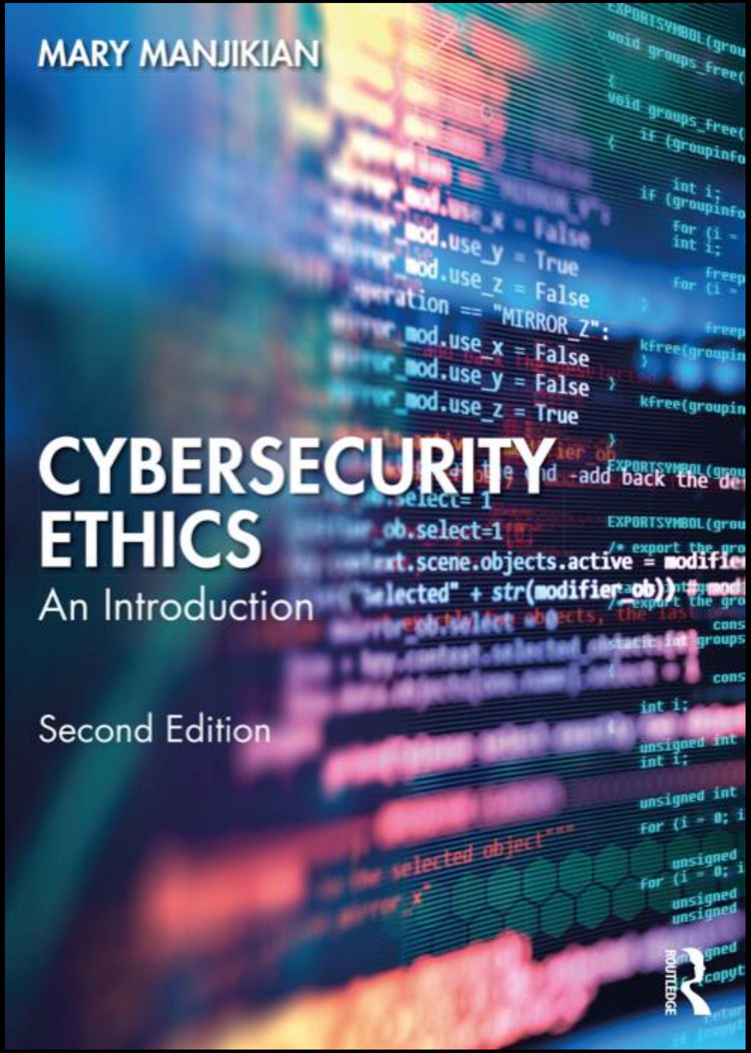
TDDE61 Ethical hacking
Lecture 4: Ethics

Mikael Asplund

LINKÖPING
UNIVERSITY

Material

- https://www.ida.liu.se/~TDDE61/resources/
  - Ethics
- Online textbook
- Ethical codes and vulnerability disclosure guidelines
- Incidents and other reading



Morality

- A system of guidance for human behaviour
- Different from other guidance systems
  - Law
  - Etiquette
  - Self-interest
  - Tradition

