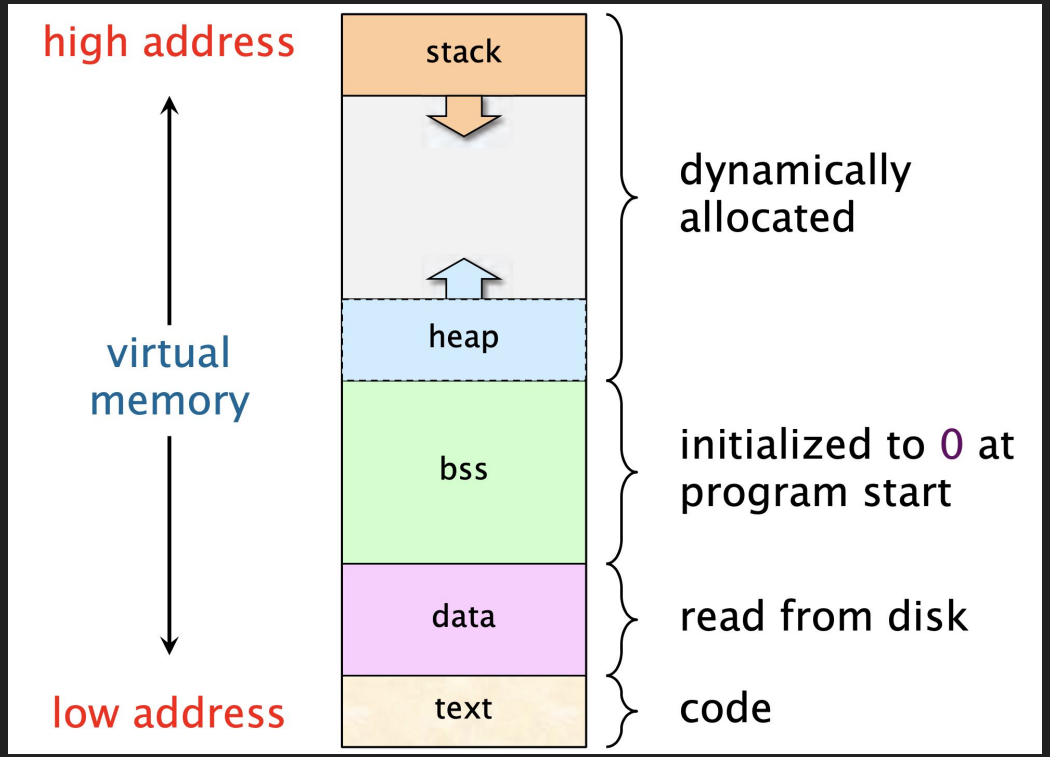
Reverse Engineering, Stack Smashing, and NSA-Published Dragons

