EECS 444 Homework 3 Part 1

Yida Liu

October 29, 2019

1 Crackme

We change the equality condition in line 00401243 from "JE" to "JNE", which will bypass the conditions and jump to the success dialog.

```
00401243      75 07          JNE SHORT CRACKME.0040124C ; Original JE
00401245    . E8 18010000    CALL CRACKME.00401362
0040124A    .^EB 9A          JMP SHORT CRACKME.004011E6
0040124C    > E8 FC000000    CALL CRACKME.0040134D ; jump to success dialog
```

2 Crackme 2

By analyzing the assembly, we realize that the original code performs the following, for a given name

1. Sum the uppercase ASCII value of the input names.
2. XOR 0x5678
3. XOR 0x1234

After this, a number is generated as the password.