CSCI 1800 Cybersecurity and International Relations

Course Overview

John E. Savage

Brown University
Administrative Issues

• Introductions to the course TA staff
• Announcement of class meetings
  – Lectures – Mondays & Wednesdays in BH 166
  – Weekly sections – sign up online next week
  – With instructor – after class & by appointment
• Collaboration policy
• iClicker questions at the end of lectures
• Waitlist is being assembled
Course Introduction

• Cyberspace is the global network of computers. It includes clouds, control systems, & smart phones.
  – The Internet arrived on January 1, 1983.
  – Cyberspace emerged with the browser around 1991.
  – It is powered by algorithms – recipes for computations.

• We explore technological, policy, social, economic, international & security dimensions of cyberspace.

• Algorithms try to keep users on social media sites
  – An unanticipated use: Influence political opinions
Categories of Course Topics

• Technology/Policy Overview
  – Introduction to these topics
• Security
  – Crime, confidentiality, integrity, conflict
• Economics
  – Employing its levers; impact of CS on economics
• Governance
  – Roles for individuals, organizations, and governments
• Contemporary Topics
  – Disinformation, intelligence, software security, conflict
Assignments

• Lecture participation
  – iClickers will measure participation

• Three short response papers

• Final paper on a topic of your choice

• Section discussions on course topics
  – Class will be divided into nine sections

Points

  5
  45
  35
  15

  100
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 is an important but challenging place
  – We are very dependent upon it
  – Critical resources are now accessible
  – Theft, disinformation, and espionage are rampant

• Our challenge is to make it more secure.
  – If we fail crime and disruptions will increase, and
  – conflict may result

• To address these challenges
  – We need people who understand policy and technology
Encoding Data with Bits and Packets

- An image consists of rows of pixels, say 640 by 480
- Each pixel typically consists of 3 colored dots, RGB
- Intensity of dots (in bits per dot) determines color
- An image is specified by a long sequence of bits
- To transmit, bits grouped into packets, e.g. 1024 bits.
What is the Internet?

- Collection of networks, each run by an **autonomous system** – a manager of IP addresses.
- Data streams broken into **IP packets** and **routed** using an **Internet protocol**. Paths taken by IP packets may vary.

Three networks, two routers, and one domain name server (DNS)
The Internet Has Become Wild West

- The gunslingers – Hackers
- The town – Hundreds of millions of marginally protected computers
- Where are the sheriffs?
  - We once slapped a badge on a hacker & expected to be protected.
- 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 paths
• Packet networks invented in US & UK in 1960s.
• Experiments begin in US in 1970s and 80s.

ARPANET as envisioned in ‘69
History of the Internet

  – Other packet switched protocols lose out to Internet
  – Example of the network effect – when a technology achieves market dominance, others die off

• Internet fully emerges in 90s with introduction of browsers and the World Wide Web.

• Explosive growth follows.
The Internet Today

- ~84K autonomous systems (subnetworks)
- ~20 billion connected devices in 2017
- The Internet is an integral element in the world economy.
Why is the Internet So Effective?

• All the intelligent technology is at the periphery.
  – In the phone network the smarts are inside
  – And controlled by monopolies

• Initially no one controlled the Internet
  – It is now heavily regulated in autocratic countries
  – US and others are now concerned about its openness

• The Internet standards process is wide open!
  – Governed by a multi-stakeholder process.
Internet Naming and Routing
The Domain Name System (DNS)

• Each packet has source & destination IP address
  – Addresses are needed to get to destinations and back
• Because IP addresses hard to remember, humans use domain names, such as www.brown.edu.
• Translate it to an IP address, e.g. 128.148.128.180
More on Domain Names

• **128.148.128.180** represents **four** 8-bit numbers
  – 128 = 10000000; 148 = 10010100; 180 = 10110100
  • \(2^7\) \(2^6\) \(2^5\) \(2^4\) \(2^3\) \(2^2\) \(2^1\) \(2^0\)
  • 1 0 0 1 0 1 0 0 1’s represent powers of 2
  • 128 + 16 + 4 = 148

