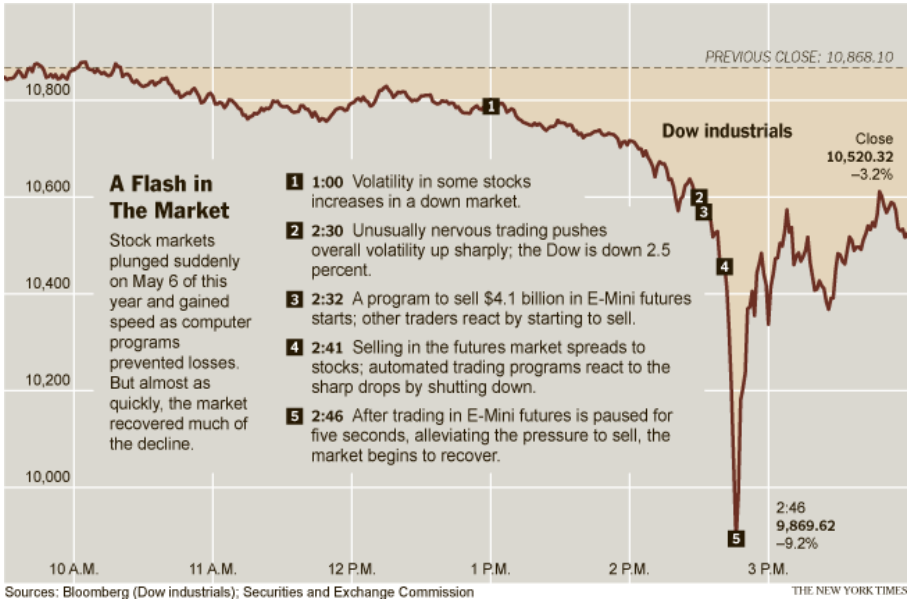
Program trading systems are software systems.

- Are they uniquely bug or vulnerability-free?
- Unique testing / programmers?

Multiple markets:

- Currency markets
- Debt markets
- Unregulated dark pools

Interconnected by arbitrage



Possible threat vectors

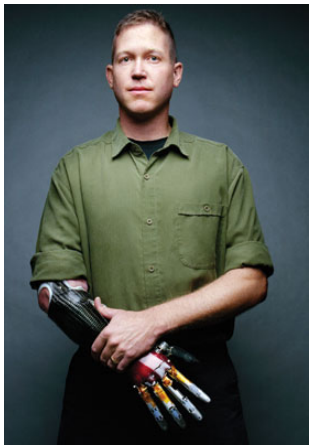
- Illegal commercial actors (e.g., manipulators)
- Nation-states attempting to cause economic damage/loss of confidence
  - Misinformation
  - Manipulation
  - Rogue traders, or
  - Malware in / controlling program trading systems

