CS-301 Fall 2020 Mini-Exam 3

September 15, 2021

1 Adversarial Thinking

The infamous hacker group WHACK plans to steal a total of 1,000,000 CHF from the accounts of NotSoSec Bank. WHACK have already gained access to the transferMoney.php script running on the bank's web server which receives input from the web form shown in notSoSecOnline.html. From the web server script WHACK learns that, other than the account holder, also the bank's director has the right to issue small money transfers from any of the bank's accounts. From Twitter, WHACK learns that the bank's director is very passionate about skiing and often checks the weather forecast for the mountains. Assuming that WHACK can not directly modify the transferMoney script, describe an attack that could enable WHACK to reach their goal of stealing 1,000,000 CHF. What class of common weaknesses is your suggested attack?

transferMoney.php

```
<?php \n
/* start session */
session_start();
switch ($_SESSION[ username ]) {
  case $_POST[ account_holder ]:
    /* Check if current sessions user matches account holder */
    $origAccount = getAccount($_POST[ account_holder ]);
    $destAccount = getAccount($_POST[ destination_account ]);
    /* Check that requested amount is below threshold
                          for high risk transfer */
    if ($_POST[ amount ] > 500,000) { //if higher terminate session
        echo "The requested amount is too high.";
        exit;
    }
    /* If all conditions fulfilled transfer
    requested amount to destination account */
    send_money($origAccount, $destAccount, $_POST['amount'])
    break;
```

```
    case $usernameDirector:
        /* Check if current session's user is the bank's director */
        $origAccount = getAccount($_POST[ account_holder ]);
        $destAccount = getAccount($_POST[ destination_account ]);
        /* Check that requested amount is below threshold
        for high risk transfer */
            if ($_POST[ amount ] > 10,000) { //if higher terminate session
                echo "The requested amount is too high.";
                exit;
            }
        /* If all conditions fulfilled transfer
        requested amount to destination account */
        send_money($origAccount, $destAccount, $_POST['amount'])
        break;
    default:
        /* If current sessions user is neither account holder
        nor director end session */
        echo "Only the account holder or the bank director can
                    issue this payment!";
        exit;
}
?>
```

notSoSecOnline.html

```
<h3>
  NotSoSec Online Banking
</h3>
<form action="/url/transferMoney.php" method="post">
 Name of Account Holder: <input type="text" name="account_holder"/><br/>
 Name of Destination Account: <input type="text"
                                name="destination_account"/><br/>
 Requested Amount: <input type="text" name= amount ">
   <input type="submit" name="submit" value= Transfer ">
</form>
```

2 STRIDE

After the release of the COVID-19 vaccine, life is back to normal. The EPFL bar, Satellite, is re-opening. In order to celebrate this event, Satellite decides to have a special offer where if a student buys a beer, they get an additional free beer. If a professor buys a beer, they also get a free beer. There is an extra condition that this offer is only valid up to a purchase of three beers for professors. Students do not have a limit on this offer; they can purchase as many beers as they want and they get a free beer for every purchase.

When a customer orders a beer at the bar, the bartender first checks their CAMIPRO for their status (student/professor). The bartender updates a log-book with the customer's ID, status, and the number of beers that they have purchased. If they are eligible for free beer, they provide the free beer along with the purchase.
Perform a STRIDE analysis of this scenario. Write three possible threats (three letters of STRIDE). For each threat, describe what can go wrong and suggest a possible countermeasure to fix it.

3 What you know or who you are

You are opening a new bank account at NotSoSec Bank and are asked to choose between two different authentication mechanisms to access your online account.
Option 1 is to use an 8 character password that would be stored as a salted hash on the bank's server.
Option 2 is to use your fingerprint with a dedicated fingerprint reader provided to you by the bank. To authenticate, the reader sends your fingerprint to the bank's server where it is processed and compared to the stored biometric template.
Once you have decided on the authentication mechanism you will not be able to change it.
Which of the two options would you choose in this case? Why do you think this is the favourable option? Justify your choice in relation to the use case in the question. Take into account security considerations, as well as the usability advantages and disadvantages of these mechanisms mentioned in the lectures.

4 What you know or what you have

You are opening a new bank account at NotSoSec Bank and are asked to choose between two different authentication mechanisms to access your online account.
Option 1 is to use an 8 character password that would be stored as a salted hash on the bank's server.
Option 2 is to use a card reader provided to you by the bank that establishes a shared secret with the bank's server for every new login attempt. To authenticate, you have to insert your card into the reader which generates a random 12 digit number that you have to type into the bank's login website.
Once you have decided on the authentication mechanism you will not be able to change it.
Which of the two options would you choose in this case? Why do you think this is the favourable option? Justify your choice in relation to the use case in the question. Take into account security considerations, as well as the usability advantages and disadvantages of these mechanisms mentioned in the lectures.

