Day 12

Hacking
CFAA
Aaron Swartz
Responsible disclosure

Hacktivism
BART
Stuxnet
US v Lori Drew
Hacking

0 Intentional, unauthorized access to computer systems
0 Phase 1: The joy of programming
  0 Early 1960s to 1970s: positive term
  0 A "hacker" was a creative programmer who wrote elegant or clever code
  0 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
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

0 White hat – RESPONSIBLE DISCLOSURE
0 Black hat
0 Gray hat
Defending against hacking

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

http://newyork.cbslocal.com/2017/03/01/electrical-grid-hacking-attack/
Defending against hacking

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

Hacking robots: Why it could be a lot easier than it should be

Security researchers say they have found a number of security flaws across a range of robots.

By Danny Palmer | March 1, 2017 -- 15:11 GMT (07:11 PST) | Topic: Security

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

https://vimeo.com/25118844
Exclusive: U.S. tried Stuxnet-style campaign against North Korea but failed - sources
Sony Pictures hack
2014
Well, you can't keep a good thing covered up forever! Rent it today for $5.99 (also support freedom of art expression)

The Interview
youtube.com
Security

0 Security is often playing catch-up to hackers as new vulnerabilities are discovered and exploited.

0 Defending systems from hackers is now an in-demand career path
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

0 Many young hackers have matured and gone on to productive and responsible careers.
0 Sentencing depends on intent and damage done.
0 Most young hackers receive probation, community service, and/or fines.
0 Not until 2000 did a young hacker receive time in juvenile detention.
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.
US v. Lori Drew

Photos: AP/Nick Ut and Tina Meier, 2008
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.
9/2013 Aaron Swartz

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

Prosecutors cited the CFAA to charge Aaron Swartz with a felony when he began downloading JSTOR articles using MIT access.

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'

As of 10/2018:
https://www.govtrack.us/congress/bills/114/hr1918