IEMS5710A Assignment #2

Due: 8 Dec 2024

Problem 1: Hash Functions

(1) Assume that partial `sha1` hashcode and partial password plaintext have been disclosed, find the complete password plaintext.

- Partial password: `1*m*-*7*o`
- Partial hashcode: `f4de626*6792a8a*f1b8154*d448a5a*ddc44f1*`

(2) One server has experienced a data breach, exposing the hash codes of 50 users, as detailed in `Problem1_md5_shadow.txt`. The hash codes were generated using the `md5` hash function, combining 8-digit passwords with random salt strings. Can you recover the original passwords?

Problem 2: Buffer Overflow

The following code aims to check the password input by the user. If `strcmp()` checks the user input equals to the stored password, then `unlock()` function gives the corresponding permission to the user, otherwise not.

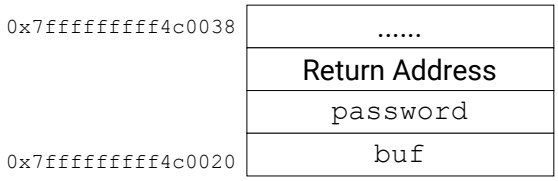
```
void get_password(chat*);
void unlock();
void backdoor();

void check_password() {
    char password[8];
    char buf[8];

    get_password(password);
    gets(buf);
    if (strcmp(buf, password) == 0)
        unlock();

label:
    return 0;
}
```

Assume that this program runs on a 64-bit x84 Linux machine, and the stack at point `label` (*i.e.*, before `check_password()` returns) is shown as follows:



(1) Explain why using `gets()` functions is vulnerable. How to eliminate this vulnerability?

(2) This program is vulnerable to a buffer overflow attack, allowing the user to grant permission without providing the correct password. Explain the reason for this vulnerability and demonstrate how to exploit it.

(3) `backdoor()` is located at address `0x41f`. Construct a string that will jump the program into the function `backdoor()`.

Problem 3: T/F Questions

- (True/False) A TLS session may use more than one key when transmitting data from a client to a server.
- (True/False) Hashcode can be used to defense MITM attacks.
- (True/False) IPSec and SSL/TLS operate on the same layer in the OSI model.
- (True/False) A birthday attack is used to find the preimage of a given hash code.