CSCI 1800 Cybersecurity and International Relations

Course Overview

John E. Savage
Brown University
The Purpose of This Course

• Explore technology, policy, social, economic, international and security dimensions of cyberspace
  – Cyberspace is the global network of computers, cloud storage, control systems, and smart phones

• Goal: Provide an intro to the technological and policy dimensions of cyberspace.
Assignments

• Five short analysis papers
  – First due on February 15th.
• Group projects, each a response to a cyber crisis
  – Teams hold press conference and speak for and against an issue or person that has been in the news
• Mid-semester project: Encryption Legislation or Critical Infrastructure.
• Final paper on a topic of your choice
Course Organization

• Course materials are available via course website. Useful books:
  – *Intro to Computer Security* by Goodrich & Tamassia, Addison Wesley
  – *Cybersecurity and Cyberwar* by Singer & Friedman, Oxford.

• Meetings
  – Classes: Mondays and Wednesdays 3:00-4:20, CIT 368
  – At least two guest speakers
  – Ten weekly small group meetings (Labs)

• Grading
  – 10% Group project
  – 25% Five short analysis papers
  – 20% Midterm project
  – 25% Final paper
  – 20% weekly labs (Participation + Reading Response)
What Will You Gain From this Class?

- Develop public speaking skills
- Write a combined technology/policy paper
- Understand current cybersecurity landscape
- Complete a course with a WRIT designation
Overview of Today’s Lecture

• Introduction to the Internet
• Internet Naming and Routing
• The Hazards of Internet Globalization
• Internet Attacks
• Policy Responses
• Outline of the course
Introduction to the Internet
The Impact of the Internet

• Internet has revolutionized commerce, is changing cultures, and engaging governments
The Global Cyber Challenge

• Cyberspace has become a dangerous place
  – Critical resources are accessible
  – Theft and espionage are rampant
  – Privacy regularly invaded

• We must strive to make it more secure
  – If we fail, crime will increase and conflict might result
  – Ominously, nations are preparing for conflict

• Introduces new policy and technology challenges.
  – We need people conversant with both.
What is the Internet?

• Collection of networks, each run by an autonomous system – a manager of IP addresses.

• Data streams broken into packets and routed using a protocol (e.g. TCP/IP). Paths taken by IP packets may vary.
The Internet Has Become The Wild West

• The gunslingers – Hackers
• The town – Hundreds of millions of marginally protected computers
• Where are the sheriffs?
• How do we protect ourselves and our assets?
• How do we know if we are protected?
History of the Internet

- First public switched telephone network (PSTN) built in 1875 – communicates via fixed circuits
- Packet networks invented in US & UK in 50s-60s
- Experiments begin in US & France in 70s & 80s.

ARPANET as envisioned in ‘69
History of the Internet

• Transmission Control Protocol (TCP) and Internet Protocol (IP) invented in ’73 by Cerf and Kahn, adopted by US military in 1983.
  – Other packet switched protocols lose out.
• Internet fully emerges in 90s with introduction of browsers and the World Wide Web.
• Explosive growth follows.
The Internet Today

- ~64K autonomous systems
- ~4 billion assigned IP addresses
- It is an integral element in the world economy.
Why is the Internet So Effective?

- All the smarts are at the periphery.
  - Smarts of PSTN are inside, controlled by monopolies
- No one controls the Internet
  - Need permission to connect to PSTN, not for Internet
- Internet only mildly regulated in West
- Most Internet standards created via an open multi-stakeholder process.
Internet Naming and Routing
The Domain Name System (DNS)

- Packets have source and destination IP addresses.
- IP addresses are hard to remember. Domain names, such as www.brown.edu, are humanly readable.
- Must translate domain name to binary IP address, e.g. 192.0.32.10.
Translating A Domain Name

• **Translation** of www.example.com into 192.0.32.10
  – Ask root zone server for IP address of .com server.
  – Ask .com server for IP address of example.com server.
  – Ask example.com server for IP address of www.example.com, namely, 192.0.32.10 (= IPC)
Converting IPv4 Addresses to Bits

• For the curious, IP = 192.0.32.10 is short hand for
  • $192_{10} = 11000000_2 \ (1 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0)$
  • $0_{10} = 00000000_2$
  • $32_{10} = 00100000_2 \ (0 \cdot 2^7 + 0 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0)$
  • $10_{10} = 00001010_2$

  – IP = 11000000 00000000 00100000 00001010
  – Spaces substitute for periods

• IPv4 addresses have 32 bits. $\approx 4 \times 10^9$ IPv4 addresses.
• IPv6 address has 128 bits, $\approx 3.4 \times 10^{38}$ addresses!
• A **DNS resolver** translates a domain name to an IP address.
DNS Resolvers

• If the mapping from domain name to IP address is cached locally, provide it. Otherwise
  – Resolver visits root zone to get address of top-level domain (TLD) (e.g. .com).
  – Resolver visits TLD to get address of second-level domain (e.g. example.com).
  – More visits may be needed to get IP address.

