CSCI 1800 Cybersecurity and International Relations

Technology & Policy Challenges

John E. Savage

Brown University
Outline

• History of computers and networks
• Societal impact of the Internet
• Making systems secure
• Examples of cybersecurity policy formulation
• Internet governance
• Is cyber conflict possible?
History of Computers & Networks
Cyberspace Summary

• Cyberspace is the Internet, host computers, applications, stored data, networks and traffic.
• Internet is collection of independently managed subnetworks (autonomous systems or ASes).
  • Important: the Internet is privately owned/managed
• Traffic flow (i.e. routing) decided by ASes
• The Domain Name System (DNS) maps domain names into physical IP addresses (bit strings).
Brief History of Computers

• The first recorded use of word “computer” in 1613.
  – A computer was a person who performed computations.
• Mechanical aids to computation are very old.
  – Abacus (3,000 BC), astrolabe (150BC), slide rule (17th AD)
  – Jacquard Loom (1801), Analytical Engine (1837), Hollerith
    punched card tabulator (1880s), and Zuse 3 (1941).
• First vacuum tube-based programmable computers
  – Eniac (1946), Manchester computer (1948).
• The wiki page* on computers is very good.

* See https://en.wikipedia.org/wiki/Computer
The Abacus (2,700 BC)

- The abacus is used for arithmetic operations.

- The abacus is a model for modern computers!
- It stores data and computes with human help.
Astrolabe (8$^{th}$ Century BC)

- A device for measuring angles, typically with the horizon.
Arithmetic Machines

• Machines to add & subtract in decimal system designed by
  – Shickard (~1623)
  – Pascal (1640s)
Jacquard Loom (1746)

• The **Jacquard Loom** was one of the first programmable devices
Difference Engine (1822)

- Designed by Babbage to compute polynomials
Analytical Engine (1835)

- (Part of) Babbage’s general-purpose computer
- Had both “store” and “mill”!
Zuse Z3 (1941)

- Considered the world’s first working programmable, fully automatic (electromechanical) computing machine.
The Eniac (1946)

- The **ENIAC** (1946) considered to be the first general-purpose **electronic** computer
Etymology of the Computer Bug

• The actual first computer bug was a moth found trapped in an electromagnetic relay of the Harvard Mark II computer.
Punched Card (1700s – 20\textsuperscript{th} Cent.)

- A 1970s punched card containing one line from a Fortran program
The Computer Industry

- Driven by micro miniaturization of devices.
- Transistor (a switch) became available in 1950s.
- Invention of the integrated circuit (1958/9) led to exponential growth of devices per unit area over time (Moore’s Law).
  - Moore’s Law is now ending
- In 1958, one transistor per chip. In 2019, $40 \cdot 10^9$ transistors/chip!
Computer Networks

• First computer networks* emerge in 1950s
• ARPANET, Internet precursor, emerged in 1969.
• Networks of many different sizes now exist.
  – Local, regional, national, international
• Multiple communication technologies are used.
  – Twisted pair, coaxial, optical fiber, radio (wireless)
• Many protocols are employed.
  – TCP/IP (Internet), Ethernet (local net)

* See https://en.wikipedia.org/wiki/Computer_network
Societal Impact of the Internet
Political Power of Social Media

- Governments limit access to information
  - Google and NYT not available in China
  - Turkey shut down Internet during its elections

- Social media – facilitates organizing & recruiting
  - Arab Spring (2010-14), ISIS emerges (~2011-12)

- Fake news is lucrative and disruptive
  - The Follower Factory (NYT, 1/27/18), Devumi sells followers
  - Kompromat (компромат) is increasingly practiced
Critical Infrastructure at Risk

• A networked economy is more fragile
  – Computers can be hacked, networks blocked

• Critical infrastructure (CI) is now on the Internet
  – Exposes nations to damaging attacks
    – Supervisory control & data acquisition (SCADA) systems
      • They control electrical grid, plants, water delivery, etc.
      • Can experience cascading failures

• Cloud computing has become very popular.
  – More secure but clouds provide big targets.
A Chemical SCADA System
Just-in-Time (JIT) Delivery

• Greatly facilitated by the global Internet
• UK Study done by Lord Cameron in 2007*:
  – 80% of grocery sales occur in 4-5 chains.
  – Only 4-5 days of food supply on shelves.
  – UK is “nine meals away from anarchy”.
  – UK food supply is totally dependent on oil.
  – If oil supply were cut off, law and order would break down in three full days.
• Fragility of JIT systems is worrisome.
• Too many systems in modern economies are JIT.

