Engineering Ethics & Security

CSCI-370

Ethics

- External system (rules of conduct)
- Group, culture, profession, etc
- Context dependent
  - Is it wrong to drive 100 mph?
- Enforced by ruling bodies

Morals

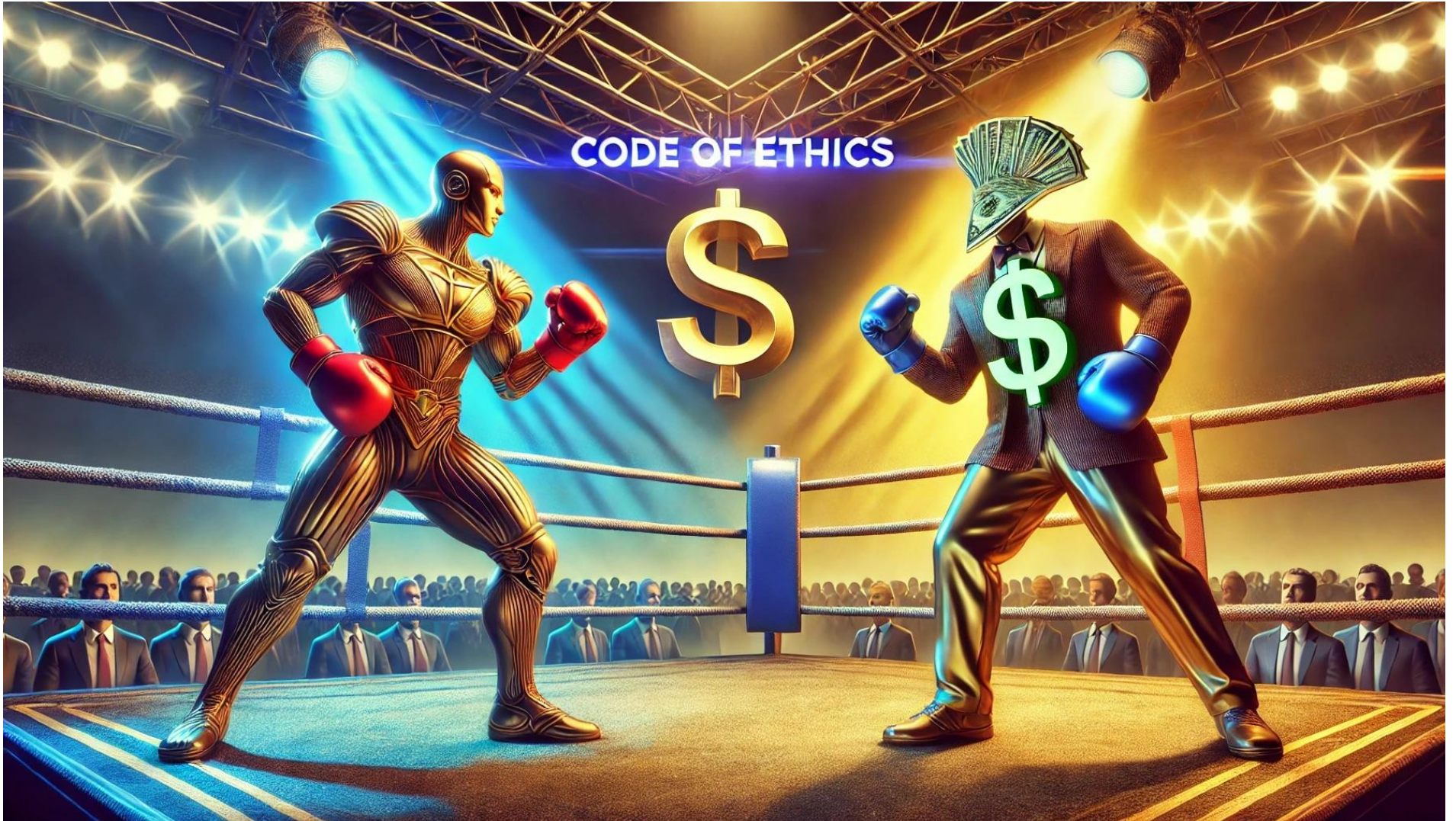
- Internal beliefs (yours) on right and wrong
- Ultimate personal compass
- Consistent with beliefs
- No enforcement body

Time & Money

“Software is eating the world.” - Marc Andreessen (2011)

“When an online service is free, you're not the customer. You're the product.”

