



Congratulations! You passed!

TO PASS 80% or higher

Keep Learning

GRADE

100%

Week 3 - Problem Set

LATEST SUBMISSION GRADE

100%

1. Suppose a MAC system (S, V) is used to protect files in a file system

1 / 1 point

by appending a MAC tag to each file. The MAC signing algorithm S is applied to the file contents and nothing else. What tampering attacks are not prevented by this system?

- ☒ Changing the last modification time of a file.
- ☐ Replacing the contents of a file with the concatenation of two files on the file system.
- ☐ Changing the first byte of the file contents.
- ☐ Replacing the tag and contents of one file with the tag and contents of a file from another computer protected by the same MAC system, but a different key.



Correct

The MAC signing algorithm is only applied to the file contents and does not protect the file meta data.