Week 05
Crash Course On Law and Ethics

Slides By: Thomas Quig

sigpwny{i_am_NOT_a_lawyer}

Announcements

O2F - nth Place!!

Shirts - Please check your emails!!!! I'm going to start giving them away

Server repair update!

Ethics (What not to do)

Tech people can be assholes sometimes

Examples of what not to do

Theranos - Ponzi Scheme

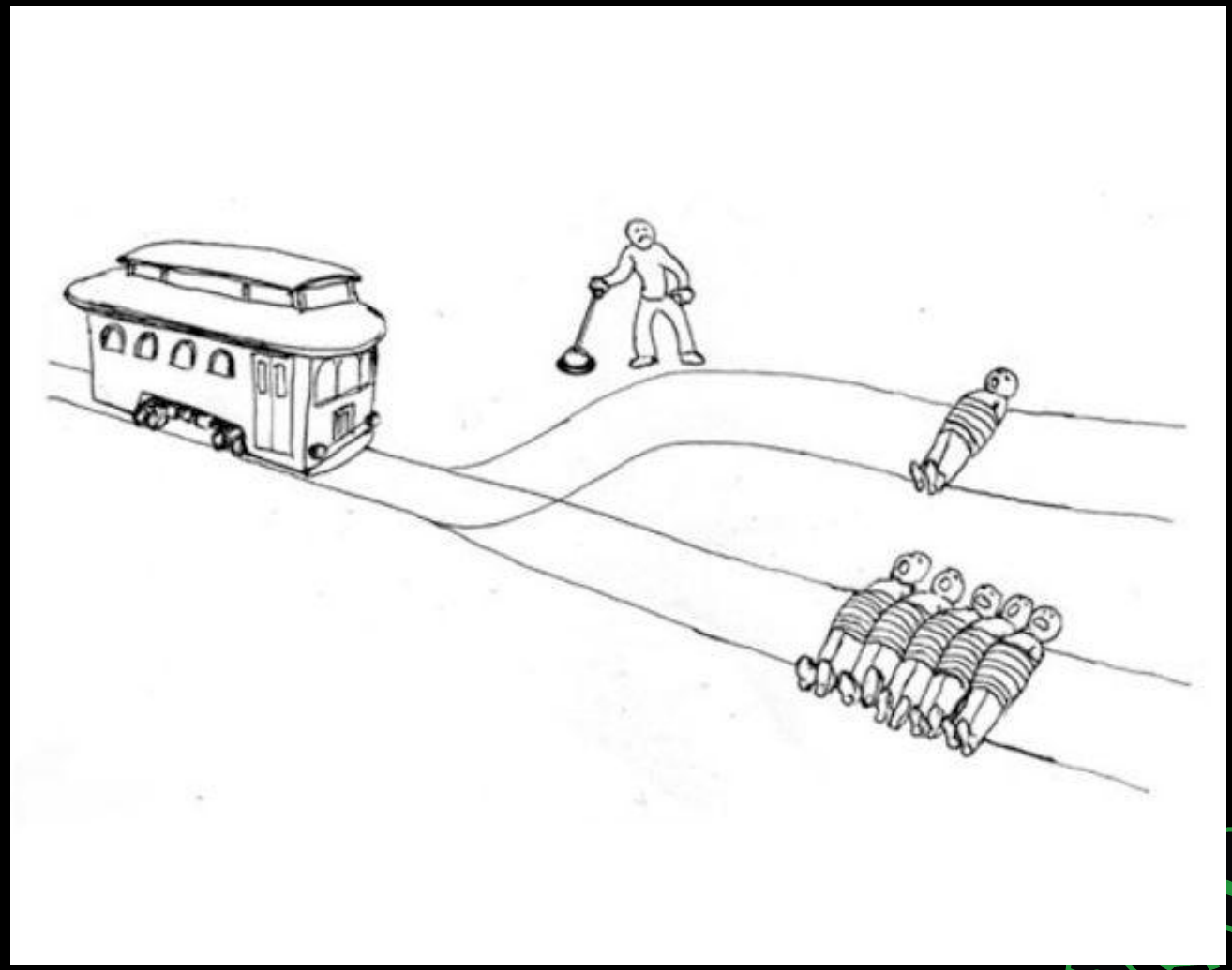
