Conclusion

Riccardo Scandariato

Institute of Software Security, TUHH, Germany

scanda***to @ tuhh**.**de

MSc Course "Secure Software Engineering"

Marketing ☺

- NEW COURSE !!!

- Cybersecurity Data Science (MSc)
  - Solving security problems…
  - …using ML/AI

- SoSe 22-23

- Lecture (3 CP) + Project (3 CP)
  - Similar structure as the "Secure SW Eng" course

Agenda

- Exam preparation
- Course discussion

EXAM PREPARATION

Format

- Five questions

- Question [20pts]
  – Short text to intro to topic
  – 4 sub-questions, [5 pts] each
- Or a case study [20 pts]
  – Case description
  – Couple of exercises, [10 pts] each

- Total of **100 points**

Grading

[50, 54]   →   4.0

[55, 59]   →   3.7

[60, 64]   →   3.3

[65, 69]   →   3.0

[70, 74]   →   2.7

[75, 79]   →   2.3

[80, 84]   →   2.0

[85, 89]   →   1.7

[90, 94]   →   1.3

[95, 100]   →   1.0

- Just a guideline
- E.g., upgrade possible

What [is / is not] in the exam

- Included
  - All lectures (see below)
  - Project labs

- Not included
  - Guest Lecture 12 (no slides)

Example question

Describe / reflect / connect / compare

- (5 pts) **Describe.** What are the threat categories of the STRIDE acronym? Provide an example of generic threat for each category

- (5 pts) **Connect.** How are the STRIDE categories related to security objectives (like CIA)?

- (5 pts) **Describe.** Describe how STRIDE works. Why is it called a model-based and knowledge based technique?
  - **Reflect**: challenges? Plus/cons

- **Compare.** Difference and similarities between threat analysis with MUCs and with STRIDE? **Reflect.** E.g., can they be applied at the same level of abstraction?
  - **Describe.** What is the input for both techniques?
  - **Describe.** What is the final outcome of a threat analysis with MUCs?
  - **Reflect.** Can STRIDE threats be uses to derive SRs? If yes, how? If no, why?

Case study question

Do

- "Here is the description of a small application."

  – (10 pts) Model it as a DFD. Explain your choices. What aspects are important to model from the perspective of a security analysis?

  – (10 pts) (Here is the DFD) find and describe 3 threats: type, location, scenario

IN SUMMARY

I care about

- Conceptualization, enablers, principles behind the scenes
(how something is possible, what is the mechanism involved from a conceptual point of view)
- Motivations
(why things are done in a certain way)
- Examples
- Identifying connections between concepts
  - Similarities / Differences
  - Advantages / Disadvantages
- Precise/technical language

Do not

- Answer with one line or with a bulleted list of keywords

  – **Argument your answer, explain terms, provide an example, etc**

- Use unscientific reasoning (e.g., "and this is bad")

  – Def of "bad"

  – Why is it "bad" (e.g., consequences)

  – Is it always "bad"?

THANK YOU !!!

Thank you for weaking up early ☺
It was a pleasure to have you in my class