CIS551*: Computer and Network Security

Jonathan M. Smith

jms@cis.upenn.edu

(Strongly prefer e-mail interactions)

* Also numbered TCOM401

Prerequisites

- No formal prerequisites; advanced undergraduates can take the course
- Programming experience and familiarity with networking advisable
- Most important: Curiosity and willingness to think!!!

Administrative

- Office Hours:
  - M@4PM, W@9AM, in 604 Levine
  - Or, by *confirmed* e-mail appointment
- No text. Assigned reading, slides, notes
- TA: Sahil Hirpara, sahilh@seas, OH TBD
- Hanjun Xiao, hanjunx@cis, OH TBD
- Read for 1/22: “Symantec W32.Stuxnet Dossier”, Version 1.4 (February 2011)

CIS551: Evaluation

- 15% mid-term exam 1 (2/12)
- 15% mid-term exam 2 (3/26)
- 15% HW1 (individual)
- 15% HW2 (group)
- 15% HW3 (group)
- 20% final exam (TBD)
  - Exams can cover lectures, reading, HW
- 5% class participation – so speak up!

Integrity policy

- Don’t cheat – I have a (well-deserved…) reputation for intolerance
  - This includes copying from others, others performing work for you (rent-a-coder, etc.) and using “archived” HWs and questions
  - We use moss, etc. and our own archives
  - Details: see `~jms/cis551/collab.html`
- Desperate @due date?, broken group?, etc.? - see TAs or I for help ASAP!

Who are you (slide 1)?

1. Who are undergraduates?
2. Who are SEAS students?
3. Who are M.S. students? Ph.D.?
4. Who has programmed ☺?
5. Who has programmed in C?
6. Who has programmed in assembly?
7. Who has programmed using sockets?

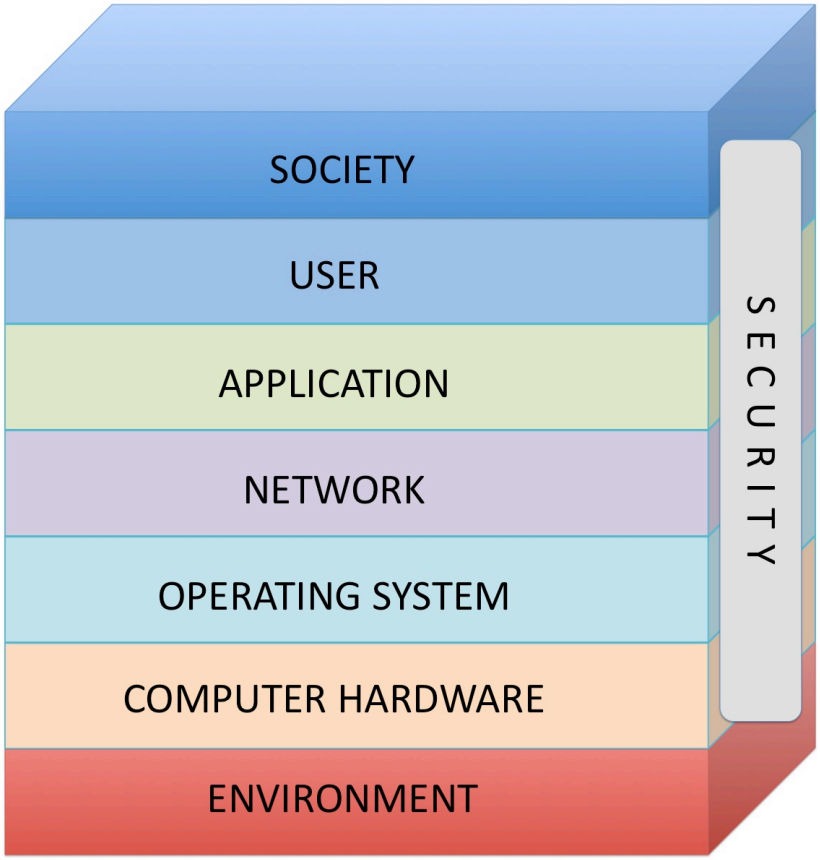
Who are you (slide 2)?

