Usable Security & Privacy, Evaluation 1

CS60081, Autumn 2020

8:15 pm to 9:20 pm, 7th October, 2020
Full marks: 60
Answer ALL questions

IMPORTANT INSTRCUTIONS

Taking the exam: You need to log into zoom, keep your video on during taking the test (so that we can monitor you during the exam). You will use pen and paper to write the exam,

Decorum: Throughout the examination, you are strictly expected to have their cameras on, directing towards their workspace including themselves. Arrange your laptops/desktops/mobiles beforehand to save time during the examination. Disconnecting video for a long duration will be grounds for suspecting malpractice.

You need to keep your workplace, your hands and your mobiles visible to us. We are trying to avoid the visibility of your answers in the papers to the rest of them. Once you open your question paper, refrain yourself from using your PC/laptop from searching for anything or typing during the exam.

Tip: Install Adobe scan and, MS Teams in your phone to make the whole process easier. In that case, your laptop acts as a camera, while you are using your mobile for checking the questions, scanning and uploading the answers.

Submission: You can do either of two things (i) take pictures of your answer script pages, name the pictures page1.jpg, page2.jpg, page3.jpg etc., zip the pictures and upload the zipped file via CSE Moodle. (ii) Put all the pages sequentially in a pdf file and upload the pdf to KHARAGPUR Moodle. YOU HAVE TO USE PEN AND PAPER TO GIVE THE EXAM.

Policies: Note that, if we face problems with your answer script e.g., cannot open your submitted zipped file, cannot read the text in pictures (due to bad resolution), cannot determine the page order from the file names (or the pages in the pdf is jumbled up), or we find you copying, it will affect your marks.

Malpractice: If any group of students found to have similar work in their answer sheets, all of them will receive the maximum penalty with no grace. We expect you to not take help from the internet, your copies, textbooks, slides or video recordings during the exam. Note that this is not an open-book exam. If found otherwise, you will be penalized.

PLESE WRITE YOUR NAME AND ROLL NO. ON THE TOP OF THE FIRST PAGE OF YOUR ANSWER SCRIPT. WE WILL NOT EVALUATE YOUR ANSWER SCRIPT WITHOUT IT.

Question 1. Please answer each of the question below (for Multiple choice questions you need to choose ALL the correct answers to a question) [**2 x 5 = 10]**

1.1. In the "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook" paper, how was the survey takers compensated (answer in 1 sentence).

1.2. From "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0" paper, explain any two "irreversible" actions (one sentence per action).

1.3. Menlo report introduced an explicit principle for ethical studies "Respect for Law and Public Interest". In Belmont report which principle contained this principle of "Respect for Law and Public Interest"? Why (Explain in one sentence)?

Beneficen

1.4. In "Privacy Wizards for Social Networking Sites" paper, using what method did Fang et. Al. chose the friends to label? Please explain the process in no more than 3 sentences.

1.5. In the "Social Phishing" paper, describe (1-2 sentence each) two gender-based characteristics that Jagatic et. Al. has shown to have *increased* the clicking rate on phishing emails.

1. Females more likely to click on phishing mails in general

Question 2. Choose the correct answer for each of the questions (write down all that apply) **[3 x 2 = 6]**

2.1. Which of the following is not a typical component of a consent form?

A) Debrief
B) Risks and benefits
C) Purpose of study
D) Procedures

2.2. study is said to have ecological validity if:

A) It uses environmentally-friendly supplies and has a small carbon-footprint
B) It can be generalized beyond the study's research setting
C) It uses a representative sample of participants selected at random
D) Participants perform realistic tasks in an environment that approximates the real-world environment where such tasks would be performed

2.3. Which of the following should you typically do while conducting deceptive studies, in order to meet ethical requirements?

