

Jun 25, 2024

# Introduction to Computer and Network Security

## Part 1

### Question 1 [70 points]

A software company just announced the latest feature for its operating system: WinDoss. The feature, called Memento, consist of a system that periodically captures screenshots of the monitor and stores them in a folder. The screenshots are then used to fill a searchable database containing all the text automatically extracted from them.

Consider that:

- the screenshots are stored without encryption;
- the folder in which the screenshots are stored can be accessed without any kind of control;
- the content of the folder can be tampered with, allowing to add and delete unwanted screenshots.

You are a security expert called to comment on the new feature. Preliminarily, you must clarify some general notions:

1. [5 points] describe the CIA triad;
2. [5 points] describe the authenticity and non-repudiation security properties;
3. [25 points] describe the architecture of an access control system encompassing authentication and authorization; along with a drawing of its structure;

and then answer the following questions about the feature Memento feature of the WinDoss operating system:

4. [10 points] how can an attacker interfere with each element of the CIA triad?
5. [10 points] does the Memento feature provide authenticity and non-repudiation? Why?
6. [10 points] is it ok to store the hash of the screenshot if we want to extract their content at a later time? Why?
7. [5 points] consider a computer with a single user and with this feature enabled. Would applying pseudonymization techniques (to the screenshots) protect the privacy of the user?

## Part 2

### Question 2 [30 points]

In the context of data protection and privacy, (a) explain the linkage attack on anonymized dataset with an example, (b) explain the trade-off between anonymity and utility in the context of realizing data sets, and (c) describe the technique of k-anonymity and explain how it can mitigate linkage attacks.

---

Please, remember...

Be sure to annotate the following information on each used sheet of paper (possibly, 2 sheets at most)

- Name
- Surname
- Student ID number
- Question number