Hacking

Alex Voitik and Chris Little

White vs Black Hat

Black hat hackers aim to compromise the security of a computer system for personal gain.

White hat hackers are “ethical hackers,” they are experts in compromising computer security systems who use their abilities for good, ethical, and legal purposes.

One of the First Hackers

Kevin Mitnick

Always saw technology as a challenge, he tried to gain access to sensitive materials just to see if he could.

Learned the ins and the outs of how the phone companies worked in order to play pranks on friends and to make long-distance phone calls for free.

Fell into trouble when he tried using his talents to gain information from deep within the Pacific Bell Company.

No laws were in place yet for the crimes he was committing, so they drafted laws in order to incarcerate him.

Criminal?

After his sentence was over, he started Mitnick Security Consulting, LLC, which specializes in white hat hacking.

He never sold what he found, and he used tools at his disposal in order to access the information.

Was Kevin Really Wrong?

- He was doing things that he had the legal power to use, like his own phone and his own personal computer.
- In reality, he only pushed buttons in a certain way that basically anybody could
- What ethical issues are shown in his story?

Kevin’s Style

Social Engineering

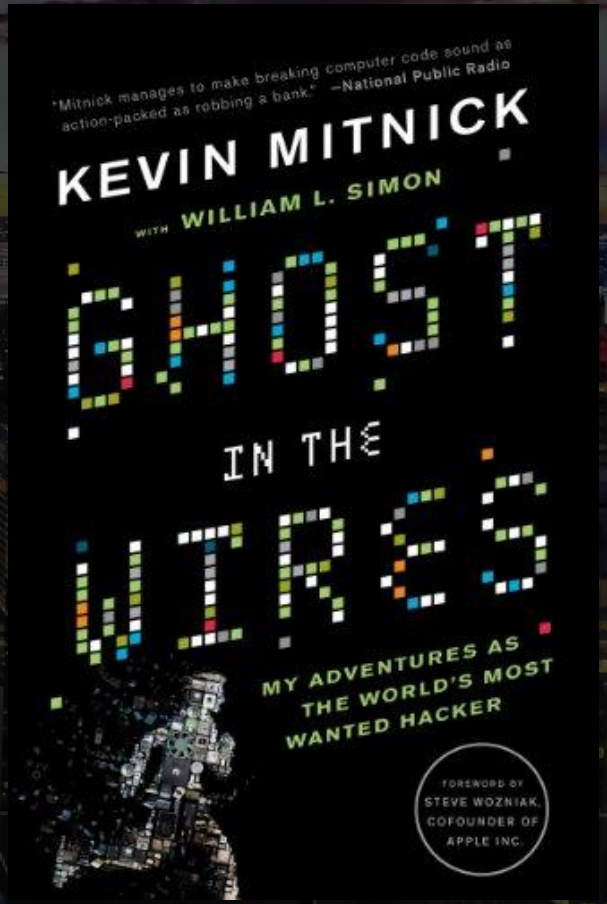
Kevin used social engineering in many of his exploits. Social engineering is the psychological manipulation and reading of social cues in order to influence situations.

What ethical issues can arise from using this form of “real-life” hacking?

Black to White:

Now Kevin uses his abilities to see exploits in systems to show companies where the vulnerabilities are.

Is this really different from what he was doing before? He is still seeing the sensitive information, and he is still breaking the systems using a mixture of hardware as well as social engineering.



Laws on Hacking

The Computer Fraud and Abuse Act

What is a “protected computer”? How is it different from a normal computer?

18 U.S. Code § 1030 (a) (2) - Fraud and related activity in connection with computers

(a) Whoever—

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) [1] of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer;

The Computer Fraud and Abuse Act

18 U.S. Code § 1030 (e) - Fraud and related activity in connection with computers

(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term "protected computer" means a computer—

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;

Government & Hacking

Patriot Act section 217

“section 217 also makes the law technology-neutral. Section 217 places cyber-trespassers--those who are breaking into computers--on the same footing as physical intruders. Section 217 allows the victims of computer-hacking crimes voluntarily to request law enforcement assistance in monitoring trespassers on their computers... hacking victims can now allow law enforcement officers into their computers to catch cyber-intruders...This, in essence, is what was occurring prior to the PATRIOT Act.”

