Ethical Hacking

Hackers are (or could be) actually good, pleasant and extremely intelligent people who could keep computer criminals on the run.
Ankit Fadia

Professionalism - Classroom

- Attendance
- Participation in class
- Respect of others
- Timeliness
- Quality of work
- Constructive use of Lab time.
- Secondary:
  - Setting of priorities
  - Time management

Ethics

- Difficult, sometimes impossible choices
- Some say not natural, but learned
  - Nietzsche, Ayn Rand
  - Used to suppress the commoner
- Conscience choice on your part
- You will learn things in this class that will tempt you

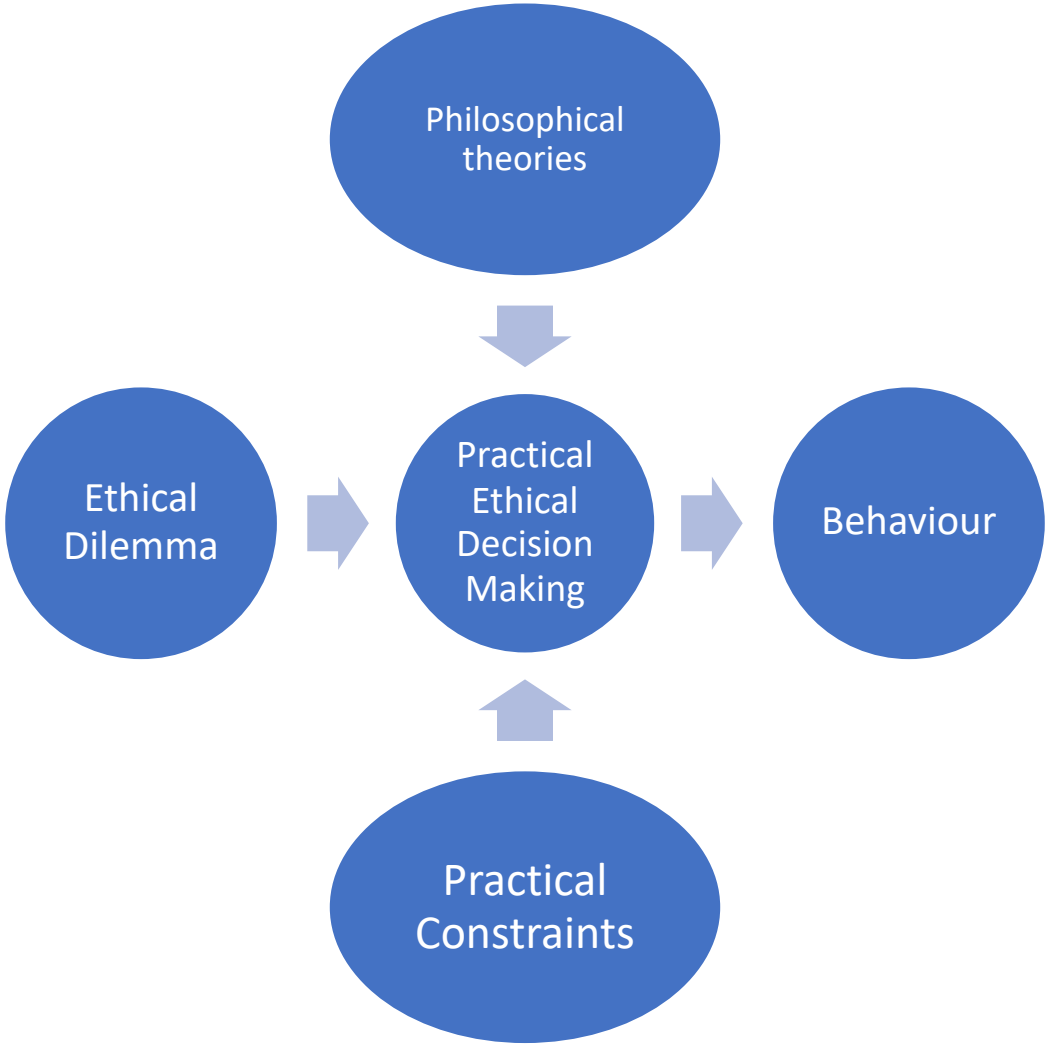
Code of Conduct vs Ethics

- Code of Conduct
  - Imposed by others
  - What must/must not be done
  - Rules
- Code of Ethics
  - Self imposed
  - Who we are/What we stand for
  - Guidelines or guiding principals

