CS590 DSP: Data Security and Privacy **Spring 2022**

Homework #1

Due date & time: 11:59pm on February 1, 2022. Please hand in your homework on Brightspace.

Late Policy: You have three extra days in total for all your homeworks and projects. Any portion of a day used counts as one day; that is, you have to use integer number of late days each time. If you exhaust your three late days, any late homework won't be graded.

Additional Instructions: (1) The submitted homework must be typed. Using Latex is recommended, but not required.

Problem 1 (10 pts) Confidentiality, Integrity, Availability.

- (3 pts) State what is Confidentiality, Integrity, and Availability.
- (3 pts) For each, give two examples where they are violated.
- (4 pts) Identify two computer security control measures on your computer(s). Which of the three properties Confidentiality, Integrity, and Availability do they aim at providing? What kinds of adversaries they **cannot** defend against?

Problem 2 (10 pts) Unix Access Control.

- (2 pts) Explain why the setuid bit is needed in UNIX DAC?
- (4 pts) What security problems can be caused by using the setuid bit? What can one do to mitigate the problem?
- (4 pts) Explain how the sticky bit on directories affect UNIX file access control, and why it is needed.

Problem 3 (15 pts) More Unix Access Control. On a UNIX/Linux system, create a directory, that includes sub-directories the following. Submit a printout of running "ls -ailR" on this directory. You can copy/paste the printout into your homework.

- A sub-directory named "dir1" such that any other user on the system can create/delete any files under the directory, but cannot do a listing of the file names in the directory.
- A sub-directory named "dir2" such that any other user on the system can create files in the directory, can do a listing of the file names in the directory, but can delete only the files owned by the user.
- A sub-directory named "dir3" such that any other user can see the file names under the directory, but not access any of the file.
- Create an executable file with name "test" under "dir1" such that the setuid bit on the file is set.
- Create a hard link with name "test" under "dir2" to the file dir1/test.

- Create a symbolic link with name "test" under "dir3", and make it point to the file dir1/test.
- After submitting the printout, delete either dir1/test, and see how this affect dir2/test and dir3/test. Describe your findings.

Problem 4 (20 pts) Read Chen, Wagner, and Dean: "Setuid Demystified"
https://www.usenix.org/legacy/events/sec02/full_papers/chen/chen.pdf

Answer the following problems. Don't write too long, stay within one page for the answer.

1. Describe a way to support both permanent and temporary dropping of privileges using just euid and ruid.
2. Use your words to describe the two security vulnerabilities identified in Section 7 of the paper.
3. Summarize the guidelines in Section 8 of the paper.

Problem 5 (20 pts) Read Norman Hardy's "The Confused Deputy".

https://dl.acm.org/doi/10.1145/54289.871709

- Explain what is the confused deputy problem.
- Explain how capability-based system solve the confused deputy problem.
- Explain how is the confused deputy problem manifested in setuid root programs in UNIX DAC, and how this problem is addressed in UNIX DAC.
- Recall the weaknesses exploited by the malwares we have examined (Morris). Are they related to the confused deputy problem?

Problem 6 (25 pts) Read the paper "Linux Capabilities: making them work" by Serge E. Hallyn and Andrew G. Morgan.
https://www.kernel.org/doc/ols/2008/ols2008v1-pages-163-172.pdf

- Explain what are the advantages and disadvantages of capability model compared to `setuid-bit` and effective UID approach.
- Is it true that the capability bounding set can only affect the permitted capability set? Can a process still run with capabilities suppressed by the bounding set? Explain your answers.
- What secure risk(s) will be introduce if a process can add capabilities back into its bounding set?