Highly Dependable Systems – Sistemas de Elevada Confiabilidade

First Exam – April 11, 2024 – 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] Explain the concept of fault forecasting (or prediction). Then, give a specific example of how fault forecasting could be useful if you were responsible for developing a new cloud storage service (like Amazon S3 or a similar service). Indicate a dependability attribute of your choice, and detail how fault forecasting could be used to meet a certain goal for that attribute.

Security Fundamentals.

2. a) [1.5 points] Alice and Bob need to communicate with confidentiality and integrity, but they are operating in a restricted environment where only public key cryptography is available and no other primitives are available (namely they cannot use hash functions or symmetric encryption). Define precisely what these two properties mean in this context, and explain how Alice and Bob can use the available public key cryptography to guarantee these properties.

Fault tolerant distributed algorithms.

3. Consider the signed echo broadcast protocol we learned in class (where echo messages are digitally signed with public key cryptography).

a) [1.5 points] Prove that this does not provide the totality property required by reliable broadcast by giving a counter example timeline of an execution (in this answer you must draw the message flow between four processes in the lines below, where each line corresponds to the execution of one process with time going from left to right). (Recall that totality means that if some message is delivered by any correct process, every correct process eventually delivers a message.)

p

q

r

s

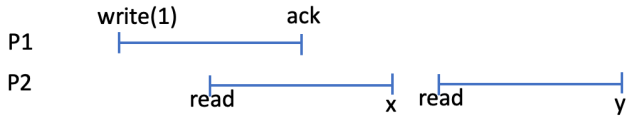
b) [2 points] Formally prove that the signed echo broadcast protocol meets the consistency property, which states that if some correct process delivers a message m and another correct process delivers a message m', then m = m'.

c) [1.5 points] Two student of this course, Anabela and Bartolomeu, are discussing which protocol to use for a system that processes financial transactions for a bank. In this scenario, nodes are powerful server machines connected by bandwidth constrained links, and the parameter f is set of a very high value (e.g., tolerating on the order of tens of faults). Anabela argues that they should use authenticated echo broadcast and Bartolomeu thinks they should use signed echo broadcast. Who would you support and why?

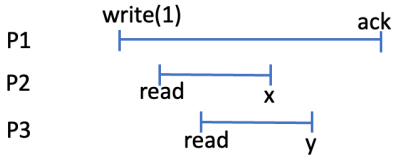
Number		Name	

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

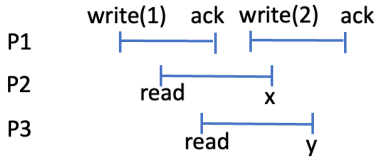
Execution A:



Execution B:



Execution C:



a) What are **all** the possible pairs of valid read return values (x,y) in case of a:

i) [1 point] Regular register:

Execution A:

Execution B:

Execution C:

ii) [1 point] Atomic register

Execution A:

Execution B:

Execution C:

5. [2 points] Draw a timeline for an execution of the round-change part of the IBFT protocol (from the project), where node p is the leader and crashes in the beginning of the execution, triggering timeouts at all other replicas, and replica **s** takes longer than the others to timeout. Give as much detail as you can regarding the message arguments and write down (below the timeline) all the assumptions your message diagram makes about the initial state of the execution.

p

q

r

s

Assumptions made about the execution state:

Bitcoin, Ethereum and Solidity

6. a) [1 points] One of the key differences between classical consensus and Nakamoto consensus is the existence of forks in the latter. Explain why forks may happen in Nakamoto consensus.

6. b) [0.5 points] Explain why and under which conditions forks are prevented in classical consensus.

6. c) [0.5 points] In light of the previous answers, why doesn't Bitcoin use classical consensus?

Number		Name	

7. [1 points] Some accounts in Ethereum are not owned by a person or an organization. What are these other accounts called, which attributes do they contain, and what is their purpose?

8. [1 points] Consider a hypothetical deployment of Ethereum where all the transactions submitted to Ethereum are issued by honest participants. In this scenario would gas still be necessary? Why?

9. [1.5 points] What is the concept of reentrancy? Explain, using the example of the DAO attack, which assumption made by smart contract programmers was invalidated by reentrancy.

Smartcards

10. [1.5 points] Suppose that a smartcard uses the following code to check a PIN that was input from a terminal:

```
bool check_pin(const char input[]){  // adapted from Wikipedia, lic. CC BY-SA 4.0
  const char correct_pin[] = "123456";
   if (strlen(input) != strlen(correct_pin)) return false;
   for (int i=0; i<strlen(correct_pin); i++){
       if (input[i] != correct_pin[i]) {
           return false;
       }
   }
   return true;
}
```

This code snippet contains several vulnerabilities to simple power analysis attacks. Rewrite it below to fix these vulnerabilities.

TEEs.

11. [1 point] Trusted Execution Environments, and SGX enclaves in particular, provide three main security mechanisms. Discuss one of those mechanisms and provide an example scenario where it could be used.