• To determine who owns **domain name**
  – Visit ICANN WHOIS at [https://whois.icann.org/en](https://whois.icann.org/en)
  – Provide the Universal Resource Locator (URL) [www.brown.edu](http://www.brown.edu) or IP address **128.148.128.180**.
The Domain Name System (DNS)

- Domain names must be translated into IP addresses
- E.g. IP address of www.example.com is 192.0.32.10
- Device needing an IP address, contacts its local domain name resolver.
The Domain Name System (DNS)

- Domain name resolver consults root zone server
- This server provides IP address for .com server
- .com server provides address for example.com server
- This server provides IP address for www.example.com
Domain Name System Translations

• A local **DNS resolver** translates domain names to IPs.
  – If the mapping from domain name to IP address is **cached** locally, it is used.
  – Otherwise a resolver visits a **root zone server** to get address of **top-level domain** (TLD) of an URL (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 are now connected

• Global Internet makes local resources accessible remotely.
  – Miscreant in country A can cause mischief in B.

• Cost of efficiency is increased risk!
Critical Infrastructure

• Financial and banking systems
  – Federal Reserve Bank of Boston handles > $5 trillion of transactions per day!
  – > $10 trillion/day of wire transfers via undersea cables
  – Compare this to US GDP which is $20 trillion/year

• Power grid is highly vulnerable to attack.
  – Russia attacked Ukraine grid.
  – 3,300 US companies provide electricity
# 16 US Critical Infrastructure (CI) Sectors

<table>
<thead>
<tr>
<th>Chemical</th>
<th>Commercial Facilities</th>
<th>Communications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical Manufacturing</td>
<td>Dams</td>
<td>Defense Industrial Base</td>
</tr>
<tr>
<td>Emergency Services</td>
<td>Energy</td>
<td>Financial Services</td>
</tr>
<tr>
<td>Food and Agriculture</td>
<td>Government Facilities (includes electoral systems)</td>
<td>Healthcare and Public Health</td>
</tr>
<tr>
<td>Information Technology</td>
<td>Nuclear Reactors, Materials, and Waste</td>
<td>Transportation Systems</td>
</tr>
<tr>
<td>Water and Wastewater</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

See https://www.dhs.gov/critical-infrastructure-sectors
Interdependencies of the CI

Source: Dutch TNO
SCADA Systems Are in CI

• **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 maintain steady state
  – Large changes can cause **cascading** failures.
Opinions on Internet

• Pres. Obama\textsuperscript{1}:
  – “… our interconnected world presents us, at once, with great promise but also great peril.”

• Former Dir. National Intelligence McConnell\textsuperscript{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.”

\textsuperscript{1} Remarks on May 29, 2009
\textsuperscript{2} Washington Post, February 28, 2010
Examples of Damage

• Mandiant Corp 2013 profile of government hackers
  – PLA 3rd Department Unit 61398 in Shanghai responsible for stealing terabytes of data from ≥ 141 orgs since 2006.
  – Maintained access to computers for average of 356 days!
• Good news: In 2016 Crowdstrike reported a 94% drop in theft of intellectual property for commercial use after US/China agreement of 9/15.
• Bad news: In 2018 theft back to 2015 levels!
• Kaspersky Lab estimates Carbanak crime ring stole > $1B since 2013 from > 100 banks in 30 nations!
• Snowden reveals NSA global surveillance in 2013!
• Ransomware now a billion dollar business!
Internet Attacks
Three Types of Internet Attack

• Seize control of a computer
  – Exploit a **software hole** or **phish** a user & load **backdoor**
  – Attacks can occur via email, browser, USB, CDs, IM, Twitter
  – Top 10 vulnerabilities account for 85% of break-ins, some old.