Ethics

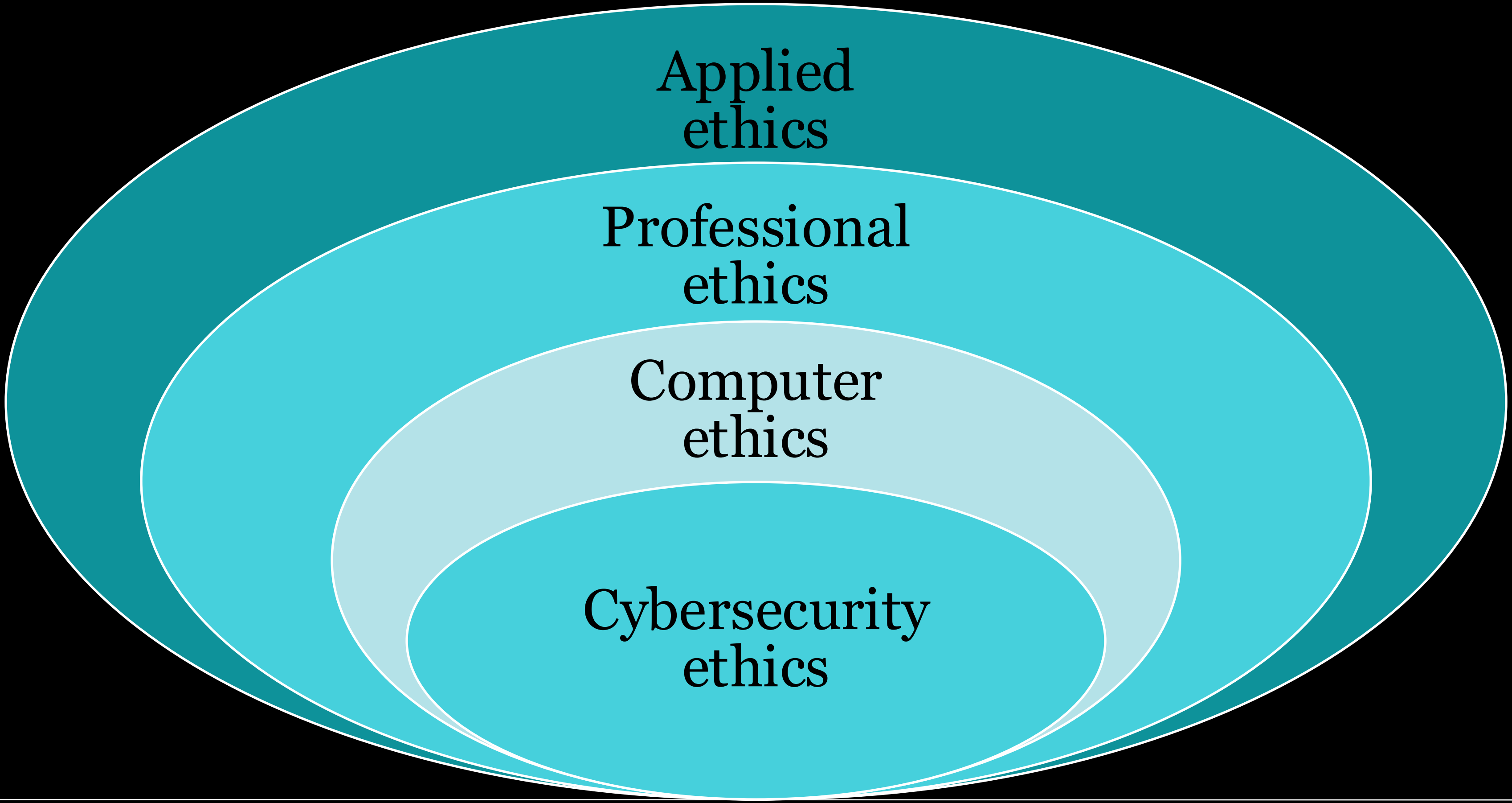
- “Ethical” often used synonymously to “moral” – “Ethical hacking”

- A branch of philosophy
  - Ethics is the philosophical study of morality
  - Supports moral reasoning

Some branches of ethics

- Applied ethics
    - Determining what is moral in a given situation
- Normative ethics
    - What are our moral duties?
    - How can we reason about what is right and wrong?
- Metaethics
    - Questions about how we can reason about ethics
    - Does moral objectivity exist?