Facebook - Cambridge Analytica

The NSA - Spying on every single citizen

Ethical Models

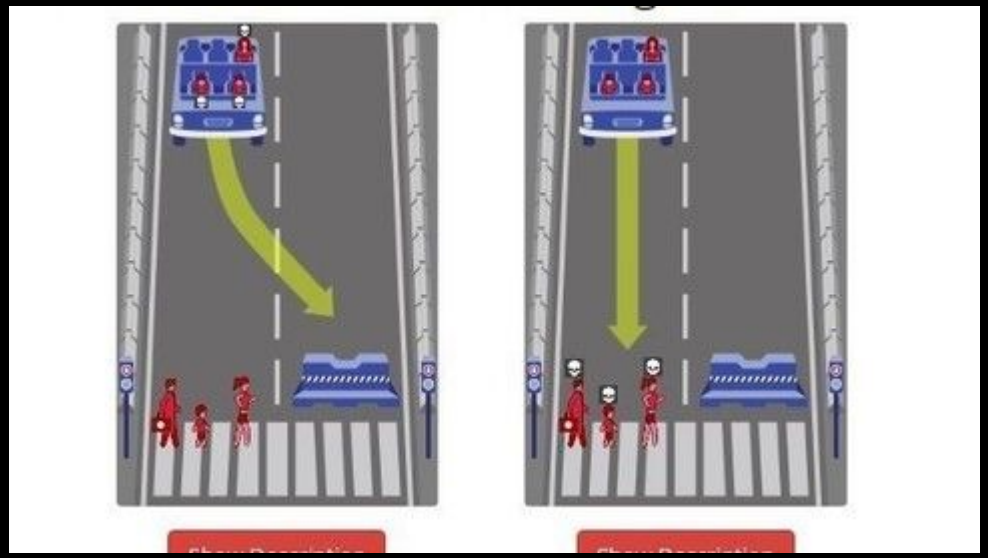
You are a switch operator near a trolley, the trolley is going down a track towards 5 people.

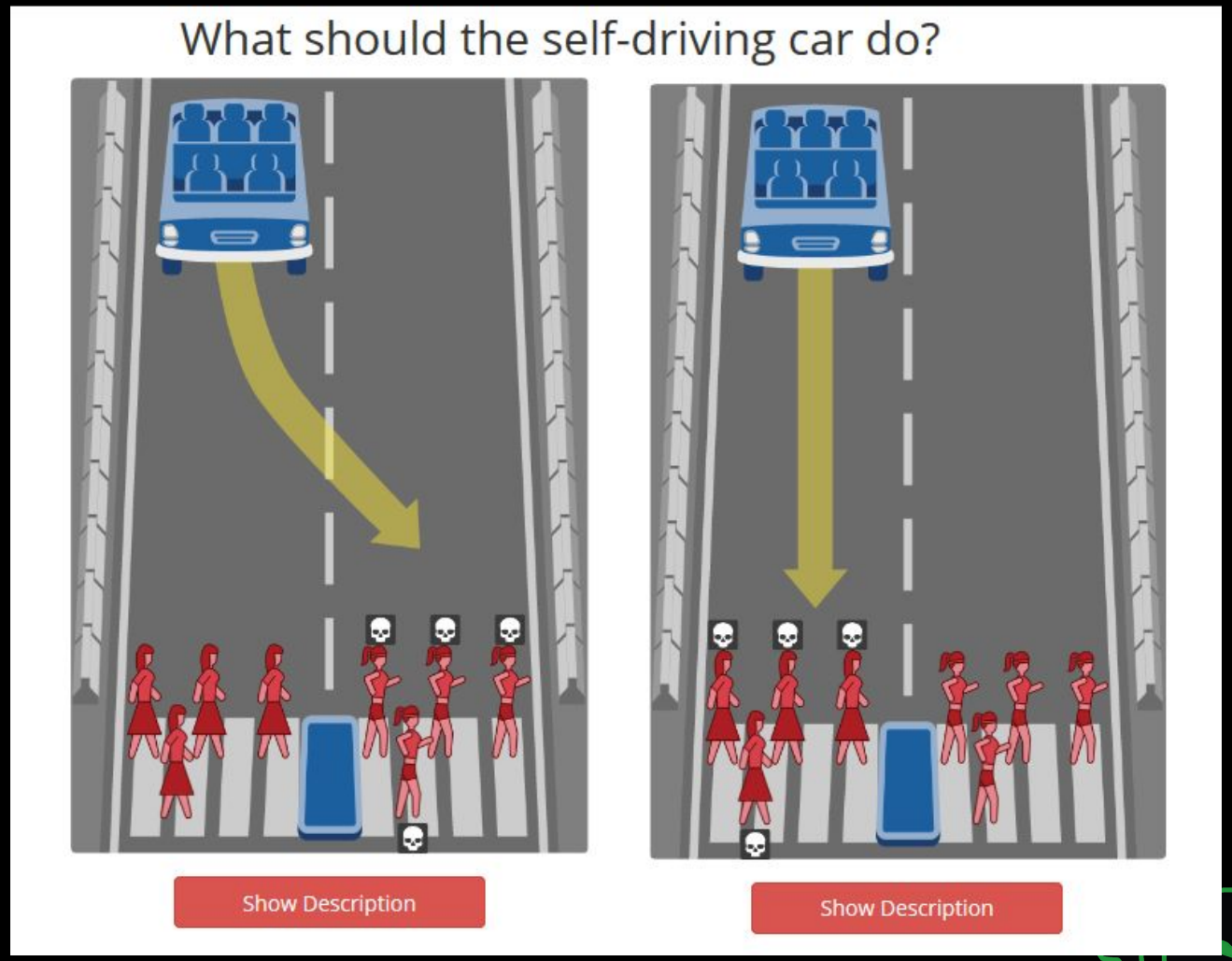
You can pull the switch and save the 5 people, but at the cost of one person.



