Sample Essay Questions

CS463 Midterm Exam

These are examples of questions that might appear on the Midterm Exam.

463.1: Introduction

Describe three key changes that have affected host security.

463.2: Social Networks

In [Dey 12] a number of techniques were explored to estimate missing data. Discuss three of the techniques used to estimate the age of a user whose age was unknown. What auxiliary data was used in those techniques, and what data, if any, did the authors use when the auxiliary data was not available? How did the study establish the ground truth to verify the effectiveness of their techniques?

463.3.1 Machine Learning

You have been asked by your employer to develop a machine learning classifier to determine when an attacker has stolen the login password of a user and is using their account. Prepare a proposal in which you explain each of the five steps to developing a machine learning classifier and your preliminary ideas about what to do in each step.

463.3.2 Adversarial Machine Learning

Give an example of causative attack and an example of exploratory attack on spam filters. Describe each of the attacks addressing the following questions:

(1)  What is the assumption on the adversary’s capability?

(2)  What is the goal of the attack?

(3)  What is the strategy of the attack?

463.4 Crypto Constructs

What is homomorphic encryption? Describe a scenario where homomorphic encryption would be useful and explain why it would help.

463.5 De-identification

Define the concept of k-anonymity. Given the following dataset, make modifications to release the dataset in a 2-anonymous way. You can also add records if needed. Treat each of the column types except the List of Apps as a quasi-identifier.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Google Id | Sex | Age | Zip | List Of Apps |
| awesome@gmail.com | F | 25 | 61800 | Angry Birds, Facebook, YouTube, Snapchat |
| [cool@gmail.com](mailto:cool@gmail.com) | M | 64 | 61521 | OnTrack Diabetes, Uber, Snapchat |
| fast@gmail.com | F | 32 | 61222 | Runtastic, Netflix |
| shtherapy@gmail.com | M | 35 | 61800 | Amazon Shopping, Angry Birds, Facebook, YouTube |
| smart@gmail.com | F | 20 | 61435 | WolphramAlpha, CNN, BBC |

463.6 Trusted Computing

463.6.1 SGX

Describe the trust assumptions of the SGX system explaining what components need to be trusted and which do not. Illustrate a use of this trust architecture for a specific example, using the example to illustrate why it is reasonable to trust some parties and not others.

463.6.2 Models

List and state each of the three rules of the Biba Integrity Model. Explain why each of the rules is reasonable, illustrating each with an example.

463.7 Information Flow

Use the non-interference relation :| defined in [GougenM82] to define the concept of a communication channel between groups G and G' though which only commands from a set A can pass. (This can be done with two relations.)

463.8 Crypto Models

Provide the definition of perfectly secret encryption. What is the main result about perfectly secret encryption schemes?

Bob thinks he has designed a provably secure computationally secure encryption scheme. However, he is worried that the key space is too small. He requests your expertise as a CS463/ECE424 student.

1. In order to help Bob, you need to recall what computational security is. *Briefly explain what a computationally secure encryption scheme is.*
2. You tell Bob that there are two approaches for computationally secure encryption: the concrete approach and the asymptotic approach. *Briefly explain the two approaches and how they differ.*
3. You tell Bob that his scheme is secure if no probabilistic polynomial time (PPT) adversary can break it with better than negligible probability of success. *Explain what probabilistic polynomial time mean. Explain what a negligible probability of success is.*
4. Bob asks you about attacks. *Briefly explain what a brute-force attack is. What is the adversary’s probability of success?*
5. Bob explains to you that his key generation algorithm works by picking a uniformly random key of bits, for some fixed constant , where is the security parameter. *What is the size of the key space: i.e., how many possible keys are there?*
6. Prove or disprove that if a PPT adversary attempts a brute-force attack on Bob’s scheme the probability of success is negligible. (Hint: express the probability of success as the ratio of the adversary’s running time and the size of the key space. Is this ratio a negligible function?) Keep in mind that the security parameter of Bob’s scheme is .
7. What is the minimum value of that Bob should use to guarantee a security level equivalent to AES-128? Assume that and that the construction has no inherent weakness.

463.9 HIT

What is the concept of genomic exceptionalism and how does it impact the way privacy must be managed for genomic data?

What is the Direct To Consumer (DTC) genomics? Discuss ways in which DTC will impact privacy for genomic data.