Usable Security & Privacy, Evaluation 2

CS60081, Autumn 2020

3:00 pm to 4:05 pm, 16th November, 2020
Full marks: 60
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 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. [2.5 x 8 = 20 marks]

Phishing attack is a type of social engineering attack where the attacker initiates a fraudulent communication with the user (typically via email), often impersonating themselves as trustworthy sources like system administrators, close relatives or sometimes even Nigerian princes who inexplicably want to give the user a lot of money (and naturally need user's banking and personal information). Then the attacker tries to abuse the trust of the user by attempting to obtain sensitive information like credit card information, passwords or bank account details. The attackers might even attempt to install virus or ransomware to infect the user's computer by asking the users to visit malicious websites or install malicious softwares.

A new IIT Kharagpur student, Prabhat, believes he has invented a new technique, which he calls PhishProtect, to train people to detect and avoid phishing attacks. Prabhat begins to design a study to evaluate PhishProtect in which IIT Kharagpur faculties receive the PhishProtect training, and then a week later receive a phishing email containing a link (sent from Prabhat, but made to look fraudulent, e.g., from a Nigerian prince). Prabhat will measure what proportion of recipients click on the phishing link in this email. Prabhat asks your help with this PhishProtect evaluation. Please answer each of the questions below.

1.1. Prabhat heard that he might want to have a control condition in his study. He intends to have a between-subjects design for his study. How could Prabhat modify his study to have an appropriate control condition (describe the control condition and why it is appropriate)?

1.2. Once Prabhat adds the (between-subjects) control condition from Part (a), what should his null hypothesis (H0) be?

1.3. Describe the control condition if Prabhat intends to have a within-subjects design (instead of a between-subjects design).

1.4. Prabhat adds the (within-subjects) control condition from Part (c), what should his null hypothesis (H0) be?

1.5. What is a possible confound Prabhat might want to worry about in his study design? Why?

1.6. What is/are the names and types of dependent variable(s) in the study as described?

1.7. To what degree is this proposed study externally valid? Why?

1.8. What possible confound do Prabhat want to avoid by not informing the participants beforehand that he will send an email that will look fraudulent to test the effectiveness of the PhishProtect training they took?

Question 2. Prabhat is feeling inspired and now decides to run a qualitative interview study to understand how people living in IIT Kharagpur use security and privacy tools for sending encrypted email. He decided to record the interviews of his participants and then transcribe the data into text for analysis. Answer the following questions.
[(3 x 2) + 1 + 3 = 10 marks]

2.1. Which coding technique might Prabhat use to answer each of the question? Why? (Just naming the technique will not be awarded any marks)
A) How many participants are currently using encryption to send emails?
B) Which encryption tool those participants are using?
C) Why are they using encryption for sending emails?

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

2.3. How should Prabhat integrate this second person into the process to get final codes?

Question 3. This question is based on definition of Cohen's kappa metric. Please show the calculation for each question (stating only answer will not be awarded marks).
[4 + 4 + 7 = 15 marks]

3.1. Imagine during coding two coders C_1 and C_2 are assigning any one of the three labels L_1, L_2 and L_3 to each piece of text. Ultimately, they arrived at the following confusion matric at the end of one round of coding (called a Latin square):

Coder C_1		**Coder C_2**		
		L_1	**L_2**	**L_3**
	L_1	3n	2n	n
	L_2	n	3n	2n
	L_3	2n	n	3n

n is a positive integer constant (greater than 1) in the table. Compute the inter-rater agreement using Cohen's kappa for this labeling.

3.2. Now consider the labels L_2 and L_3 are merged (used as one code) during coding, compute be the inter-rater agreement (Cohen's kappa value) in the table of 3.1.

3.3. Now 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 C1	**Coder C2**					
		L_1	**L_2**		**L_{k-1}**	**L_k**
	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 labeling for all k > 1 and n>1, 0 < Cohen's kappa < $\frac{1}{k}$

Question 4. Please answer the following questions. **[1+1+1+1+1 +2 = 7 marks]**

4.1. Prabhat recruits some participants with iOS or Android phones running the latest version of each operating system. He runs security software on each phone and counts the number of security problems found. What statistical test is most appropriate for studying whether iOS or Android users have more security problems, on average? Choose all that apply.

a) Logistic regression
b) t-test/ANOVA
c) Pearson's Correlation
d) Chi-squared test

4.2. What type of variable is the number of computers a study participant owns? Choose all that apply.

a) Discrete
b) Continuous
c) Nominal
d) Ordinal

4.3. What kind of variable is the version of the operating system that the participant runs on their primary computer? Choose all that apply.

a) Discrete
b) Continuous
c) Nominal
d) Ordinal

4.4. What is a Chi-Square test? Choose all that apply.

a) A significance test used to analyze quantitative data
b) A significance test used to analyze categorical data
c) A significance test used to analyze quantitative and categorical data
d) A significance test used to analyze parametric data

4.5. When would you use ANOVA instead of a t-test? Choose all that apply.

a) ANOVA should be used instead of a t-test for studies that have more than two conditions
b) ANOVA should be used instead of a t-test for comparing the means of multiple groups
c) ANOVA should be used instead of a t-test for between-subjects experiments involving 2 conditions
d) ANOVA should be used instead of a t-test for within-subjects experiments involving 2 conditions

4.6. 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 a popular cryptocurrency, funded by the researchers, to buy items from the dark web using the Tor browser. Group A is tasked with buying cakes for 1000 INR. Group B is tasked with buying stolen Netflix credentials for 100 INR. An evaluation of the usability of purchasing items on the dark web will be done through analyzing timing data.

Question 5. Please answer the following questions in no more than 5 sentences.
[4 x 2 = 8 marks]

5.1. In "Moving Beyond Set-It-And-Forget-It Privacy Settings on Social Media" paper Mondal et. al. did a post specific survey where they selected 5 random posts and then 6 *specific* friends for each post. Why did they not select random friends for each post?

5.2. In "Lethe: Conceal Content Deletion from Persistent Observers" paper Minaei et al. defined deletion privacy as Likelihood ratio (LR). However, they did their evaluation with respect to a metric called "Decision threshold", why?

5.3. In "Forgetting in Social Media: Understanding and Controlling Longitudinal Exposure of Socially Shared Data" Mondal et al. introduced the notion of "inactivity-based withdrawal" which is a modification of “age-based withdrawal”. Give one advantage and one disadvantage of inactivity-based deletion compared to “age-based withdrawal”.

5.4. In “Oh, the Places You’ve Been! User Reactions to Longitudinal Transparency About Third-Party Web Tracking and Inferencing” paper Weinshel et al. mentioned that “*Over 90% of participants were surprised by something presented in Longitudinal:Interests*”. Argue for or against this statement “Based on the results reported in this paper majority of users do not realize what topics the trackers can infer about their interests over time”.