EECS 444 HW3(1)

Name: Mingan Huang

Network ID: mxh805

Q1:

Just follow every step on the slides, then change line 00401241 from “cmp EAX,EBX” to “cmp EAX,EAX”, so that this program will no longer check if the username and serial are matching and prints out we are correct. At the end save all changes into another executable file called “CRACKME_Y.exe”.

Q2:

Analyze “CRACKME.exe” using Ollydbg, then we could conclude the algorithm to generate the serial for any username is as follows:

1. Capitalize each character in the username
2. Computes the sum of all upper case characters
3. XORs the sum with 0x5678
4. XORs to serial with 0x1234
5. Check

We could either calculate the serial by hand or write up a program to calculate the serial for username.

Calculate the serial by hand:

1. Capitalize “mingan” to “MINGAN”
2. M: 77
   I: 73
   N: 78
   G: 71
   A: 65
   N: 78
   Sum = 77 + 73 + 78 + 71 + 65 + 78 = 442
3. XOR 442 with 0x5678 = 57C2
4. XOR 22466 with 0x1234 = 45F6
5. Convert “45F6” to decimal is 17910

6. Doing the same thing for all usernames
   mingan: 17910
   shifu: 17715
   yujie: 17866
   yiming: 17793

We could also use a program to calculate the serial: