Highly Dependable Systems – Sistemas de Elevada Confiabilidade – MEIC/METI
2nd Exam – July 22, 2022 – 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. Answers can be in English or Portuguese.
Justify all answers.

Number		Name	

Dependability fundamentals

1. In which dependability technique is the Risk Priority Number (RPN) used? What aspects are kept into account in order to compute the RPN?

2. What does the expression “five nines” mean in the context of dependability?

3. Provide a taxonomy of the main reasons limiting the coverage of a fault tolerance mechanism?

Security Fundamentals.

4. What property does a Perfect Cipher guarantee? How can a Perfect Cipher be implemented?

5. Provide an example of the surreptitious forwarding attack and discuss one possible solution to avoid this attack.

Fault tolerance.

6. Consider an NMR system, with N=5. and a reliability of 0.95 under the assumption of an ideal voter. How does the reliability of the system changes if the voter's reliability is estimated to be 0.9?

Number		Name	

7. Can the increase of the replication factor of a component lead to a degradation of the overall reliability of the system? Justify the answer. If the answer is yes, specify under which assumptions this is possible.

Smartcards

8. Describe the memory linearization attack and provide an example of how it can be exploited.

9. Provide an example of a side-channel attack targeting smartcards aimed to extract cryptographic material (e.g., private keys) from a smartcard.

Fault tolerant distributed algorithms.

10. By which property/properties do an “eventually perfect failure detector” and a “perfect failure detector” differ?

11. Can eventually perfect failure detectors be implemented in an asynchronous system? Justify the answer.

Byzantine fault tolerance

12. The Byzantine Fault Tolerant Consensus algorithm presented in the theory classes is based on the EpochConsensus algorithm. What properties does the EpochConsensus algorithm guarantees?

Number		Name	

13. Which aspects of the State Machine Replication approach for the crash failure model need to be adapted/revised when moving to a Byzantine failure model?

14. Why a Byzantine Quorum composed by more than (N+f)/2 is guaranteed to exist only if f<N/3?

Blockchain.

15. Describe how the crypto-puzzles used in systems like Bitcoin operate. Discuss also how it is possible to adjust the complexity of the puzzle.

16. What is the difference between the Proof-of-Work and Proof-of-Space mechanisms?

Trusted computing.

17. The Trusted Platform Module can store a relatively small number of cryptographic keys in its internal shielded locations (i.e., within the TPM chip). Yet, for privacy purposes, users are recommended to use a large number of Attestation Identity Keys, i.e., one for each service/application they interact with. Such a large number of keys typically does not fit within the TPM internal storage. What mechanism is used to store the AIKs securely outside of the TPM, while guaranteeing that they can only be retrieved by the machine equipped with the TPM that generated them?

Question	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Grade	1	1	1	1	1	1	1	1	1	1,5	1,5	1,5	1,5	1,5	1	1	1,5