Ethical Hacking

CS103f: Ethical Foundations of Computer Science

April 9, 2019

When is Hacking Ethical?

Hacking to Raise Awareness

- Security companies and academics often use hacking/penetration testing as a way to find (and eliminate) security flaws in a system
- Identifies flaws in open source (and closed source) software
  - Apache security holes
  - OS vulnerabilities
- Identifies flaws in critical systems
  - Bluetooth exploits in cars
  - Exploits in voting machines

Hacking to Punish ”the Bad Guys”

- Consider the case of Ashley Madison. Given that it affected only people committing adultery, was breaking into their system and stealing user data okay?

A) Yes

B) No

Things to Consider…

- Is your hacking intended to help people?
- Is your hacking intended to reveal something people need to know?
- Who will be hurt by your hacking?
- What are you gaining from this hacking?

What about the Legality?

Hactivism Legality

- Case of Aaron Swartz and JSTOR
  - Swartz wrote a script to download JSTOR research papers in bulk on the MIT network with intent to reproduce them on an open access site
  - JSTOR has a EULA that forbids using scripts to download hosted documents
  - Federal District Court charged Swartz under the Computer Fraud and Abuse Act (CFAA) for violating the JSTOR EULA
  - Trial never brought to court as Swartz committed suicide
    - Charges being dropped
    - Open access laws introduced but not yet voted on

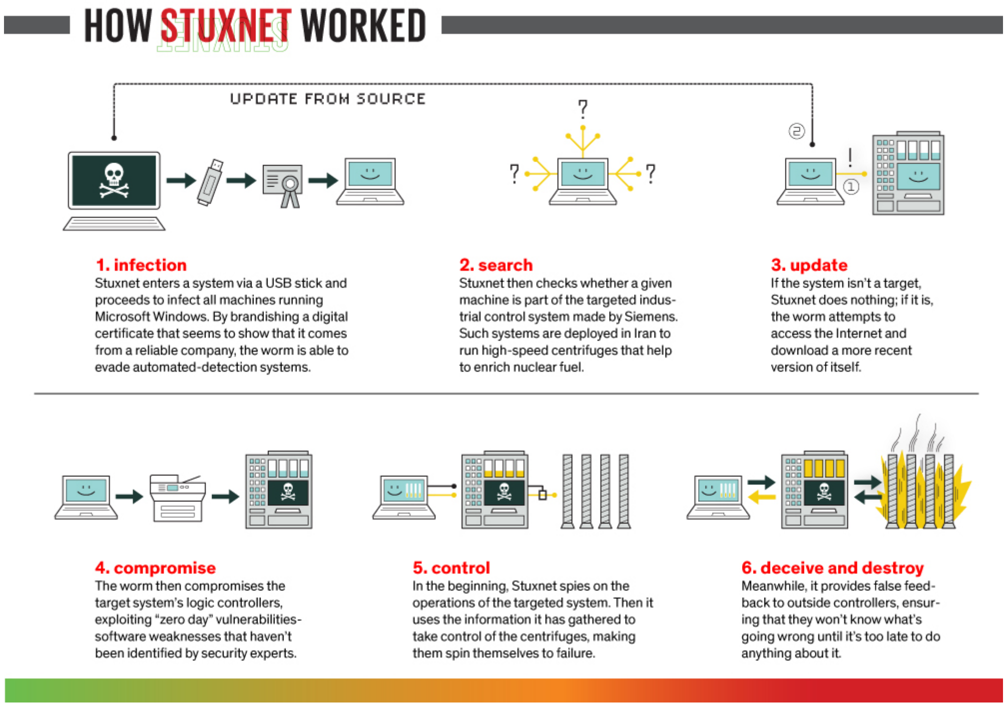
Hactivism Legality

- Case of Edward Snowden and the NSA
    - Snowden was an NSA contractor
    - Fled to Hong Kong with leaked information on the NSA’s Prism program
        - Program spying on both US and UK citizens
        - Program spying on nations including China, Germany, Brazil, and Mexico
    - Snowden charged with theft of government property and violation of the Espionage Act of 1917
    - Currently in exile in Russia

What about the Government?

- When should a state be able to using technology/hacking against other sovereign nations?

Case Study: Stuxnet



HOW STUXNET WORKED

1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

References

- https://users.cs.duke.edu/~chase/cps49s/carnivore-history.html
- https://www.theguardian.com/technology/2013/jun/02/aaron-swartz-hacker-genius-martyr-girlfriend-interview
- https://www.bbc.com/news/world-us-canada-23123964