Cybersecurity Ethics

This research is supported by Award #1542465: RET Site: Cyber Security Initiative for Nevada Teachers (CSINT)

Our Ethical Code…

Q: Do you have an "ethical code"?

Q: Where does this ethical approach come from?

Q: How do you think most people decide what is ethical and what is not ethical?

Q: How important is this…should we worry about it?

Q: How do you teach the principle of ethics to students in your classroom?

A Definition

eth·ics

ˈeTHiks/

noun

- moral principles that govern a person's behavior or the conducting of an activity.
  i.e. "medical ethics also enter into the question“

- the branch of knowledge that deals with moral principles
  (philosophy)

synonyms: moral code, morals, morality, values, rights and wrongs, principles, ideals, standards (of behavior), value system, virtues, dictates of conscience "your so-called newspaper is clearly not burdened by a sense of ethics"

A Definition

vir·tue

ˈvərCHo͞o/

noun

1.1.

behavior showing high moral standards.

"paragons of virtue"

2.2.

(in traditional Christian angelology) the seventh highest order of the ninefold celestial hierarchy.

synonyms: goodness, virtuousness, righteousness, morality, integrity, dignity, rectitude, honor, decency, respectability, nobility, worthiness, purity; More

A Definition

mor·al

ˈmôrəl/

noun

plural noun: **morals**

1.1. a lesson, especially one concerning what is right or prudent, that can be derived from a story, a piece of information, or an experience.
"**the moral of this story** was that one must see the beauty in what one has"

2.2. a person's standards of behavior or beliefs concerning what is and is not acceptable for them to do.
"the corruption of public morals"

synonyms: moral code, code of ethics, (moral) values, principles, standards, (sense of) morality, scruples"he has no morals"

A Definition

Ethic – a principle

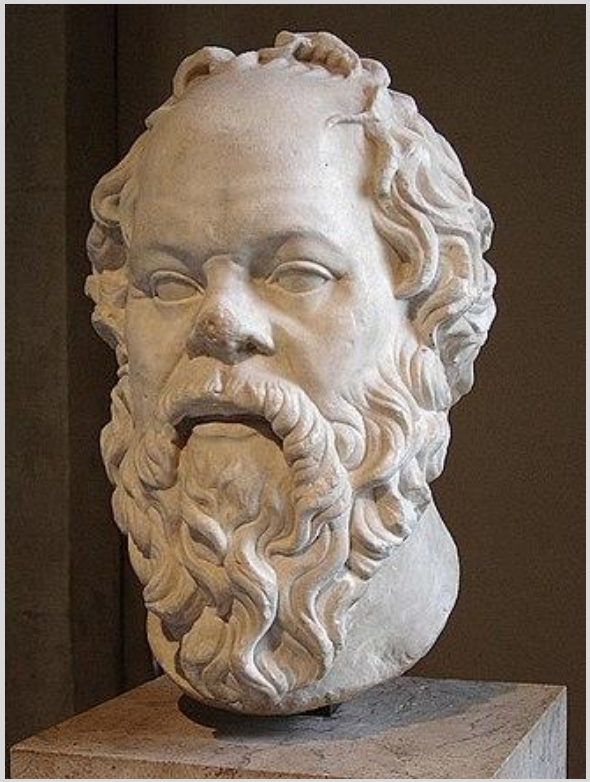
Virtue – an action

Moral – a belief

Key Thinkers on Ethics

Socrates

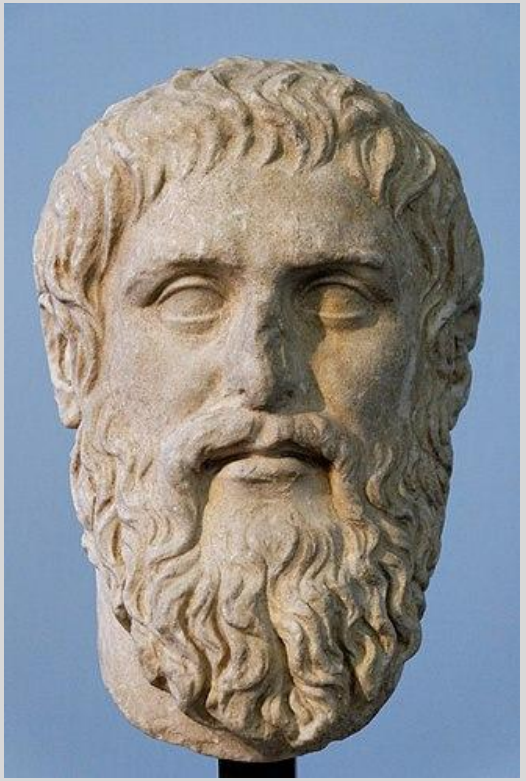
- **Virtue is key to living an ideal or “good” life**
- **Virtue is obtained by gaining knowledge**
- **Therefore, virtue can be taught and learned**
- **Knowledge (and virtue) should be sought before personal interests**
- **Knowledge is sought as a means to ethical action**



