

U.S. National Cybersecurity

Martin Casado · Keith Coleman

Sponsored by William J. Perry

***MS&E 91SI
Fall 2006
Stanford University***

**Why are we talking about
cybersecurity?**

Case 1: Blue Security DoS

- May 2006, anti-spam company “Blue Security” attacked by PharmaMaster
- PharmaMaster bribed a top-tier ISP's staff member into black holing Blue Security's former IP address (194.90.8.20) at internet backbone routers.
- Blue Security moves to protect itself
- Attack disrupts the operations of five top-tier hosting providers in the US and Canada, as well as a major DNS provider for several hours.
- Blue security folds ☹️

Case 2: Slammer Worm

- **January 2003**
Infects 90% of vulnerable computers within 10 minutes
- **Effect of the Worm**
 - Interference with elections
 - Cancelled 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: September 11

- **Wireless Tower on Top of Trade Center Destroyed**
- **AT&T has record call volumes**
- **“Flash” usage severely limits availability**
- **Rescue efforts hampered**

Physical Vulnerability!

Legitimate Usage!

Case 5: “Titan Rain”

- Successful network intrusions on U.S. military installations
- Increasing in frequency since 2003
- Originating from China
- Successful intrusion into...
 - U.S. Army Information Systems Engineering Command at Fort Huachuca, Arizona
 - Defense Information Systems Agency in Arlington, Virginia
 - Naval Ocean Systems Center in San Diego, California
 - United States Army Space and Strategic Defense installation in Huntsville, Alabama
 - more...

What's really going on here

Increasing Dependence

- **Communication (Email, IM, VoIP)**
- **Commerce (business, banking, e-commerce, etc)**
- **Control systems (public utilities, etc)**
- **Information and entertainment**
- **Sensitive data stored on the Internet**
 - **e.g.**
- **Biz, Edu, Gov have *permanently* replaced physical/manual processes with Internet-based processes**
- **Navy command dissemination?**

Security Initially Not a Priority

Other design priorities often trump security:

Cost

Speed

Convenience

Open Architecture

Backwards Compatibility

And It's Really Hard ...

- **Hard to retrofit security “fixes”**
- **No metrics to measure (in)security**
- **Internet is inherently international (no real boundaries)**
- **Private sector owns most of the infrastructure**
- **“Cybersecurity Gap”: a cost/incentive disconnect?**
 - Businesses will pay to meet business imperatives
 - Who's going to pay to meet national security imperatives?

An Achilles Heel?

This level of dependence makes the Internet a target for **asymmetric attack**

Cyberwarfare
Cyberterrorism
Cyberhooliganism*

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

* Coined by Bruce Schneier, Counterpane

The Challenge

Clearly not just a technical problem. Requires consideration of **economic factors, public policy, legal issues, social issues** etc.

That's what this class is about.

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. 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. 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




+ with the goal of
protecting operations
and assets

One way to think about it

cybersecurity = security of information systems and networks with the goal of protecting operations and assets

One way to think about it

cybersecurity = **security** of information systems and networks with the goal of protecting operations and assets



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 with the goal of protecting operations and assets

One way to think about it

cybersecurity = **security** of information systems and networks in the face of attacks, accidents and failures with the goal of protecting operations and assets



**availability, integrity
and secrecy**

One way to think about it

cybersecurity = availability, integrity and secrecy of information systems and networks in the face of attacks, accidents and failures with the goal of protecting operations and assets

(Still a work in progress...comments?)

In Context

corporate cybersecurity = availability, integrity and secrecy of information systems and networks in the face of attacks, accidents and failures with the goal of protecting a corporation's operations and assets

national cybersecurity = availability, integrity and secrecy of the information systems and networks in the face of attacks, accidents and failures with the goal of protecting a nation's operations and assets

What This Class is All About

Cybersecurity Questions

- How vulnerable is the United States to a cyberattack? Are we heading for an “electronic pearl harbor”?
- What areas of vulnerability require the greatest attention in order to improve our national cybersecurity?
- With what parties must the government work in order to make significant cybersecurity improvements?
- Are market forces sufficient to provide for US national cybersecurity? Should the government get involved to change these forces, and if so, how?

Cybersecurity Questions

- Is the Internet an appropriate platform upon which to operate infrastructure systems critical to US economic or government operation?
- What characteristics would we want in an “Ideal Internet”?
- Can the current Internet evolve into a network with significantly improved security guarantees or will another system need to be created?
- Does greater Internet security necessarily entail decreased online privacy?

Schedule & Syllabus

Sept. 28	Introduction
Oct. 5	Technology & Policy 101
Oct. 12	An industry perspective Guest Speaker: Stephen Hansen, Google & Stanford
Oct. 19	Market incentives and security metrics Guest Speaker: Kevin Soo Hoo, McAfee
Oct. 26	Cybersecurity and law Guest Speaker: Jennifer Granick, Stanford Law School
Nov. 2	Reinventing the Internet Guest Speaker: Martin Casado, Computer Science
Nov. 9	Network warfare Guest Speaker: Chris Eagle, U.S. Naval Postgraduate School
Nov. 16	A future critical information infrastructure Guest Speaker: David Alderson, California Institute of Technology
Nov. 30	Liability, negligence and cyberinsurance Guest Speaker: Erin Kenneally, San Diego Supercomputing Center
Dec. 7	Legislative debate

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
 - Public Policy
 - Economics
 - Social Issues

Course Logistics

Basics

- Course website will have latest readings & updates:

<http://msande91si.stanford.edu>

- 2 units, S/NC
- No prerequisites
- Location: Wallenberg 160-325

Course Format

Class Format:

- Pre-class readings (fresh, interesting stuff)
- Submit two discussion questions
- Lecture and Q&A with expert guest speaker

Our Evaluation

The Cybersecurity Legislative Debate

- You'll be defending one of two pieces of proposed legislation
- In groups, create an in-class presentation backing a single position on one of the bills. You will debate an opposing group and your will defend your stance against questioning from the rival group and the class at large.
- Panel of celebrity judges will vote on the winner of each debate.

Grading & Expectations

Our expectations are simple:

- Do all readings
- Submit pre-class discussion questions
- Significant in-class participation
- Completion of final legislative debate project

This should be fun!

Enrollment

- Limited to 20 students
- Student Info Questionnaire
- Looking to audit? Talk to us after class.

Contact

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

Thank You