Reimplementation of Carburizer

Louisa Bessad

5 août 2014

1. Abstract

To improve the reliability of systems we have to ensure input checking from the driver verify every access to drivers, no matter the position of this access on the Kernel's code. We have to look for different types of code. In this way we will create patches using Coccinelle.

2. Looking for different types of code

First, we will look for two types of loop ; loops that use as an exit condition functions that call drivers or a pointer value that assigns the return of one of these functions. In this case if the function never returns a value that allows to exit of the loop, it could cause the crash or the hanging of the system. And loops with infinite exit condition ; for(; ;) and while(1) that use an alternative calling a driver function to exit of the loop without any break. It could cause the same problems than the previous type of loop. These two types of loop will be considered as loop without timeout. We will define as a timeout a variable that is incremented or decremented in the condition of the loop or another assignment (such as $\ll=$ *or* $\gg=$).

3. Solutions

To find loops without a timeout we will apply two semantic patches to the Linux3.2.59 Kernel. There is a smeantic patch for each type of loop : for and while. The patch will furthermore modify a loop that matches to avoid infinite looping. We inserted the same code that is used by Carburizer. For instance these codes :

---

4. Results

We have counted the number of each type of loop on the Linux3.2.59 Kernel. Then we have counted the loops found by our patch. During the execution of patches some files have been skipped by Coccinelle to avoid a very long execution time. It appeared that whatever the computer used to execute the patches without the timeout option of Coccinelle, the execution could never end. For those files the analysis must be made by a programer. The following array shows the result of these executions :

	infinite loop	EXN files	total loop
while	3463	97	9342
for	367	87	27616