Homework 1: SY308

MIDN Mckenzie Eshleman

1. An ATM machine uses three different pillars of cybersecurity being confidentiality, authentication, and integrity. For confidentiality the ATM is trying to protect the users account information from unauthorized access. Having the user input their card and then the pin helps allow for only the authorized user is using the ATM. For authentication the two factor process of inputting the atm card and putting in the correct pin helps verify the identity of the correct user. The last pillar is integrity meaning the protection of information of the user's account information from any unauthorized modifications. Two examples of security principles that could be added is another form of authentication like finger prints since a user's card and pin can be taken. Another example would be to have a face authentication to help insure that the user is who they say they are.
2.
    a. Principle: Complete Mediation
    Explantation: The principle of complete mediation is every access must be monitored and controlled. This means that if the Big Banks servers are down or the ATM does not have a connection then an access control mechanism must be triggered and not allow access to any user. A person who had a fake card or account could then figure out when the systems are down and take $300.

    b. Principle: Fail-safe Default
    Explanation: Unless an entity is given explicit access to an object, it should be denied access to that object. Meaning that if the hacker did not insert their credit card to pay for internet service then the access should be denied.

3. Title: 30,000 Unsuspecting Rose Bowl Attendees were Scooped Up in a Facial Recognition Test

    URL:
    https://onezero.medium.com/90-000-unsuspecting-rose-bowl-attendees-were-scooped-up-in-a-facial-recognition-test-18c843909858

    First Paragraph: During the Rose Bowl game on January 1, 2020 thousands of fans were being watched. Before the game started thousands of attendees were being captured by a facial recognition system in the FanFest activity area by an ad tech company called VSBLTY. Four cameras were hidden underneath digital signs capturing data on attendees, generating 30,000 points of data on how long they looked at advertisement, their gender and age, and an analysis to try and identify weapons or whether or not they were on a watch list of suspicious persons.

Second Paragraph: This attack violates the confidentiality pillar of cybersecurity because the people that were in the FanFest did not explicitly give permission to allow their face to be recognized. After the information was leaked that VSBLTY used facial recognition many of the attendees did not know that this was happening. Neither the Rose Bowl or VSBLTY gave any statements about what happened at the game, the company did not ask permission to use live facial recognition.

Third Paragraph: Some countermeasures that could have been made to stop this kind of attack is to first ask permission or give a written or verbal message saying that live facial recognition will be taking place at the event. Then the attendees that do not want to be a part of the live facial recognition could have opted to not go to the FanFest.

4. NZRAGNFGSYFPLQCNABHAFNGZUAANSVHUBHXVXWANANFAGSLUULVMLBEWRJLUYHYUAANWK NZVXVRHXEIENHWNPWFXJBJHRL
    a. L = 3
    - NAFYLNHNUNHHXNFSUMEJYUNNXHIHPXJL
    - ZGGFQAAGASUXWAALLLWLHAWZVXEWWJH
    - RNSPCBFZAVBVANGUVBRUYAKVRENNFBR

    b. Plain Text: The goal of encryption is to maintain confidentiality that is to keep the plain text hidden from an eavesdropper.
    c. Steps: To discover the plain text of the vigenere cipher was through frequency analysis, i split the cipher text into two but could not get any results. I then split the text into the key length of 3. I then looked at the double N's on the bottom key letter which resulted to be E, this gave me the key of USN and I got the plain text above.
5. For the python code I could not get it to work. I went to MGSP and still was running into issues. This is the code I have.