A) Make sure the participants do not find out the purpose of the study at any point
B) Inform participants at the beginning of the study that deception may be used
C) Pay the participants
D) Debrief the participants at the end of the study

Question 3. A new IIT Kharagpur student, Prabhat, has not taken the Usable Security and Privacy class. Prabhat asks you for help with a survey he is conducting to explore the susceptibility of IIT Kharagpur affiliates to password guessing attacks (attacker guessing the password for each user) in social media. You read Prabhat's survey draft and tell him that it's a good thing he came to you for advice! Every question seems to have a problem. Edit each question and/or its answer choices to minimize the confounds and other serious issues present in each question. **[8 x 3 = 24]**

3.1 Have you ever fallen victim to a password guessing attack?

_____Yes _____No

3.2. IIT Kharagpur's good password creation training is easy to follow:

____ Strongly agree ____ Agree ____ Neutral ____ Disagree ____ Strongly disagree

3.3. How do you access Facebook?

_____ On browser _____On my Android or iPhone

3.4. I am more diligent about protecting against password guessing attacks when using my Facebook account than when using my Twitter account.

_____Strongly agree _____Agree _____Neutral _____Disagree _____Strongly disagree

3.5. Rate your technical expertise on a scale of 1 (lowest) to 5 (highest).

____1 (lowest) _____2 _____3 _____4 _____5 (highest)

3.6. How much do you hate typing in the password to log into Facebook?

_____A little _____Some _____A lot

3.7. How many times have you fallen victim to a password guessing attack in the past year?

_____

3.8. How often do you believe someone is launching a password guessing attack on you?

_____ Very often _____Somewhat _____often _____Not very often at all

---

Question 4. Prabhat is now trying to make the study even better. **[3 x 2 = 6 marks]**

4.1 Why might the findings of this study not apply to the average Internet user (give three distinct reasons)?

4.2. Due to this survey being distributed to IIT Kharagpur students, what specific type of validity does this experimental design lack? Give the specific term, as well as an explanation of why it lacks this type of validity (answer in maximum 3 sentences).

4.3. Instead of running a survey, Prabhat decides to run an in-person lab study in which participants use a simulated social media login screen and try to guess the password of other participants. What specific type of validity would this experimental design lack? Give the specific term, as well as an explanation of why it lacks this type of validity (answer in maximum 3 sentences).

Question 5. Prabhat is feeling encouraged and wants to do another study. This study will take place on the IIT Kharagpur campus with IIT Kharagpur students (assume a non-pandemic situation) **[4 x 2 = 8 marks]**

Each day for a week, Prabhat recruits IIT Kharagpur students to participate in his study. People are paid 5,000 INR to participate for one hour, and they can participate as many times as they want.

Prabhat assigns prospective participants who have iPhones to Group A and participants who have Android phones to Group B.

Participants in Group A read newspaper articles about the surveillance society (how everyone is watching you), while participants in Group B read newspaper articles about the glorious history of Kharagpur city. Participants in both groups then answer a 20-question survey designed to capture privacy attitudes.

Prabhat enters the names of all participants who completed the survey thoroughly into a lottery for an additional INR 10,000. At the end of each day, Prabhat emails all participants and tells them who won the gift certificate so he or she can collect it the next day.

Answer each of the questions below in no more than 5 sentences.

5.1 What's wrong with letting people participate as many times as they want?

5.2 What are at least two ways in which IIT Kharagpur students are not representative of the general population?

5.3 Prabhat runs the study. Based on his data group A chose stronger passwords. So he concludes that using an iPhone leads an individual to have higher privacy concerns. Why is making this type of conclusion problematic? Give two reasons.

5.4. Why is compensating participants INR 5,000 problematic?

Question 6. You want to check if reading academic security research papers help a student to use cryptographic function calls in coding *correctly*. **[1 + 2 + 3 = 6 marks]**

6.1. Write ONE research question (as a relation between variables).

6.2. For each of the variables in your research question, describe how you would measure it.

6.3. Describe how would you design a study to address the research question within 10 sentences (please be specific).