Kaler's Gradations

- Kaler's Gradations of Self-Interest and Morality – where is what you are doing falling on this?
  - Ultra Moral (self-sacrificial altruism)
  - Extraordinarily Moral (altruism without self-sacrifice
  - Ordinarily Moral (equal self-interest to others)
  - Quasi-moral (disproportionate but not dominant self-interest
    - Dividing line between moral and self-interest
  - Quasi-egoism (self interest dominant but not total)
  - Egoism (total self interested)

Ethical Reasoning Process



Example from Twitter

- It is sometimes OK to say “no”, as this quote from Twitter says:
- Jamie Kyle (@buildsghost)
- Normalize telling your company “I’m not building that” I did it my third week at Discord over a privacy concern and they just went “Yeah okay, we can go without it” and that was the end of it
- Posted 11:56 AM · Sep 29, 2020
- The Only Thing Necessary for the Triumph of Evil is that Good Men (sic) Do Nothing

Difference between hacker and cracker

- Traditional vs. current definitions of hackers

The definition of ethical hacking (SecuritySearch, 2006) is “a computer or network expert who attacks a system on behalf of its owners, seeking vulnerabilities that a malicious hacker can exploit”. Ethical hacking is one of the growing areas of ethics and Information Security. The term “ethical hacker” has become popularized by corporations hiring security professionals to test their systems for vulnerabilities and describing these individuals as “ethical hackers”.

White Hat Hacking

- White hat, black hat, and gray hat hackers
- White Hat;
  - For good, fun, security, learning
- Black Hat;
  - Malicious intent
  - Organized crime
- Gray Hat
  - Morality most often the difference

Wikipedia example of White Hat hacking

- An example hack could be with Microsoft Windows and its ability to use cryptographic libraries built into the operating system. When shipped overseas this feature becomes nearly useless as the operating system will refuse to load cryptographic libraries that haven't been signed by Microsoft, and Microsoft will not sign a library unless the U.S. government authorizes it for export. This allows the U.S. government to maintain some perceived level of control over the use of strong cryptography beyond its borders.
- While hunting through the symbol table of a beta release of Windows, a couple of overseas hackers managed to find a second signing key in the Microsoft binaries. That is, without disabling the libraries that are included with Windows (even overseas), these individuals learned of a way to trick the operating system into loading a library that hadn't been signed by Microsoft, thus enabling the functionality which had been lost to non-U.S. users.
- Whether this is good or bad may depend on whether one respects the letter of the law, but is considered by some in the computing community to be a white hat type of activity.

MIT hacker ethic

- be safe
- do not damage anything
- be funny, at least to most of the people who experience it
- not damage anyone, either physically, mentally, financially, or emotionally

Rotary's Guiding Principles

- Business self test for betterment of communities, but relevant
- Four way test
- Of the things we think, say, or do
    1. Is it the TRUTH?
    2. Is it FAIR to all concerned?
    3. Will it build GOODWILL and BETTER FRIENDSHIP
    4. Will it be BENEFICIAL to all concerned?

Legal Consequences

- Some of the skills from WebSec can be criminally misused.
- Crimes can be broken into 3 broad categories
  - Computer as a tool – hacking activities
  - Computers as target of the crime – viruses, identity theft, hacked
  - Computers incidental to the crime – servers and infrastructure used for hate speech/ threats against political leaders

