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

2nd Exam – July 07, 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. Answers can be provided in English or in Portuguese.

Number		Name	

Dependability fundamentals.

1. What is the relation between a fault, error and failure? Provide an example of a system with a fault, an error and a failure

2. Services can fail in different ways. Provide an example of a content inconsistency failure.

3. What is the relationship between fault removal and fault forecasting?

Security Fundamentals.

4 A company needs to secure the communication between a temperature sensor and a base station that share a secret symmetric key. The sensor emits one temperature reading per second of 8 bits in size which should be communicated to the base station as fast as possible. How do you recommend that this is implemented?

Fault tolerance.

5 Consider a system with 5 redundant modules. To maximise fault tolerance, is it preferable to have a NMR of a Hybrid with Spares configuration? Justify.

6 Consider a (7,4) Hamming code defined by the following table:

	d1	d2	d3	d4
p1	Y	Y	N	Y
p2	Y	N	Y	Y
p3	N	Y	Y	Y

Suppose the parity checks p2 and p3 fail. What can you conclude if p1 also fails? And if p1 does not fail?

Number		Name	

Smartcards

7 How can Smartcards contribute to multi-factor authentication?

8. In the context of Smartcards, how does a a side channel attack differs from a physical attack? Provide an example of a side channel attack.

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

8. How can this problem be solved using a Perfect failure detector? Justify the answer.

9. How can this problem be solved using an Eventually Perfect failure detector? Justify the answer.

Number		Name	

Byzantine Fault tolerant distributed algorithms.

10. Consider the Byzantine consensus problem with Strong Validity. Is it possible to decide a value proposed by a Byzantine leader? Justify the answer.

11. ~~the Byzantine consensus problem~~ In the IBFT protocol, if the algorithm is not making progress, correct processes can send NEWEPOCH messages to trigger an epoch change. Describe the steps required for the epoch change to happen.

Blockchain.

12. "PoW consensus favors safety while classical Byzantine consensus favors liveness". Do you agree with this affirmation? Justify.

13. 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?

Trusted computing.

13. 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.

14. What is the role of the Platform Configuration Register in ensuring the guarantees provided by the Trusted Boot Service?

Number		Name	

Question	1	2	3	4	5	6	7	8	9	10	11	12
Grade	3	2	2	1	2	1	1.5	1.5	1.5	1.5	1.5	1.5