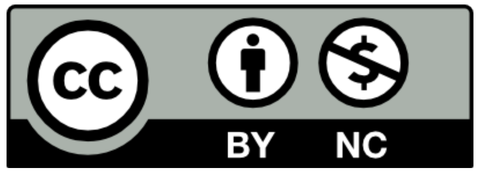
Computer Security and Ethics

Steven M. Bellovin

https://www.cs.columbia.edu/~smb



CS@CU

Teaching Hacking

- Is it ethical to teaching hacking skills in a university?
- Does this teach necessary skills for defenders?
- Does it teach skills only necessary for attackers?
- Should such courses have an ethics unit?

Is Hacking Bad?

From Cliff Stoll's "The Cuckoo's Egg":

- Not new: "'So what? Somebody's always had control over information, and others have always tried to steal it. Read Machiavelli. As technology changes, sneakiness finds new expressions.'"
- "'A computer system isn't private like a house,' Laurie responded. 'Lots of people use it for many purposes. Just because this guy doesn't have official permission to use it doesn't necessarily mean he has no legitimate purpose in being there.'"
- 'Whenever a fun-loving student breaks into systems as a game (as I might once have done), and forgets that he's invading people's privacy, endangering data that others have sweated over, sowing distrust and paranoia.'

CS @CU

Hack-Back

- By whom? Governments? Victims? Vendors? Vigilantes?
- What is an acceptable goal?
  - Botnet takeover for neutralization?
  - Disinfect machines?
  - Gather evidence?
  - Deter attackers?
- What if attribution isn't certain? What if innocent victims' computers are used to launch the attack?

Cyber Weapons/Lawful Hacking Software

- Is it ethical to work on such tools?
- Are such weapons “inherently indiscriminate”, which would make them illegal according to the Laws of War?
  - What about “preparing the battlefield”?
- Is lawful hacking software too easily abused by authoritarian governments?

Hacktivism

Rob Joyce, NSA Cybersecurity Director

> However, when an individual in Europe or the U.S. “decides that they are going to take on hacktivist activities on behalf of Ukraine — I think that's over the line.”
>
> “It's an inherently government activity. It impacts our ability to set and enforce norms. And it also adds to the noise,” Joyce explained. “There's a lot of nation state activity being cloaked in the guise of activists. When we add that ambiguity we're giving cover and allowing Russia to do things that they can point to … out into the misinformation disinformation space.”

(https://therecord.media/russia-ransomware-attacks-logistics-supply-chain-ukraine)

Vulnerability Disclosure

- Should researchers disclose vulnerabilities publicly? Should they wait a few months, to let patches be developed and deployed?
- Does it help defenders look for indications of compromise?
- Or does it teach attackers what to do?
- Should “bug bounty” programs, where vendors reward researchers who find holes, include non-disclosure agreements (NDAs)?

Monitoring

- Is it proper to monitor other people's Internet traffic and computer use to see if they've been hacked?
  - What about just the metadata and not the content?
- Who should be allowed to do this? Governments? ISPs? Employers? Software vendors?
- If consent is sought, would it really be voluntary?

Questions?

(Mandarin duck, Central Park, January 11, 2019)

CS@CU