Highly Dependable Systems / Sistemas de Elevada Confiabilidade

MEIC

Sample Exam

1. Should a system designer see the concepts of fault prevention and fault tolerance as alternative techniques or are they complementary to each other? Explain your answer.

2. Suppose that Alice wants to communicate with Bob through an insecure network. Both of them have <public,private> key pairs, and they know each other's public keys (KpubA and KpubB) but keep their private keys to themselves (KprivA and KprivB).
   a. If Bob wants to send Alice confidential message, how can this be done? Please describe all the necessary steps at both the sender and the receiver.
   b. If Alice wants to confirm the authenticity and integrity of a message sent by Bob, how can this be done? Please describe all the necessary steps at both the sender and the receiver.

3. How would you compare (in terms of the advantages of using one versus the other) space redundancy versus time redundancy? Your answer must list at least 2 advantages of one of the choices and 1 advantage of the other.

4. What is typically stored in a SmartCard's ROM and in its EEPROM? Justify the answer.

5. Suppose that you hire a security consultant who tells you that access control to a secure location should be done using exclusively a fingerprint reader, since he or she believes it is infallible. Do you think this is good advice and how would you reply it? Justify your answer.

6. Explain the concept of remote attestation, and explain how you could use it to offer a cloud computing service with the integrity guarantee that the cloud provider would not modify or delete the contents of every mail that is sent or received.

7. The leader election problem can be formulated as follows: there are no inputs, and each process i outputs several <LEADER,j> events stating that process i is, at that point in time, elected by process i as being the current leader. The correctness condition states that all correct processes should eventually unanimously elect the same correct leader, and that choice will never be modified subsequently. (By correct we mean processes that do not suffer a crash fault throughout the execution.)
   a. Is the correctness condition a safety condition or a liveness condition?
   b. Consider the following trace of an execution where neither process crashes, and where "pi.leader(pk)" indicates that process i has elected process k as the leader.
      p1.leader(p1), p2.leader(p2), p1.leader(p2), p1.leader(p1)
      Does this trace obey the correctness condition? If your answer is negative and your answer to question (a) is that it is a liveness condition, then you should also extend the trace in order to make it obey the correctness condition.

8. What are the main differences between a Byzantine regular register and an atomic register? Provide an example of an application that can use an atomic register but not a regular one.