May the 4th - Fuzzing project report

Goal 🏆

- **Read docs** about **Dyninst** and especially, his part on **static intrumentation analysis** (**binary rewriting**)
- **Create a script** with **Dyninst** to **hook** a **conditional loop** and **print** some informations about the running (name function, args, and so on …)
- **Test** what I have done with a little binary “Hello world !!” with some conditional loop

What I have the last week ? 👨‍💻

Resources

Dyninst : The principal website
DyninstAPI : A huge doc to understand the DyninstAPI
Binary rewriting example : To help me to begin with some example explications and code
How to use Dyninst : Others examples

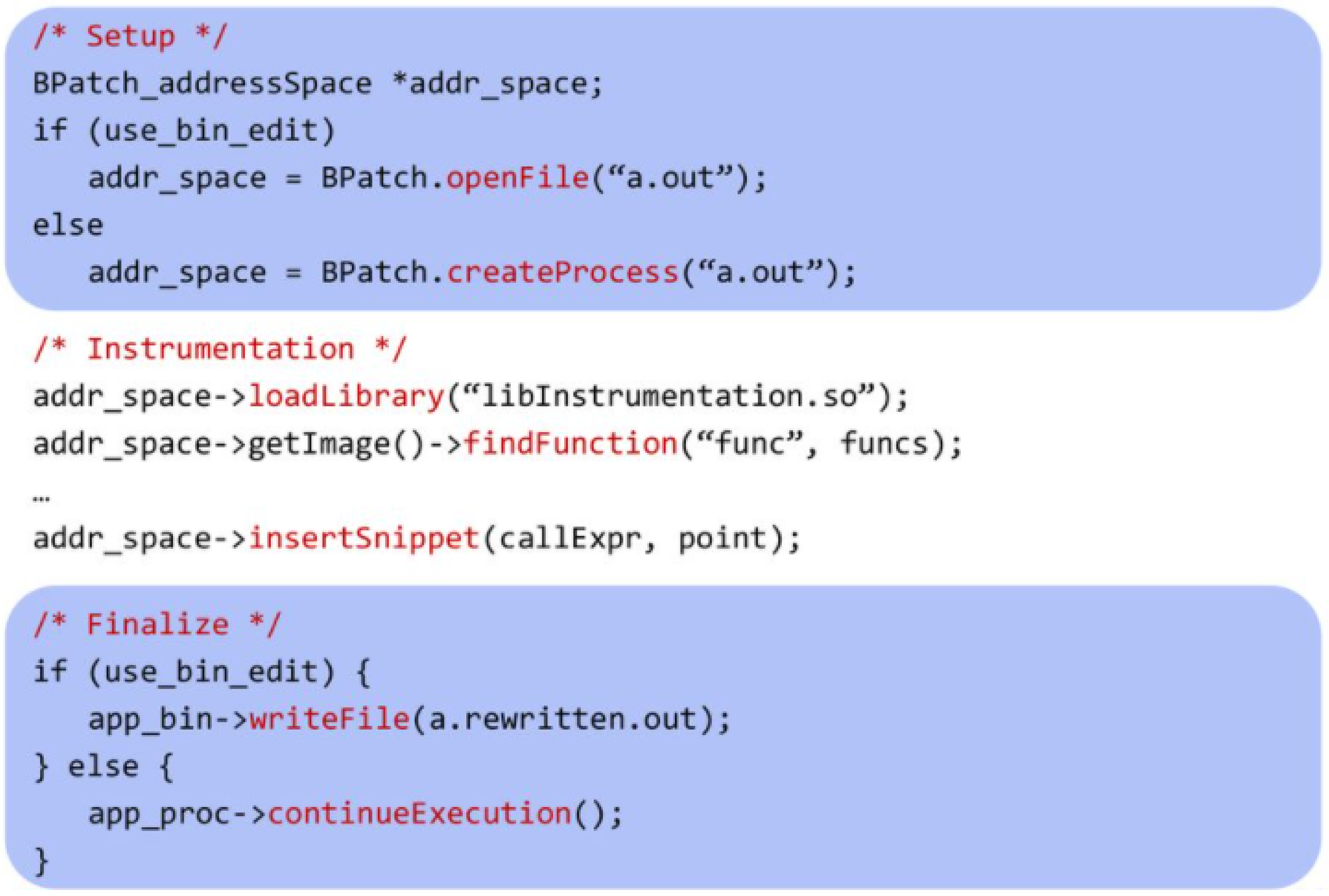
Dyninst

I searched some docs about **static instrumentation analysis** with **Dyninst**. I had to sort informations because **Dyninst** can be also do **dynamic instrumentation analysis**.

I've seen that **Dyninst** was based on an **API**. I must have to focus on what is really important for my **purpose** (because there is a lot of informations). It was really **difficult**.

So, to focus on what I have to do, I'm based on : **static binary rewriting**

Example of binary rewriting



```
/* Setup */
BPatch_addressSpace *addr_space;
if (use_bin_edit)
   addr_space = BPatch.openFile(“a.out”);
else
   addr_space = BPatch.createProcess(“a.out”);

/* Instrumentation */
addr_space->loadLibrary(“libInstrumentation.so”);
addr_space->getImage()->findFunction(“func”, funcs);
…
addr_space->insertSnippet(callExpr, point);

/* Finalize */
if (use_bin_edit) {
   app_bin->writeFile(a.rewritten.out);
} else {
   app_proc->continueExecution();
}
```

Where I stopped ? 🛑

Now, I have to create a **script** to automatize the **binary rewriting** such as the exemple in above. I have to insert a **hook** on a specific **conditional loop** and choose what I want to print.