Name: Le Dao
CS166-02
Homework 1

Problem 1- 4, 6, 10-13, 15 chapter 1
Write a paragraph about an exploit in the news using terminology from chapter 1
Run hw1.c

Problem 1

a. Confidentiality is protecting the information from unauthorized reading. Integrity is protecting the information from being changed. Availability is allowing data to be accessible to the right person.
b. Example that confidentiality is more important than integrity is that you have some sensitive photos, or explicit content in your smart phone. What matter the most in this case is preventing them from hackers out there who might have your sensitive content published to the internet.
c. Example that integrity is more important than confidentiality is in banking system. For banks, the first concern is integrity, then second concern is confidentiality. The first problem that customers are worried is someone taking money from their account, instead of someone know how much money in their account.
d. Example that availability is an overriding concern: government press releases. They have to be accessible to the public at all time.

Problem 2

From a bank's perspective, usually the integrity of its customer's data is more important on both customer's view and the bank's view.

Problem 3

a. Confidentiality is represented in AOC through credit cards information of the players who pay a monthly fee to play chess, it is important because hackers might try to retrieve the credit cards numbers.
b. Players of AOC might get their scores changed.
c. Availability is concerned because a DDoS might happen to the service.

Problem 4 (AOC)

a. Cryptography is used to encrypt customers' credit card numbers, that lead to their home address, etc.
b. Access control is used in authentication, such as customer/player has to enter password when they want to log in.
c. Security protocols can be used to help encrypting credit cards information over the networks.
d. Software should also be concerned in AOC in some cases. For example, the software that AOC's customers downloading has to be secured.

Problem 6

a. Some privacy concerns that deals with RFID tags are tracking people.
b. Three concerns that deals with security concerns are tempering of RFID devices, cryptographic tools that protect RFID, and the cloning of RFID devices.

Problem 10

a. The Germans can make a new cipher machine, or sending false messages that make the Allies think they are true.
b. The Nazi probably did not know that Enigma was broken, or they thought that “some security is better than no security”

Problem 11

a. Biometric authentication would work fine. Modern day iPhone is using fingerprints instead of password.
b. We can use a yubi key for two factor authentication for Gmail account.
c. Gmail account can be set up with two factor authentication. User must enter their password as normal, then uses either a yubikey, or their cell phone to complete the second step logging in.

Problem 12

a. Sometimes when I want to download a software, or anything from a cloud storage, a captcha is required. In order to solve a CAPTCHA, I have to look at a picture and enter the letters in that particular picture.
b. Machine learning
c. Look and guess
d. The CAPTCHA might bring difficulties for old people, people who have limited vision/hearing.
e. I have to enter every time I want to gain access to something.

Problem 13

a. “When the protocol fails, a brief warning is given to Alice and Bob, but the transaction continues as if the protocol had succeeded, without any intervention required from either Alice or Bob.” - this is suitable to convenience but provide no security at all.
b. “When the protocol fails, a warning is given to Alice and she decides (by clicking a checkbox) whether the transaction should continue or not.” - this method might work the best, if and only if the warning is sent directly to Alice through her email/personal phone number.
c. “When the protocol fails, a notification is given to Alice and Bob and the transaction terminates.”- this method is secured, but provide little to no convenience. One solution for this could be in previous situation.
d. “When the protocol fails, the transaction terminates with no explanation given to Alice or Bob.” - this method provides to convenience to the customer at all, despite being secured.

Problem 15

a. Because hacker can take advantage of the bug to bring damages.
b. Again, Trudy can exploit the software through a bug.
c. By operating an exploit.

Current event

Around the end of November 2017, hackers were exploiting a vulnerability to expose Tor Browser users in Firefox. Basically this zero day exploit affected Firefox by exploit against Tor Browser users by anonymous attackers to leak identifications of the users. How it worked was a **malware** that ran in the background of Windows OS via memory corruption flaw in Firefox browser.

Link to article: http://thehackernews.com/2016/11/firefox-tor-exploit.html

Hw1.c

```
/*
 * Name: Le
 * Class: CS166-02
 * Date: January 1 2016
 */
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

/*
 A sample run of this program, compiled to the executable 'revstr':
       $ ./revstr
       Usage: ./revstr <word to reverse>
       $ ./revstr hello
       Rev string is olleh
       $ ./revstr racecar
       Rev string is racecar
       $ ./revstr spartan
       Rev string is natraps
 */

 void myreverse(char* input, char rev[], int len)
 {
        int x;
        for (x = len - 1; x >= 0; x--)
        {
               rev[len - 1 - x] = input[x];
        }
        rev[len] = input[len];
 }

/**
 * You may ***NOT** change the main method in any way.
```

```
 */
int main(int argc, char* argv[]) {
  if (argc < 2) {
        printf("Usage: %s <word to reverse>\n", argv[0]);
        exit(1);
  }
  char* input = argv[1];
  int len = strlen(input);
  char rev[len + 1]; // Adding one for the null terminator
  myreverse(input, rev, len);
  printf("Rev string is %s\n", rev);
}
```