Usable Security & Privacy, Evaluation 1

CS60081, Autumn 2021

3:00 pm to 4:00 pm, 7th September 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. Please answer each of the questions below briefly.

[2 + 2 +2 + 1 + 1 + 2 = 10]

1.1. Please answer the following questions about the paper "*Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0*" by Whitten et. al.

1.1.1. Write the primary hypothesis of this paper (at most 2 sentences)
1.1.2. To test the hypothesis, the authors used two Usability Evaluation methods in their study. Name those methods and briefly define what is done in those methods (one sentence per method).
1.1.3. State and explain any two "irreversible" actions (one sentence per action) presented in the paper.

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. Choose the correct answer for each of the questions (select all that apply)

[2 x 5 = 10]

2.1. As discussed in the class, in this paper "A Summary of Computer Misuse Techniques," by Peter G. Neumann and Donn B. Parker, 1989, What kind of security misuses consists of scavenging (physical or otherwise).

A) External Misuses
B) Masquerading
C) Passive Hardware Misuses
D) Using trapdoors to bypass intended controls

2.2. Which of these attacks are Active attacks?

A) Eavesdropping
B) Man-in-the-middle attack
C) DoS
D) Using Trojan Horse

2.3. According to Solove's pluralistic notion of privacy, which of the following lies under the notion of Information Dissemination?

A) Exposure
B) Intrusion
C) Blackmail
D) Identification

2.4. A study is said to have external and 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

2.5. What are the etiquettes of creating a good research question?

A) It should have at least one independent variable.
B) The variable we choose should be measurable
C) There should be exactly two variables and the relationship should be clearly defined.
D) The outcomes should be such that they could only be evaluated by statistical models.

Question 3. Prashant, a student of IIT KGP, is trying to understand phishing attacks. He is investigating the public reaction and awareness towards phishing emails. For his study, he reaches out to students of certain departments(CSE and others) along with some professors as well. He is paying 500 Rs. to each of the participants, and a participant can participate at most 4 times in the research.
The process he intends to use is - he will send some malicious emails from his numerous fake accounts (most of them are normal ones, and some of them containing malicious contents) and then he will analyse if his participants clicked on the link and why.
Answer the following questions:

[2 x 4 = 8]

3.1. What is wrong with letting participants participate at most 4 times in the research?

3.2. 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.

3.3. What would you do to solve the above problem?

3.4. Prashant starts monitoring the activities of the people who by mistake became a victim of the malicious emails he sent for his study. He found some banking credentials of

certain people and intended to use them to rob them. Name two kinds of misuses and attacks he is intending to do. Explain why (one sentence per misuse)

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 x 3 = 6]

4.1. Write any 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.

Question 5. Find one problem in each of the questions below and rewrite the question/answer to fix the problem : **[2 x 3 = 6]**

5.1. Have you ever used Telegram software for sharing pirated movies?
_____ Yes _____ No

5.2. Did your computer ever get compromised?

_____ Yes _____ No

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

_____ iOS _____Android _____Linux _____Windows