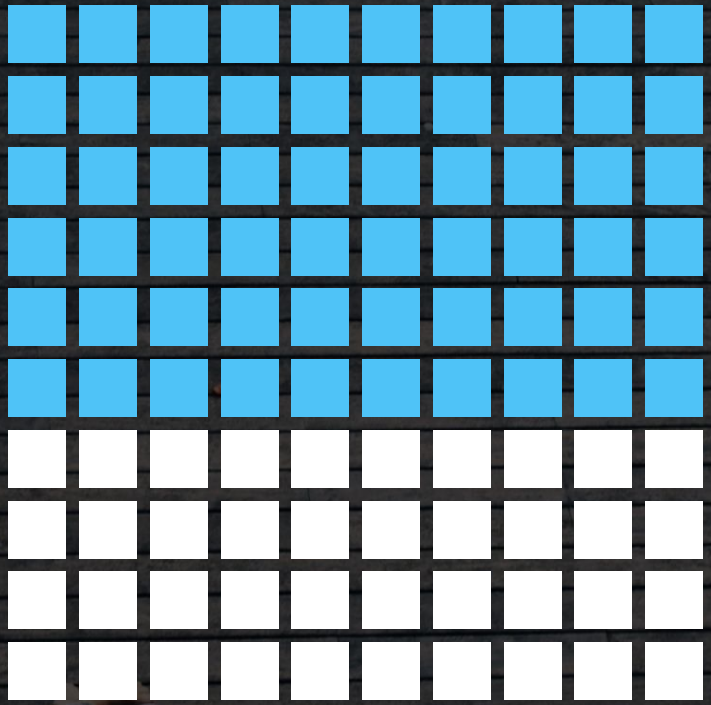
“It can be said that section 217, in a very significant way, enhances privacy. First, it is carefully crafted to ensure that law enforcement conducts monitoring against trespassers in a manner entirely consistent with protecting the privacy rights of law abiding citizens. Second, the essence of the section-- o help catch hackers--serves a vital function in the FBI's ability to enforce data privacy laws.”

https://archives.fbi.gov/archives/news/testimony/computer-provisions-of-the-usa-patriot-act

Case Study

A hacker finds a flaw in the security of a major credit card company. He sends a list of credit cards to the company.

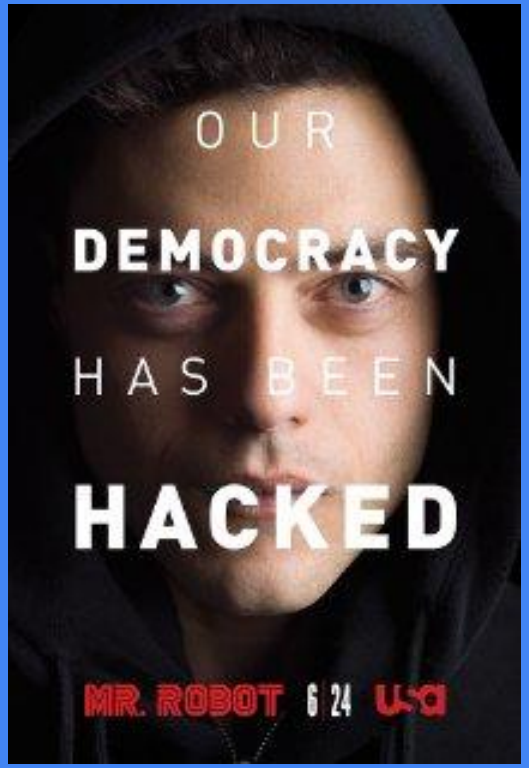
A college student searches “how to hack” on google for a project. The NSA records the IP Address



Other Examples?

Hacking is very popular in the media, can you name some examples of recent stories?

What are the ethical issues that arise from these stories?



Sources:

https://en.wikipedia.org/wiki/Kevin_Mitnick
https://www.law.cornell.edu/uscode/text/18/1030
https://archives.fbi.gov/archives/news/testimony/computer-provisions-of-the-usa-patriot-act
http://www.howtogeek.com/157460/hacker-hat-colors-explained-black-hats-white-hats-and-gray-hats/

Images from Google images