Day 12

Hacking
CFAA
Aaron Swartz
Responsible disclosure
Hacking

- Intentional, unauthorized access to computer systems
- Phase 1: The joy of programming
  - Early 1960s to 1970s: positive term
  - A "hacker" was a creative programmer who wrote elegant or clever code
  - A "hack" was an especially clever piece of code
Phase 2: 1970s to mid 1990s

- Hacking took on negative connotations
- Breaking into computers for which the hacker does not have authorized access
- Still primarily individuals
- Companies began using hackers to analyze and improve security
Phase 3: The growth of the Web and mobile devices

- Beginning in mid 1990s
- The growth of the Web changed hacking; viruses and worms could be spread rapidly
- Political hacking (Hacktivism) surfaced
- Denial-of-service (DoS) attacks used to shut down Web sites
- Large scale theft of personal and financial information

![Chart showing the biggest risks to the broader economy](chart.png)

**What financial companies think are the biggest risks to the broader economy**

1. **Cyber risk** 78%
2. Geopolitical risk 69%
3. Impact of new regulations 45%
4. Britain's exit from the E.U. 38%
5. U.S. Federal Reserve monetary policy 25%
6. Sudden dislocation in financial markets 25%
7. Interconnectedness risk 24%
8. Significant business continuity event 19%
9. Funding liquidity 18%
10. Major compliance / governance event 18%

Percentage of respondents in a survey of financial service companies to identify the top five systemic risks to the broader economy, looking ahead into 2018 and beyond | Source: Depository Trust and Clearing Corporation
Is there such a thing as “harmless” hacking?

- Responding to non-malicious or prank hacking uses resources.
- Hackers could accidentally do significant damage.
- Almost all hacking is a form of trespass.
Use of hacking to promote a political cause

Disagreement about whether it is a form of civil disobedience and how (whether) it should be punished

Some use the appearance of hacktivism to hide other criminal activities

Hacktivism or simple vandalism?

Is hactivism the only option?

Anonymous vs. BART
Colorful Hacking Hats

White hat – RESPONSIBLE DISCLOSURE

Process of reporting security vulnerabilities to someone who can fix them rather than sharing or profiting from them

Black hat

Gray hat
Pentagon has announced it would consider and treat some cyber attacks as acts of war, and the U.S. might respond with military force.

The more we depend on tech, the more crucial protection becomes.

http://newyork.cbslocal.com/2017/03/01/electrical-grid-hacking-attack/
Hackers could have opened the flood gates on a dam in New York in 2013, but the gates were offline for maintenance.

Another hacker was in the process of trying to poison the water supply in a Florida town in February when a worker noticed and stopped it.

Rather than risk a spill or other pipeline disaster after a ransomware attack last month, operators of an East Coast pipeline shut it down, leaving millions waiting in long fuel lines.

Such close calls are ratcheting up fears about how vulnerable the nation’s infrastructure is to cyberattacks. Experts say there are more to come and the attacks could be far more devastating than anything seen so far unless the United States girds its critical systems against a growing onslaught of digital intrusion.
Hacking as foreign policy

Cyber Firm: The NSA Is Out-Hacking the Chinese and the Russians

Cybercom to Elevate to Combatant Command

May 3, 2018
News
By Lisa Ferdinando

https://www.defense.gov/News/Article/Article/1511959/cybercom-to-elevate-to-combatant-command/
Beginning in 2008, damaged equipment in a uranium enrichment plant in Iran
Exclusive: U.S. tried Stuxnet-style campaign against North Korea but failed - sources
Who is responsible for security?

- **Developers** have a responsibility to develop with security as a goal.
- **Businesses** have a responsibility to use security tools and monitor their systems to prevent attacks from succeeding.
- **Home users** have a responsibility to ask questions and educate themselves on the tools to maintain security (personal firewalls, anti-virus and anti-spyware).
Laws against Hacking

1984:

**COMPUTER FRAUD AND ABUSE ACT (CFAA)**

- Includes government computers, financial and medical systems, and activities that involve computers in more than one state, including all computers connected to the Internet.

- Under CFAA, it **is illegal to access a computer without authorization**.

- Cost < $5k = misdemeanor, >$5k = felony.

- The USA PATRIOT Act expanded the definition of loss to include the cost of responding to an attack, assessing damage and restoring systems.

Textbook p244
Catching Hackers

- Law enforcement agents read hacker newsletters and participate in chat rooms undercover.
- They can often track a handle by looking through newsgroup or other archives.
- Security professionals set up ‘honey pots’ which are Web sites that attract hackers, to record and study.
- Computer forensics specialists can retrieve evidence from computers, even if the user has deleted files and erased the disks.
- Investigators trace viruses and hacking attacks by using ISP records, router logs and MAC addresses.
Young hackers

- Many young hackers have matured and gone on to productive and responsible careers.
- Sentencing depends on intent and damage done.
- Most young hackers receive probation, community service, and/or fines.
- Not until 2000 did a young hacker receive time in juvenile detention.
CFAA: update needed?

- The CFAA predates social networks, smartphones, and sophisticated invisible information gathering.
- Some prosecutors use the CFAA to bring charges against people or businesses that do unauthorized data collection.
- Is violating terms of agreement a form of hacking?

Normally, a breach of contract is not a criminal offense. But under CFAA, breaking Facebook’s terms of service could be classed as a criminal act, as could checking personal email on a work computer.

http://www.dmlp.org/threats/united-states-v-drew
US v. Lori Drew

Photos: AP/Nick Ut and Tina Meier, 2006
Los Angeles — In a highly unusual use of a federal law generally employed in computer fraud cases, a federal grand jury here on Thursday indicted a Missouri woman accused of using a phony online identity to trick and taunt a 13-year-old girl, who committed suicide in response to the cyberbaiting.

Summary

**Threat Type:** Criminal Charge  
**Status:** Concluded  
**Date:** 05/15/2008  
**Disposition:** Dismissed (total)  
Verdict (plaintiff)  
**Location:** California  
**Legal Claims:** Computer Fraud and Abuse Act  
**Verdict or Settlement Amount:** N/A

On May 15, 2008, Lori Drew was indicted in federal court in California for her alleged role in a hoax on MySpace directed at Megan Meier, a 13-year-old neighbor of Drew's who committed suicide in October 2006 after a "boy" she met... [read full description]
“The court ruled back in 2012 that merely violating a website’s terms of use is not a crime under the federal computer crime statute, the Computer Fraud and Abuse Act. But some companies, like Oracle, turned to state computer crime statutes—in this case, California and Nevada—to enforce their computer use preferences.”
http://www.slate.com/articles/technology/technology/2013/02/aaron_swartz_he_wanted_to_save_the_world_why_couldn_t_he_save_himself.html

https://www.youtube.com/watch?v=eFGa9sGKqpE
Aaron's Law

Purpose:
- to clear up the vagueness of current legislation, define “exceeds authorization.”
- To bring “proportionality” to sentences

Large companies are advocating against it (source).

Forbes:

Aaron's Law Is Doomed Leaving US Hacking Law 'Broken'

Did not pass:

Private interests are also holding up discussions around the CFAA. Various companies are known to have lobbied on Capitol Hill in an attempt to block change. Business software maker Oracle has been busy trying to influence lawmakers. As its publicly available lobbying disclosures note, the company spent vast sums in 2013 on fighting Aaron's Law. Oracle said it had no comment.

https://www.govtrack.us/congress/bills/114/hr1918