U.S. National Cybersecurity

William J. Perry
Martin Casado · Keith Coleman · Dan Wendlandt

MS&E 91SI
Spring 2004
Stanford University

Why are we talking about cybersecurity?

Case 1: Internet Under Siege

- **February 7 - 9, 2000**
  Yahoo!, Amazon, Buy.com, CNN.com, eBay, E*Trade, ZDNet websites hit with massive DOS
- Attacks received the attention of president Clinton and Attorney General Janet Reno.
- **"A 15-year-old kid could launch these attacks, it doesn't take a great deal of sophistication to do"**
  – Ron Dick, Director NIPC, February 9
- U.S. Federal Bureau of Investigation (FBI) officials have estimated the attacks caused $1.7 billion in damage

* The Yankee Group, 2000

Case 2: Slammer Worm

- **January 2003**
  Infects 90% of vulnerable computers within 10 minutes
- **Effect of the Worm**
  - interference with elections
  - canceled airline flights
  - 911 emergency systems affected in Seattle
  - 13,000 Bank of America ATMs failed
- **No malicious payload!**
- **Estimated ~$1 Billion in productivity loss**

Case 3: WorldCom

- **July 2002**
  WorldCom declares bankruptcy
- **Problem**
  WorldCom carries 13% - 50% of global internet traffic. About %40 of Internet traffic uses WorldCom's network at some point
- **October 2002**
  Outage affecting only 20% of WorldCom users snarls traffic around the globe
- **Congressional Hearings**
  Congress considers, but rejects, extension of FCC regulatory powers to prevent WorldCom shutdown

Vulnerabilities are not just technical

Case 4: It's a Jungle Out There

- The Internet is highly, globally connected
- Viruses/worms are legion on the Internet and continue to scan for vulnerable hosts
- Hackers scan loo[illegible]s to attack

With Live Demo!

What's really going on here

Increasing Dependence

We are increasingly dependent on the Internet:

Directly

- **Communication (Email, IM, VoIP)**
- **Commerce (business, banking, e-commerce, etc)**
- **Control systems (public utilities, etc)**
- **Information and entertainment**
- **Sensitive data stored on the Internet**

Indirectly

- **Biz, Edu, Gov have *permanently* replaced physical/manual processes with Internet-based processes**

* Based on slides by David Alderson, CalTech

Security Not A Priority

Other design priorities often trump security:

Cost
Speed
Convenience
Open Architecture
Backwards Compatibility

An Achilles Heel?

Combination of dependence and vulnerability make the Internet a target for **asymmetric attack**

Cyberwarfare
Cyberterrorism
Cyberhooliganism*

and a weak spot for **accidents and failures**

* Coined by Bruce Schneier, Counterpane

Hard to Manage Security

- **No metrics to measure (in)security**
- **Internet is inherently international**
- **Private sector owns most of the infrastructure**
- **Cost/incentive disconnect?**
  - Businesses will pay to meet business imperatives
  - Who's going to pay to meet national security imperatives?

The Challenge

A solution to this problem requires both the right **technology** and the right **public policy**.

This is the cybersecurity challenge.

What is “cybersecurity?”

Some Definitions

According to the U.S. Dept of Commerce:

n. **cybersecurity**: *See “*information security”

n. **information security**: The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

Some Definitions

According to H.R. 4246 “Cyber Security Information Act”:

cybersecurity: “The vulnerability of any computing system, software program, or critical infrastructure to, or their ability to resist, intentional interference, compromise, or incapacitation through the misuse of, or by unauthorized means of, the Internet, public or private telecommunications systems or other similar conduct that violates Federal, State, or international law, that harms interstate commerce of the United States, or that threatens public health or safety.”

Some Definitions

According to S.I. 1901 “Cybersecurity Research and Education Act of 2002”:

cybersecurity: “information assurance, including scientific, technical, management, or any other relevant disciplines required to ensure computer and network security, including, but not limited to, a discipline related to the following functions:

(A) Secure System and network administration and operations.
(B) Systems security engineering.
(C) Information assurance systems and product acquisition.
(D) Cryptography.
(E) Threat and vulnerability assessment, including risk management.
(F) Web security.
(G) Operations of computer emergency response teams.
(H) Cybersecurity training, education, and management.
(I) Computer forensics.
(J) Defensive information operations.

Some Definitions

According to S.I. 1900 “Cyberterrorism Preparedness Act of 2002 ”:

cybersecurity: “information assurance, including information security, information technology disaster recovery, and information privacy.”

