Attack-Defense Tree Project

This project is for a grade.

This project is also part of a study, and if you consent to your responses being used to further our understanding of ADTs, please fill in the consent form either in-person, via email or via Brightspace. Regardless of your participation in the study, you still have to do the project. Your participation in the study will NOT affect your grade.

There are **3** parts to this project. Starting with part 1.0, the assignment is graded.

The perception questions are graded. There is no correct answer, and they are graded based on completion.

The immediately following **3** questions are **optional**. They help us further our understanding of ADT comprehensibility. These questions will not affect your grade.

- How many years of programming experience do you have?
- Did you attend the lecture on Threat Modelling?
- Had you heard of threat models before this lecture? If yes, which?

1 Assembling ADTs

1.1 Task Questions

The following attack **leaf** nodes are provided. The overall goal of this scenario (and thus the root node of the tree) is **Rob bank**. Assemble an attack-defense tree using these leaf nodes. You may add any intermediary nodes you wish.

Attack leaf nodes:

- Hire Outright
- Promise part of the stolen money
- Threaten insiders
- Buy tools
- Steal tools
- Gain Access
- Walk through front door
- Locate start of tunnel
- Find direction to tunnel

Defense leaf nodes:

- Personnel Risk Management
- Check employee financial situation

1.2 Perception Questions

The following questions are all about your perceptions. This helps us to understand your experience with these structures. We hope this will guide the development of these structures.

For the first set of questions, the response should be according to the following likert scale.

1. Totally agree
2. Somewhat agree
3. Neither agree nor disagree
4. Somewhat disagree
5. Totally disagree

The second set of questions is a short response section. Please provide us a short description of your thoughts.

You are graded on this section. There is no correct answer. Your grade is determined based on your effort. If you respond to all the questions and provide a reasonable amount of effort on the short response questions, you will get full marks.

1.2.1 Likert Questions

1. I find the structure of attack tree easy to understand
2. Given all the nodes of an attack tree, it is easy for me to assemble the tree
3. Given only the leaf nodes of an attack tree, it is easy for me to assemble the tree.
4. I would rather define my own intermediary nodes
5. The process of assembling the attack tree helped me better understand the attack scenario.

1.2.2 Short Response Questions

1. What did you find most difficult about this task? Why?
2. How did you go about solving this task? What was your methodology?

2 Building ADTs

The following text scenario is provided for you. Please create a complete attack defense tree **of this scenario**. **Do not add extra information that is not in the scenario**. Try to encapsulate the entire scenario with an attack-defense tree (don't leave any aspect of the attack scenario out).

Scenario:

The goal is to open a safe. To open the safe, an attacker can pick the lock, learn the combination, cut open the safe, or install the safe improperly so that he can easily open it later. Some models of safes are such that they cannot be picked, so if this model is used, then an attacker is unable to pick the lock. There are also auditing services to check if safes and other security technology is installed correctly. To learn the combination, the attacker either has to find the combination written down or get the combination from the safe owner. If the password is such that the safe owner can remember it, then the safe owner would not need to write it down.

2.1 Perception Questions

The following questions are all about your perceptions. This helps us to understand your experience with these structures. We hope this will guide the development of these structures.

For the first set of questions, the response should be according to the following likert scale.

1. Totally agree
2. Somewhat agree
3. Neither agree nor disagree
4. Somewhat disagree
5. Totally disagree

The second set of questions is a short response section. Please provide us a short description of your thoughts.

You are graded on this section. There is no correct answer. Your grade is determined based on your effort. If you respond to all the questions and provide a reasonable amount of effort on the short response questions, you will get full marks.

2.1.1 Likert Questions

1. I prefer reading attack trees to text descriptions of attacks.
2. The process of building the attack tree helped me better understand the attack scenario.

2.1.2 Short Response Questions

1. What did you find most difficult about this task? Why?
2. How did you go about building the ADT? What was your methodology?
3. What was the first node you added to your tree?

3 Creating ADTs

Construct an attack defense tree of a scenario of your choice. Your tree should be complete (covers all reasonable attack scenarios) and reasonably large.

3.1 Perception Questions

The following questions are all about your perceptions. This helps us to understand your experience with these structures. We hope this will guide the development of these structures.

For the first set of questions, the response should be according to the following likert scale.

1. Totally agree
2. Somewhat agree
3. Neither agree nor disagree
4. Somewhat disagree
5. Totally disagree

The second set of questions is a short response section. Please provide us a short description of your thoughts.

You are graded on this section. There is no correct answer. Your grade is determined based on your effort. If you respond to all the questions and provide a reasonable amount of effort on the short response questions, you will get full marks.

3.1.1 Likert Questions

1. The process of creating the attack tree helped me better understand the attack scenario I selected.
2. I feel I could have achieved the same understanding by writing a text description of the attack.
3. The ADT I created would help me communicate my threat scenario.

3.1.2 Short Response Questions

1. What did you find easy about using ADTs?
2. What did you find difficult about using ADT?
3. Do you think ADTs have a place in the cybersecurity industry? If so, where? If not, why not?
4. What aspects, if any, do you think are missing from ADTs?
5. Do you hope to encounter ADTs in the future?