8. Who has written a buffer overflow?
9. Who has written a virus?
10. Who has written a worm?
11. Who has used a packet sniffer?
12. Who has used `nmap`?
13. Who encrypts their hard drive?
14. Who encrypts their e-mail?

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

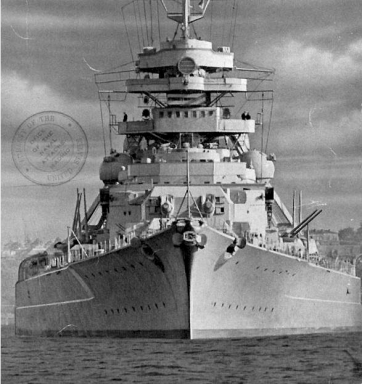
Approach: Sincoskie NIS model



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

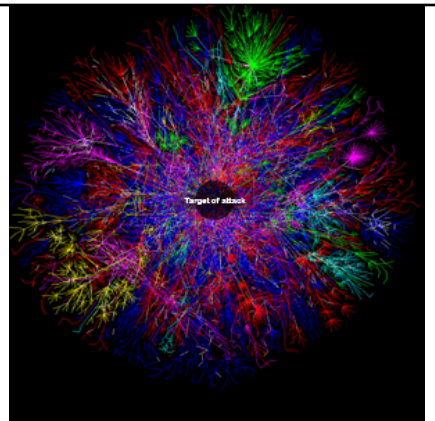
What is cyberwarfare?

- (Nation-state?) aggression using computers as weapons
  - And, defense against such attacks
- Many possible actors (individuals with botnets, Lulzsec, criminal gangs, etc.)
  - Issues are scale, capabilities, willingness
- Why, how and what can be done?



