MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

NATIONAL TECHNICAL UNIVERSITY

"KHARKIV POLYTECHNICAL INSTITUTE"

Department of Computer Engineering and Programming

«Software Means of Information Protection »

*Laboratory work report No 8*

*Topic: «* **Reverse engineering of programs that use CLR and JVM technologies** *»*

Student:

Group. KH 919 I.E

Ayoub EL-HADDADI

Verified by:

Lecturer Viktor CHELAK

Kharkiv – 2022

***Purpose of work***:

To acquire practical skills in protecting executable files from third-party programs, creation of new functionality using implicit in use software for the x64 platform in the masm64 environment.

***Individual task:***

Variant 8: c + e\*a + f\*d + b;

Where b, c, d, e, f - At the discretion of the user (must be declared as fields), the numbers a є {a1, a2, a3, a4} are given by an array (string: name, surname).

**Algorithm of the program:**

*Program in C#:*

This program request a password from user, this password is stored is separated class, in private fields we have: name and surname (string), random constant variable b, c, d, e, f, and initialized password variable to 0.

We create a constructor that we contain password calculation, and a getter for password field to get password value (unsigned integer).

For password calculation according to variant we use:

foreach(char a in name)

{

password += (uint)(c + (e \* a) + (f \* d) + b);

}

In main function, we create an object of password class, and request from user to input password, finally we compare input password with password stored in class, if they are matching we display an info message box with “Correct password” message if not we display error message box with “Incorrect password” message.

*Reverse engineering part*:

For reverse a .NET program we use dnspy, we just open executable file with this software and we can see all program source code even private fields.

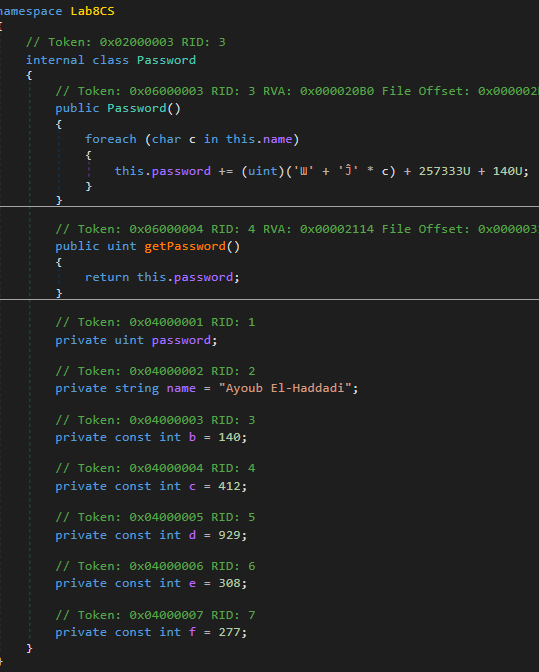


Figure 1: LabCS.exe in dnspy

As we can see, the constant value are taking a form of characters, and Unicode values. For creating a new program that displays the password we just copy constructor content and “name” field, initialize an unsigned integer field that will contain result, finally display it in console.

*Program in Java:*

For creating program part we just do the same steps with pervious program, we create a password class with private fields and constructor that calculates password value, we use same constant values, and a getter for password field.

Calculating password part:

for(char a : name.toCharArray()){

password += c + (e \* a) + (f \* d) + b;

}

*Reverse engineering part*:

Compiled .java files are .class files so for reversing these files we use java decompiler that can open class files and display its source code.

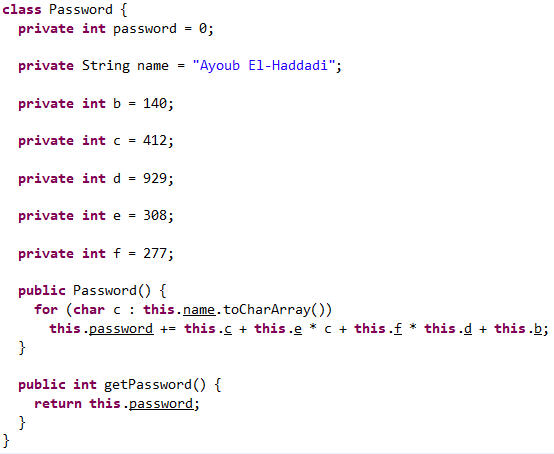


Figure 2: Password.class in java decompiler

For creating a new program that displays the password we take the constant values (name, b, c, d, e, and f) and constructor content (loop).

*Note: in loop inside constructor we can notice two variable with same name “c” one is integer constant one is name character, the one with “this” keyword is the class field which means is the integer constant.*

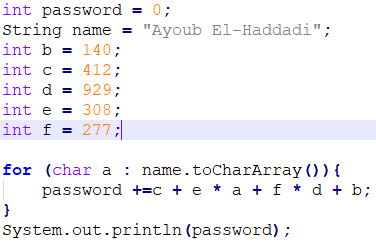


Figure 3: Java reversed program.

**Source Code**

Full source code of this lab you can find it in:

[**https://github.com/Elh-Ayoub/RP\_Labs/tree/main/lab8**](https://github.com/Elh-Ayoub/RP_Labs/tree/main/lab8)

**Results of the program:**

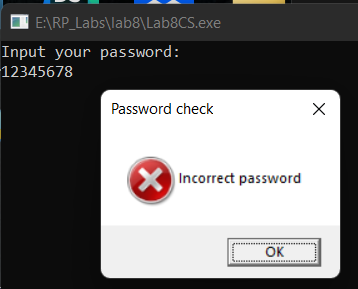


Figure 1 – Lab8CS try incorrect password

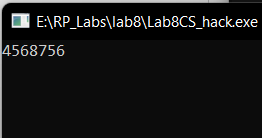


Figure 2 – Lab8CS reversed program

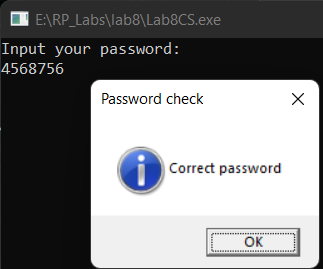


Figure 3 – Lab8CS try correct password

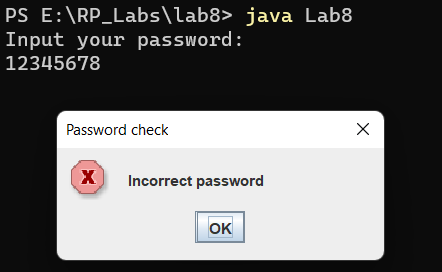


Figure 4 – Lab8.java program

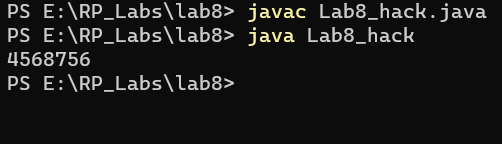


Figure 5 – Lab8 java reversed program

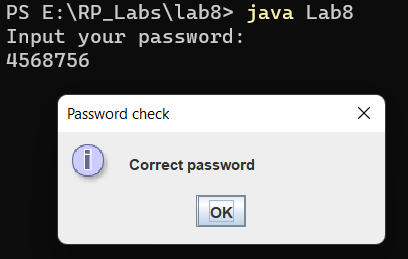
****

Figure 6 – Lab8 java try correct password

**Conclusions:**

As a result of laboratory work we gained a practical skills in reverse engineering of programs that use CLR and JVM technologies, and rewrite a program that request a password, with a program that display the correct password.

**You can also find this report in:**

<https://github.com/Elh-Ayoub/RP_Labs/tree/main/Docs>