Cybersecurity for Future Presidents

Lecture 14:
Cyberwarfare and Other Topics for Future Presidents

Any Questions?

- About previous lecture?
- About homework?
- About reading? (Cyber warfare)

My office hours:
Wed. afternoon, 12-3pm,
442 RH.

For next week: Study for the final!

Cybersecurity events from the past week of interest to future (or current) Presidents:

- Supreme Court approves changes to criminal procedures
  - allows judges to issue warrants to use remote access to search electronic storage media and seize or copy electronic information located within or outside their district if the location "has been concealed through technological means"
    - Civil liberties groups complain this makes it too easy for "law enforcement hacking" of anonymous computers, located anywhere
- IoT: Samsung SmartThings vulnerabilities surfaced by U of Michigan Students; Samsung responds
- Michigan legislators introduce draft law to criminalize auto hacking
- Claude Shannon 100th Birthday (April 30)
  - Founder of information theory
- Satoshi Nakamoto ← Craig Steven Wright(?)

What is Cyberwarfare?

Some Relevant examples:

Estonia DDOS, defacements 4/27/2007:

- Context: relocation of Soviet-built WWII memorial and grave markers from downtown Tallinn (national capital) to Tallinn Military Cemetary, seen as an insult by Russians and Russian Estonians
- Event: massive DDOS and defacements of Estonian websites, including Estonian parliament, banks, news portals, and political parties

Georgia DDOS, defacements, traffic re-routing, July-August 2008:

- Context: Russia/Georgia shooting war over South Ossetia province
- Event: DDOS and defacement attacks swamped and disabled websites of numerous South Ossetian, Georgian, Russian and Azerbaijani organizations. Also re-routing of Georgian Internet traffic through servers in Russia and Turkey

Stuxnet and Saudi Aramco

Stuxnet, 2007-2010

- Context: Concern that Iran trying to develop nuclear weapons
- Event: Complex malware attack targeting centrifuge controllers at Iranian nuclear facilities
- Focused on physical damage to specifically targeted facilities

Saudi Aramco, Aug 15, 2012

- Context: aftermath of Stuxnet and continuing Saudi/Iran tensions
- Event: Virus wiped 30,000 (!) hard drives in Saudi national oil company (Aramco). Restoration required purchasing replacement drives; 5 months to recover.
- "Cutting Sword of Justice" group claimed responsibility; widely thought that Iran was behind this; probably insider access

Ukraine Power Grid

Ukraine, Dec. 23, 2015

- Context: Tensions over Ukraine eastern provinces, Crimea annexation, and Russia/Ukraine/EU relations
- Event: well-planned attack used hijacked credentials to usurp control of portion of Ukraine power grid and issued commands opening breakers and taking 30 substations offline, blackout hit 230,000 people. Overwrote firmware at 16 substations, preventing remote recovery. Took out two UPS (Uninterruptible Power Supply) backups and launched coordinated attack against the phone system to prevent call-ins.

Law of Armed Conflict (LOAC)

Principles of Law Of Armed Conflict (LOAC)

- Distinction: engage only valid military targets; distinguish among lawful combatants, noncomatants, and unlawful combatants.
- Proportionality: loss of life and property damage incidental to attack must not be excessive in relation to military advantage gained
- Military Necessity: limit actions to those necessary to accomplish a legitimate military objective
- Unnecessary suffering: Prohibits weapons, materials, methods of warfare that cause superfluous injury or unnecessary suffering

In general, use of force / armed attack is justified only in self-defense

Espionage is not considered a use of force

Cyberattack vs. Cyberexploitation

Terms	Cyberattack	Cyberexploitation
Approach/Intent	Degrade, disrupt, deny, destroy attacked infrastructure and systems/networks	Conduct smallest intervention consistent with desired operations
Primary relevant domestic law	US Code Title 10 authorities	US Code Title 50 authorities
Operational Agency	US Cyber Command	NSA
Personnel	Warfighters	Intelligence Community

Complexities

- Both cyberexploitation and cyberattack generally require the same kind of access to computing resources
  - But they come under different authorities (U.S. CodeTitle 50 vs Title 10), which means different organizations are authorized to pursue them
- Indirect effects of cyberattacks are hard to anticipate
- Cyberattacks are complex to plan and execute
- Identity of the party behind a significant cyberattack can be concealed relatively easily (compared with kinetic attack)
  - Proxies, (like privateers)
- Cyberattacks are relatively inexpensive (and so may be open to non-state actors)
- Cyberweapons once used may be thrown back at you
- Cyberweapons once used may become useless (because holes can be closed)