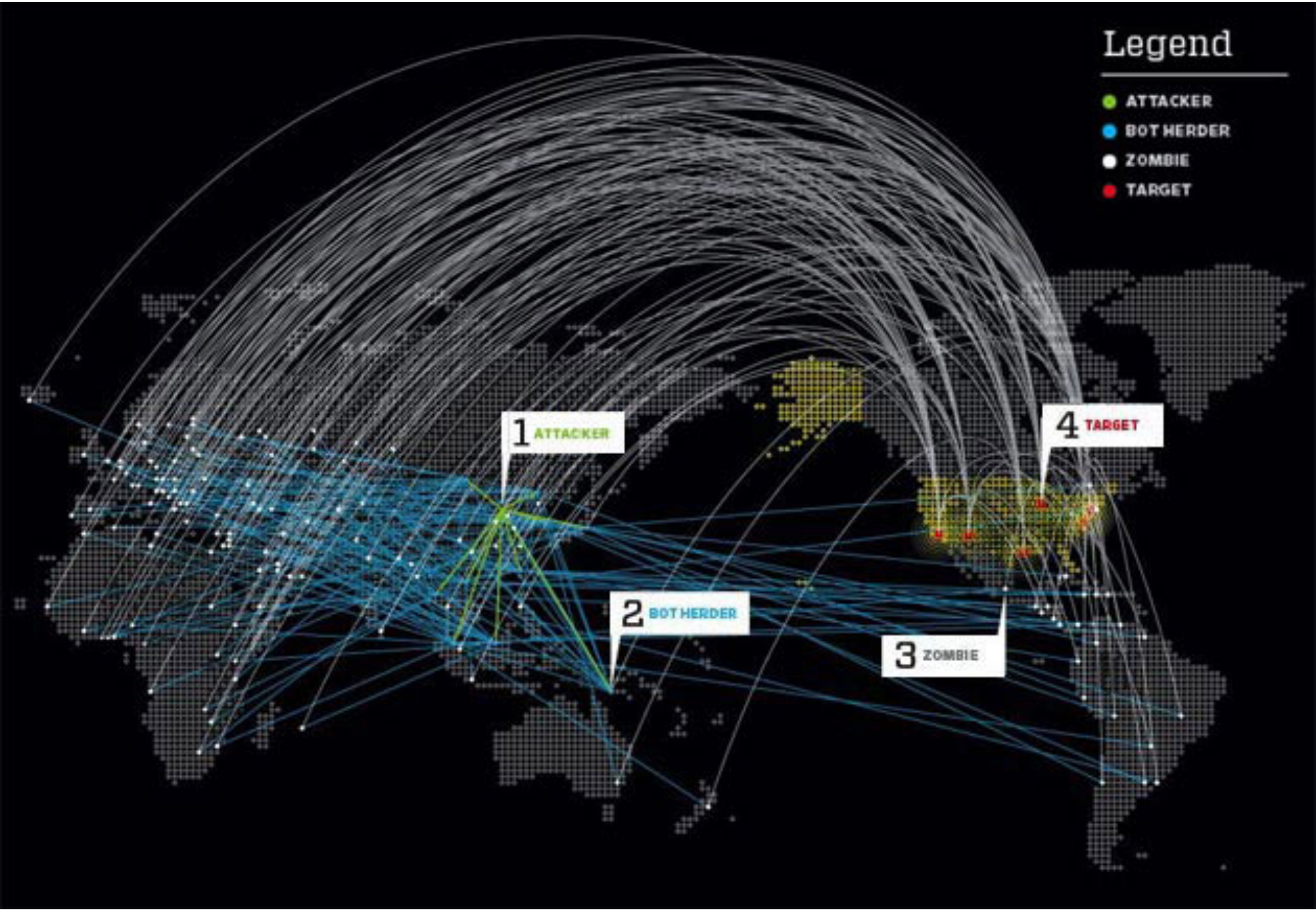
Kinetic versus Cyber

Attribute	Kinetic	Cyber
Effects	Variable (largely known, e.g., guns, bombs)	Variable (largely unknown)
Coverage	Limited by materiel	Global
Speed	Limited by transport	Possibly instantaneous
Cost (as %GDP)	Significant	Near zero
Industrial base important?	Extremely	No
Attributable	Yes, at scale	Not clear, at any scale



Denial of Service

- Security Properties ("CIA"):
  - **C**onfidentiality: Keeping it to yourself
  - **I**ntegrity: It's what you think it is
  - **A**vailability: You can get at it
- If you depend on the net
  - Availability: your packets get through
  - "Best effort" (IP service) not enough
  - 1M machines send one 1KB packet/second
    - 8 Gbits/second – overwhelms most links


Legend
ATTACKER
BOT HERDER
ZOMBIE
TARGET
1 ATTACKER
2 BOT HERDER
3 ZOMBIE
4 TARGET

Attribution (who did it?)

- Kinetic weapons: easy
- Internet: source addresses not needed for routing, anonymity tools

"On the Internet, nobody knows you're a dog."

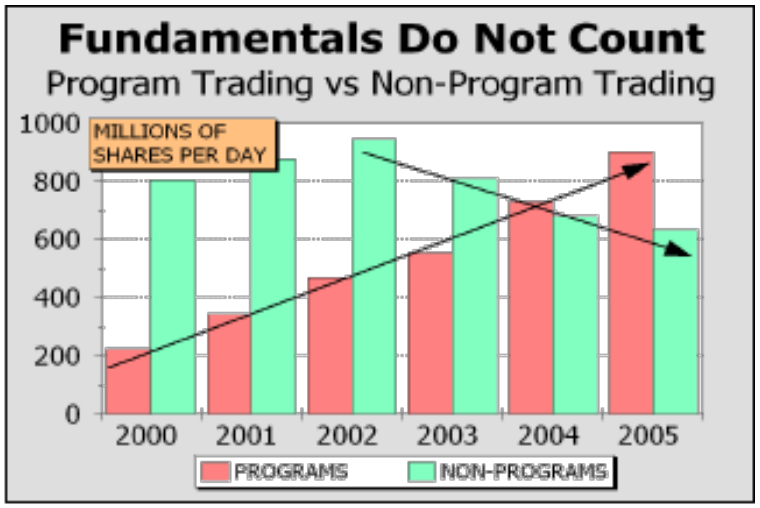
Weapons

- Botnets – large populations of 0wned machines
- Worms – self-propagating software
- Viruses – persistent malware
- Zero-day attacks
  - Unknown, therefore no signature/defense
- Overlap with cybercrime!

