

Cheat sheet tips:

- Risks lecture 1 en 2 are important to write down.
- Lectures of Christina Kolb are important for the test, ignore the company lectures.

Practice Exam (during lecture)

According to this course, what vocabulary belongs to security?

- ✓ Probability
- ✓ Threats
- ✗ Failures

According to this course, what vocabulary belongs to safety?

- ✓ Cost
- ✓ Extended multilevel model
- ✗ Attack trees
- ✗ Intended behaviour

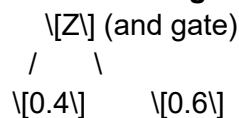
Note: fault trees = safety, attack trees = security.

What are the different elements that make up the structure of an attack tree?

Answers:

- Basic events (start of the attack)
- Intermediate events (Following states after start)
- Top event (Goal of the attack)
- Logic Gates: and/or
- Probability/cost/time

Following the attack tree, calculate the cost of Z



Answer: 1

Name all security types of the CIA triad (e.g. What does CIA stand for?)

Answer:

- Confidentiality
- Integrity
- Availability

Name all elements of the extended multi-level model

Answer:

- Human level
- System level
- Sub-system level
- Information level
- Component level

Which of the security types of the CIA triad are present on the different levels of the extended multi-level model?

Answer: All!

Availability = the system should be available

Integrity = when the system doesn't maintain integrity, the system will break

Confidentiality = You want the data a robot collects or processes on the information level to be confidential

What is the cyber intrusion kill chain?

A set of steps that must be taken in order to attack a system.

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command & Control
- Actions on Objective

When should you use the cyber kill chain v.s. Stride?

Answer:

Killchain: very detailed steps

STRIDE: broader approach

Note: the practice exam is based on the beginning of the course.

Real Exam:

The questions I managed to remember/collect so far are: (there may be mistakes)

1a According to this course, what vocabulary belongs to security?

- Attacks ✓
- Threats ✓
- ? ✗
- Unintended behaviour ✗

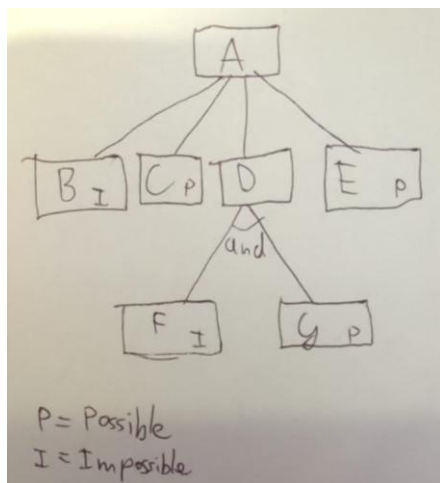
1b According to this course, what vocabulary belongs to safety?

- Cost ✗
- Extended multi-level model ✓
- Fault trees ✓
- ? ✗

2a. Name all attack tree components as explained in this course.

Answer:

- Basic events (start of the attack)
- Intermediate events (Following states after start)
- Top event (Goal of the attack)
- Logic Gates: and/or
- Probability/cost/time



2b. From the given attack tree above (ofc, with actual info instead of A, B, C, etc), indicate what parts of the attack tree correspond with the terms of 2a.

Possible answer:

- Top Event: A
- Intermediate Event: D
- Basic Events: B, C, D, F, G
- Probabilities: P, I
- Logic gates: <drawing of the different connections>

2c. Calculate the probability of event X ([0.7] -- [X, AND] -- [0.8])

Answer: 0.56

3a. Name each element of the CIA triad and define what they mean. Both the words and the meaning.

3b. What levels are in the extended multi-level model?

3c. What elements of the CIA triad apply to the extended multilevel model?

Answer: All

3d. For each of the elements of the extended multi-level model, write down an example for each of the elements of the CIA triad.

4a. Name all STRIDE stages and explain what they mean.

4b. What is the difference between STRIDE and NIST?

4c. Explain NIST by applying each step to a case (think one of yourself).

4a. Name all NIST phases and explain what they mean. (RESIT)

4b. How does NIST compare from STRIDE? (RESIT)

4c. Give an example of a case where you would use STRIDE instead of NIST, by applying each of the components from STRIDE. (RESIT)

5a. Name 3 principles of persuasion and 1 risk

5b. Give 4 examples of a safety problem and a cybersecurity problem, and use the principles and risk from question 5a.

5c. For the examples in 5b, what are the economical stakeholders and explain further safety/security implications.