Norms and Diplomacy

- Norm: agreed standard of behavior
  - What norms might we have for cyber attacks?
    - No attacks against critical infrastructure?
- Countries are talking, but there is a long way to go
- Tallinn Manual an initial attempt to document how international law applies to cyber warfare, produced by a NATO center for cyber defense
- Difficulties:
  - Cyber is relatively low cost; non-state actors are a factor
  - Deterrence is difficult when accountability is lacking
- But note that in nuclear world, better defense was de-stabilizing (because the country might be able to survive a nuclear exchange, hence more willing to start one)
- While in cyber world, better defense could be stabilizing – attacks are less likely to be effective, making investment in them less productive

Cyberwarfare issues for the future President

- Defense: how do we protect ourselves from cyber attacks?
  - Protecting military systems isn't sufficient
  - Protecting critical infrastructures involves cooperation with private sector
  - How to create the incentives for private sector to create a resilient/defensible infrastructures?
- Offense:
  - What weapons do we need?
  - How can we be sure they will work?
  - How do we limit collateral damage?
  - How do we decide when to use them?

On the Horizon

1. Continuing declines in cost of computation, storage, and communication
2. Practical private information retrieval
3. Homomorphic encryption
4. Quantum key distribution
5. Quantum computing (quite different from #1 and still pretty far off)

Quantum Key Distribution

- Conveying the key securely (without it's being overhead or copied somehow by an eavesdropper) between two parties has always been a critical difficulty in the use of encryption
- It's the reason we don't generally use one-time pads
- It's the reason public key cryptography is interesting and useful
- But **what if the act of copying the key actually perturbed it**, so the receiver could detect whether the key had been copied or not?
  - Sort of like a tamper-evident seal on a box
  - You can't keep the intruder out, but you can tell of the box has been opened
- That's the idea behind quantum key distribution and quantum communications generally
- Single photons, polarized in different directions, are sent over a channel
- The communications channel is generally either free space or an optical fiber.
- There are commercial companies marketing this technology, e.g. MagiQ

Quantum Computing

- Quantum computing
  - Superposition and Entanglement properties
  - Qubits vs. conventional bits
  - In some respects, akin to old analog computers
- People have been working on building these machines since late 1990's
- Main source of interest today: ability to factor large numbers quickly, which would break RSA
  - However, people aware of this possibility have been working on quantum-resistant crypto for quite some time
- Some machines on the market now, but some controversy about these as well
- Might see it in my lifetime. Good program for physics research

Questions that I think a future President should be able to answer (and that I hope you can answer!)

- What are computing and communication about?
  - How do we model computers and what are the limits of what they can do?
  - How do we model communication and what are the limits to communication?
  - How do computing/communication networks function?
- What is cybersecurity about?
  - What are we trying to protect and from what kinds of threats?
  - How do we model/think about cybersecurity in systems?

Questions - 2

- How do cyberattacks work?
  - Attacking through inputs, side channels, supply chain, humans
- What is cryptography and how can it help?
  - Symmetric and asymmetric cryptography
  - Cryptographic hashes, digital signatures, certificates
  - How cryptography can support anonymous communication (TOR)

Questions - 3

- How can humans be associated with actions taken by computers?
  - Accountability through
    - Cryptography
    - Access controls
    - Forensics
- How has public policy (treaties, laws, regulations) developed in areas of concern for future leaders, such as:
  - Surveillance, legal access to communications and stored data
  - Use of computing technology in elections
  - Privacy in relation to online searching
  - Security and privacy of long-lived data such as genetic data
  - Digital currencies
  - Cyber warfare

Questions - 4

How have policy and economic incentives/disincentives affected cybersecurity?

