The Ethical Implant Documentation

University of the Fraser Valley, School of Computing

Project Manager: Anisa Quintyne (300189601)

Lead Writer: Surbhi (300215388)

Game Designer: Guneet Bakshi (300196598), Gursagar Chahal (300192061)

Graphics Designer: Harsh Arora (300206519)

Documentation Lead: Guneet Bakshi

Quality Assurance: Gursagar Chahal

CIS 485: Ethics & Other Management Issues

Parsa Rajabi

Oct. 29, 2025

https://lqu2.github.io/CIS-485/

Case Study Chosen

The reason why we have chosen Medical Implant Risk Analysis is that it poses serious ethical concerns in the field of medical technology and information protection. The case studies the privacy and safety issues of a company, Corazón, in regards to an implantable heart monitoring device. This example shows the practical significance of ethical responsibility and data privacy, which are the core aspects of professional behaviour in the ACM Code of Ethics.

We intend to adapt this case study into a Twine game to challenge players on certain ethical dilemmas in the workplace.

Prototype Workflow

The Twine prototype is designed in the form of a branching-choice that enables the player to make ethical choices as a developer or hacker who has discovered a weakness in the wireless implant.

Introduction: Presents Corazón and the implant system.

Gathering: The player discovers potential weaknesses in the implant.

Choice Node: Person will choose to either report privately or to publicly leak the exploit.

Outcomes:

Responsible reporting results in the improvement of the system.

Legal concerns and reputation losses but transparency of the information is promoted through the public disclosure.