Cybersecurity ethics



Applied ethics

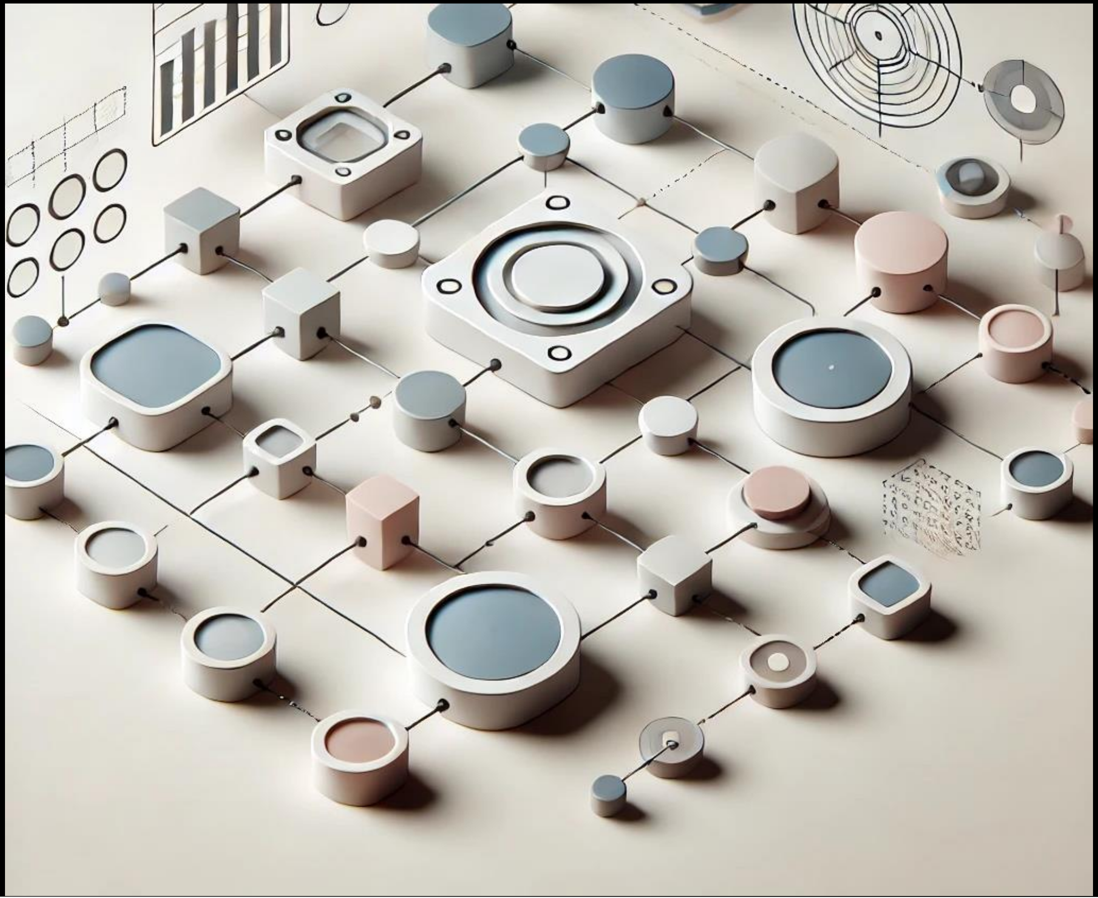
Professional ethics

