1. Which statement is *most* accurate about the configuration management problem? **1 point**

- Existing protocols cannot handle new types of attacks.
- Given the programming mechanism, security protocols are often not appropriately parameterized to be effective.
- There is no established security protocol for mobile applications.
- There are established security protocols, but they cannot be implemented because the smartphone is resource-constrained.

2. Consider a biometric authentication system for a mobile computing application. It obtains a user's biometrics and compares it to a database of similar biometrics obtained from a large set of other users. The comparison is done using a support vector machine-based algorithm. The SVM is trained for a two-class classification problem, where the class for a given user is called the "client class," and the class for all other users is called the "world class." **1 point**

Suppose that an adversary is trying to guess a signal that gets classified as "client class." Since the "world class" is publicly available, the adversary obtains a data point from the database and uses a hill climbing strategy. In this strategy, the adversary has black box access to the machine learning algorithm. This means that the adversary can provide any input to the machine and obtain the soft class labels. The soft class labels are the evaluations of the equation $wx + b$, for any input x. The adversary does not know w or b.

Which methods are *valid* hill climbing strategies? *Select all that apply.*

- [x] Use an evolutionary algorithm to iteratively improve the input so that, in each iteration, it gets closer to the class
- [ ] Design an attacker and observe the interaction between the attacker and the SVM classifier to derive an input that gets classified as legitimate input
- [ ] Use random search in the feature space to find an input that gets classified as the desired class
- [x] Use a gradient descent mechanism to obtain an input that minimizes the error function (1 – soft class label)^2

3. Consider a biometric authentication system for a mobile computing application. It obtains a user's biometrics and compares it to a database of similar biometrics obtained from a large set of other users. The comparison is done using a support vector machine-based algorithm. The SVM is trained for a two-class classification problem, where the class for the concerned user is called the "client class," and the class for all other users is called the "world class." **1 point**

Suppose that an adversary is trying to guess a signal that gets classified as "client class." Since the "world class" is publicly available, the adversary obtains a data point from the database and uses a hill climbing strategy. In this strategy, the adversary has black box access to the machine learning algorithm. This means that the adversary can provide any input to the machine and obtain the soft class labels. The soft class labels are the evaluations of the equation $wx + b$, for any input x. The adversary does not know w or b.

Using hill climbing strategies in this scenario, is it possible to obtain w and b of the original machine?

- Yes
- No

4. Consider a biometric authentication system for a mobile computing application. It obtains a user's biometrics and compares it to a database of similar biometrics obtained from a large set of other users. The comparison is done using a support vector machine-based algorithm. The SVM is trained for a two-class classification problem, where the class for the concerned user is called the "client class," and the class for all other users is called the "world class." **1 point**

Suppose that an adversary is trying to guess a signal that gets classified as "client class." Since the "world class" is publicly available, the adversary obtains a data point from the database and uses a hill climbing strategy. In this strategy, the adversary has black box access to the machine learning algorithm. This means that the adversary can provide any input to the machine and obtain the soft class labels. The soft class labels are the evaluations of the equation $wx + b$, for any input x. The adversary does not know w or b.

Now suppose the system is modified so that whenever an input from the world class is used for illegitimate access, the system raises an alarm. If an attacker uses the same hill climbing strategy as before, will the attacker be successful?

- No, because the as soon as attacker queries the machine using an input from the world class, the alarm will be raised and the system will be shut down for any further inputs
- Yes, because the attacker can disable the alarm using an input from client class and then continue doing hill climbing
- Yes, because the attacker can subvert the alarm using data from world class
- Yes, because the attacker still can query the machine regardless of the alarm

5. Which statements are *most* accurate in the context of criticality aware access control mechanisms? *Select all that apply.* **1 point**

- [ ] During criticality, access should be granted to authorized users only, regardless of their probability of potential mitigation.
- [x] During criticality, access should be granted to users who have the highest probability of mitigating the criticality.
- [x] After the criticality is mitigated, it is imperative to reinstate the previous access control rules.
- [x] After criticality, if access control is not handled properly, the system can be open to security attacks.

6. What is adversarial sample manufacturing? **1 point**

- It is a security problem where, using black box access to a machine, novel inputs are generated based on solving an optimization problem.
- It is a defense mechanism where a machine generates spurious inputs and trains itself to recognize such false data.
- It is a security problem where data snooped in the past are repeated and presented to a system as new data.
- It is a security problem where the source of the data cannot be verified and is untrustworthy.

7. Suppose that a mobile app (ChargeBuddy) has been developed, which an Electric Vehicle (EV) owner can use to search wirelessly for a local charging station (CGS). The app lists the nearby CGSs and provides relevant information, such as the current price of charging and the distance from the EV owner's current location. The EV owner selects the preferred CGS and is responsible for reaching the chosen CGS within a specified time-period. On reaching the chosen CGS, the EV owner starts charging the EV. **1 point**

Which action can cause the demand in a particular substation to increase beyond the supply cap?

- Not showing the nearest CGS but showing the second farthest
- Increasing the price of a given CGS
- Only showing the nearest CGS and not any others
- Drastically decreasing the price of CGSs in a given area

8. Consider a recommendation system (e.g., Netflix). Suppose that there is a malicious user with 10,000 fake email addresses. The user creates 10,000 Netflix accounts, and each account has the same user characteristics (same age, gender, likes, and dislikes). However, each fake user provides contradictory movie reviews. For example, a given fake user may claim to like Romantic Comedy films, but it rates "50 First Dates" (a Romantic Comedy) 1 out of 5 stars, whereas it rates "The Joker" (an Action Thriller) 5 out of 5 stars. **1 point**

What effect might this have on the recommendation system?

- The system will not be affected.
- The system may give wrong recommendations to a user for a short time, but as usage history builds it will start to give better recommendations.
- The system may give consistently incorrect recommendations to a real user with a long, legitimate usage history.
- The system may give consistently wrong recommendations to a real user with no usage history.

9. Consider a recommendation system (e.g., Netflix). Suppose that there is a malicious user with 10,000 fake email addresses. The user creates 10,000 Netflix accounts, and each account has the same user characteristics (same age, gender, likes, and dislikes). However, each fake user provides contradictory movie reviews. For example, a given fake user may claim to like Romantic Comedy films, but it rates "50 First Dates" (a Romantic Comedy) 1 out of 5 stars, whereas it rates "The Joker" (an Action Thriller) 5 out of 5 stars. **1 point**

What type of attack is this?

- ○ Replay attack
- ○ Zero day attack
- ◉ Poisoning attack
- ○ Presentation attack

10. Is an electroencephalogram (EEG) a valid biometric? **1 point**

- ○ No, because EEG varies between individuals
- ○ Yes, because EEG comes from the human body
- ◉ No, because EEG varies over time and there is no unique pattern
- ○ Yes, because EEG is unique for a given person

DONE