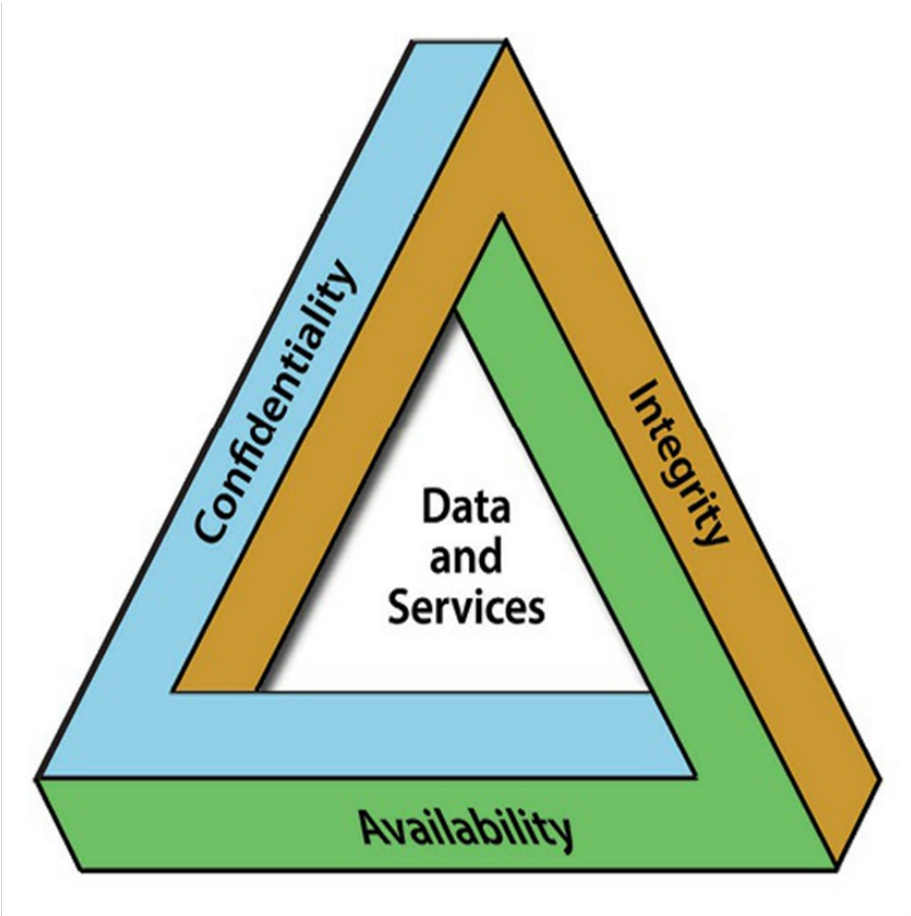
CIA

- **Confidentiality** supports the principle of “least privilege” by preventing unauthorized disclosure of information to those who(people, systems) do not have the need (need-to-know), or right, to access it. An important measure that the security architect should use to ensure confidentiality of information is data classification. Control Example(s): Encryption

- **Integrity** refers to efforts made to prevent unauthorized or improper modification of systems and information. It also refers to the amount of trust that can be placed in a system and the accuracy of information within that system. Control Example(s): segregation of duties, approval checkpoints

- **Availability** refers to efforts made to prevent service disruption and/or productivity. Control Example(s): up-to-date and active anti-malicious code detection system, incident management plans, disaster recovery planning.

CIA Triangle



Data Breaches

- **Incident** – A security event that compromises the integrity, confidentiality, or availability of an information asset.
- **Breach** – An incident that results in the disclosure or potential exposure of data.
- **Data Disclosure** – A breach for which it was confirmed that data was actually disclosed (not just exposed) to an unauthorized party.

Social Media

- Many companies that are hiring often look at social media activities, especially of technology hires
  - Don’t share what you are doing – shows recklessness
  - Don’t contribute to group attacks similar to the ones in support of Julian Assange

Certification

- From many venders
- EC-Council – 4 levels
- SANS
- Computer Ethics Institute (CEI)
- National Conference on Computing and Values
- The Working Group on Computer Ethics
- National Computer Ethics and Responsibilities Campaign (NCERC)

Steps to Hacking a System

- Search for vulnerable systems/components
  - Track security bulletins for operating systems et al
- Execute code to get a list of usernames and/or encrypted passwords
- Run hacking tools to decrypt password list

- May be augmented with social engineering (human vulnerability)

Some steps to stop hackers

- Double encryption of passwords
  - update users set password = md5(md5($password),$secretvar);
- Prevent root access at every opportunity
- Push less sensitive data to web servers, rather than all data
  - Data not on a web server or a web accessible server cannot be compromised
- Keep systems up to date with respect to security bulletins
- Continually review access and error logs

To stop a thief, you must think like a thief.