“We cannot have a society in which, if two people wish to communicate, the only way that can happen is if it’s financed by a third person who wishes to manipulate them.” - Jaron Lanier


CODE OF ETHICS

Ethical Principles - Daniels Fund

Integrity

Act with honesty in all situations

Trust

Build trust in all stakeholder relationships

Accountability

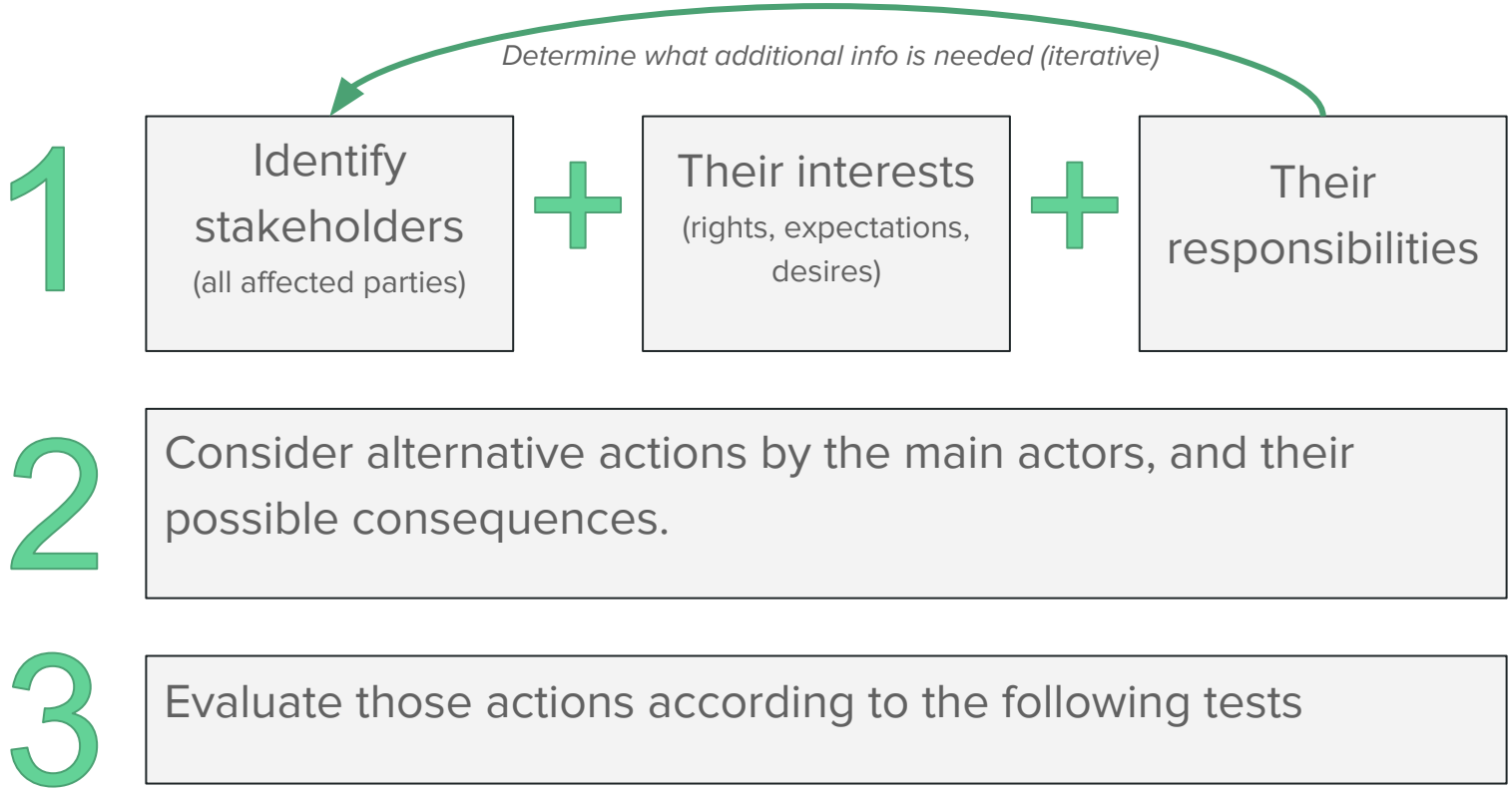
Accept responsibility for all decisions

Transparency

Maintain open and truthful communications

https://ethics.mines.edu/ & https://danielsfund.mines.edu/

General Approach to Engineering Ethics - Michael Davis



*presented by M.C. Loui, April 5, 2017 adapted from Michael Davis

Ethical Considerations Plan

Which ACM/IEEE [illegible] opment of your product? Why?

Which ACM/IEEE [illegible] What can be the negative impa[illegible]

Apply two Tests articula[illegible] Ethics Framework slides for th[illegible]

What are the ethical co[illegible] software quality plan is not implemented properly (or is not comprehensive enough)?

This is what you have to do in your final report!

Ethical Tests - Michael Davis Tests (adapted)

Harm test: Does this option do less harm than any alternative? Do the benefits outweigh the harms?

Reversibility test: Would this choice still look good if I traded places? (i.e., if I were one of those adversely affected by it?)

Professional test: What does the Software Engineering code of ethics say about this problem? What would my colleagues say?

Common practice test: What if everyone behaved this way?

Legality test: Would this choice violate a law or a policy of my employer?

Publicity test: How would this choice look on the front page of a newspaper?

Mirror test: Would I feel proud of myself when I look into the mirror?