Computer ethics

Cybersecurity ethics

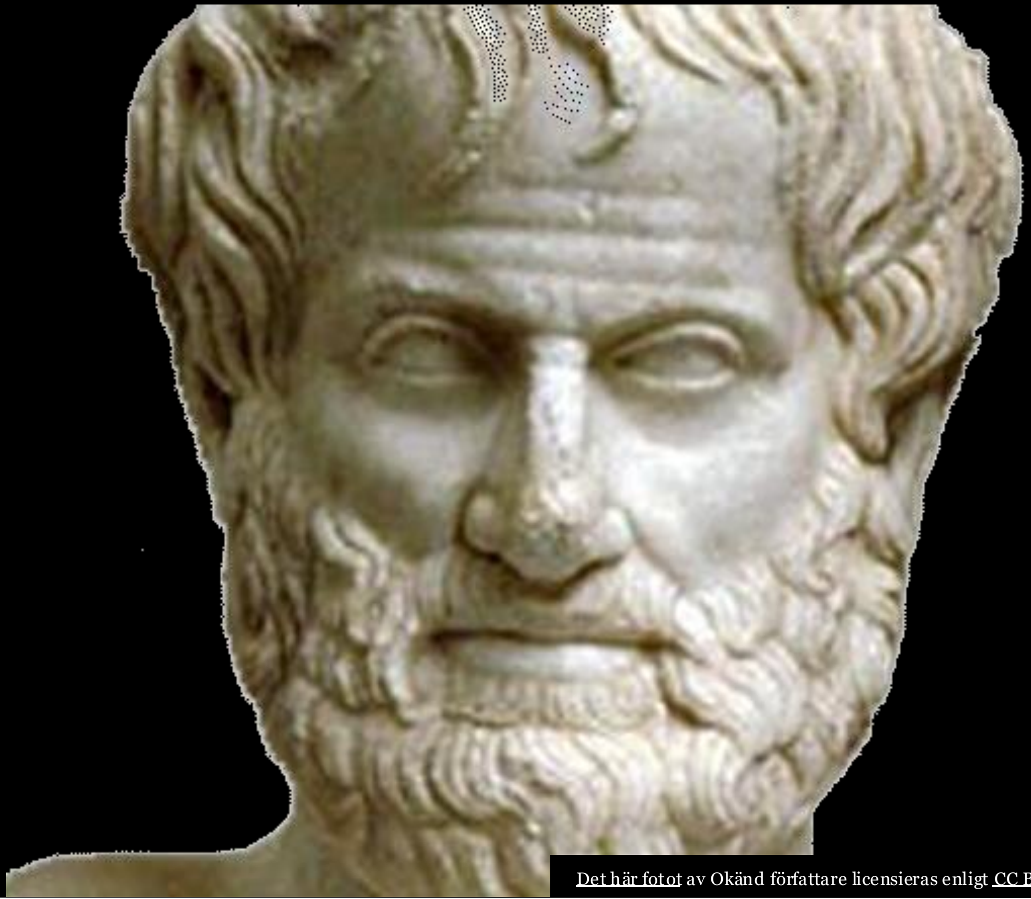
Ethical frameworks (normative)

