CSCI 245 Life, Computers, and Everything
Prof. Felipe Perrone
Activity 7

This activity will have you work in teams to study and to apply two professional codes of ethics: the ACM code and the ACM/IEEE-CS SE code. (The four scenarios below were produced by the ACM Integrity Project https://ethics.acm.org/.)

Each team will be assigned one of four scenarios and will submit the result of their work using this form. Teams should elect *one person to record and to submit* their conclusions and *another person to summarize and report* their scenario and findings to the class.

Discuss the scenario with your team to reach the best possible understanding with the information you are given. For your scenario only:

1) Determine the facts of relevance for ethical analysis.

2) Determine who is affected in the situation and what each party stands to gain or to lose.

3) Identify any moral hazard(s) in the scenario.

4) Determine whether and how any principles of the **ACM code** were either upheld or violated. You should be able to enumerate the relevant principles, but also to explain how the relate to the scenario.

5) Explain whether the **ACM/IEEE-CS code** applies to your scenario.

6) Determine the consequences of a computing professional being found to have violated the **ACM code**.

Case 1: Malware Disruption

"Rogue Services advertised its web hosting services as "cheap, guaranteed uptime, no matter what." While some of Rogue's clients were independent web-based retailers, the majority were focused on malware and spam. Several botnets used Rogue's reliability guarantees to protect their command-and-control servers from take-down attempts. Spam and other fraudulent services leveraged Rogue for continuous delivery. Corrupted advertisements often linked to code hosted on Rogue to exploit browser vulnerabilities to infect machines with ransomware.

Despite repeated requests from major ISPs and international organizations, Rogue refused to intervene with these services, citing their "no matter what" pledge to their customers. Furthermore, international pressure from other governments failed to induce national-level intervention, as Rogue was based in a country whose laws did not adequately proscribe such hosting activities.

Ultimately, Rogue was forcibly taken offline through a coordinated effort from multiple security vendors working with several government organizations. This effort consisted of a targeted worm that spread through Rogue's network. This denial-of-service attack successfully took Rogue's machines offline, destroying much of the data stored with the ISP in the process. All of Rogue's clients were affected. No other ISPs reported any impact from the worm, as it included mechanisms to limit its spread. As a result of this action, spam and botnet traffic immediately dropped significantly. In addition, new infections of several forms of ransomware ceased."

Case 2 - Medical Implant Risk Analysis

“Corazón is a medical technology startup that builds an implantable heart health monitoring device. The device comes with a smart phone app that can monitor and control the device wirelessly, as well as storing a persistent record that can be shared with medical providers. After being approved by multiple countries’ medical device regulation agencies, Corazón quickly gained market share based on the ease of use of the app and the company’s vocal commitment to securing patients’ information. To further expand their impact, Corazón worked with several charities to provide free or reduced access to patients living below the poverty line.

As a basic security mechanism, Corazón’s implant could only be accessible through short-range wireless connections, requiring the phone and implant to be in close proximity. Data transferred between the app and the device employed standard cryptographic algorithms, and all data stored locally on the phone was encrypted. To support on-going improvement, Corazón had an open bug bounty program inviting disclosure of potential vulnerabilities in their app.

At a recent security conference, an independent researcher claims to have found a vulnerability in the wireless connectivity. The researcher presents a proof-of-concept demonstration where a second device in close proximity could modify commands sent to the implant to force a device reset. The attack relied on the use of a hard-coded initialization value stored in the implant device that created a predictable pattern in the data exchanges that could be manipulated. In consultation with Corazón’s technical leaders, the researcher concludes that the risk of harm with this attack is negligible, given the limited capabilities of the device.”

Case 3 - Automated Active Response Weaponry

"Q Industries is an international defense contractor that specializes in autonomous vehicles. Q's early work focused on passive systems, such as bomb-defusing robots and crowd-monitoring drones. As an early pioneer in this area, Q established itself as a vendor of choice for both military and law enforcement applications. Q's products have been deployed in a variety of settings, including conflict zones and non-violent protests.

In recent years, Q has suffered a number of losses, as protestors and other individuals have physically attacked the vehicles with rocks, guns, and other weapons. To reduce this problem, Q has begun to experiment with automated active responses. Q's first approach was to employ facial recognition algorithms to record those present and to detect individuals who may pose a threat. This approach was shortly followed by automated non-lethal responses, such as tear gas, pepper spray, or acoustic weapons, to incapacitate threatening individuals.

Q has recently been approached—in secret meetings—by multiple governments to expand this response to include lethal responses of varying scales. These capabilities range from targeted shooting of known individuals to releasing small-scale explosives. When Q leadership agreed to pursue these capabilities, several of Q's original engineers resigned in protest. Some of these engineers had previously expressed concern that the non-lethal responses had inadequate protections against tampering, such as replacing tear gas with a lethal poison. Knowing that these individuals were planning to speak out publicly, Q sued them for violating the terms of their confidentiality employment agreement."

Case 4 - Malicious Inputs to Content Filters

"The U.S. Children's Internet Protection Act (CIPA) mandates that public schools and libraries employ mechanisms to block inappropriate matter on the grounds that it is deemed harmful to minors. Blocker Plus is an automated Internet content filter designed to help these institutions comply with CIPA's requirements. To accomplish this task, Blocker Plus was designed with a centrally controlled blacklist maintained by the software maker. In addition, Blocker Plus provided a user-friendly interface that made it a popular product for home use by parents.

Due to the challenge of continually updating the blacklist, the makers of Blocker Plus have begun to explore machine learning techniques to automate the identification of inappropriate content. During the development of these changes, Blocker Plus combined input from both home and library users to aid in the classification of content. Pleased with their initial results, Blocker Plus deployed these techniques in their production system. Furthermore, Blocker Plus continued to collect input from users to refine their learned models.

During a recent review session, the development team reviewed a number of recent complaints about content being blocked inappropriately. An increasing amount of content regarding gay and lesbian marriage, vaccination, climate change, and other topics not covered by CIPA, had been added to the blacklist. Initial investigations into these incidents suggested that there were a number of activist groups that had exploited Blocker Plus's feedback mechanism to provide input that corrupted the classification model. Determining that there was no easy way to correct the model, Blocker Plus's leadership chose to disable accounts linked to the activist groups, while keeping the existing model intact in the hope that a correction could eventually be made. The legal and business risk, they determined, would be greater by switching to an outdated model that failed to block known bad content."