EECS 565 Intro Information & Computer Security

Homework 2

Your name:

Authentication.

1. User Alice wants to access the File Server (FS) in a private network through Kerberos. So, she first logs in to the Authentication Server (AS) and authenticates herself using her password. During the login session, Alice and AS exchange the following messages:

   Alice → AS: m1= ID_TGS||timestamp_Alice
   Alice ← AS: m2 = **ENC**(< K_1||Ticket_TGS||ID_TGS||timestamp_AS >, K_Alice)
   where Ticket_TGS = **ENC**(< K_1||ID_Alice||ID_TGS||timestamp_AS||lifetime>, K_TGS).

   Assume: K_Alice is the secret key of Alice and K_TGS is the secret key of the Ticket-Granting Server (TGS). ENC(m,k) denotes using a symmetric key encryption algorithm to encrypt the message m with the key k, and "||" denotes concatenation.

   a. Please explain how could the AS verify the secret key K_Alice.
   b. What is K_1? Who generate it?
   c. Can Alice read the content of Ticket_TGS? Can Alice forge the ticket? Can Alice reuse the ticket in another time?
   d. How could the ticket-granting server authenticate Alice?

2. Please explore the certificates pre-installed in your browser and pick one certificate as an example to show its CA, the principal, signature, timestamp, and expiration. (You can describe the data or use a screenshot and note the content)

Database Security.

3. To prevent the inference attacks, the database systems implement multiple controls. Please list these controls discussed in the lecture and pick one to explain which type of inferences it prevents.

4. What is the tracker attack? Can we use access control to prevent this attack? If so, briefly explain how this access control could be impletemented?

Operating System Security

5. What is protection domain?

6. Protection domains can be implemented with access control matrix. Consider a system with 3 files (F1-F3) and a printer. 4 protection domains are defined: (1) a process running in domain D1 can read files F1 and F3; (2) a process in domain D2 can read F2, write F3, and execute F1; (3) a process in domain D3 can print files to printer; (4) a process in D4 has the same privileges as the one in D2. In addition, it can also read F3 and write F2. Could you please compose an access control matrix to describe the protection domains in this system.

	F1	F2	F3	Printer
D1	read		read	
D2	execute	read	write	
D3				print
D4	execute	read, write	read, write	

7. Set user (setuid) and set group (setgid) programs are powerful mechanisms provided by the Unix system to manage access to sensitive resources through control invocation. However, because of this, this mechanism has potential security risk. Bugs in such programs have led to many compromises. Please briefly explain why this mechanism is needed in Unix and which security problems a bugged setuid program may cause.

Software Security

8. Explain how to use "NOP sledding" to assist buffer overflow attacks.

9. Standard C library functions such as gets(), strcpy(), sprint() are unsafe. Take gets() and fgets() as an example, explain why fgets() is more secure.

10. The below program has a buffer overflow vulnerability. Please identify the unsafe function used in the program and explain why.

```
void hello(char *tag){
    char inp[16];
    printf("Enter value for %s: ", tag);
    gets(inp);
    printf("Hello your %s is %s\n", tag, inp);
}
```