By Stephen Liu

Provide an example of a system, in which confidentiality is more important than integrity or availability. Explain why.

A database at a medical facility which stores patients' private information. A leak of confidentiality will expose personal information to attackers. Integrity and availability can be recovered manually and will not have any permanent effects if reduced.

By Pooya Jafarian

Provide an example of a system, in which integrity is more important than the other two properties. Explain why.

~~Example: An accounting system~~

Example: An accounting system:
In an accounting system that records information about a companie's incomes and outcomes, the finantial information is not very confidntial and revealing the information will not cause serious problems but changes in financial Information results in serious problems.

By Nima Kaviani

2. (2 points) Define when a crypto system is secure.

A Crypto System is considered secure when there is no known shortcut attack found for it. and the best way to find the key is to perform an exhaustive search.

By Natalie Silvunovich

3. (2 points) Give an example of two crypto systems A & B such that A is secure, according to the definition of a secure cryptosystem, and B is not, yet an attack on A is less computationally expensive than the best attack on B.

the best way to attack the Caesar Cipher is brute-force, but there are only 26 keys, so it is not very secure. Breaking the Vigenère cipher is more difficult and more expensive, but since there is a "short-cut" (distance factoring) that is better than brute-force, it is considered secure.

4. (5 points) True or False?

By Evard Taivo

5. (2 points) What does the Kerckhoff's Principle state?

That the protection of the key is more important than the protection of the algorithm. An algorithm will eventually be deciphered and its weaknesses discovered. It is the key that is the most important in crypto.

6. (3 points) Give an example of a system, computer-based or not, in which even though threats and vulnerabilities are significant, the overall risk is very low. Explain how it could be.

Linux OS?
Home Alarm System

Home Alarm System - threats & vulnerabilities known
- risk is low because household goods are heavy & difficult to sell
- there are "softer" targets that yield cash more quickly
- physical presence of family & neighbours is deterrent
- many houses in Lower Mainland, difficult to know from outside which are protected by alarms
- deterrence of security & police response & jail → consequences - easy to catch w/stolen goods

By Fahimeh Raja

7. (4 points) Imagine that you have a fancy car. Consider the risk of your car being stolen while it's parked on campus during this quiz. For each of the four ways of managing this risk, give one example of what you could have done. Be specific.

1. accept the risk : I accept the risk that one may knows that I am in quiz and may steal my car. but I bring my car

2. avoid the risk : I know that some one may know that I am in quiz session & I can not check my car, so I do not bring my car to campus

3. transfer the risk : I buy an asurance for my car, that in case it is stolen, they pay the money, and so I transfer the risk to insurance company.

4. reduce the risk : I can reduce the vulnabrity by putting security alarm in my car, or I can park it in a secure parking.

8. (3 points) Explain the difference between authentication and authorization.

authentication uses mechanisms to find who can have access to the system.

authorization is preventing from breaking the rules & we consider what actions the authenticated person can do.

9. (3 points) What are the required properties of good <u>hash function</u>? Select all applicable.

A. collision resistance
B. efficient
C. invertible
D. the key should not be reused
E. "one-wayness"

Answers: A E

Question 2 and 5 were misunderstood by some students.
In the question 4 there were so many mistakes
Half of the students did not answer question 7 completely
Most of the students choose B as a part of answer in question 9.