5 What you have or who you are

You are opening a new bank account at NotSoSec Bank and are asked to choose between two different authentication mechanisms to access your online account.
Option 1 is to use a card reader provided to you by the bank that establishes a shared secret with the bank's server for every new login attempt. To authenticate, you have to insert your card into the reader which generates a random 12 digit number that you have to type into the bank's login website.
Option 2 is to use your fingerprint with a dedicated fingerprint reader provided to you by the bank. To authenticate, the reader sends your fingerprint to the bank's server where it is processed and compared to the stored biometric template.
Once you have decided on the authentication mechanism you will not be able to change it.
Which of the two options would you choose in this case? Why do you think this is the favourable option? Justify your choice in relation to the use case in the question. Take into account security considerations, as well as the usability advantages and disadvantages of these mechanisms mentioned in the lectures.

6 ASLR infoleak

You are trying to exploit an executable, CanYouHackMe, on a system that has ASLR enabled. CanYouHackMe uses libc version X. Using your amazing hacking skills, you have managed to find the address of the printf() function. Does knowing the address of printf() help you determine any other libc function's address? Justify your answer.

7 Better Prevent than cure?

You get hired by the security team at Coldcloud, a content delivery network with thousands of users. Next month, Coldcloud will be the live content provider for the final of a League of Legends tournament with millions of fans. Fearing the increase in customers, they program their servers to be able to receive and execute scripts received by the function increaseCapacity(script). This way, they can write the scaling script on the fly, adapting it to the number of customers. To avoid that a rogue employee can create havoc with this script. They ask you whether it is better to implement Data Execution Prevention, a Stack Canary, both, or none. Make a recommendation and justify your answer.Justify.
(Recall that they are trying to serve millions of users, and countermeasures are costly, so they should only be implemented if they address a problem)

8 Exchange1

Alice sends a message m to Bob as follows:

$Enc(pkb, o), Sign(ska, o), m$ xor o, where o is a random string with length double the length of m, $(len(o) = 2 * len(m))$.

Can Bob read the message? Can Bob be sure that the confidentiality and integrity of the message is preserved? Can Alice repudiate having sent the message? Justify your answer.
Alice and Bob know each other's public key.
- $Enc(pkb, x)$ - Asymmetric encryption of x with B's public key.
- $Sign(ska, x)$ - Digital signature of x with A's secret key.

9 Exchange2

Alice sends a message m to Bob as follows: $Enc(pkb, k), Sign(ska, k), Stream(k, m)$, where k is a randomly generated symmetric key.

Can Bob read the message? Can Bob be sure that the confidentiality and integrity of the message is preserved? Can Alice repudiate having sent the message? Justify your answer.
Alice and Bob know each other's public key.
- $Enc(pkb, x)$ - Asymmetric encryption of x with B's public key.
- $Sign(ska, x)$ - Digital signature of x with A's secret key.
- $Stream(k, m)$ - Encrypting *m* with a stream cipher with the symmetric key k.

10 Exchange3

Alice sends a message *m* to Bob as follows:

$k1$, $Enc(pkb, k2)$, $Stream(k1$ xor $k2, m)$, $Sign(ska, m||k1)$, where $k1$ and $k2$ are randomly generated symmetric keys.

Can Bob read the message? Can Bob be sure that the confidentiality and integrity of the message is preserved? Can Alice repudiate having sent the message? Justify your answer.

Alice and Bob know each other's public key.
- $Enc(pkb, x)$ - Asymmetric encryption of x with B's public key.
- $Sign(ska, x)$ - Digital signature of x with A's secret key.
- $Stream(k, m)$ - Encrypting m with a stream cipher with the symmetric key k.
- $x||y$ - Concatenation of two string x and y.

11 Destination Hawaii

You decide to use GoVacation, a new program that allows you to reserve very cheap hotel rooms for your vacations. Someone leaked to you the source code, so you know how the executable works. Provide a line that contains a bug in

this code and explain if you could use it to reserve a room even if there was no space at the destination. If the programmer used a stack canary, would you still be able to exploit the bug?

```
int customers[100] = { 0 };
/* array of 100 integers initialized to 0 */
char checkReserved(char* destination) {
        /* function to check online whether a room is reserved */
        /* it returns a room number if the destination has space */
        /* it returns 0 if the destination does not have space */
        /* if the destination does not exist, it crashes */
}
1: int GoVacation(int customerID) {
        /* one byte: room number if destination has free room, 0 otherwise */
2:              char room;
        /* destination name  */
3:              char destination[40];
        /* reads desired destination from keyboard */
4:              gets(destination);
        /* checks in there is a room in the destination */
5:      room = checkReserved(destination);
        /* if there is room, assign it to the customer */
6:              if (room != 0) { customers[customerID] = room };
7:              return 0;
   }
```

12 RoboTAs

The COM-301 TAs want to go early to Sat, so they need to grade fast.They have decided to automate the process using machine learning.
As this function cannot be integrated in Moodle, they write their own script to generate the mini-exam. One student got the chance to see one of the TAs screens over their shoulder and they have the script and are making it available for the rest of the class. Provide a line that contains a bug in this code and explain if you could use it to increase your grade. If the TA used a stack canary, would you still be able to exploit the bug?