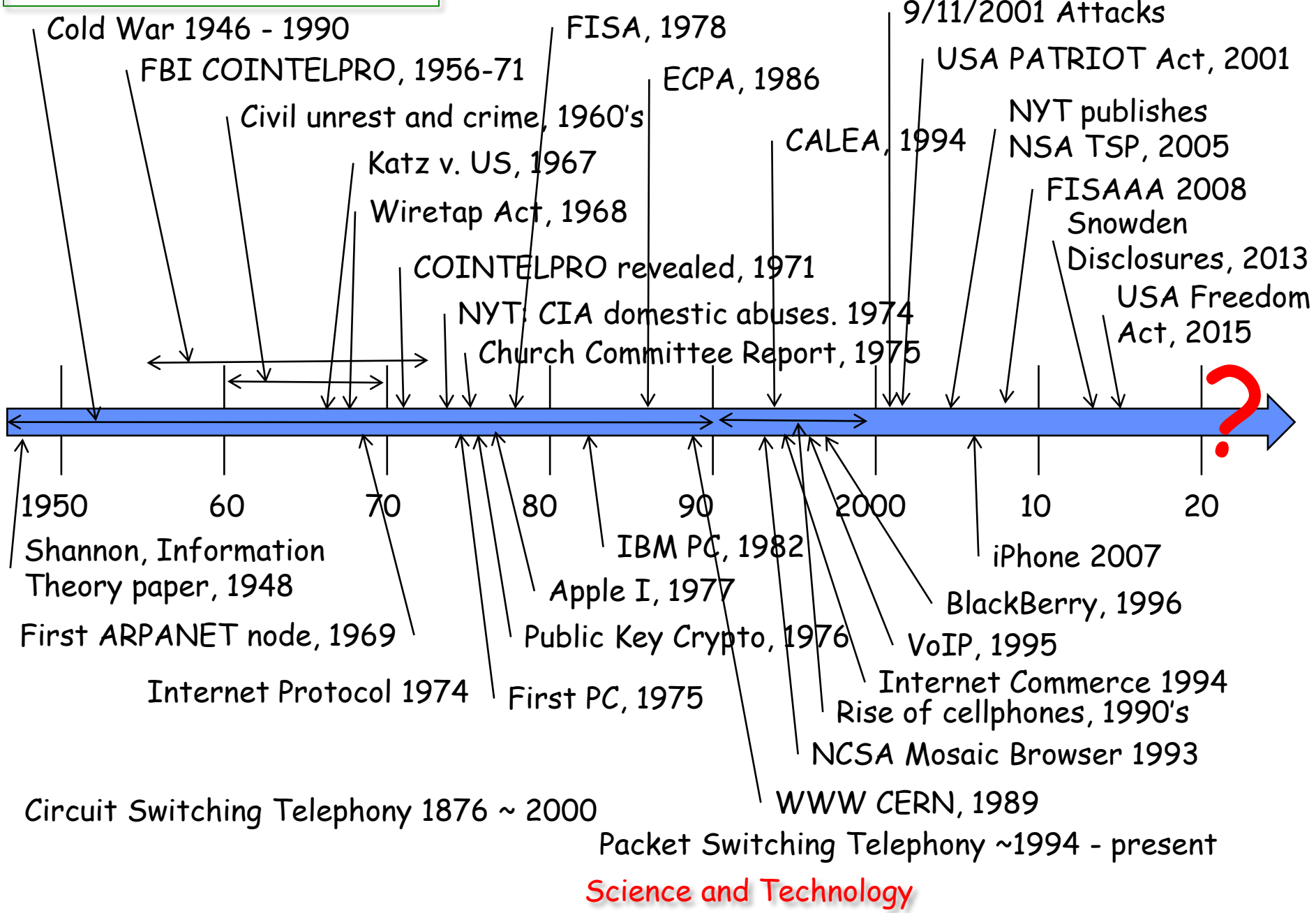
- Cost (time and resources) to build security in
- Difficulty of assessing/measuring security of a product
- Lack of liability for developers

Finally,

What are the right questions for a future leader to ask when presented with decision alternatives relating to cybersecurity?

- Technology matters, but so do
  - Economic effects
  - Social/Behavioral effects
  - International effects

What's Next?


Public Events and Legislation
Cold War 1946 - 1990
FBI COINTELPRO, 1956-71
Civil unrest and crime, 1960's
Katz v. US, 1967
Wiretap Act, 1968
COINTELPRO revealed, 1971
NYT: CIA domestic abuses. 1974
Church Committee Report, 1975
FISA, 1978
ECPA, 1986
CALEA, 1994
9/11/2001 Attacks
USA PATRIOT Act, 2001
NYT publishes NSA TSP, 2005
FISAAA 2008
Snowden Disclosures, 2013
USA Freedom Act, 2015
?
1950
60
70
80
90
2000
10
20
Shannon, Information Theory paper, 1948
First ARPANET node, 1969
Internet Protocol 1974
First PC, 1975
Public Key Crypto, 1976
Apple I, 1977
IBM PC, 1982
WWW CERN, 1989
NCSA Mosaic Browser 1993
Rise of cellphones, 1990's
Internet Commerce 1994
VoIP, 1995
BlackBerry, 1996
iPhone 2007
Circuit Switching Telephony 1876 ~ 2000
Packet Switching Telephony ~1994 - present
Science and Technology

And now your questions…

- How to secure particular technologies (or will they ever be secure?
  - Cellphones
  - Encryption
- How to secure particular information or systems generally
- Future of digital currency
- Future of cyberwarfare
- Future of cybersecurity generally
- Future of technology and society

Thank you!
You are a great class!
Be well, work hard, do great things!

- This course may be reincarnated.
- Please take seriously the course feedback forms
- Also feel free to send emails to me directly if you don't mind revealing your identity
  - What worked well?
  - What didn't work as well?
  - What was missing?