C → Executable

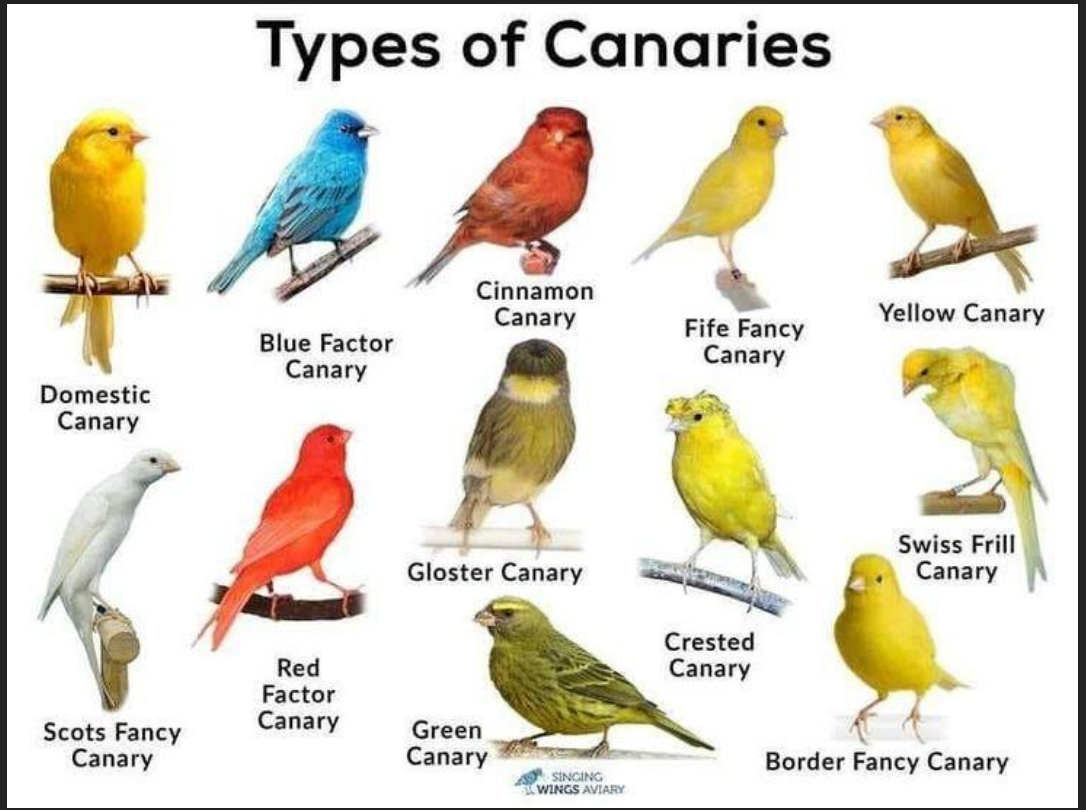
1. Compilation splits code into different segments– code, data being read, etc.
2. The stack is used to store data as the program executes. Variables or functions add to the stack, and returns “pop” values back off.



Birds

Stack Canaries

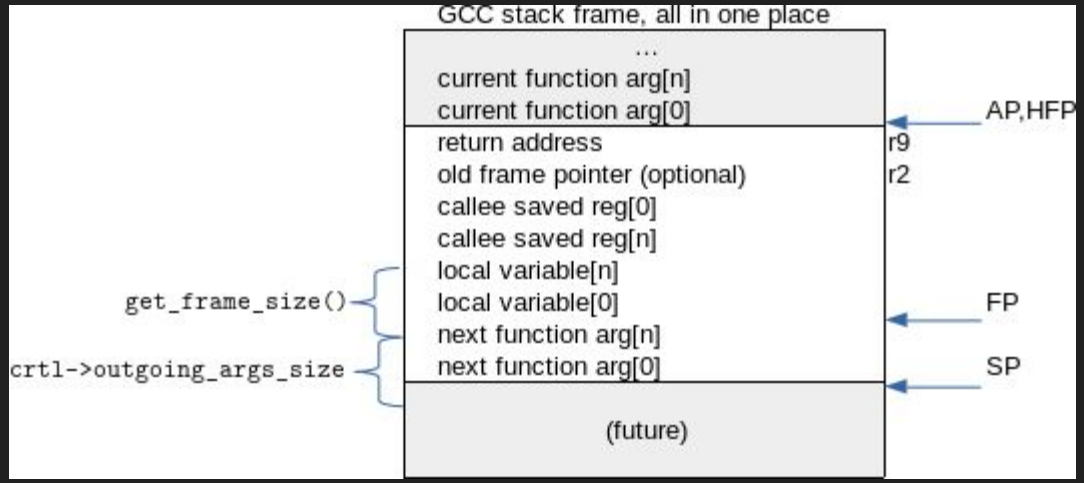
Canary in a coal mine– The stack canary is an arbitrary value pushed onto the stack. If the canary is damaged in some way, (hint hint) the program panics and locks down.



Canaries on the stack

Live whiteboard demo time!

