CS381 Exercise 11

Name: Zhang Yupeng

Student ID: 5130309468

1. 电子银行口令卡 : it has 8X10 numbers, each time we use 2 numbers, there are 80X79/2 different choices in total. Question: why only 80X79/4 are used? (Hint: compute the complexity of attack)

Solution:

If we use all the pairs of the e-bank key card, which is $\frac{80\times79}{2}$, then we can implement the attack. We assume that the adversary can get the pair which the user has used to communicated with the bank. Then the adversary can easily get all those numbers if the pair of numbers is randomly chosen.

However, if we use only $\frac{80\times79}{4}$, the chance that the adversary get all the pairs is decreased sharply. So in the reality, we use only $\frac{80\times79}{4}$.

2. Design your own scheme for password choosing. Requirement: easy to use, change, remember and hard to break.

Solution:

To satify the demand for easy using, easy changing, easy to remember and harf to break, I design my own scheme for password generation.

First, I use 4 basic element of strings for the password, my first name " `zhang` ", my birthday " `1124` " and my favourite football team " `manutd` " and my dog's name " `yilu` ". Then I add the identifier of my account, which is the string of the company name, for example, if it's my QQ account, I use " `tencent` ", and if it's my Microsoft account, I use " `microsoft` ". Then, I combine the 4 strings together by make the first character of each string a capital character and use ' `!` ',' `!` ',' `@` ', ' `$` ' to combine them which represent 1,1,2,4 in the keyboard.

For example, my password of QQ account will be `Zhang!1124!Manutd@Tencent$Yilu` , obviously, it's meaningful and easy to remember, and it will be different in my different accounts so that even an adversary break one of my key, it cannot get all my keys. And it's hard to break because it contains many information only known to me.

3. What would happen if the server V in Denning AS Protocol is compromised?

Solution:

If the server V in Fenning AS Protocol is compromised, it's obvious that any message sent to V can be revealed to the adversary.

Since the authentication is done by the authentication server(AS), the ticket has no information about authentication, so the adversary which control the server V and intercepts the communication after the authentication stage and re-direct the transmission to connect to the server V directly. Thus the message will be attacked or leaked.

4. In example 5 and 6, there is a direction indicator (B). Find a reply attack if that B is removed, i.e., if the protocol is:

– challenge $B \rightarrow A : C$

– response $A \rightarrow B : f_{KAB}(C)$

– Hint: re-direction

Solution:

The reply attack can be implemented as following:

First, the adversary intercept all the transmitted messages between A and B and store them.

When B challenges A, the attacker intercepts the message C and send a falsified C_f to A.

When A responses, the attacker intercepts $f_{KAC}(C_f)$ and send $f_{KCB}(C)$ to B.

By reply the transmition, both A and B cannot realize the transmitted message is falsified for thatthere is no direction indicator B.