• Each computer uses a potentially different resolver
Hazards of Internet Globalization
Globalization Introduces Risks

• **Efficiency** encourages *migration* of applications to the Internet.
  – **Critical infrastructures** have been connected to the Internet!

• Local resources accessible globally!
  – Risk of attack has increased greatly.
Critical Financial Infrastructure

• Financial and banking systems
  – CHIPS, main US bank clearance system, clears $1.5 trillion/day
  – Compare to US GDP which is ~$17.4 trillion/year
  – Federal Reserve Bank of Boston processes ~ $5 trillion of transactions/day!
Critical Electricity Infrastructure

- Ex: Power grids are vulnerable to attack
  - See below: Ukraine blames Russia for 2015 outage
  - US Electricity Information Sharing and Analysis Center warns its members about such attacks.

12/24/2015

Dear customers!

Dec. 23, 2015, from 15:35 - 16:30, third parties were made illegal entry into information-technological system of remote access to equipment telecontrol substations of 35-110 kV JSC "Kyivoblenergo."

As a result, it was disconnected 7 (seven) 110 kV substations and 23 (twenty three) substation 35 kV. This led to the repayment of about 80,000 different categories of customers on the reliability of electricity supply.

Electricity was restored to all consumers employees of the Company at 18:56 the same day.

We apologize for the situation and thank you for your understanding.

PJSC "Kyivoblenergo"
US Critical Infrastructure Areas
Interdependencies of the CI

Source: Dutch TNO
SCADA in Critical Infrastructure

- **SCADA**: Supervisory control & data acquisition
- These systems control power, water, etc.
- They were not designed to be secure
  - Some have hard coded passwords
  - Many are connected to Internet
- Many SCADA systems are **fragile**.
  - They respond automatically to changes.
  - Large changes can cause cascading failures.
Opinions on Internet

• Pres. Obama\(^1\): “... our interconnected world presents us, at once, with great promise but also great peril.”

• Former Dir. National Intelligence McConnell\(^2\): “As the most wired nation on Earth, we offer the most targets of significance, yet our cyber-defenses are woefully lacking. ... The problem is that we lack a cohesive strategy to meet this challenge.”

1. Remarks on May 29, 2009
2. Washington Post, February 28, 2010
Example of Damage

- Mandiant Corp 2013 report
  - PLA 3\textsuperscript{rd} Department Unit 61398 in Shanghai responsible for stealing terabytes from ≥ 141 orgs since 2006.
  - Maintained access to computers for average of 356 days!
  - One of 20+ Chinese units engaged in advanced persistent threats (APTs)
Example of Damage

- McAfee Corp July 2013 report
  - $100B loss/year to U.S. economy & 508,000 jobs
  - $100-$500 Billion annual loss globally
Examples of Damage

• NSA global surveillance revealed by Snowden
  – Revealed highly sensitive US information
  – Reputation of American companies adversely affected
Internet Attacks
Some Internet Attack Types

• Seize control of a computer
  – Exploit hole in an application or operating system and load a Trojan (horse) – a “backdoor”
  – Attacks occur via email, browser, USB, CDs, IM, Twitter

• Distributed denial of service (DDoS) attack
  – Multiple computers send packets to one computer, thereby overwhelming it
  – “Low Orbit Ion Cannon” is software for DDoS attacks

• Routing attacks
  – Redirect users to malicious web sites
Outline of a Typical Attack

1. Target clicks on link from “trusted” source causing a visit to a website that has a malicious payload.
2. Target’s browser downloads and runs payload that exploits a hole in browser.
3. Malware sets up backdoor and connects to attacker’s command and control servers.
4. Attacker now has complete control of computer.
5. Attacker can steal or change intellectual property.
Traditional Advice to Avoid Infection

• Use a firewall.
• Update operating systems, APPs and anti-virus software.
• Don’t visit suspicious sites or open such email.
• Be careful on Facebook and Twitter.
• Heed browser warnings when visiting sites.
• But this is not sufficient!
Botnets

• Networks of compromised computers (bots)
  – Some botnets sold pennies/PC for lifetime of botnet.
  – Mac botnets are more expensive

• Botnets can be used to
  – Launch DDoS attacks
  – Send spam, decrypt passwords, etc.