- Virtue ethics
- Utilitarian ethics
- Deontological ethics



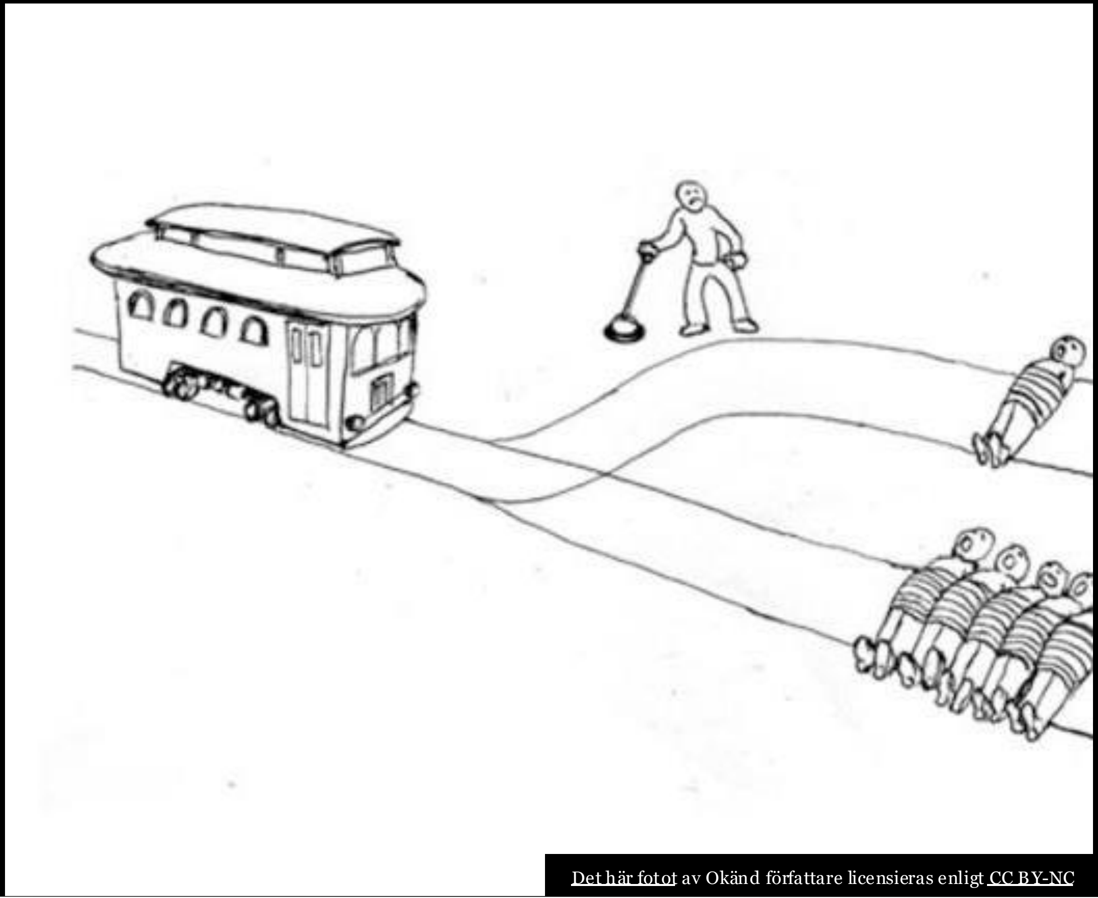
Virtue ethics

- Aristotle: our purpose is to act well as human beings
- Intent of the agent matters
- Virtuous ≠ Saintly
- Basis for many professional ethics



Utilitarian ethics

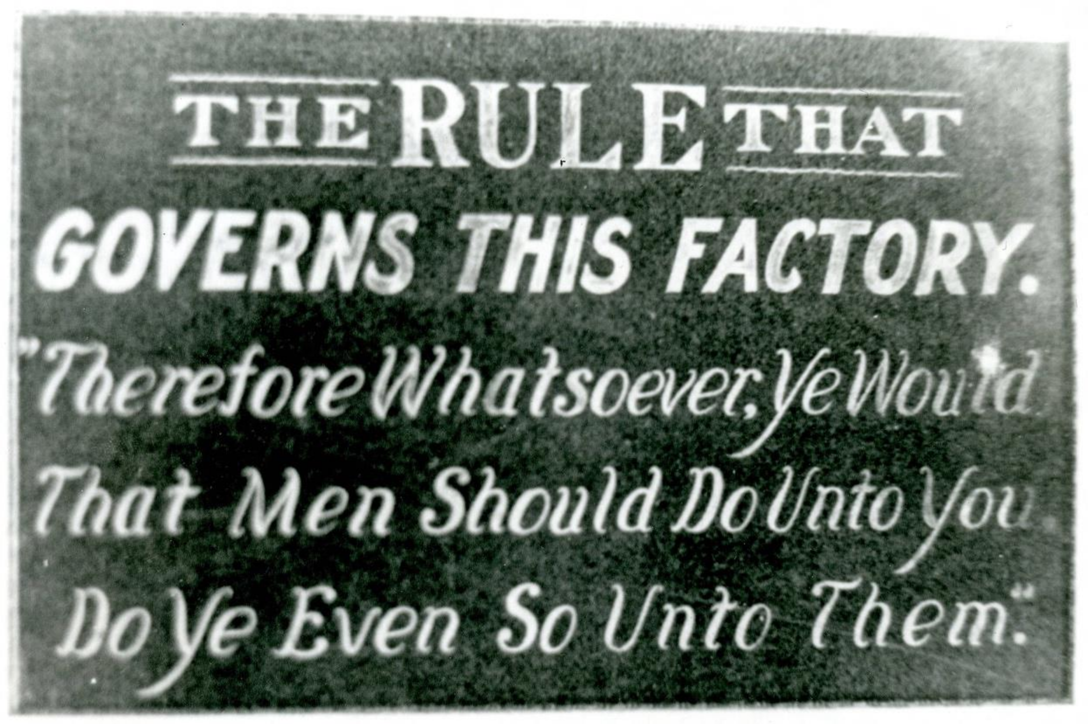
- The consequence is what matters
  - Not the intent
- Optimize the outcome of possible actions – best overall situation (both good and bad)
- Situational
- Programmable?



