

CS 461 / ECE 422 Information Assurance

HW #2

Due submitted to Compass by 3:30 p.m. Feb. 28

1. Of the two ways of ways of slicing an Access Control Matrix (by row, or by column), explain which of these (if either) would likely be faster at checking an access by a given user to a given object. Explain which of these (if either) would likely require less overall storage space than another.
2. Consider a Unix system, and a file `/home/prof/ece422/exam/key.doc`. `prof` is a user, with home directory `/home/prof`. `staff` is a group that contains `prof` and user `TA`. Suppose that the permissions on these directories (and file) are

Name	user	group	permissions
home	root	root	drwxr-x-r-x
prof	prof	staff	drwxr-x—x
ece422	prof	class	drwxr-x—x
exam	prof	prof	drwxrwx---
key.doc	prof	staff	-rw-r-xr-x

- Which of the following accesses are permitted (circle)
- User `prof` can delete file `key.doc`
  - User `TA` can add a new file `corrected-key.doc` to subdirectory `exam`.
  - User `student` can read file `key.doc`
  - User `TA` can execute the `ls` command on path `/home/prof/ece422` and see all the names of files and directories it contains.
3. Describe the difference between segmented memory, and paged memory, with respect to the security mechanisms each can employ and efficiency of memory use.
  4. Could one implement a “tagged architecture” in software only, or is it absolutely necessary for there to be hardware support? Discuss the issues and any tradeoffs that may exist.
  5. Suppose that a password may be comprised of any strings from the set `{a-z, A-Z, 0-9, -, _, ~, !, @, #, $, %, ^, &, *, +, -}`, with the provision that the first character must be alphanumeric (e.g., from `a-Z`, `A-Z`, or `0-9`). An “attack” is considered to be the event that an attacker obtains a list of 100 password hashes, where the attacker knows that a hash output comes from is one of 4096 different possible hash functions that the attacker can compute. The attacker can generate, hash (once) and test against the list  $10^6$  passwords per second (the hash+test is the dominate cost, you can assume the password itself takes 0 time to generate). How long should the system administrator insist passwords be to ensure that the probability of any one of the passwords being discovered in 1 year of sustained attack is less than 0.1? For simplicity, assume
    - a. That all passwords are exactly of the minimum length
    - b. The attacker knows this password length
    - c. The attacker generates passwords at random (allowing for duplicates)