• Botnets change command & control hosts often
  – Makes suppression difficult.
Stuxnet – Paradigm Shift in Malware

- An extremely sophisticated and complex worm that emerged in July, 2010 and infected more than 100,000 hosts.
- Targeted Siemens programmable logic controllers for SCADA systems used in nuclear fuel refinement.
- Aimed primarily at Iranian nuclear industry.
  - President Ahmadinejad acknowledged setback.
- A new era in cyberwarfare emerged!
- This is a warning to all SCADA system operators!
Networks Are Also Vulnerable

• Local network protocols easily spoofed.
• Routers and DNS servers can also be targeted.
  – Hacker can steal a user’s traffic.
  – DNS security improvements being introduced now.
• Border Gateway Protocol (BGP)
  – Autonomous systems (AS) use BGP to invite traffic.
  – It plays a vital role in routing Internet traffic.
  – Has been misused, disrupting global traffic for hours
Some Major BGP Routing Outages

• Feb 24, 2008 – For about two hours connection to YouTube was lost around the world due to action by Pakistan Telecom

• April 8, 2010 – For 20 mins routes to 32,000+ networks directed to China Telecom, affecting Facebook, Twitter, etc.

• August 27, 2010 – 1% of Internet inaccessible for 30 mins due to Duke and RIPE experiment and buggy CISCO router code.

• These and many other examples illustrate fragility of BGP.
• Forbes (4/9/10) called BGP announcements “cybernukes.”
How Did This Mess Develop?

• Market forces have led to monocultures
  – Common operating systems and applications.
  – Result: Network is as weak as its weakest link.
• We concentrate resources for efficiency
  – Internet has too many choke points.
  – Cloud computing is popular – saves time and energy – but centralizes data/programs, providing big target
  – 99% of transcontinental Internet traffic runs on undersea cables.
Policy Responses
Characteristics of the Internet

• Global reach and integrity
  – Need confidence that domains can be reached

• Permission-less innovation
  – Ability to create new service without permission

• Accessibility
  – Easy to add content or a server, attach new network

• Spirit of collaboration
  – Multiple stakeholders cooperate

1. Based on speech by Sally Wentworth
   At Dutch Embassy, Wash DC 2/21/12
Policy Objectives

• Preserve best features of Internet.
  – Requires education, trust development, negotiations
  – Protect privacy and civil liberties
  – While protecting national interests, including security

• Improve cyber defenses.
  – Can’t eliminate attacks but can reduce severity.

• Find ways to deter or mitigate attacks
  – Cooperate to make DNS & BGP more secure.

• Reduce risks through international negotiations.
Deterrence to Cyber Conflict?

• Threat of retaliation is a deterrent, but...
  
• First, we need
    – Attribution with very high assurance.
    – Assurance that collateral damage will be limited.
    – Knowledge of potential domestic repercussions.

On the Internet, nobody knows you’re a dog.
What Should Nations Do?

• Develop domestic **legislation** to
  – Encourage/require improved **vendor cybersecurity**
  – Facilitate **sharing threats** between companies/USG
  – Encourage development of **cyber insurance**
  – While preserving privacy

• Formulate **Internet governance strategies**
  – Work with most influential governments
  – Work with Internet users

• Fund **research and development** on
  – Cybersecurity technology
  – Policy formulation
There is Hope for Better Security

• **Leap-ahead technologies** are promising
  – Find ways to create variants of common software
  – Develop economic incentives to improve security
  – Integrate secure identity management into systems

• **Crypto computing** may be possible
  – Encrypt data and programs so that computations can be done without decryption.

• **Governments** now engaged
  – Many meetings, small and large, all over the globe
Course Outline

• Introduction to the Course (2 lectures)
• Basic Internet Infrastructure (4 lectures)
• Internet Governance (2 lectures)
• Security (3 lectures)
• Student Group Presentations (3 lectures)
• Transnational Issues (2 lectures)
• Cyberwar (2 lectures)
• Policy Topics (4 lectures)
Conclusion

• Cyberspace is a complex new medium.
• We are slowly coming to grips with the challenges it presents.
• Decades of research, policy development, legislation, and international negotiation will be required to tame cyberspace.
• It won’t be easy but can be very interesting
• Course provides an intro to this exciting topic
Upcoming Assignments

• Sign Up for Lab Section by: February 3rd
• First Lab: Week of February 8th
• First Analysis Paper due February 15th