Todo in demo:
- explain stack
- show how functions are added
- smash stack with canary



Now what?

Sometimes, we are able to leak information about a stack canary. This can be done if an exploit lets you read memory off the stack, or determine how the canary was created. Viewing the source code can be helpful for this, but usually isn’t feasible with pre-built programs. To view the src we need…

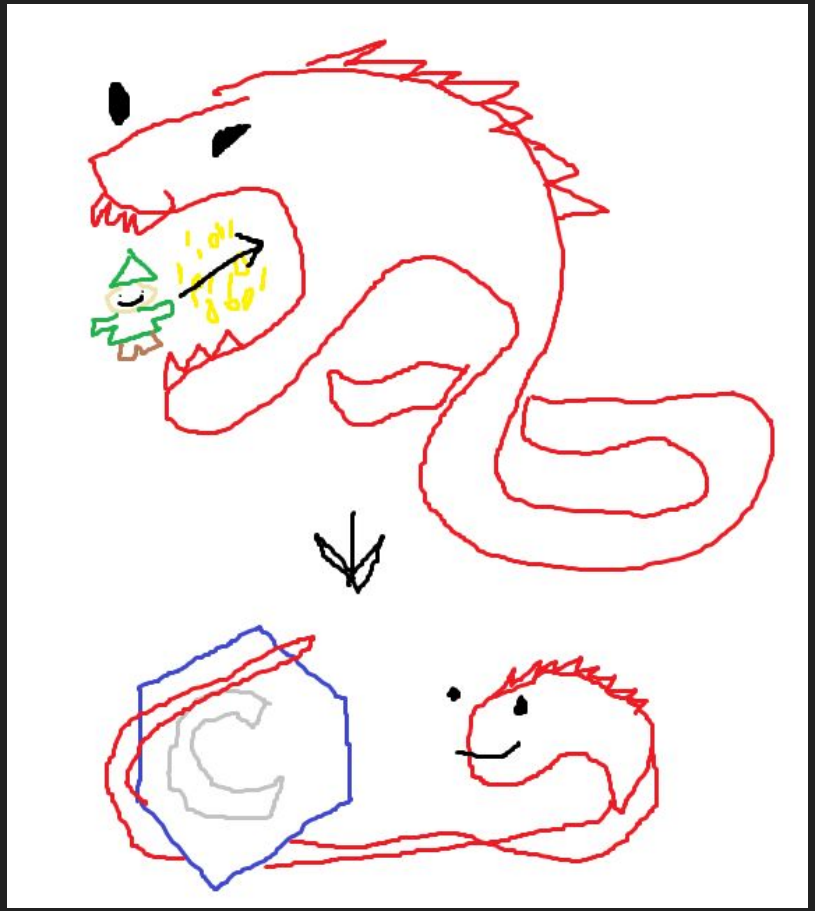
Elfs and Dragons

Ghidra

- Reverse engineering tool that decompiles and analyzes code
- Published by the Feds
- Somewhat scuffed, but free and the most popular option
- Installation is a bit weird, we can help troubleshoot ad-hoc

How Ghidra Works

1. Read ELF (binary)
2. Disassemble to Assembly instructions
3. *Decompile* to pseudo-C code
    a. Ghidra does its best to recreate source code but is heuristic
4. Analysis
    a. Data flow
    b. Symbols, functions, etc
5. Interactive annotation
    a. **This is the part you do!**



Live Demo!

1. Download example binary from discord
2. Test binary
3. Open ghidra
4. Load binary
5. Identify Function(s)
    a. How to find main, different functions, and their addresses
6. Fun and Profit

Challenge time (soon)

1. This is where I will put things that I forgot to mention but would be good reference for the chal
2. Ghidra Installation Tips:
   a. The installation guide is somewhat scuffed. If you are on linux/similiar, there may be a package for your distro you can use. For example, on Debian+friends there is a SNAP for it.