Questionaire on

Subject of Examination (legible if possible ;)) SPIS

Security and privacy in Information Systems

☒ Oral
○ Written

○ Oral Reexamination

Date: Feb. 2020
Duration: 15 min

Examiner: Prof. Rafael Schaefer
Programme of Study: ET

Preparation

a) Continuous attendance at lectures? ☒ Yes ○ No

b) Effects of a): ☒ Positive ○ None ○ Negative

c) Amount of time spent on preparation: 1,5 days ☒ by yourself ○ group work

d) Prior knowledge from other lectures/practical experiences?

Information Theory

e) What resources did you use? (*literature, websites etc.*)

slides, lecture notes ← ~~could [illegible]~~

f) Can you give any advice on the preparation of this exam?

understanding concepts and talking about those is good. no detailed proofs needed (in my case at least) If you can support your thesises using Math, do that!

↑ inform. theory!

Exam

a) Had there been any agreements on form or contents of the exam? Were they met?

only lecture Topics / not presentated topics / Yes

b) Advice on behaviour during the exam:

chilled atmosphere, make it at your pace!

c) Examination style: (*atmosphere, questions: clear or unclear, in depth knowledge or general questions, specific interposed questions, specific questions in case of knowledge gaps, . . . ?*)

Questions very general. Tell him what you know about the topic what you want to explain. Asks further, if sth. not explained clearly and he knows, you know it

Other questions

a) How were you graded? (*optional of course*) 1.0

b) Do you think this grade is appropriate? ☒ Yes ○ No (*why not?*)

c) Would you recommend this exam? ☒ Yes (*to whom especially?*) ○ No (*why not?*)

anyone who wants to know about Information theory

d) Do you have any other advice or remarks about this exam?

Lecture progresses slowly. not too much in there, no fear!

Contents of the Exam: Please try to reproduce as many questions as possible. At which points did the examiner ask for derivations, at which for analytic proof? *(If the space here is not sufficient do not hesitate to add additional sheets. But please staple the pages and number them.)*

- PIR

↳ 1st scheme $C^* = \frac{1-\frac{1}{n}}{1-(\frac{1}{n})^K}$

↳ secret sharing scheme $C^* = 1-\frac{1}{n}$

↳ name Capacity C^*!

- Differential Privacy ϵ-DP what is it

o ↳ LPM
EPM
FPM
SPM

what is best to use,
what are drawbacks (LPM ggf. low utility)

o Serial / parallel usage

- Biometric Authentication
  - difference security / privacy

$$\begin{tikzcd} & K_1, W_1 \\ X^n \arrow[ur] \arrow[dr] & \\ & K_2, W_2 \end{tikzcd}$$

$I(W_1; X^n) \overset{!}{\le} \delta$
⇒ Markoff
⇒ so that $I(W_n; K_n)$ also small

no proofs.
no technical calculations

Thank you for your help! **Your fellow students.**