See http://www.utne.com/environment/nine-meals-away-from-anarchy-zm0z13jzros.aspx
Cloud Computing

• Third-parties provide computing & storage.
  – E.g. Google, Amazon, HP, IBM, Microsoft
  – Using replication and full-time staffs, clouds are more secure than personal computers

• They also present big targets.
  • Chip vulnerabilities impact clouds (e.g. Meltdown)

• Fortunately, operators can afford good security
  • Some can provide better security than companies
Making Systems Secure
Software Complexity = Insecurity

• Software complexity continues to grow.
  – 2007 Mac OS X 10.4 – 86 Million lines of code (LOC)
  – 2010 Windows 10 – 50 Million LOC
• Number of errors grows with software complexity
• If 1 security error/10³ LOC $\Rightarrow$ 86,000 bugs in OS X
• A software engineer can only write several 10s of lines of documented & tested lines of code per day.
• Thus, writing secure code is very challenging!
Cyber Attacks

• Attacker motivation
  – Script kiddies seek fun
  – Criminals seek profit
  – Hacktivists have a political agenda (e.g. Anonymous) – they use DDoS
  – Nation states seek information, compromising or not
  – Terrorists seek recruits and may launch attacks
Inside, Close-In, Remote Attackers

- Insider theft
  - Represents greatest risk
- Close-in attackers *can*
  - Communicate via WiFi
  - Sit at console
  - Listen to noise emanating from a computer
- Remote attackers *can*
  - Impersonate a user over the phone – social engineering
  - Probe and attack hosts via the Internet
  - Attack via a compromised website
  - Manipulate the Domain Name System
  - Launch a man-in-the-middle attack
  - Phish
Intro to Internet Governance
Government Group of Experts (GGE)

• UN convened five GGE sessions to examine existing and potential cyberspace threats and propose cooperative responsive measures.
• Representative proposed norms, e.g.
  – International law applies online as well as offline
  – States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs
  – States should not engage in or support espionage for commercial advantage
Brief History of UN Involvement

• US develops Internet & runs DNS until ‘16
• Internet Engineering Task Force (IETF), premier standards body, created in US in 1986
• In 1998 Russian Federation expresses concern to UN that cyberspace technologies could be destabilizing and affect security of nations.
• World Summit on Information Society (WSIS) (2003-5) launched by UN to develop cyberspace agenda, effort to build the information society
Current System for Managing Internet

• ICANN manages domain names
  – ICANN decides which suffixes allowed (i.e. .ru or .xxx)
  – Regional Internet Registries (RIRs) issues IP addresses to Registrars & numbers to autonomous systems.

• Computer emergency response teams (CERTs) monitor health of Internet, coordinate action

• Internet technology decided by open process
  – Through the IETF and W3C

• Anyone can contribute

Current System for Managing Internet

• Internet service providers (ISPs) and ASes* (private orgs.) provide service and route traffic
• ISPs connect together at exchange points (IXPs)
• Security of DNS and routing handled privately
• Individual governments legislate nationally
• Some intergovernmental coordination exists on cybercrime
• But, no organization is in charge of it all!

* AS = autonomous system
Internet Governance Today

- Internet governance not as controversial today as it was 2013.
- US Department of Commerce proposed to relinquish its control to ICANN in 2014.
- The transition occurred on October 1, 2016.
  - ICANN is now independent!
Is Cyber Conflict Possible?
Offense & Defense in Cyberspace

- US created CYBERCOM headed by 4-star general who also heads the National Security Agency

- Many other countries have “stood up” their own cyber commands.
Cyber Conflict

• Is cyber conflict possible?
  – What might be the nature of a conflict?
  – Could it lead to widespread loss of electricity?
  – Could it lead to kinetic warfare?

• Would it constitute an existential threat?
  – Bulletin of Atomic Scientists doomsday clock just moved from two minutes to 100 sec. to midnight
  – Cyber viewed as a threat multiplier
Snowden Controversy

- In 2013 Edward Snowden, a contract National Security Agency (NSA) employee began releasing* NSA secret documents.
- NYT and others urged amnesty
- Gen. Hayden & others call him traitor.
- What is your assessment of this incident?

* https://www.theguardian.com/us-news/the-nsa-files
Review

• Cyberspace presents many technical, policy and diplomatic questions.

• To address them we need to understand the
  – Technologies involved
  – Existing policies and agencies setting them
  – Determine what is at risk, and
  – Formulate new policies and get them adopted
  – Ask how to get governments to cooperate on this