

The solution

Target : crackme 2 by Cruehead

Cracking group: BIW-reversing

Tutor: Detten

Date: 03/09/1999

OK, let's crack the bastard :)

Enter any password. Put a breakpoint on GetDlgItemTextA (type 'bpx getDlgItemTextA' in SI).

SI breaks... You can see the false password is stored in 40217E.

Trace on until you pass the call in which is checked if you use uppercases or not.

The next call is where the hash calculation takes place...

Watch and learn :)

```
:00401399 33DB      xor ebx, ebx      ->empty register ebx
:0040139B 33FF      xor edi, edi      ->empty register edi
:0040139D 8A8FA3214000 mov cl, byte ptr [edi+004021A3] ->move first letter of hash-key* to cl register

:004013A3 8A1E mov     bl, byte ptr [esi]      ->move first letter of wrong password to bl register

:004013A5 84DB      test bl, bl        ->is it the last letter?
:004013A7 7408      je 004013B1        ->if yes jmp to end of routine
:004013A9 32D9      xor bl, cl         ->XOR false password, hash-key) **
:004013AB 881E      mov byte ptr [esi], bl      ->move hash-code of false password to esi
:004013AD 46        inc esi            ->Next letter of false password
:004013AE 47        inc edi            ->Next letter hash-key
:004013AF EBEC      jmp 0040139D        ->Back to beginning of routine for next letter

:004013B1 C3        ret
```

* hash-key in address 4021A3: Messing in bytes

hex= 4D-65-73-73-69-6E-67-5F-69-6E-5F-62-79-74-65-73

** The hash calculation for every corresponding letter is:

XOR (password), (hash-key) = Hash code

Now some reversed engineering :)

The calculation: (Hash code) XOR (hash-key) = correct password

The only thing we still need to find is the hash code. We have to find the place in the program where the correct hash-code is compared with the false hash(calculated from our 'wrong' password)

We step a little further until we see the following:

```
:004013B8 33FF      xor edi, edi
:004013BA 33C9      xor ecx, ecx
:004013BC 8A0D18214000 mov cl, byte ptr [00402118]
:004013C2 8B742404   mov esi, dword ptr [esp+04]
:004013C6 BF50214000   mov edi, 00402150
:004013CB F3        repz
:004013CC A6        cmpsb ->compare!!!
:004013CD C3        ret
```

at the address 4013CC we see the correct hash-code: (d 402150)

```
Letter :   1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16
Hash code : 1F 2C 37 36 3B 3D 28 19 3D 26 1A 31 2D 3B 37 3E zie **
Hex :      52 49 44 45 52 53 4F 46 54 48 45 53 54 4F 52 4D
Dec :      R  I  D  E  R  S  O  F  T  H  E  S  T  O  R  M
```

we start with the hash-code and we reverse it to the correct password :)

for the complete newbies, a few examples...

Use the windows-calculator (or better :)

1F XOR 4D = 52 = R

2C XOR 65 = 49 = I

and so on...until you find the whole REAL password

Detten (BIW-reversing)