Attacks

- DoS and DDoS (deny availability of net)
- Disabling non-cyber (“kill switch” for electric, telephone, banking, etc.)
  - “Critical infrastructures”
  - See next slide
- Controlling (cyber-defenses, banking, cameras, radars, planes, ships, etc.)

Example Cyberinfrastructure: Markets



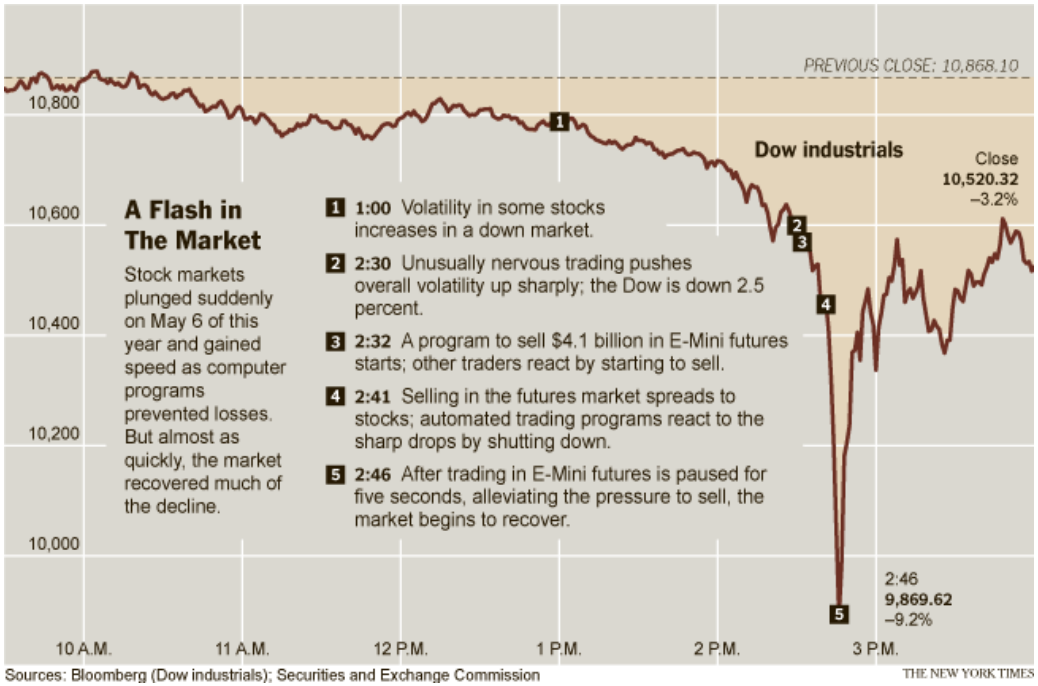
Program trading systems are software systems.

- 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 for markets

- 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

Not new thoughts…

- “soldiers no longer have a monopoly on war”, and “financial wars and computer virus wars which will dominate the future…“, from *Unrestricted Warfare*, Qiao Liang & Wang Xiangsui, PLA, Feb. 1999
  - See http://www.c4i.org/unrestricted.pdf

- “vulnerabilities are subject to exploitation…by financial terrorists, intent on destroying the American financial system”, from *Economic Warfare: Risks and Responses*, Kevin D. Freeman, June 2009

Defenses

- "Air gap" – keep machines off the net
  - Increasingly difficult – software updates?
  - Malware can also travel by memory stick
- Treat "critical infrastructure" specially
- Network-embedded "perimeter" defenses
  - Firewalls and intrusion detection systems
  - Rate-limiting, packet filtering, pushback?
- Good software ☺; good machine hygiene ☺; national network cutoffs (IP "kill switch")???