*presented by M.C. Loui, April 5, 2017 adapted from Michael Davis

The Challenger Disaster

January 28, 1986

https://science.ksc.nasa.gov/shuttle/missions/51-l/docs/rogers-commission/Appendix-F.txt

Codes of Ethics

ACM: https://www.acm.org/code-of-ethics

Computing professionals' actions change the world

IEEE: https://www.computer.org/education/code-of-ethics

Because of their roles in developing software systems, software engineers have significant opportunities to do good or cause harm

ACM

1. GENERAL ETHICAL PRINCIPLES - fundamental ethical principles that form the basis for the remainder of the Code

2. PROFESSIONAL RESPONSIBILITIES - addresses additional, more specific considerations of professional responsibility

3. PROFESSIONAL LEADERSHIP PRINCIPLES - guides individuals who have a leadership role, whether in the workplace or in a volunteer professional capacity

4. COMPLIANCE WITH THE CODE.

ACM Section 1

1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing

1.2 Avoid harm

1.3 Be honest and trustworthy.

1.4 Be fair and take action not to discriminate.

1.5 Respect the work required to produce new ideas, inventions, creative works, and computing artifacts.

1.6 Respect privacy.

1.7 Honor confidentiality.

ACM Section 2

2.1 Strive to achieve high quality in both the processes and products of professional work.

2.2 Maintain high standards of professional competence, conduct, and ethical practice.

2.3 Know and respect existing rules pertaining to professional work.

2.4 Accept and provide appropriate professional review.

2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.

2.6 Perform work only in areas of competence.

2.7 Foster public awareness and understanding of computing, related technologies, and their consequences.

2.8 Access computing and communication resources only when authorized or when compelled by the public good.

2.9 Design and implement systems that are robustly and usably secure.

IEEE

1. PUBLIC – Software engineers shall act consistently with the public interest.

2. CLIENT AND EMPLOYER – Software engineers shall act in a manner that is in the best interests of their client and employer consistent with the public interest.

3. PRODUCT – Software engineers shall ensure that their products and related modifications meet the highest professional standards possible.

4. JUDGMENT – Software engineers shall maintain integrity and independence in their professional judgment.

5. MANAGEMENT – Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance.

6. PROFESSION – Software engineers shall advance the integrity and reputation of the profession consistent with the public interest.

7. COLLEAGUES – Software engineers shall be fair to and supportive of their colleagues.

8. SELF – Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession.


Forbes
THE
FRESHMAN


OceanGate

Security

Bug Free Code

... is not practical

NASA's seL4 Microkernel (formally verified)

- 10-12 errors per 1k LOC in critical systems -> 0.11 (~100x decrease)
- 20x cost increase (~$3800 per LOC)
- Expensive and slow

You will write code containing a critical security vulnerability

https://www.nasa.gov/history/sts1/pages/computer.html

What is “secure”?

“Maintain data security”

“Keep it secure”

“Encrypt all the data”

A secure system resists attacks within the expected threat model at an acceptable cost

Push an adversary to disproportionate effort - different for military, life/death, and a hobby app

Consider asset value, threat actors, capabilities

Goal: give you the tools to analyze security in a precise and practical way

How?

Threat Modeling

STRIDE (spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege)

- What are you building?
- What can go wrong?

Data Flows (SVA)

- Follow the data, find the threats
- Use your architecture diagrams!

Foundational Models

- CIA (confidentiality, integrity, availability)
- DREAD (Damage, Reproducibility, Exploitability, Affected users, Discoverability)


Threat


Vulnerability

Example Threat: Tampering

Can the hacker maliciously modify something at rest or in transit?

Sample user story: “As a user, I want to be able to save my shipping information for future use.”

Sample threat: “As an attacker, I want to tamper with the shipping address to re-route the product”

Sample vulnerability: “Lack of caller validation on the “update shipping information” request results in modification of another user’s shipping info”

Foundational Tools

Authentication - identity

Authorization - access control

Input Validation – data trustworthiness

Cryptography - confidentiality (& integrity)

Crypto Concepts

- Kerckhoff's principle: A system should remain secure even if everything about it is public, except the secret key
- Never roll your own crypto
- Different types of crypto for different goals

Symmetric Cryptography

- Encrypt large amounts of data quickly
- Weakness: key distribution

Asymmetric Cryptography

- Secure key exchange, identity, signatures
- Weakness: slow, inefficient

Hash Functions

- Integrity, proof
- Weakness: irreversible by design

Attack Frameworks

- OWASP Top 10 (top vulnerabilities affecting applications)
- MITRE ATT&CK (adversary tactics & techniques)
- CWE (common weakness enumeration)

What are you going to do about it?

- Understand the threat model for your project
- Come up with a credible security story for your application
- Prioritize & protect against threats

“We will secure our application data” ->

“The main threats against our application are A B C and we plan to X Y Z to mitigate those threats to an appropriate degree”

(Not homework assignments!)