INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR

Mid-Autumn Semester Examination 2022-23

Date of Examination: ______________ **Session: (FN/AN)** ____ **Duration: 2 hrs** **Full Marks:** 50

Subject No. : CS60081 **Subject :** Usable Security and Privacy

Department/Center/School: Department of Computer Science and Engineering

Specific charts, graph paper, log book etc., required N/A

Special Instructions (if any) : N/A

Instructions:

- *This question paper consists of THREE (03) pages and FIVE (05) questions.*
- *Attempt all questions. All parts of the same question must be answered together.*
- *Make reasonable assumptions if necessary, and state any assumptions made. No clarification can be provided in the examination hall.*
- *All working steps must be shown. Writing the answer without showing steps will not be given any credit. You can use calculators.*

Question 1. Please answer each of the questions below briefly.

[1 + (1 + 1) + (1 + 2) + 1 + 1 + 2 = 10]

1.1. Please answer the following questions about the "Imagined communities" paper by Acquisti et al.

1.1.1. The paper is about Facebook privacy, but asked participants about "threat of terrorism" in the survey, why? (one sentence)
1.1.2. What were the method(s) of recruitment for this study? Why did the authors choose these method(s) (1—4 sentence)
1.1.3. What are two potential problems with *validity* of the results reported in the paper? Why the findings of the paper still useful?

1.2. Please answer the following questions about the paper "*Evaluating the Contextual Integrity of Privacy Regulation: Parents' IoT Toy Privacy Norms Versus COPPA*" by Apthorpe et al.

1.2.1. State the common provenance behind data privacy protection laws across countries as explained in the paper (1 to 3 sentences).
1.2.2. Fill in the blank: COPPA laws are only applicable to data collection from children under age ________________"
1.2.3. State any two results that the authors concluded from their study. One sentence per result.

Question 2. Answer these short questions (2—4 sentences each)

[2 x 5 = 10]

2.1. Other than attention check questions (e.g., *please click option C in this question*), mention two distinct strategies to detect if a survey-taker is just clicking through your survey without reading them.

2.2. Suppose that it is revealed that a doctor is recording the interaction with the patient without the patient's explicit permission. Using contextual integrity theory identify which of the contextual parameter value or values are violated in this scenario according to social norms. Why?

2.3. Assume, you are marked as an Engineer in a phone directory service, but you are a Doctor. You come to know about this issue and contact the phone directory service for changing your expertise to Doctor. However, they asked 1,000 INR for changing this entry. Which Fair Information Practice Principle (FIPP) is this phone directory service violating? Why?

2.4. State TRUE or FALSE: A system without authentication can provide authorization guarantees. How? (no marks without explanation)

2.5. You wanted to check how many members of KGP InfoPriv Society (KIPS) somehow exploited ERP using security bugs and have seen data that they are not authorized to access. You asked direct questions to a few KIPS members you personally know regarding exploiting ERP system. Name and briefly describe two confounds in your design that will potentially bias your results.

Question 3. Mayank, a student of IIT KGP, and a Gymkhana member is trying to understand the susceptibility of campus community towards phishing attacks and whether current configuration of institute firewall configuration is making the users more secure. He did not take a Usable Security and Privacy class so he requested your help to review his survey. You read Mayank'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.

[2 x 8 = 16]

3.1. Completing a phishing training from IIT KGP will definitely help me to protect against phishing attacks

______Strongly agree ______Agree ______Neutral ______Disagree ______Strongly disagree

3.2. The IITKGP filewall blocking some of my emails is annoying for me

______Strongly agree ______Agree ______Neutral ______Disagree ______Strongly disagree

3.3. I am more alert about checking for phishing attacks when reading messages in my IITKGP inbox than when reading messages in my personal Gmail inbox.

______Strongly agree ______Agree ______Neutral ______Disagree ______Strongly disagree

3.4. How much do you hate receiving emails that containing links?

______A little ________Some ______A lot

3.5. How many times have you fallen victim to a phishing attack in the past year? ______________

3.6. Have you ever used Telegram software for sharing pirated movies?
____ Yes ____ No

3.7. Did your computer ever get compromised?

____ Yes ____ No

3.8. Are you an expert in using any of the following systems? Tick all that apply.

_____ iOS _____Android _______Linux ____Windows

Question 4. BEST is a new password manager. It allows users to store their passwords and view them whenever required, obviously after authorization. BEST smartly avoids the trouble of making the user remember a master password, and allows access via voice recognition to the stored passwords. Users are required to register their voice at the time of installation. The same is used to access the passwords or change the registered voice in future.

You, as a Usable Security and Privacy student, are tasked with the security analysis of the BEST password manager system.

[2 + 2 + 2 + 1 = 7]

4.1. Write one threat model for protection against unauthorized password access in BEST. Please list attacker action, capability, and access in your threat model.

4.2. Write ONE research question (as a relation between variables) to compare the ease of access b/w using a master password and voice recognition for viewing the passwords.

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

4.4. What is your control condition for your design?

Question 5. Typosquatting is a type of social engineering attack based on user mistakes of entering spelling of a url. It's also called a URL hijacking, a sting site, or a fake URL attack. E.g., a typosquatted version of **example.com** will be **exanple.com** or **examplemoreexamples.com.** Attackers use such domains (owned by them) by showing users malicious websites which often download malware or steal user credentials.

You created a browser plugin called "TYPOSQUASH" as part of your start up idea which used machine learning and stored recent hashes of webpages to detect if the domain you are visiting is typosquatted with some accuracy (the plugin sometimes make errors). Accordingly, the plugin alerts the users.

You, as a Usable Security and Privacy researcher now need to do the security analysis of TYPOSQUASH to get first round of your funding.

[2 + 2 + 2 + 1 = 7]

5.1. Write a threat model where TYPOSQUASH will be useful. List attacker action, capability, and access in your threat model.

5.2. Write ONE research questions (as relations between variables) to verify that TYPOSQUASH makes users more secure in your threat model.

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

5.4. What is your control condition for your design?