One way to think about it

cybersecurity = security of cyberspace

One way to think about it

cybersecurity = security of cyberspace

information systems and networks

One way to think about it

cybersecurity = security of information systems and networks

One way to think about it

cybersecurity = security of information systems and networks

security in the face of attacks, accidents and failures

One way to think about it

cybersecurity = security of information systems and networks in the face of attacks, accidents and failures

One way to think about it

cybersecurity = security of information systems and networks in the face of attacks, accidents and failures

security and reliability

One way to think about it

cybersecurity = security and reliability of information systems and networks in the face of attacks, accidents and failures

(Still a work in progress.)

In Context

corporate cybersecurity = security and reliability of corporate information systems and networks in the face of attacks, accidents and failures

national cybersecurity = security and reliability of the nation's information systems and networks in the face of attacks, accidents and failures

Cybersecurity as a Discipline

Now we have our goal. How do we achieve it?

Must understand the four factors that play into the cybersecurity equation:

- Technology
- Public Policy
- Economics (of stakeholders and incentives)
- Social Influences (e.g. Big Brother fears)

What This Class is All About

Goal of the Class

Answer the question:

Is today's Internet is an appropriate platform on which to operate critical infrastructure services that affect U.S. national security?

How We'll Get There

- Understand threats to today's Internet infrastructure
- Develop a framework for analyzing the factors in the Cybersecurity equations
- Explore and analyze not only the technical options for securing the Internet but also consider political, legal, and economic means able to combat the problem

What You Will Come Away With

- Working knowledge of how the Internet infrastructure operates and who the major cybersecurity policy actors are.
- Frameworks within which to understand and analyze cybersecurity issues.
- Knowledge about current salient issues in cybersecurity.
- Connections and resources to help you in cybersecurity related research.

The Bottom Line

We need people who can do both policy and technology

What This Class is Not

- This class is **not**…
  - "How the Internet works"
    - Take *CS244A Networks*, or *CS193i Internet Systems*
  - "How to hack"
    - Take *CS155 Computer Security*
  - "Cryptography and privacy"
    - Take *CS255 Intro to Cryptography*
  - "File sharing and music piracy"

What This Class Is

- This class **is**…
  - A look at the bigger picture
  - A chance to consider all the factors that play into cybersecurity
    - Technology
    - Policy
    - Law
    - Economics

The Stanford Cybersecurity Center

Stanford Cybersecurity Center

- **What it is:**
  An interdisciplinary research center designed to bring together the minds and ideas of Stanford's leading experts in Technology, Public Policy, Business and Law to address the cybersecurity challenge
- **Goal:**
  Foster the development of *both the technology and the public policy* needed to meet the cybersecurity challenge
- **What we do:**
  Education: Create and sponsor courses like this one
  Research: Foster collaborative research between disciplines (and launch new projects)
  Outreach: Collaborate with the Silicon Valley and Washington, DC communities
- **Who it is:**
  Students, faculty, researchers from CS, EE, MS&E, CISAC, Stanford Law School, etc…
- **How to get involved:**
  Research opportunities, discussion forums, lecture series, courses…
  Visit http://cybersecurity.stanford.edu or speak with us after class.

Course Logistics

Basics

- Course website will have latest content & updates:
  http://msande91si.stanford.edu
- 2 units, S/NC
- No prerequisites
- Location: TBD

Course Format & Grading

Class Format:

- Pre-class readings and discussion questions posted to class forum.
- In class discussion of readings
- Lecture by expert guest speaker
- Q & A discussion for more in depth discussion about the speaker's topic.

Expectations:

- Attend every session, do all readings and discussion questions.
- Final short explorative talk on a topic of personal interest in cybersecurity.

Schedule & Syllabus

March 31	Introduction Overview of the Cybersecurity Challenge
April 7	Technology 101: Background on Networks, the Internet, Hacking and Cyber Attacks
April 14	Policy 101: Background on U.S. Cybersecurity Policy
April 21	Enforcing Cybersecurity *Guest Speaker: Mary Rundle, Stanford Law School*
April 28	Bad Things Can Happen On (or To) the Internet *Guest Speaker: Dan Geer, Verdasys*
May 5	Information Warfare and Defense *Guest Speaker: Chris Eagle, Lieutenant Commander, U.S. Navy*
May 12	Crypto: What it Can and Can't Do *Guest Speaker: Dan Boneh, Computer Science*
May 19	A Problem of Incentives? *Guest Speaker: Kevin Soo Hoo, Sygate*
May 26	What Features Do We Want in a Critical Infrastructure Platform? *Guest Speaker: David Alderson, CalTech*
June 3	Presentations & Wrap up

Enrollment

- Limited to 20 students
- Student Info Questionnaire
- This course may be offered again in Autumn 2004

Thank You

- Contact
  - Website: http://msande91si.stanford.edu
  - Instructors: cybersecurity@stanford.edu
- Office Hours
  - By request (send email)
  - Individual questions after class

Thank You