Relevance

This applies in tech!





Ethical Models

Utilitarianism

- What creates the most “Utility” is good
-

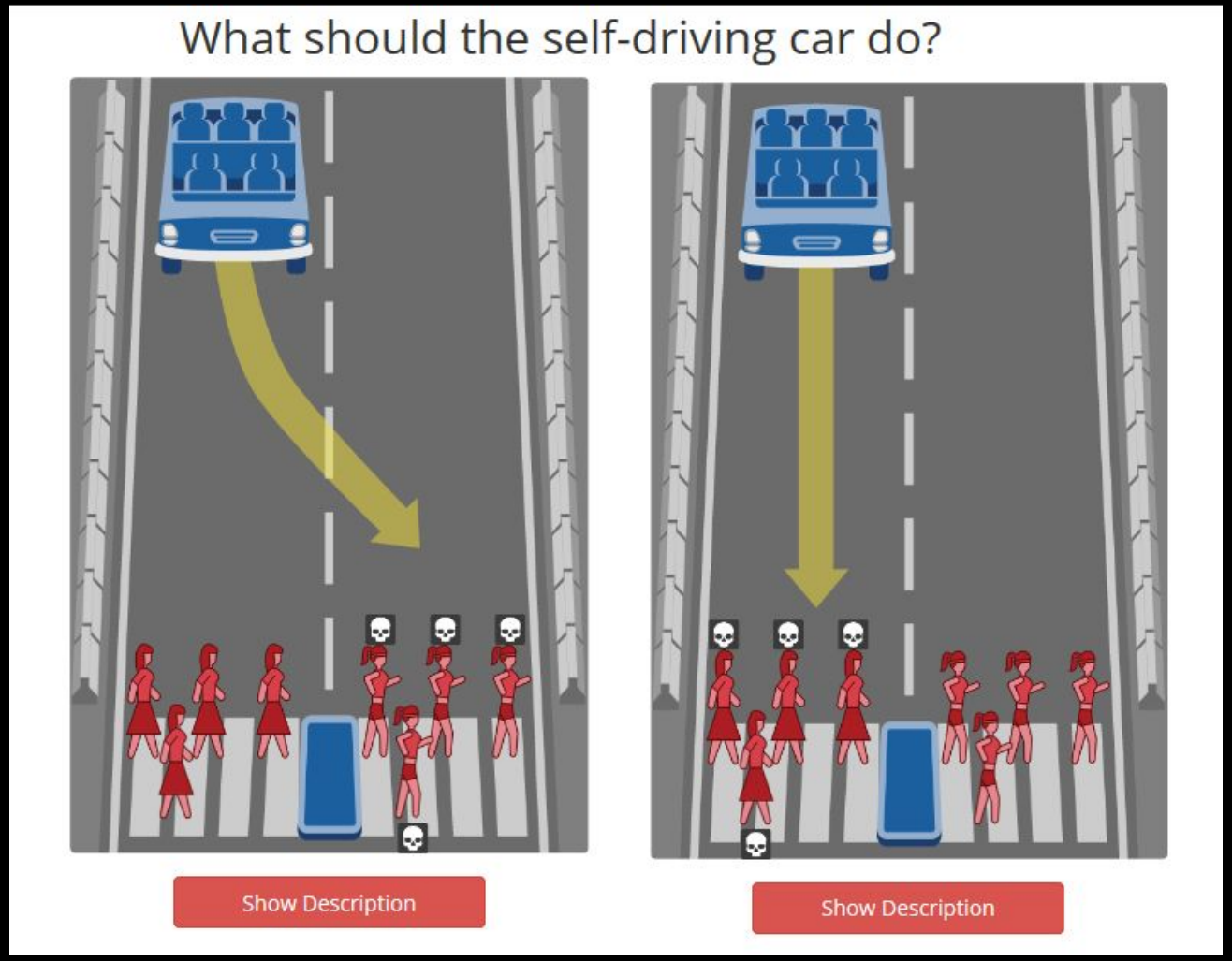
Deontological (Duty-based)

- Morality is founded in one moral agents’ obligations to another
- People are the end

Virtue (Character based)

- Morality is grounded in Virtue
- Relative to culture

What does the car do?



