ECE 750: Usable Security and Privacy - Practice	Marks obtained ↓
Date: July 8, 2025, Total questions: **8** Total points: **74**	
ID: Name:	Time: 40 minutes

Page:	2	3	4	5	6	7	Total
Points:	16	6	10	12	20	10	74
Score:							

Mock Instructions

Practice only - This "Exam" is only for practice, it will not impact your final grade in any way.

40 minutes - We will only be spending 40 minutes today taking the exam, in the real exam you would have 2.5 hours.

Select questions - Read the questions and then take the exam out of order. So start with the questions you are most interested in or that you think you will do the best at. I expect few if any people will complete this exam in 40 minutes.

Merged exam - I merged a couple USEC exams together to make this one. These are all real questions that appeared on finals. But the exam is a bit more password/authentication heavy than a real exam would be.

Original Instructions

No aids allowed. All you are allowed is a pen and pencil.

Use space provided. Answer the questions in the spaces provided. If you run out of room for an answer you can use the back of the page but clearly note in the original answer space that the back was used.

Point value in right-hand margin. The number of points each question is worth is listed in the right hand margin. The number of points and the space provided are roughly indicative of how long of an answer is expected.

Pencils and pens allowed. Both pens and pencils are allowed. Pencil marks need to be clearly present or erased. If it is unclear if a mark is or is not present then it is up to the discretion of the grader and this point cannot be contested later.

Scratch paper. At the end of the exam there are two blank pages marked "SCRATCH PAPER", you may tear these off and use them as scratch paper.

Online safety

1. When people talk about being "safe" online they mean safe against certain threats. Name two threats actors that general people might consider to be a threat online. I am looking for people, groups, or organizations that could be considered threats, I am not looking for technical threats. The next question will use the threats you name, so I recommend reading it as well before answering. (2)

   a: _____

   b: _____

2. For both of the two threats you named in question 1, what technical protections other than encryption could be used to defend against the threat, and why are those protections effective for this specific threat? (6)

Passwords

3. Imagine an attacker was able to gain access to the shadow password file on a Linux server. The file contains usernames, hashed passwords, and their associated salts. The attacker wants to find the passwords of users like root.

   (a) We learned about online and offline password guessing attacks. Is the attacker most likely to use an online or an offline attack in the above situation? Briefly describe what about the situation makes your chosen attack the most appropriate for the attacker. (4)

   (b) Imagine a user is assigned a 4 character password randomly selected from a possible set of 56 characters. The password is used on a website that uses lockout. If more than 10 passwords are attempted against 1 user name, then the system locks the account for 24 hours. Under what assumptions might this password be considered sufficiently secure? (4)

Online Experiment

4. Long random passwords are better for security because they are harder to guess. But long truly random passwords are bad for usability because they are challenging for people to remember.

   To better understand what length random password people can reliably remember Edith designs an online user study. She recruits people using an online survey platform like Amazon Mechanical Turk and requires them to have a high positive rating on the platform. She uses survey software to create an online experiment where users see information and answer questions via a webpage. Users in her study go through the following steps:

   1. Consent to be part of research.
   2. Survey software randomly decides if they will get a 6, 9 or 12 character password, and then creates and records a random password of that length containing at least one upper case, one lower case, one number, and one symbol. The user is shown the password and told they will need to enter this password later in the study.
   3. On the next page the user is asked to enter the password to make sure they remember it, if they enter the wrong password, they are shown the password again and reminded they need to remember it.
   4. The user then fills out the IUIPC scale. (A set of survey questions measuring privacy.)
   5. The user is asked to enter their password. No feedback is given about if it is correct or wrong.
   6. The user then fills out the SeBIS scale. (A set of survey questions measuring security behavior intention.)
   7. The user is asked to enter their password. No feedback is given about if it is correct or wrong.
   8. The user fills out a set of demographics questions including age, gender, native language, and current ocupation.
   9. The user is asked to enter their password. No feedback is given about if it is correct or wrong.
   10. They are thanked for taking part in the survey.

   To analyze the results, Edith counts how many times participants enter their password correctly on steps 5, 7, and 9 producing a score between 0 and 3. She then uses t-tests to see if there is a statistically significantly difference in the mean number of errors between each pair of password lengths.

   Answer the questions below about the study. Feel free to use the step numbers above in your answers.

