Highly Dependable Systems – Sistemas de Elevada Confiabilidade

1st Exam – April 27 – 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. [1.5 points] Dependability was defined as "the ability to deliver service that can be justifiably trusted". Explain, with the help of a concrete example, how the use of trusted execution environments (TEEs) can increase the dependability of a system.

**Security Fundamentals.**

2. a) [1.5 points] The PBFT protocol by Castro and Liskov was a breakthrough in that field, to a large extent to the use of MACs instead of public key signatures. Explain what are the advantages and downsides (or challenges) associated with replacing signatures with MACs in a BFT consensus protocol. In your explanation of the challenges, please provide a concrete example associated with your course project.

b) [1 point] In recent years, the use of MACs in BFT consensus protocols has become less and less critical, and many blockchains no longer use MAC-based protocols. Give one of the possible reasons for this fact.

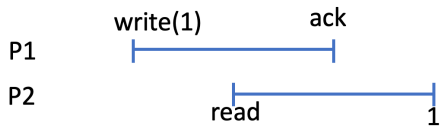
**Fault tolerant distributed algorithms**.

5. a) [1.5 points] The Byzantine authenticated echo broadcast solves the consistent broadcast problem but does not provide the totality property of the reliable broadcast problem (which states that if some message is delivered by any correct process, then every correct process eventually delivers a message). Prove this statement by means of a counter-example timeline of an execution with four processes (p,q,r,s) where process p is the sender.

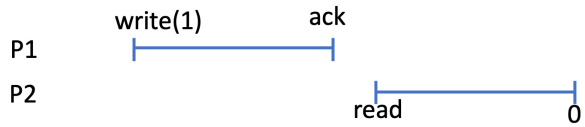
b) [1.5 points] Two students of the course, Andreia and Belmiro, are discussing possible ways to fix the authenticated echo broadcast to allow it to solve the reliable broadcast problem. Belmiro claims that this can be fixed without adding an extra round of messages through the single change of having processes finish the protocol (producing a DELIVER event) when receiving a single ECHO message instead of waiting for a quorum. Andreia claims that Belmiro's protocol does not ensure correctness. Who is right? Prove your answer in a precise and formal way.

6. Consider the following executions (A, B, C, D) of a register algorithm:
(In all executions, the initial value of the register is zero.)

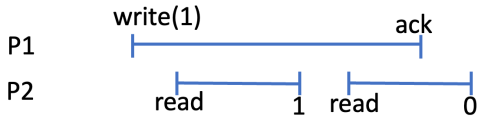
Execution A:




Execution B:

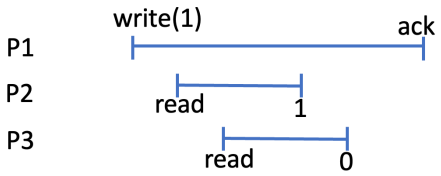



Execution C:



| Number | | Name | |
|---|---|---|---|

Execution D:




a) [1 points] Which of these executions obey the specification of:

i) Regular register:

| |
|---|
| |

ii) Atomic register

| |
|---|
| |

b) [0.5 points] For each of the atomic executions, draw the justifying serialization points in the respective execution diagrams.

c) [1.5 points] Choose (or, in case you have not answered the previous question, construct) an execution that is regular but not atomic, and then provide a timeline of an execution where the (1,N)-Byzantine regular register algorithm we learned in class (with single phase reads and single phase writes) that produces this execution trace.

**Bitcoin, Ethereum and Solidity**

7. [1.5 points] In PoW blockchains, a block is considered "finalized" (i.e., added to the main chain in a given position) when *K* subsequent blocks have been added on top of it. What are the tradeoffs when setting the value of *K*? In other words, what are the advantages and disadvantages of setting a small (versus large) value for *K*?

| |
|---|
| |
| |
| |

8. [1.5 points] Blockchain transactions cause a transition in the state of the blockchain from an old to a new state. When comparing Bitcoin versus Ethereum, there is a significant difference in terms of the expressiveness of how these state transitions are determined. Explain why this is the case.

9 [1.5 points] The two students Andreia and Belmiro are now debating the re-entrancy attack (at the root of the DAO attacks from last decade). Andreia explains that this attack was due to a concurrency problem, namely two concurrent invocations of the same function of a smart contract, but Belmiro claims that she is wrong because there cannot be any concurrency in Solidity, due to the fact that transactions are executed one at a time, in the order in which the Ethereum blockchain determines. Please explain who is right and why.

**Smartcards**

10 [1.5 points]. An EEPROM (electrically erasable programmable read-only memory) is a non-volatile memory that is mostly only read, but can occasionally be rewritten by applying special programming signals. Which of the following parts of the smartcard state is stored in an EEPROM? Explain why that is the case.

i) Variables containing the temporary state of the smartcard application
ii) Operating system
iii) Cryptographic keys associated with the card
iv) Self-test procedures

| Number | | Name | |
|---|---|---|---|

11 [1.5 points] Which of the following statements is true? Justify your answer

i) A side channel attack is a specific type of a power analysis attack
ii) A power analysis attack is a specific type of a side channel attack

| |
|---|
| |
| |
| |
| |

**TEEs.**

12. [1 point] Explain what is a replay attack on persistent data stored by a TEE.

| |
|---|
| |
| |
| |
| |

13. [1.5 points] Andreia and Belmiro need to write an SGX enclave that implements a persistent key-value store (a storage system with an interface that maps keys to objects, and stores this mapping in persistent storage).

To defend against replay attacks, Andreia has the idea of encrypting the data with a symmetric key which is sealed and stored on a disk. Furthermore, while the SGX enclave is running, the enclave maintains in its memory the hashes of the most recent value of each object. This will protect against replay attacks while the SGX enclave is running and data is stored on disk (outside the enclave), but not when the enclave or the machine restarts. However, Belmiro points out that for a very large system it will be impossible to keep all these hashes in the SGX enclave memory.

Design a variant of Andreia's proposal that provides the same dependability guarantees while scaling to a much larger number of objects stored by the system.

| |
|---|
| |
| |
| |
| |