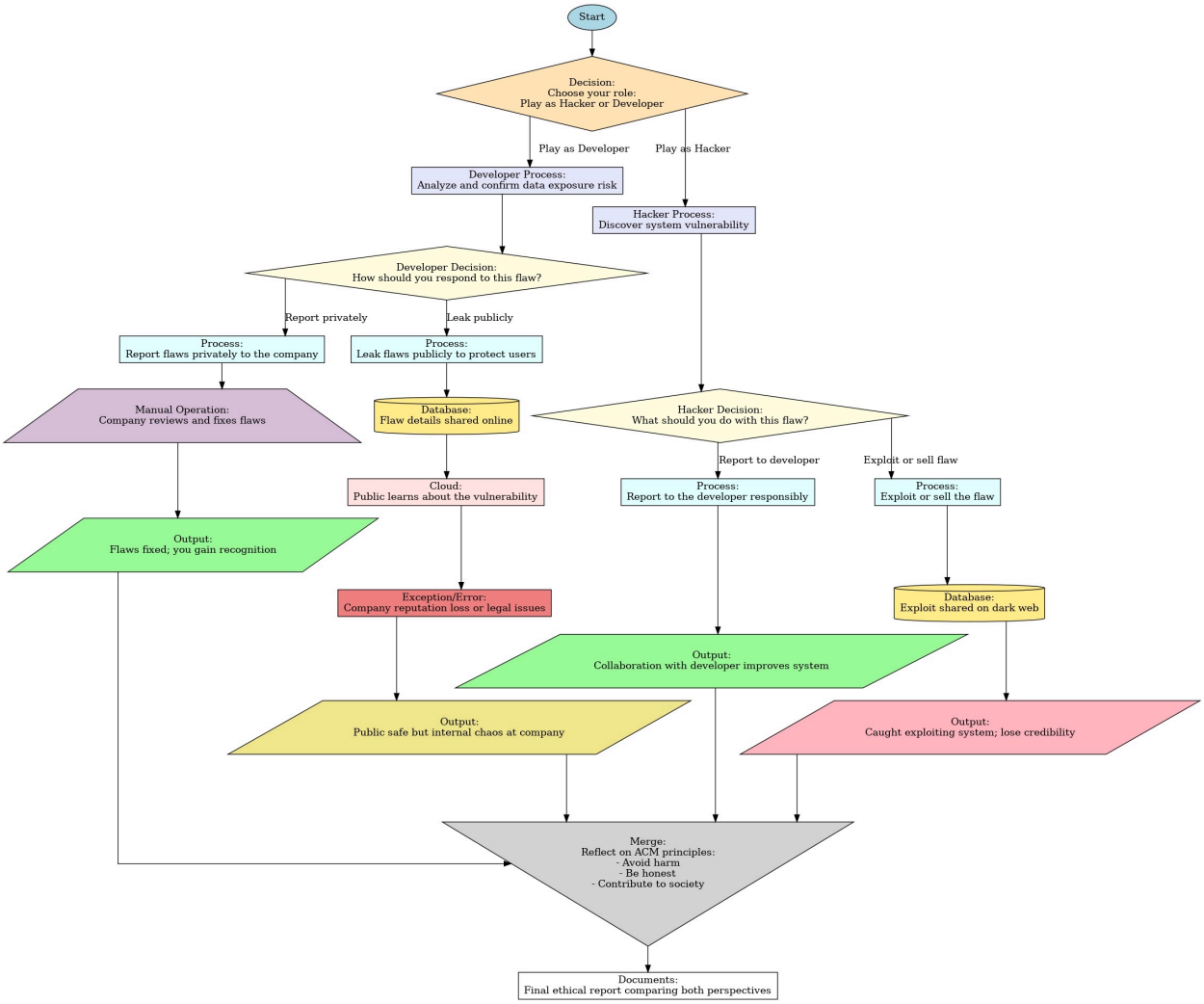

Figure 1

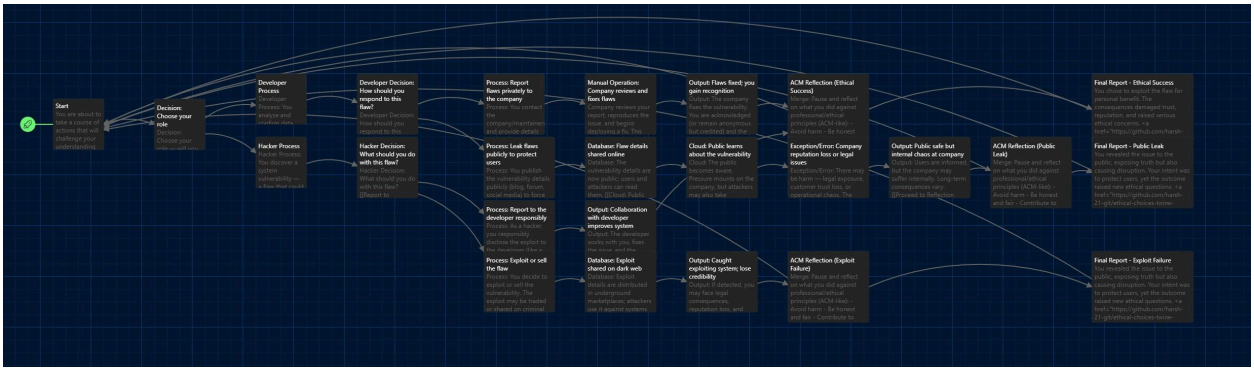

Figure 2

List of ethical dilemmas

1. A developer faced with a flaw decides to keep it private and discuss it with the company. You decide to be dishonest with the public by not sharing that users' data is at risk. You instead try to fix this flaw internally with the company, trying to ensure a robust and secure system, but still risking public safety since you don’t know how long this flaw will take to fix, and users don’t know that their data is at risk. In the end, the flaw is resolved, ensuring public safety as well as a secure system and avoiding harm.
2. A developer faced with a flaw decides to leak the flaw to the public. They wish to leak the flaw in an attempt to protect users. You wished to be honest and avoid harm, but the flaw being public means an attacker can also access it. This negatively impacts the company since customers are lost and shareholders pull out in fear of ethical concerns. Although you protected the public, you caused chaos in the company.
3. A hacker finds a flaw in a company and reports it to the developer. You want to respect privacy, be honest, and avoid harm by contacting Corazón and informing them about the flaw. Although there is a chance that the company distrusts you due to a lack of credibility, you may also receive little to no reward. You overall protect the public and help improve the company for little to no gain, with a small chance of recognition from the company.
4. A hacker finds a flaw in a company and decides to exploit or sell it. You decide to exploit Corazón's data flaw for personal gain, disregarding privacy or potential harm to the public and the company. You sell it on the dark web, making money, and now this flaw is spread around the dark web, which an attacker uses against the company. This can negatively impact you if it is found out that you were the original leaker, causing loss of credibility or potential legal action.

References

[1]“Case Study: Medical Implant Risk Analysis,” *Acm.org*, 2024. https://www.acm.org/code-of-ethics/case-studies/medical-implant-risk-analysis