Usable Security & Privacy, Evaluation 3

CS60081, Autumn 2021

3:00 pm to 3:50 pm, 16th October 2021
Full marks: 45
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 | 8 x 1.5 = 12 marks

- You have now completed the Usable Privacy and Security course and Arun, a friend of yours approached you for your help. He wants to run a study to know the effectiveness of his new password manager app---ArPass. So, he designed a survey to uncover the login failure rates of entering passwords using password managers. Naturally, his goal is to check if ArPass is better his rival password manager---KgpPass. Arun now wants to deploy the study. Since, he will be paying each participant, he wants to figure out the analysis plan first. Arun created a within subjects design with a group of Campus users.

    - 1.1. Write a suitable H_0 for Arun's experiment

    - 1.2. What statistical test would you suggest for Arun's experiment for checking the hypothesis? Why? (no marks without explanation)

    - 1.3. What is the interpretation of Type-I error in Arun's design?

    - 1.4. What is the interpretation of Type-II error in Arun's design?

- Arun now wants to check what is his target population? In other words which demographics he can nudge to adapt his password manager. For this purpose, he created a full factorial design for ArPass and created another survey. In this survey he plans to collect answer to the question: "*Are you willing to continue using ArPass*" on a daily basis with 5-point Likert scale options. He also plans to collect demographics data for his participants: age, gender, educational qualification, number of years of using computers (in years) and number of years on internet usage (in years).

    - 1.5. What is/are the statistical test(s) Arun should use on the survey data for finding his target population? Why? (no marks without explanation)

    - 1.6. How will he use the proposed test to find answer to his question? Write the procedure (in 2—4 sentences)

    - 1.7. What is the α value Arun should take during his analysis for your proposed test? Why? (no marks without explanation)

    - 1.8. Finally, Arun wants to know *why* some of his participants will not continue using ArPass. What qualitative coding method should he use on participants' responses? Why? (no marks without explanation)

Question 2 | (4 x 2) = 8 marks

Arun has now sold his ArPass startup and recruited by the city of Kharagpur to look over their IT department. He still needs your help with his job. Arun creates a new domain, www.khragpurcity.io and want to set up HTTPS for better security

- 2.1. Arun heard that he needs to get a HTTPS certificate and for that he needs to approach a Certificate Authority (CA). Describe what the certificate will do.

- 2.2. Arun wants to eliminate the step of approaching the CA and ask you to create a *self-signed* certificate for his domain. Would he face any problem(s) with such a certificate? Why or why not?

- 2.3. Arun is now very careful and only visits websites over HTTPS while at work. Is his employer (the City of Kharagpur) still able to tell which exact urls does he visit? Why or why not? (no marks without explanation)

- 2.4. Hackers from Kolkata are attempting to guess the mayor's password, attempting to log in over and over with likely passwords. What are two possible steps Arun can take to minimize the chance of them succeeding (without contacting the Mayor of course, he is currently on vacation)?

Question 3 | (2 + 1) + (2 + 3 + 7) = 15 marks

Please answer the following questions:

3.1. Gaw et al.'s SOUPS'06 paper "Password Management Strategies for Online Accounts" investigates password reuse extensively.

- Write 4 reasons from the paper for reusing passwords.
- Describe one approach to effectively make users stop reusing passwords while not compromising security of passwords

3.2. Imagine that you are given a password of 32 symbols. Each symbols of the password are taken from a set of 16 symbols. Moreover, the password is a concatenation of 4 words, each word comprising of 8 symbols. These 4 words are chosen at random (with possible repetition) from a word dictionary which contain 10,000 words of length 8 (all created using random combination of 16 symbols). Given this setup, please answer the following questions (you need to show your calculation)

- Calculate the guess entropy of this password for a brute force attacker without any background knowledge about the dictionary.

- Calculate the guess entropy of this password for a brute force attacker who has access to the full dictionary.

- Calculate the *expected* guess entropy of this password for an attacker who has access to a random subset of 1000 words from the dictionary (you need to use the *expected number of guesses*).

Question 4 | (1 + 2) + (1 + 2) + 1 + 1 + 2 = 10 marks

Please answer the following questions.

- 4.1. In "CCCC: Corralling Cookies into Categories with CookieMonster" by Hu et al. what are the categories of cookies considered? Give one example for each of the type of data included in each of the cookie categories as discussed in class.

- 4.2. In "CCCC: Corralling Cookies into Categories with CookieMonster" by Hu et al. the mentioned encountering the OOV problem? What is the OOV problem described in the context of the paper? How did they solve the problem?

- 4.3. Mondal et al.'s "Forgetting in Social Media: Understanding and Controlling Longitudinal Exposure of Socially Shared Data" noted that residual activities are a potential privacy issue. What are residual activities?

- 4.4. Mondal et al.'s "Moving Beyond Set-It-And-Forget-It Privacy Settings on Social Media" mentioned that they have shown two consent forms to the participants. Please explain why did they need two forms?

- 4.5. Define and describe (1 line each) the four principle of NEAT guidance on how to create effective security warnings and notices for end users