COSC130 Fundamentals of Cybersecurity and Privacy

Tutorial Week 2 Solutions

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?

   SOLUTION:

   We will denote expected gain by E(Gain).

   We consider all possible outcomes, and for each one, we determine the probability (chance, likelihood) and the gain. The probability for each outcome is a number; the probabilities for all outcomes must add up to 1, otherwise, we did not consider all the outcomes. In this example, there are two outcomes, Peter winning and Peter losing.

   The chance of winning is 10%, which is the same as 0.1 expressed as a number between 0 and 1 (0% corresponds to 0 and 100% corresponds to 1). The gain in the case of winning is $100 – Peter will get $200 but he already paid $100 for the ticket, so his net gain is $100.

   The probability of losing is 0.9 (or 90%), and the gain is -$100 that Peter paid for the ticket.

   We organise this in a table:

	Probability (chance, likelihood)	**Gain**
Win	0.1 (or 10%)	$100
Loose	0.9 (or 90%)	-$100

   To obtain the expected gain, for each outcome we multiply the probability by the gain, and add them all up:
   E(Gain) = 0.1 * 100 + 0.9 * (-100) = 10 – 0.9 * 100 = 10 – 90 = - 80

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

Solution:

a. **Expected Utility Maximisation**
For each of the three solutions, there is a single outcome with probability 1.
Anti-malware 1: E(Gain) = -1000 * 1000 = - 1,000,000
Anti-malware 2: E(Gain) = - 100 * 2,000 = - 200,000
Anti-malware 3: E(Gain) = - 100 * 2,000 = - 200,000
We should choose Anti-malware 2 or 3. Other considerations may be used to resolve the tie, including what is stored on each computer.

b. **The Maximin Rule**
We compute the gain for the worst outcome. As there is a single outcome in each of the solutions, the result will be the same as in a).
Anti-malware 1: Worst_Outcome_Gain = -1000 * 1000 = - 1,000,000
Anti-malware 2: Worst_Outcome_Gain = - 100 * 2,000 = - 200,000
Anti-malware 3: Worst_Outcome_Gain = - 100 * 2,000 = - 200,000
We should choose Anti-malware 2 or 3.

c. **Deontological theory**
Here we assume that the only relevant duty/obligation is to protect life.
Anti-malware 1: No loss of life
Anti-malware 2: No loss of life
Anti-malware 3: No loss of life
We can choose any of the three solutions.

d. **Rights-Based Theory**
We assume that the only relevant right is the right to life.
Anti-malware 1: No loss of life
Anti-malware 2: No loss of life
Anti-malware 3: No loss of life
We can choose any of the three solutions.

e. **Contractualism using MiniMax Complaint Principle**
We compute gains for the strongest individual complaint and select the minimum.
Anti-malware 1: Gain = -1,000
Anti-malware 2: Gain = - 2,000
Anti-malware 3: Gain = - 2,000
We should choose Anti-malware 1.

f. **Ex Ante Contractualism**
We compute expected gains for the strongest individual complaint and select the minimum.
Anti-malware 1: E(Gain) = -1000

Anti-malware 2: E(Gain) = - 2,000
Anti-malware 3: E(Gain) = - 0.1 * 2,000 + 0.9 * 0 = -200 +0 = -200
We should choose Anti-malware 3.

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

Solution:

a. **Expected Utility Maximisation**
For each of the three solutions, there is a single outcome with probability 1.
Anti-malware 1: E(Gain) = -1000 * 1000 = - 1,000,000
Anti-malware 2: E(Gain) = - 100 * 20,000 = - 2,000,000
Anti-malware 3: E(Gain) = - 100 * 20,000 = - 2,000,000
We should choose Anti-malware 1.

b. **The Maximin Rule**
We compute the gain for the worst outcome. As there is a single outcome in each of the solutions, the result will be the same as in a).
Anti-malware 1: Worst_Outcome_Gain = - 1000 * 1000 = - 1,000,000
Anti-malware 2: Worst_Outcome_Gain = - 100 * 20,000 = - 2,000,000
Anti-malware 3: Worst_Outcome_Gain = - 100 * 20,000 = - 2,000,000
We should choose Anti-malware 1.