How this applies to security?

Incident Response

Vulnerability Research and Reporting

SocEng attacks etc.

Security Ethics

- Mitigating Risk
  - Risk = Expectation of loss expressed as probability
- Hacker "Ethics" (Stephen Levy)

1. Access to computers should be unlimited.
2. All information should be free
3. Mistrust authority
4. Hackers should be judged by their skill
5. You can create art and beauty on a computer.
6. Computers can change your life for the better.

Problems with Levy's Ethics

If information is free, write your Credit Card # on the board

Activities in cyberspace are virtual

- Separation of virtual and real

Ethical Security Research

- Hack systems with…
  - Explicit Permission
  - Expertise
  - Proper documentation

Ethical Vulnerability Reporting

Vulnerability Disclosure

- Nondisclosure
  - Keep it secret, sell it secretly, use it for your own gain.
- Full Disclosure
  - Tell literally everyone, just drop it.
  - Make sure people can protect themselves from the vuln.
- Limited Disclosure
  - Privately disclose to the vendor only so they can develop a patch.
  - Risky because you can be attacked for this

Responsible Disclosure

1. Disclose vulnerability in private to the company
   a. Do this ONLY IF THEY ARE NOT A SHITTY COMPANY (More info later)
2. Talk to vendor and agree on deadline for full disclosure
   a. Google's is 90 days
3. Maintain communication with both parties during patch dev
4. Fully disclose vulnerability when patched / after deadline

Bug Bounties

Hackerone!

Pwn2own

Company Specific Bug Bounty

The Law

Please don't go to jail

Crimes

There are lots of them

Misdemeanor vs Felony vs Capital

State vs Federal

Civil court!!!

I have a love-hate relationship with these images

What Makes it a Crime

Two Elements that make up a crime

1. Specified **state of mind** or **intent**
2. Performance of a prohibited act

Intent

- Mens Rea = “Requisite Guilty State of Mind”
  - Intent to do crimes
- Specific vs General Intent vs Criminal Negligence
- Intent Definitions Under the Law
  - Purposefully: You hoped for that outcome to happen, you tried to make it happen
  - Knowingly: You knew the outcome was practically certain, you didnt intent / want it, but you knew it would happen.
  - Recklessly: You concisously ignored unjustifiable risks that you knew were risks
  - Negligently: You should have been aware of the risks, but you were not.

Crimes (But like not really, but also yes… but like kind of…)

Solicitation - Asking

Facilitation - Assisting

Conspiracy - Planning

Attempt - Trying

Notes on Conspiracy

1. Agreement by two or more people to commit a specific crime
2. Must be COUPLED WITH OVERT ACT toward commission of crime
   a. Overt act != Illegal

Intent Matters

This is not about what is right

This is about what exists

The Law (CFAA Part One)

18 U.S. Code § 1030 - Computer Fraud and Abuse Act

- Enacted 1986
  - Hasn't been updated much since then

- Protects Data At Rest

- Very arbitrary and unclear

We could spend a whole semester talking about this, so I will try to give a super brief summary of the whole thing.

The Law (CFAA Part Two)

7 Distinct Crimes

1. Obtaining classified information to injure US or aid foreign power
2. Accessing a computer without auth **or exceeding authorized access** and obtaining information
3. Unauthorized access to US govt computers
4. Another federal crime combined with unauthorized access
5. Unauthorized access + **damage**
6. Computer password trafficking
7. Extortion + any of 1-6

The Law (Not the CFAA)

- Data-in-transit laws
- Wire fraud
- Mail fraud
- A thousand other pieces of law

Tips from not a lawyer

When in doubt, ask for permission before you do **anything**

Check what the company is, No criminal != you won't get sued.

Be quiet, get a lawyer, “anything you say can be used against you”

Be educated, know your rights, know the law

Next Meetings

Next Thursday: Reverse Engineering I

- Introduction to reverse engineering
- Critical tools to Rev (ghidra, ida etc)
- Basic strategies

Sunday Seminar: Reverse Engineering II

- Advanced Rev tactics
- More in depth analysis
- Binary analysis