Usable Security & Privacy, Evaluation 2

CS60081, Autumn 2021

3:00 pm to 3:50 pm, 5th October 2021
Full marks: 40
Answer ALL questions

IMPORTANT INSTRUCTIONS

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 from using your PC/laptop from searching for anything or typing during the exam.

Tip: Install Adobe scan and MS Teams on 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 is 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.

PLEASE 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 | 2.5 x 4 = 10 marks

A deep fake based attack is a type of social engineering attack where the attacker uses a machine generated image/video content in which a person's face is morphed with someone else's. Deep Fake based attacks are often used to create memes, to defame someone etc.

A new IIT kgp student, Ankita, wants to study about deep fakes and its corresponding awareness among the IIT kgp faculties. Her study includes the concepts of both phishing and deep fake based attacks. Ankita began to design a study to evaluate his concept in which IIT kgp faculties (across all departments) would receive training about the attacks. During the training, they would receive a fraudulent email containing a link and an attached video of the Director of the institute, addressing them to click on the link and to fill up the form (in actuality the video is a deep fake based video made by Ankita which the director has no clue about). Ankita will then measure the proportion of recipients who clicked on the phishing link for evaluation of his idea. Please answer the questions below.

1.1. Ankita got to know that she needed to have a design for his experiment and she can choose from "between subjects" and "within subjects" design. Explain (1-3 sentences each) what each of these designs are in her particular context.

1.2. What should be an appropriate control condition that Ankita would use in his study if she intends to go for between-subjects design for his study.

1.3. Is the study externally valid? Why or why not?

1.4. What possible confusion do Ankita want to avoid by not informing the participants or the Director beforehand that she will use the Director's video to falsify credible information and to send an email that will look fraudulent to test the effectiveness of the training they took?

Question 2 | (1.5 x 2) + 2 +2 = 7 marks

Ankita now decides to run a qualitative interview study to understand how the faculties in IIT Kharagpur are dealing with the deep fake based attacks. She decided to record the interviews of his participants and then transcribe the data into text for analysis. Answer the following questions.

2.1. Which coding technique might Ankita use to answer each of the questions? Why? (Just naming the technique will not be awarded any marks)

A) After the training, which broad deep fake attack strategies those participants are using?

B) What exact tools are these participants using to protect themselves to increase their privacy so that their credentials do not get stolen and they don't become the victim of deep fake based attacks?

2.2. Why would it be important for Ankita to have a second person also participate in the process described in Part 2.1? Give one clear reason.

2.3. Ankita is told to prepare an IRB submission. What purpose does the IRB serve in human-subjects research? Give two purposes and explain briefly (1-3 sentence)

Question 3 | 5 + 2 = 7 marks

This question is based on the definition of Cohen's kappa metric. Please show the calculation / explain your answers for each question (stating only answers will not be awarded marks).

3.1. Imagine during coding two coders C_1 and C_2 are assigning any one of the k labels L_1, L_2, L_3 … L_k to each piece of text. Ultimately, they arrived at the following confusion matrix after one round of coding:

		Coder C2				
		L_1	**L_2**		**L_{k-1}**	**L_k**
Coder C1	**L_1**	kn	(k-1) n	. . .	2n	n
	L_2	n	kn	.	3n	2n
	L_3	2n	n	.	4n	3n
	…	…	…	.	…	…
	L_{k-1}	(k-2)n	(k-3)n	.	kn	(k-1)n
	L_k	(k-1)n	(k-2)n	.	n	kn

Compute the Cohen's kappa for this table and show that in this labelling for all k > 1 and n>1, 0 < Cohen's kappa < $\frac{1}{k}$

3.2. From the Cohen's kappa value found above identify one problem with the coding process? How do you systematically resolve the problem?

Question 4 | 1+1+ 1.5+ 1.5+2 = 7 marks

Please answer the following questions.

4.1. Please choose the desired outcomes that surveys are useful for. Choose all that apply

A) Understand the target population, mental models
B) How do people interpret the functionalities of an interface?
C) What do people think after they use a system?
D) Do people think that a particular functionality A is not equivalent to a particular functionality B?

4.2. Which of the following is not a typical component of a consent form? Choose all that apply

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

4.3 Edit the question and/or its answer choices to minimize the confounds and other serious issues present in each question.

"Do you believe that you should update your phone number to Google and change your password every three months?"

_____ Yes _____ No

4.4 Edit the question and/or its answer choices to minimize the confounds and other serious issues present in each question.

Have you ever fallen victim to a phishing attack? Yes No

_____ Yes _____ No

4.5. Identify **two problems** with the following research study protocol.

Participants are randomly selected and randomly assigned into two groups. Both groups are tasked with using Steam (a popular online-only game store) credits, funded by the researchers, to buy in-game items from their newly developed game, *A New Beginning*. Group A is tasked with buying swords for 1000 credits. Group B is tasked with buying shields for 100 credits. An evaluation of the usability of purchasing items in the in-game store will be done through analyzing timing data.

Question 5 | (2 + 2) + 3 + 2 = 9 marks

Please answer the following questions

5.1. In the "Privacy Wizards for Social Networking Sites" paper LeFevre et. al. designed the privacy wizard system.

a) State four requirements of the privacy wizard system.
b) List the two research questions of the paper regarding evaluation of privacy wizard.

5.2. In "Quantifying the Invisible Audience in Social Networks" paper Bernstein et al. investigated how users' perceptions of their audience map onto reality. State and explain three primary components of the investigation (1-2 sentences each).

5.3 In "The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research ", the Beneficence principle reflects the concept of appropriately balancing probable harm and likelihood of enhanced welfare resulting from the research. Explain what would you do to ensure beneficence in your research study design and why.