Deontological ethics

- Categorical imperative:
  - “Always act on the maxim or principle which can be universally binding, without exception, for all humans.”
  - Immanuel Kant

- Golden rule
  - Reversibility notion



THE RULE THAT

GOVERNS THIS FACTORY.

"Therefore Whatsoever, Ye Would That Men Should Do Unto You Do Ye Even So Unto Them."

Applying ethical frameworks

Framework	Questions
Virtue Ethics Approach	• Which position best expresses my values and character? • If I choose this, can I live with myself? • Will it contribute to my own human flourishing/character development?
Utilitarian Approach	• Which position generates the greatest positive utility and produces the fewest negative consequences? • What costs are associated with each outcome? • What benefits are associated with each outcome?
Deontological Approach	• Who will be affected by this decision? • Am I treating others as a means or an end in themselves? • If my actions became a rule and I was subject to that rule, would I accept it and view it as ethical?

Case study: Google Project Zero

- 90+30 policy
  - A vendor has 90 days after Project Zero notifies them about a security vulnerability to make a patch available to users.
  - Public disclose details of the vulnerability 30 days after the patch has been made available
  - If no patch is released within 90 days, the details of the vulnerability is made public

- In-the-wild exploits: 7-day deadline

- 97.2% issues fixed within deadline

Is this a moral approach?

- From a virtue ethics point of view?
- From a utilitarian point of view?
- From a deontological point of view?

What about the exceptions?

- 6 out of 1797 cases the disclosure deadlines for Project Zero's issues were extended by Google:
  - Issue 837 -- "task_t considered harmful", 145 days
  - Issue 1272 -- "Spectre and Meltdown", 216 days
  - CVE-2020-1027 -- "In the Wild Series: Windows Exploits", 23 days (actively exploited issue under a 7-day deadline)
  - Issue 2105 -- "In-the-Wild Series: October 2020 0-day discovery", 101 days (actively exploited issue under a 7-day deadline)
  - Issue 2107 -- "In-the-Wild Series: October 2020 0-day discovery", 98 days (actively exploited issue under a 7-day deadline)
  - Issue 2108 -- "In-the-Wild Series: October 2020 0-day discovery", 98 days (actively exploited issue under a 7-day deadline)

ACM code of ethics

- Ethical principles include
  - Avoid harm.
  - Be honest and trustworthy.
  - Honor confidentiality.

- Professional responsibilities include:
  - Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.
  - Access computing and communication resources only when authorized or when compelled by the public good.
  - Design and implement systems that are robustly and usably secure.

ISC2 Code of ethics

- Code of Ethics Preamble:
  - The safety and welfare of society and the common good, duty to our principals, and duty to each other, require that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
  - Therefore, strict adherence to this Code is a condition of certification.

- Code of Ethics Canons:
  - Protect society, the common good, necessary public trust and confidence, and the infrastructure.
  - Act honorably, honestly, justly, responsibly, and legally.
  - Provide diligent and competent service to principals.
  - Advance and protect the profession.

OWASP Vulnerability Disclosure Cheat Sheet

- Researchers should:
  - Ensure that any testing is legal and authorized.
  - Respect the privacy of others.
  - Make reasonable efforts to contact the security team of the organization.
  - Provide sufficient details to allow the vulnerabilities to be verified and reproduced.
  - Not demand payment or rewards for reporting vulnerabilities outside of an established bug bounty program.

Seminars

- Will contact small groups about merging
- Form for choosing topics will come soon

Questions?

Other matters

- Lab instructions updated
- Lecture series almost settled (7 lectures)
- CTFd server somewhat delayed
- Account distribution!