

Assignment 1, CSN-212

Paras Chetal, Enrollment No. 15114049

January 19, 2017

1 Spaghetti Stack

A few months back, there was an [article](#) I read that talked about how Intel was going to combat Return Oriented Programming (ROP) based exploits by using a *shadow stack*. They've explained the *Control-flow Enforcement Technology* which they intend to use in this [publication](#). Since I've written ROP-based exploits before, I was interested in how programs could be secured against it. A shadow stack is basically a separate area of memory which resides within the secure region maintaining the invariant that all sensitive information (return address of functions for instance) is contained within that region. So, I searched a bit to how this could be accomplished. I came across the ***Spaghetti Stack*** data structure which might be useful.

The Spaghetti Stack is an N-ary tree data structure in which each node has a pointer to its parent node but no pointers to the child node. It's a stack structure in which the stack frames pushed onto the stack are not removed from the stack. They remain in memory indefinitely (before garbage collection), and can be popped again. Spaghetti stack is used in compilers for the C language, in which a symbol table is pushed which points to its parent symbol table, thus creating a block/lexical scope. It's also used in languages which support *Call with current continuation*, which allow control to return to a frame that has been executed and returned from. The elements of the spaghetti stack are dynamically allocated memory chunks, unlike the regular stack implementation which uses an array of memory with a moving pointer.

2 whoami

2.1 Past

I started coding in Java (very very basic) in 9th standard. Had to leave it after two years due to IIT preparation. Then, I started again after getting enrolled the Computer Science and Engineering undergraduate program here at IIT Roorkee around one and a half years back.

2.2 Present

I am a second-year undergraduate student at IIT Roorkee studying Computer Science and Engineering. My interests include:

Coding: Information security, networking, and software development. I am fluent in python, Java, C++, C, PHP. I regularly participate in CTFs (Capture The Flag security contests) and practice wargames. I also contribute to open source projects. I am a member of [SDSLabs](#). It is a student group that constantly tries to innovate and foster technical activities on campus. I am active on [github.com/paraschetal](#). I am one of the initial members of the InfoSecIITR group, which is a bunch of information security enthusiasts who participate in CTFs, organize regular meetups etc. I have a [blog](#) where I post occasionally.

Entertainment: I am an avid reader. My favorite genres being philosophy, sci-fi, and fantasy. I listen to music (taste varies depending on my mood), watch movies (only the very best ones), watch tv series (only the most popular ones), play sports (football, squash and swimming) in my free time. I also like spending some time alone, thinking.

2.3 Future

I see myself pursuing Masters in Information Security or Computer Science in the future. I am also passionate about hacktivism, so I might end up doing something related to it.