• Distributed denial of service (DDoS) attack
  – Send many packets to one computer, overwhelming it

• Routing attacks
  – Redirect users to malicious web sites
  – 12/10/18 Google lost control of millions IP addresses to China
Outline of a Typical Attack

• A target clicks on link from “trusted” source.
  – Link contains code which is run, giving attacker access to his/her user computer, or
  – Link connects to website that has malicious payload,
• Browser downloads and runs malicious payload that gives attacker access to machine.
• Attacker now has complete control of computer
• Attacker can steal or change intellectual property or damage attached equipment.
Stuxnet – First Cyber Weapon

• Sophisticated and complex worm that emerged in July, 2010. Infected more than 100,000 hosts.
• Targeted Iranian nuclear fuel refinement facility.
  – Destroyed almost 1,000 centrifuges!
  – President Ahmadinejad acknowledged the attack.

• Flame – data collection for Stuxnet, etc.
  – Highly complex and huge – 20 Megabytes of code!
Networks Are Also Vulnerable

• Border Gateway Protocol† (BGP)
  – Used by autonomous systems (AS) to invite traffic.
  – It plays a vital role in routing Internet traffic.
  – Based on trust. It has been misused to disrupt traffic

• Some Global Internet Traffic Disruptions
  – Feb 24, 2008 – For about two hours connection lost to YouTube due to action by Pakistan Telecom
  – April 8, 2010 –For 18 mins routes to 32,000+ networks sent to China Telecom, affecting Facebook, Twitter, etc

† See WaPo article on BGP: http://www.washingtonpost.com/sf/business/2015/05/31/net-of-insecurity-part-2/
How Did This Mess Develop?

• Market forces have led to monocultures
  – Common operating systems and applications in use.
  – 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. However, can be more secure than home computers
  – 99% of international Internet traffic on undersea cables
Policy Responses
Characteristics of the Internet

• Provides global reach, but based on trust
  – Need confidence that domains can be reached and that confidentiality not violated
• Permission-less innovation
  – Ability to create new services without permission
• Accessibility
  – Easy to add content or attach new server to network
• Spirit of collaboration
  – Multiple stakeholders cooperate

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

• Preserve best features of Internet
  – Requires education, trust development, negotiations
  – Establish norms of state behavior
  – Protect privacy, civil liberties and national interests

• Improve cyber defenses
  – Make computers and networks more secure
  – Employ best practices individually and collectively
  – Engage in risk reduction locally and internationally
Attribution

• To respond to miscreants
  – We need attribution with very high assurance.
  – Retaliation may cause collateral damage and an unpredictable response.

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

• Develop domestic legislation to
  – Encourage/require improved vendor cybersecurity
  – Share threat information between organizations/govts
  – Develop cyber insurance – have experts assess sites

• 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**
  – Apply techniques to thwart attackers
  – 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 held and international centers set up
Course Outline
Lecture Topics

• Intro to Technology & Policy Challenges
• Cyber Threats (Guest, National Intel Council)
• Computer Hardware & Software
• Hardware and Software Vulnerabilities
• Internet Naming and Routing Protocols
• Design & Operation of the Internet
• Cyber Exploits
• Attribution and Privacy
Lecture Topics (cont.)

• Major Cyber Attacks
• Secure Communications and Authorization
• Cyber Conflict
• Careers in Cybersecurity (Guest)
• Cyber Economics
• Bitcoin and Blockchains
• Transborder Crime
• Internet Governance
Lecture Topics III

• The International Norms Process
• Social Media and Propaganda
• AI and Ethics
• Engineering for Security
• Defense in Depth
• The Role of Intelligence & Info Sharing (Guest)
• Future Directions
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
Examples of iClicker Questions

• Q: The domain name system maps...
  – A - IP addresses to domain names
  – B - Domain names to URLs
  – C - Domain names to IP addresses
  – D - IPv4 addresses to IPv6

• Q: What does the term “multistakeholder” describe in the context of internet governance?
  – A - Many bodies have a vested interest in internet governance.
  – B - No one wants to be responsible for cyberspace governance
  – C - Everyone wants to use the internet but no one pays for it