   (a) List the **independent** variable(s) Edith is collecting in her study. (3)

   (b) List the **dependent** variable(s) Edith is collecting in her study. (3)

(c) The study has several internal validity problems. Describe one of them. (6)

(d) Like all studies, this study has some external validity limitations. Describe one external validity limitation. (4)

Survey study

5. Amy wants to understand if people understand how secure their own passwords are. She decides to run a survey study where she prints the survey on sheets of paper and has volunteers ask people to take the survey at places around campus that have allot of people, like the line in front of Tim Horton's, cafeterias, and the bus station. The survey asks people the questions below. After collecting the data she analyzes the password complexity and compares it to how challenging people think their password would be to guess.

> For each of the following, circle your answer or fill in the blank.
>
> i) Which best describes you: a) student, b) staff, c) faculty
>
> ii) Which of the following does your password contain: a) upper case letters, b) lower case letters, c) numbers (0-9), d) symbols (&,%,.,-, etc.)
>
> iii) Is the first character of your password an uppercase letter? YES NO
>
> iv) Does your password contain English words? YES NO
>
> v) Is the last character of your password a symbol like &, $, and @. YES NO
>
> vi) How long is your password? _____
>
> vii) Do you think your password would be challenging to guess?
> Very challenging, Challenging, Somewhat challenging, Not challenging

(a) Select one of the question's from Amy's survey above that you feel could be phrased better. State what you think is wrong with the question and propose better wording or better options. (4)

(b) What are the **independent** variable(s) that Amy is collecting? (2)

(c) What are the **dependent** variable(s) that Amy is collecting? (2)

(d) What **external validity** issues exist with this study? (4)

(e) Does Amy's study have good **internal validity**? Why or why not? (4)

Public/Private Key Cryptography

6. (a) Fill in the blanks in the following text describing Alice and Bob correctly communicating securely. Each blank needs to be filled in using one of the following words: (6)

   - Encrypt, encrypted, encrypts
   - Decrypt, decrypted, decrypts
   - Sign, signed, signs, signature
   - Public
   - Private

   Alice wants to send an encrypted and signed message to Bob who she has met in the past. When they last met in person they verified and then _____ each other's _____ keys using their respective _____ keys.

   To send an email to Bob, Alice first _____ the message using her _____ key and then _____ the resulting message using Bob's _____ key. Alice then sends the message over an untrusted connection.

   Bob receives the message and first _____ it using his _____ key. He then verifies that the message really was from Alice by verifying the _____ using Alice's _____ key.

   (b) Research, such as the *Why Johnny Can't Encrypt* paper, often mentions "confusing metaphores" in regards to encryption interfaces. Give a specific example of a metaphor related to encryption that is likely confusing for people. (4)

   (c) Would Alice and Bob's security in the interaction above be improved by using a Certificate Authority (CA)? State 'Yes' or 'No' and then briefly explain what a CA would do to help Alice and Bob OR explain why their current security practices are equal to or better than what a CA would provide. (6)

Encryption

7. The following is an excerpt from the *Why Johnny Can't Encrypt* paper which explains the steps a participant had to go through to setup their own key pair and send an encrypted message to 5 people.

> In order to [correctly send an encrypted email], a participant had to generate a key pair, get the team members' public keys, make their own public key available to the team members, type the (short) secret message into an email, sign the email using their private key, encrypt the email using the five team members' public keys, and send the result. In addition, we designed the test so that one of the team members had an RSA key while the others all had Diffie-Hellman/ DSS keys; thus, if a participant encrypted one copy of the message for all five team members (which was the expected interpretation of the task), they would encounter the mixed key types warning message. Participants were told that after accomplishing that initial task, they should wait to receive email from the campaign team members and follow any instructions they gave.

WhatsApp, a modern chat app, also does end-to-end encryption but the steps to send an encrypted message are essentially invisible to the user unless they explicitly look in the settings. Each device running WhatsApp automatically creates its own public/private key pair. The main WhatsApp server keeps a record of which public keys are associated with which users. When a user wants to chat with someone (a phone number) the central WhatsApp server provides the appropriate public key. Private keys never leave their devices.

(a) WhatsApp's approach requires the user to perform fewer steps and is therefor easier to use than the PGP approach tested in *Why Johnny Can't Encrypt*. Describe one situation where the user would be safe using PGP but not if they used WhatsApp. You can assume that they can use PGP correctly without making errors. (6)

(b) Name and briefly describe a type of study that could be used to better understand why most WhatsApp users are not manually verifying the keys they receive from the central server. You do not need to plan a whole study, a simple description is fine. (4)