COSC130 Fundamentals of Cybersecurity and Privacy

Tutorial Week 2

1. **Calculating Expected Gain**
   In a new lottery game, the chance of winning is 10%, in which case the player gets the double value of the ticket they bought. Peter buys a $100 ticket. What is his expected gain?

2. Adapted from Markus et al, 2020
   A choice of anti-malware: You are dealing with malware that turns the affected computers into nodes in a botnet performing a distributed denial-of-service attack against servers in an important hospital running 1,000 computers, which risks placing the lives of its patients at risk. You have three anti-malware tools in your arsenal, all of which are effective against malware. However, the malware is designed to retaliate by wiping out the entire hard disk as soon as it is disconnected from the malicious server. A preliminary study of the malware shows that it could be fought with three different software approaches. Each of them fails in specific ways to limit the damage. Due to time and resource constraints, you can develop only one of these before the malware spreads, causing morally intolerable human damage. Which one do you develop?

   – Anti-malware 1: It protects all computers but deletes all Excel and Word files during installation. The financial cost is estimated to $1,000 per computer.

   – Anti-malware 2: It only works on non-Apple operating systems, which entails that Apple systems will have to be quarantined (and will lose all data). The financial cost of this is estimated to be $2,000 per Apple computer. Ten percent of the computers in the botnet are Apple ones.

   – Anti-malware 3: It works perfectly on all computers, except on those with some specific UUIDs, Universal Unique Identifiers, assigned by the malware itself. It is impossible to determine the UUID generated by the malware without triggering a malware response that would erase all data. Hence, for every practical purpose, the UUID of each infected computer can be considered unknown and unknowable. It is known, however, that the malware will wipe out all the data if the last numerical digit of the UUID it assigned to device is 0. Since every Arabic numeral has the same chance of being the last numerical digit in these UUIDs, every computer has an ex-ante 10% probability of being wiped out completely and a 90% probability of being rescued completely. The financial cost of this is estimated to be $2,000 per affected computer.

Analyse the situation to determine the preferred type of anti-malware using each of the following six ethical frameworks:

a. Expected Utility Maximisation
b. The Maximin Rule
c. Deontological Theory
d. Rights-Based Theory
e. Contractualism using MiniMax Complaint Principle
f. Ex Ante Contractualism

3. The same questions as in the Exercise 3, but with different numerical values for the financial costs.

   A choice of anti-malware: You are dealing with malware that turns the affected computers into nodes in a botnet performing a distributed denial-of-service attack against servers in an important hospital running 1,000 computers, which risks placing the lives of its patients at risk. You have three anti-malware tools in your arsenal, all of which are effective against the malware. However, the malware is designed to retaliate by wiping out the entire hard disk, as soon as it is disconnected from the malicious server. A preliminary study of the malware shows that it could be fought with three different software approaches. Each of them fails in specific ways to limit the damage. Due to time and resource constraints, you can develop only one of these before the malware spreads, causing morally intolerable human damage. Which one do you develop?

   – Anti-malware 1: it protects all computers but deletes all Excel and Word files during installation. The financial cost is estimated to $1,000 per computer.

   – Anti-malware 2: it only works on non-Apple operating systems, which entails that Apple systems will have to be quarantined (and will lose all data). The financial cost of this is estimated to be $20,000 per Apple computer. Ten percent of the computers in the botnet are Apple ones.

   – Anti-malware 3: it works perfectly on all computers, except on those with some specific UUIDs, Universal Unique Identifiers, assigned by the malware itself. It is impossible to determine the UUID generated by the malware without triggering a malware response that would erase all data. Hence, for every practical purpose, the UUID of each infected computer can be considered unknown and unknowable. It is known, however, that the malware will wipe out all the data if the last numerical digit of the UUID it assigned to device is 0. Since every Arabic numeral has the same chance of being the last numerical digit in these UUIDs, every computer has an ex ante 10% probability of being wiped out completely and a 90% probability of being rescued completely. The financial cost of this is estimated to be $20,000 per affected computer.

Analyse the situation to determine the preferred type of anti-malware using each of the following six ethical frameworks:

a. Expected Utility Maximisation
b. The Maximin Rule
c. Deontological Theory
d. Rights-Based Theory
e. Contractualism using MiniMax Complaint Principle
f. Ex Ante Contractualism

4. A company serving 1,000 customers becomes aware of a vulnerability in their custom-made computer system that potentially could be exploited to damage customer devices on the Internet of Things, and in some cases even cause bodily harm to their customers. It has been estimated that in the case of such an attack, 10% of the company's customers would require device replacement worth $10,000 per customer, and another 1% of customers would suffer bodily harm requiring $1,000,000 worth of treatment per customer. The probability of such an attack in the foreseeable future is estimated to be 50%.

   It is possible to patch the discovered vulnerability and avoid such an attack, but that would require a custom design and would cost around $10,000,000. There are different opinions on the company board on whether they should do nothing or patch the vulnerability. Some members argue that their duty is to their customers, especially when there is a risk of bodily harm. Others are concerned about the high price of the security patch.

   Analyse this situation using the following ethical frameworks to recommend the right decision:

   a. Expected Utility Maximisation
   b. The Maximin Rule
   c. Deontological Theory
   d. Rights-Based Theory
   e. Contractualism using MiniMax Complaint Principle
   f. Ex Ante Contractualism

5. Identify at least 3 ethical issues with using ChatGPT and similar software to write university assignments and analyse them in the context of Virtue, Deontological and Utilitarian ethics.