Key Thinkers on Ethics

Plato

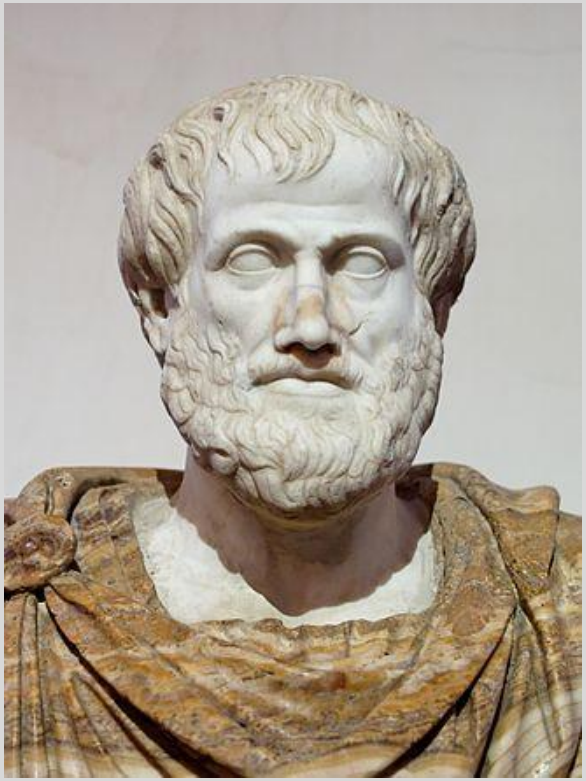
- **Central ethical question: "what sort of person should I be"**
- **Central goal of ethics: strive to be "good people"**
- **Purpose of ethics is self-interest, how to live the best life**
- **Humans are made up of a physical body and non-physical soul**
- **Physical body is unimportant; focus should be on the soul**
- **Soul had 3 parts; *Reason, Spirit, Appetite***
  - ***Reason: ability to pursue truth and knowledge (weakest part)***
  - ***Spirit: concerned with status, pursues fame and power***
  - ***Appetite: pursues pleasure and avoids pain (strongest part)***
- **Every object has a purpose**
- **Virtue helps an object achieve its purpose**
- **Justice is the virtue that allows the soul to govern the body**
  - ***Justice – proper balance among the parts of the soul***



Key Thinkers on Ethics

Aristotle

- ***The highest good and goal of human activity is the attainment of happiness***
- ***Happiness is the continuous contemplation of truth***
- ***This state is attained by living a virtuous life and the development of wisdom and the ability to reason***
- ***Moral virtue is found in a balance between excess and deficiency (never too much or too little)***
- ***No appetite is bad if controlled by reason and principle***
- ***Virtue is attained through knowledge, habituation, and self-discipline***
- ***Humans have moral responsibility for their actions***
- ***Virtuous acts require conscious choice and moral purpose***
- ***Moral virtue requires moral action in a social environment***



Key Thinkers on Ethics

Immanuel Kant

- ***Deontological (duty) ethics; the rightness or wrongness of actions does not depend on their consequences*** **but on whether they fulfill our duty**
- ***A person is good based on his motives, not on the outcome of his actions***
- ***One can have moral worth only if he is motivated by morality***
- ***Getting "lucky" does not make one "good", consequences do not matter***

Commonly Accepted Ethical Principles

- **Respect autonomy**
  - ***The individual has a right to act as a free agent***
- **Do no harm (non-maleficence)**
  - ***Our interactions with people should not cause harm***
- **Benefit others (beneficence)**
- **Be just (justice)**
- **Be faithful, true to your word (fidelity)**

Cybersecurity Ethics

"Ethics: The information systems and the security of information systems should be provided and used in such a manner that the rights and legitimate interests of others are respected."

-- NIST, Special Publication 800-14, 1996

"You can not promote the (true) idea that security research benefits humanity while defending research that endangered hundreds of innocents."

-- Alex Stamos, Former Yahoo CISO, Tweet 2015

Process

- *Laws*
- *Regulations*
- *Standards*
- *Policies*
- *Ethics*

Definitions

Hacker- An unauthorized user who attempts to or gains access to an information system.

Ethical Hacker- Hackers hired by an organization to penetrate networks and computer systems with the purpose of finding and fixing security vulnerabilities.

Hacktivist- The subversive use of computing systems to promote a political agenda, often related to free speech or freedom of information movements.

White Hat– An ethical hacker or security expert, who specializes in penetration testing to ensure the security of an organization's information systems.

Definitions

Black Hat- A hacker who "violates computer security for little reason beyond maliciousness or for personal gain". [Richard Stallman]

Grey Hat- Hackers who look for vulnerabilities in a system without permission. Will report flaws to the owner, sometimes requesting a fee to fix the issue.

Honey Pot- Decoy servers or systems setup to gather information regarding an attacker or intruder into a system.

Pen Testing– An evaluation where assessors search for vulnerabilities and attempt to circumvent the security features of a network and/or information system.

Definitions

Vulnerability Assessment- Assessment of threats and vulnerabilities, deviations from policy, level of risk, and development and/or recommendation of appropriate mitigation countermeasures.

Zero-Day Exploit- A threat actor spots a vulnerability either before the developer does or acts on it before the developer has a chance to fix it.

Full/Responsible Disclosure– Exposing vulnerabilities publicly and immediately or notifying organizations first to allow for a patch.

Keylogger- software or hardware that logs keystrokes to secretly capture private information such as passwords.

Definitions

Cyber/Data Breach- A security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an unauthorized individual unauthorized.

Cyber Crime/Terrorism/Warfare- Contrasting reasons for cyber attacks: financial; malicious or political statement; nation states. May not be clear cut distinctions.

Red Team– An exercise conducted as a simulated attempt by an adversary to attack or exploit vulnerabilities in an organization's information systems.

Blue Team- A group that defends an organization's information systems when mock attackers (i.e., the Red Team) attack, typically as part of an operational exercise.

Team Policy Debate

"Is it ethical to teach 'ethical' hacking?"

- Form two groups, pro and con
- 4 alternating 'constructive' speeches, wherein each team lays the groundwork for the basis of their argument (+/- 5 minutes)
- 4 alternating 'rebuttal' speeches, wherein the teams are expected to extend and apply arguments that have already been made, rather than make new arguments (+/- 5 minutes)
- Follow-up questions by audience to follow if necessary