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

1st Exam – June 18, 2020 – Duration of the exam: 1 hour

The answers should be handwritten in paper and uploaded to Fenix under project "First Exam" as a single PDF file. The PDF file must have the format <number>-<firstName>_<lastName>.pdf

Each sheet of paper used for the answers must have the student's name and number. Sheets that are not properly identified will not be evaluated. **In the first page, write down the Commitment of Honor below, followed by your signature:**

"By submitting this assessment online, I declare on my honor that I will solve the exam using only the authorized consultation elements, autonomously and without exchanging any information by any means, with any person or information repository, physical or virtual."

Submissions that fail to include the Commitment of Honor in the first page will not be evaluated.

For each question, the recommended number of lines for the answer is provided at the end of the question. Answers can be provided in English or in Portuguese.

All answers must be justified.

Dependability and Security

1. The concepts of Dependability and Security have in common the attributes of Availability and Integrity. Discuss the different notions of Availability within the scope of Dependability and Security. Discuss the different notions of Integrity within the scope of Dependability and Security. *[10 lines]*

2. The altitude and speed of a cargo space craft are essential measurements that must be reported back to Earth, in near real-time and as efficiently as possible, when the space craft is in flight. Each measurement consists of a 32 bit integer. The confidentiality of these measurements is fundamental for the safety of the space craft. Which cryptographic primitives would you use to protect the messages containing the measurements? *[5 lines]*

Fault tolerance

3. Consider a 32 bit hardware adder module installed in a system where reducing costs is more important than performance. The adder suffers a fault that causes the least significant bit to be stuck at 1. Describe which fault tolerant technique could be used to detect the error in this module? *[5 lines]*

Smartcards

4. How can a smartcard ensure that it is being read by a trusted smart card reader? *[5 lines]*

5. An oil company provides smart cards to its thousands of employees that allows them discounted prices at the gas stations of the company. You are hired as a security consultant after the card was copied and non-employees were found using it too. What will be your recommendations to avoid the repetition of this security breach. Justify each recommendation and its feasibility. *[10 lines]*

Fault tolerant distributed algorithms

Consider the following specification of a variant of the broadcast problem, where a fixed set of processes can have several "send(m)" events and several "deliver(m)" events, and all messages *m* in send(*m*) are distinct. Correct processes are defined as not crashing throughout the entire execution.

> [Property 1] If a correct process sends m, then it eventually outputs deliver(m).
> [Property 2] If a correct process outputs deliver(m), then all correct processes eventually output deliver(m).
> [Property 3] A message m cannot be repeated in the output of any correct process, and if a process outputs deliver(m), then m was previously sent.
> [Property 4] If, for a given correct process p, the event p.deliver(m1) precedes the event p.deliver(m2), then for any other correct process p', the event p'.deliver(m2) cannot precede p'.deliver(m1).

6. For each of the properties above, provide a trace (i.e. a sequence of send and deliver events) where that property is violated and all the other properties are preserved. Justify. *[10 lines]*

7. Do the broadcast specifications studied in classes satisfy the properties above? If yes, justify. If not, discuss how the specification above could be met. *[10 lines]*

Byzantine Fault Tolerance

8. Consider the Byzantine Broadcast (BB) problem and a system with N processes. Each process p starts an instance of BB and broadcasts a message m. After all instances of BB terminate, are all processes guaranteed to have received the same set of messages? *[10 lines]*

9. The messages exchanged by processes participating in the Authenticated Echo Broadcast and Double Authenticated Echo Broadcast implementations always contain a bcb and brb identifier, respectively. What is the role of this identifier? Is it possible to optimize the size of the messages by removing these identifiers? *[5 lines]*

Blockchain

10. When creating a block in a permissionless blockchain, miners include their own identifier in the block so that they can get a coin as a reward for producing the block. This implies that two miners might concurrently produce two distinct blocks hence leading to forks. Now, consider an hypothetical system where rewards are provided by an external mechanism and hence miners no longer need to include their identifier in the blocks they produce. In this system, are forks still possible? *[5 lines]*

[3 points] Trusted computing

11. The TPM_Extend operation is the only operation that allows applications to extend the Platform Configuration Registers (PCR) with data. Why is it not possible to write/overwrite data directly to a PCR? *[5 lines]*

12. Recall the scope of the project, where it was required to implement Byzantine registers to build a dependable service. Now, assume you have access to trusted hardware that can be deployed at the servers and/or clients. Discuss its impact on the system design and on the resulting trade-offs. *[10 lines]*

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