Highly Dependable Systems – Sistemas de Elevada Confiabilidade – MEIC/METI

1st Exam – June 18, 2021 – Duration of the exam: 2 hours

Your answers must only use the number of lines in the boxes provided next to each question. If necessary, for instance to correct a previous answer, you can use the space at the end of the exam sheet but you cannot use more lines than in the original box. Justify all answers.

Number		Name	

[3 points] Dependability fundamentals.

1. [0,5 point] Is it possible for a system with high reliability to have low instantaneous availability? Justify the answer.

2. [0,5 point] Provide an example of roll-back and example of roll-forward error handling techniques.

3. [1 point] How many seconds per day can a system with seven 9s be unavailable?

4. [1 point] Illustrate an example scenario in which one can assume failure independence between two servers, and one example in which the failure of two servers cannot be deemed as independent.

[2 points] Security Fundamentals.

5 [2 points] What is a perfect cipher? Provide an example of a perfectly secure cipher.

[3 points] Fault tolerance.

6.a [2 points] Assume a computer system whose reliability is estimated to be 40%. By what extent reliability be increased by relying on triple modular redundancy scheme with ideal voter? Justify the answer.

6b. [1 point] In a latency sensitive application, assuming that cost and energy do not represent an issue, is it preferrable to adopt a passive or an active hardware redundancy approach? Justify the answer.

Number		Name	

[3 points] Smartcards & Physical attacks

7.[2 points] Provide a specific example of how to leverage a fault injection attack to extract secrets from a Smartcard.

8. [1 point] What tools can be used to carry out a physical attack based on probing to a Smartcard that has been hardened using a protective surface mesh?

[4 points] Fault tolerant distributed algorithms.

Recall the specification of the Leader Election problem.

Eventual detection: Either there is no correct process, or some correct process is eventually elected as the leader.

Accuracy: If a process is leader, then all previously elected leaders have crashed

9. (1 point) How can this problem be solved using a Perfect failure detector? Justify the answer.

10. (1 point) How can this problem be solved using an Eventually Perfect failure detector? Justify the answer.

Number		Name	

[4 points] Byzantine Fault tolerant distributed algorithms.

11. (1 point) Consider the Byzantine consensus problem with Strong Validity. Is it possible to decide a value proposed by a Byzantine leader? Justify the answer.

12. (1 point) In the IBFT Byzantine consensus ~~problem~~ protocol, if the algorithm is not making progress, correct processes can send ~~NEWEPOCH~~ ROUND-CHANGE messages to trigger an epoch change. Describe the steps required for the epoch change to happen.

[2 points] Blockchain.

13. (1 points) "PoW consensus favors safety while classical Byzantine consensus favors liveness". Do you agree with this affirmation? Justify.

14. (1 points) Assume a synchronous system, enriched with a perfect failure detector, that uses Proof of Work as the consensus algorithm. In this scenario are forks still possible?

[3 points] Trusted computing.

15. (1,5 point) The project assumed the existence of Byzantine clients and Byzantine servers. Consider that the Healthcare Autority now mandates that all clients must issue reports from devices equipped with a Trusted Platform Module. Discuss how you could have optimized the project taking this into consideration.

16. (1,5 point) What is the role of the Platform Configuration Register in ensuring the guarantees provided by the Trusted Boot Service?