CS590 DSP: Data Security and Privacy **Duc Viet Le**
Spring 2018

Homework #1

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

- (3 pts) State what is Confidentiality, Integrity, and Availability.
  Answer:

  Confidentiality is about avoiding unauthorized disclosure of information and allowing those who are authorized to have access to the information.

  Integrity is about avoiding unauthorized modification of information and allowing authorized parties to modify in a permitted way.

  Availability is about making sure authorized users have access to data or services.

- (3 pts) For each, give two examples where they are violated.
  Answer:

  Confidentiality Using different analysis techniques to detect hidden communications or deanonymize anonymous identities (i.e. Netflix Deanonymization). Another example is cryptography attacks on encryption scheme like padding oracle attack to decrypt ciphertext of CBC mode encryption.

  Integrity One example is that there is no integrity checking for DNS queries, and it's a reason for DNS poisoning attack (i.e. Kaminsky attack). Similarly, there is no integrity checking for ARP queries in LAN network, and it's the reason for ARP poisoning attack.

  Availability One example is about DDos attacks on website services. Another example is that one can prevent authorized user from accessing the system by trying to login to the system with a wrong password multiple time to trigger its defend mechanism.

- (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?

  Answer:

Security Control Measures	Confidentiality	Integrity	Availability
SSL/TLS communications	X	X	
Bot detection/CAPTCHA			X

  - SSL/TLS may not be able to defend against adversaries who try to perform an DDOS attack by creating lots of connections.
  - Weak bot detection or CAPTCHA may not provide integrity checking or may not have lots of different challenge;therefore, those mechanisms may be subjects for adversaries who perform replay attacks (i.e. record and reuse same responses for certain challenges)

Problem 2 (10 pts) Unix Access Control.

- (2 pts) Explain why the setuid bit is needed in UNIX DAC?
  Answer. Because some operations are not modele as files. System integrity requires more than controlling who can write but how it's written

- (4 pts) What security problems can be caused by using the setuid bit? What can one do to mitigate the problem?
  Answer. Those program can setuid as root; therefore, if those programs are compromised by attackers.Then, attackers will have root access to the system. The program with setuid should be able to drop its privilege either temporary or permanently. The reason is that the program should only use the minimum privilege to perform its task to mitigate the risk of being compromised by attackers.
- (4 pts) Explain how the sticky bit on directories affect UNIX file access control, and why it is needed.
  Answer. If the sticky bit is set then only the directory's owner or root can rename or delete directories. It's needed and normally set for those directories shared by others (e.g \tmp) to prevent users with write and execution permissions from deleting or moving other users' files.

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 (15 pts) Read Granham & Denning: "Protection: Principle and Practice"
https://dl.acm.org/citation.cfm?id=1478928

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

1. Describe three places in computing/information systems where access control is used.
   Answer.
2. Describe one experience that you were frustrated by the existence of (or lack of) access control mechanisms and what you wish the access control would be changed. If you have not frustrated by access control before, think about one place where access control could be improved.
   Answer.
3. Identify one vulnerability/attack so that can be attributed to problems in the access control mechanisms?

   Answer.

Problem 5 (15 pts) Read Norman Hardy's "The Confused Deputy".

http://zoo.cs.yale.edu/classes/cs422/2010/bib/hardy88confused.pdf

- Explain what is the confused deputy problem.
  Answer. When a program runs with authority from two different sources, the program serves two masters and carries authority for each to perform it duties, and it has no way to keep those two instructions apart. In the paper presented, the confused deputy problem happened when the compiler was given home file license (one authority) to write files in its home directory, and by providing (SYSX)BILL as file name, user (other authority) who runs (SYSX)FORT can overwrite billing file with debug information.
- Explain how capability-based system solve the confused deputy problem.
  Answer. In capability-based system, to perform an access to a file, the program will be given a direct capability to the file. The capability will identifies the file and authorizes the program an access on that file. In this case, the os will know directly what file the compiler should have access to.
- Explain how is the confused deputy problem manifested in setuid root programs in UNIX DAC, and how this problem is addressed in UNIX DAC.
  Answer.
- Recall the weaknesses exploited by the malwares we have examined (Morris). Are they related to the confused deputy problem?

  Answer.

Problem 6 (15 pts) Read the following article

- Ken Thompson's "Reflections on Trusting Trust"
  https://dl.acm.org/citation.cfm?id=358210

Write a brief summary which should include: (i) How the attack described in Thompson's article work? How can it be used to compromise the security of real world systems? What are the most effective ways to defend against the attack? What have you learned?

Problem 7 (20 pts) Read Sections I and II of the report Bell La Padula: Secure Computer Systems: Unified Exposition and Multics Interpretation. Describe the Bell La Padula model as given in the report.

http://seclab.cs.ucdavis.edu/projects/history/CD/bell76.pdf