TITLE : **Secure Code Identifying Partitioning**

J. K Institute of Applied Physics and Technology
By- Mohana Krishna Polamuri
krishnapolamuri6296@gmail.com

Abstract

Now a days a simple computer system run hundreds of program from the time being of start and shutdown. As the technology is taking over the world so rapidly which results as of leaking of private information and details . So it is should be precisely taken care of the code that the code is running into secure environment securely.

In this we will learn about a technique or method for the identifying the sensitive code which may carry the data or information. Now the question is why this method ? There are so many methods which provides the method about secure code partitioning but they have some of the issues which I have tried to solve , which has been discussed below.

Introduction

Secure programming practices have significant value, but most developers are not security experts and therefore cannot take full advantage of those practices. This trend will not change. Therefore, we seek to lower the barriers of entry for writing secure system software. Our contribution towards this goal involves facilitating a specific technique for writing secure software.

There may be a lot of reason that may occur when you run your program in a machine . One of the problem may occur is on run time your information may get leaked by a hacker . So its our responsibility to run it on secure mode by minimizing the computation and resources.

Here we will discuss about how we can identify the sensitive code by semantics analysis and by performing some matrix operation over it. The general concept has been used over here is . It is the variables that contain the data and variables is passed over and over . So leaking of one line of code may leak the whole data . Basically we are tracing the whole data variables and operations.

Problem: Secure Code Partitioning

As a tool there may be many flaws and sensitive in nature. So the question arises what are the problems that it is over taking of? Many tools has been discussed which uses the Server and Client method , encapsulation and Manual Annotation for the partitioning. So by this method we usually partition the program into different categories which increases the computation time. For example a program consist of some sensitive lines for that sensitive lines we have run the whole portion of the program into the secure state . So by our method we have tried to make it minimize. Basically the problems arises are:

1) How to indentify the composite operation . for example If X is private and Y is also public then X+Y what it should be called?

2) How to maintain the all the Sensitive code so that it will not harm the result and execution of the program and keep it connected ?
3) Suppose that a public variable stores the value of private data so should be label as it sensitive or not?
4) If we use the annotation and labelling and If we do it manually. It will not be possible for the thousands lines of code .

   There were so many problem like this. We have tried to over come the above problems by making it Automation. Below the method has been discussed with an example.

Method: Secure Code Partitioning

Rather than using Client server module or manual annotations . We will try to use the following automation. Here the Security has been divided into three categories High(Private), Medium(Protected) and Normal(Public). As per their Name an integer value is assigned to High is 1 , Medium is 0 and Normal is -1. How we are going to use these values will be discussed .

for example :

```
1. Public class A{

2. Public String name ;
3. Private double Phone_No;

4. A(String N, double P){
5. Name = N;
6. Phone_No= P;
7. }
   Public void display(){
8. System.out.println("Name is " + name);
9. System.out.println(Name + " " + Phone_no);
10. }
11. }

12. Public class Test{
13. Public static void main(String args[]){
14. A obj = new A("krishna", 9998887744);
15. A.display();
16. }
17.}
```

So if we implement our logic behind the above code then first we do semantic analysis of the code and take out the Variables.
For the above code we have
Public : {Name , N}
Private :{ Phone_no, P}

N & P is included because the value N and P holds has been assigned to Name and Phone_no. So automatically these variables as gets the security label.

Now we maintain an array where we will compute the sensitivity of a line .

Variables \ Line	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Name	∞	-1	∞	∞	-1	∞	∞	-1	-1	∞	∞	∞	∞	∞	∞	∞	∞
Phone_no	∞	∞	1	∞	∞	∞	∞	∞	1	∞	∞	∞	∞	∞	∞	∞	∞
N	∞	∞	∞	-1	-1	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
P	∞	∞	∞	1	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
TOTAL	∞	-1	1	0	-2	∞	∞	-1	0	∞	∞	∞	∞	∞	∞	∞	∞

As per table if a line have value equal to or more than 1 then it should be considered as High.
if a line have value of 0 then it should be considered as Medium and if a line have less than 0 value then it should be considered as Normal.

So as per this method we can trace the variable and as per variable we can calculate the sensitivity of the line .

IMPLEMENTATION

The following java code has been implemented for the demonstration of the possibility.
We can take the Sensitive code into a class by using the object slicing method or simply by creating a function into another class and calling it by the name of the object.

CONCOLUSION

The method has been implemented in such a way , Instead of using the portion of application for just 2-3 lines of sensitive code . We are trying to minimize the computation for the faster and reliability. As i have presented the approach we are using . There are some flaws that needs to be cure .

So computers that are using the above mentioned method can be implemented with flicker which will minimize the use of TCB and execute the programs securely .

Further more developments can be done into the code and can be implemented for the different languages .