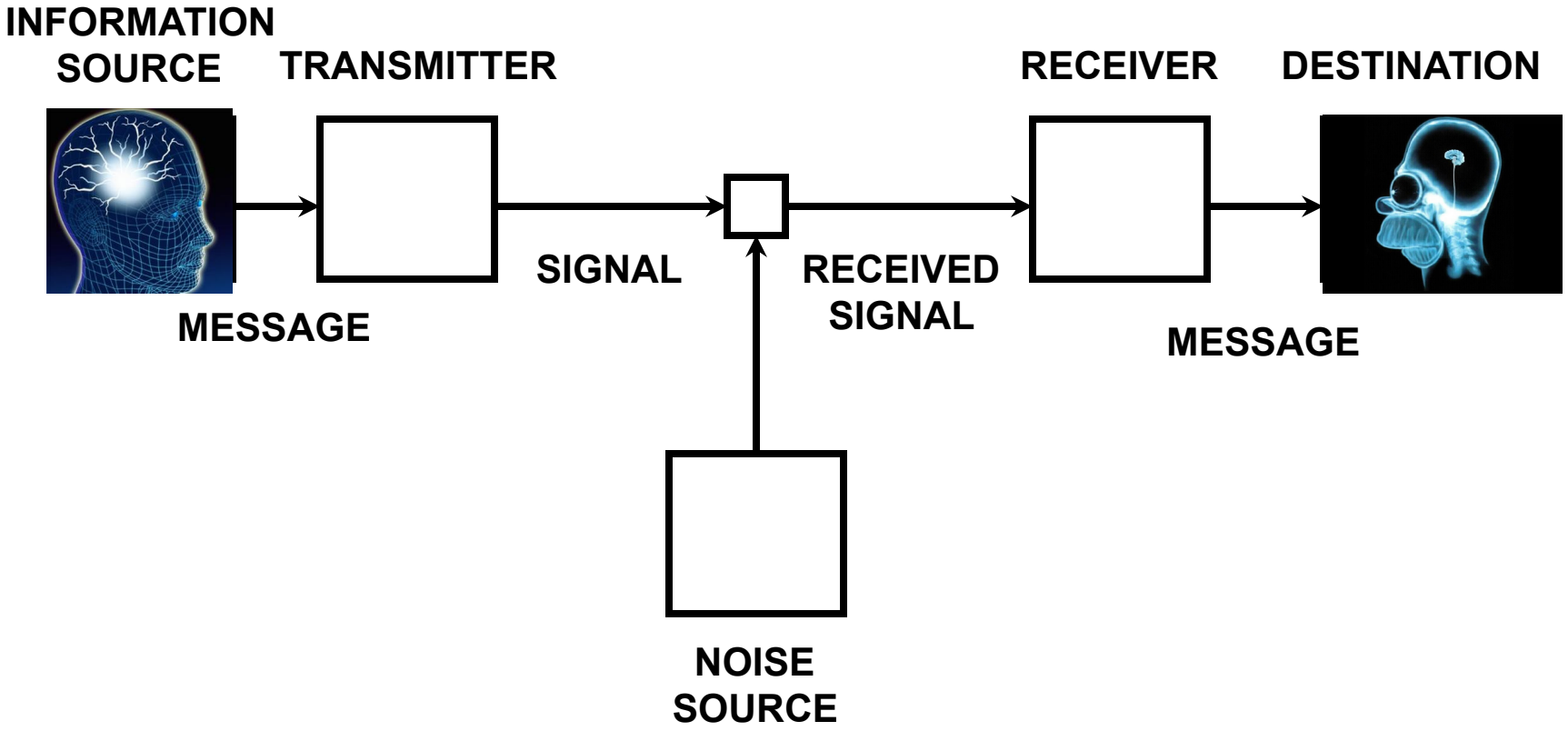
Internet of (medical) Things

- E.g., food, exercise, meds for managing personal health
  - Interact w/cloud for recommendations & reminders

Radical stuff…

- Computer human interfaces
- Desire of humans for communications
- Progress in neuroscience
  - fMRI: http://www.youtube.com/watch?v=ew-2sau6Tr8
  - Control of artificial limbs
- Applications drive networks
  - Voice, hypertext, photos, movies, …..



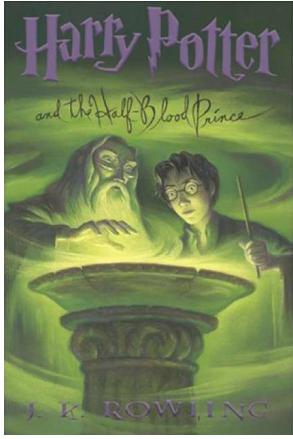


A Shannon Model for Telepathy

Can we do it by 2025?

- Brain capacity estimates range from 10**9 (Merkle) >10**21 bits (Von Neumann)
- Coding and representation?
- What goodput is required? QoS?
- Invasive or non-invasive?
- Economic trendline (fMRI big, & big $$)
  - Possibly games (stored content) or psychoanalysis
  - Method for AI, preserving carbon with silicon,

Do we want to do it?



- How do you firewall off memories?
- Once possible is there telepathic violence?
- What becomes of privacy in these circumstances?
  - The perfect lie detector?
- My prediction: curiosity usually beats prudence, but it will take a while
- Approximations will keep us busy for a while

Summary: 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