c. **Deontological theory**
Here we assume that the only relevant duty/obligation is to protect life.
Anti-malware 1: No loss of life
Anti-malware 2: No loss of life
Anti-malware 3: No loss of life
We can choose any of the three solutions.

d. **Rights-Based Theory**
We assume that the only relevant right is the right to life.
Anti-malware 1: No loss of life
Anti-malware 2: No loss of life
Anti-malware 3: No loss of life
We can choose any of the three solutions.

e. **Contractualism using MiniMax Complaint Principle**
Anti-malware 1: Gain = -1,000
Anti-malware 2: Gain = - 20,000
Anti-malware 3: Gain = - 20,000
We should choose Anti-malware 1.

f. **Ex Ante Contractualism**
Anti-malware 1: E(Gain) = -1,000
Anti-malware 2: E(Gain) = - 20,000
Anti-malware 3: E(Gain) = - 0.1 * 20,000 + 0.9 * 0 = -2,000 +0 = -2,000
We should choose Anti-malware 1.

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

Solution:

a. **Expected Utility Maximisation**
Do nothing:

	Probability (chance, likelihood)	**Gain**
No attack	0.5 (or 50%)	0
Attack	0.5 (or 50%)	1) 10% of customers will lose $10,000 each What is 10% of 1,000 customers? It is 0.1 x 1,000 = 100 customers. Then the loss is 100 x $10,000 = $1,000,000

		2) 1% of the customers will lose $1,000,000 each What is 1% of 1,000 customers? It is 0.01 x 1,000 = 10 customers. Then the loss is 10 x $1,000,000 = $10,000,000 The total loss is $1,000,000 + $10,000,000 = $11,000,000 The total gain is then -$11,000,000

E(Gain) = 0.5 * 0 + 0.5 * (-11,000,000) = -5,500,000

E(Gain) = 0.5 * 0 + 0.5 * (0.1*1000*(-10,000)+0.01*1,000*(-1,000,000)) = 0 – 0.5 * (1,000,000 +10,000,000) = -5,500,000

Security patch:

E(Gain) = - 10,000,000

Recommended solution: Do nothing.

b. **The Maximin Rule**

Do nothing:

Gain = 0.1*1000*(-10,000)+0.01*1,000*(-1,000,000) = – 1,000,000 - 10,000,000 = -11,000,000

Security patch:

Gain = - 10,000,000

Recommended solution: Security patch.

c. **Deontological Theory**

Do nothing:

Obligation to protect customers from bodily harm not honoured.

Security patch:

No bodily harm.

Recommended solution: Security patch.

d. **Rights-Based Theory**

Do nothing:

Right of customers to safety violated.

Security patch:

Right not violated.

Recommended solution: Security patch.

e. **Contractualism using MiniMax Complaint Principle**

Do nothing:

E(Gain) = - 1,000,000

Security patch:

E(Gain) = - 10,000,000

We need to decide how the $1,000,000 loss for an individual compares to $10,000,000 for a company.

f. **Ex Ante Contractualism**

Do nothing:

E(Gain) = - 0.01 * 1,000,000 = -10,000

Security patch:

E(Gain) = - 10,000,000

We need to decide how the $10,000 loss for an individual compares to $10,000,000 for a company.

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.

Solution:

Note that there is no single correct answer to this question. Many thanks to COSC130 class for their input and contribution.

1) Academic dishonesty – assignments generated by ChatCPT is presented as the student's own work.
2) At some universities including UNE, students are required to sign some form of

declaration that they will not engage in plagiarism, so by using ChatGPT they are breaching that declaration as well.
3) Statements made in ChatGPT-created assignments may be incorrect.
4) Assignments are meant to help students learn – by using ChatGPT, students are not learning.
5) If the students do not learn, there may be a discrepancy between their degrees and actual knowledge, which may be seen as fraudulent; it may also impact student's performance at the workplace, as well as performance of the company/society.

It is easy to argue that the above points speak against using ChatGPT for this purpose in both virtue and deontological ethics. For example, a person of good character should not engage in plagiarism.

In terms of utilitarian ethics, while one may argue that there are some short-term benefits to students using ChatGPT in this way, one could argue that not using ChatGPT is more beneficial to students and society at large.