Arizza Santos

Professor Dennis Rembert

10 April 2018

**Design**

**proj1.zip** contains three (3) directories:

* “src”: contains source file, including a make file that builds the analyzer program
* “bin”: contains the built analyzer executable, other binary files, and any dependent library files
* “doc”: contains User Guide that includes installation steps and typical usage instructions, and a Design document providing software components, a description of application level data storage protocol, build instructions, and a mapping of the requirements to the source code

**“doc”** directory:

* useful\_commands.txt: contains useful command line operations to check an ELF binary
* User\_guide: installation and typical usage instructions
* Design: documentation on the program

**“bin”** directory:

* analyze: the executable analyzer after building it
* mydata.bin: file that is written to after analyze runs correctly
* test: example binary file
* test.text: .text section of test

**“src”** directory:

* analyzer.c: analyzer program
* analyzer.h: header file for the analyzer program
* doubleSum.asm: assembly file that contains a function written in Intel IA32 assembly, which is used functionally as part of the analyzer program (Requirement 17)
* makefile: make file used to build the analyzer program; builds and runs analyzer on Linux for 32-bit architecture (Requirement 19), compiles and run for 32-bit (Requirement 19 and 20)
* simple\_bin\_proto.h: contains structs for information collected by analyzer program that is stored in a persistent manner so that the data can be retrieved (Requirement 11)
* test.c: sample test file used to make the test binary in “bin” directory

**Requirements Mappings**

1 and 2. Analyzer program takes in a binary built in the ELF format and verifies the format of the binary file before proceeding with analysis. In main() and verify\_format().

3. The 5 attributes that I write to the file are: machine type, MD5 of the .text section, .text size, number of sections of the binary file, and number of symbol entries. In simple\_bin\_proto.h, get\_machine\_type(), MD5 is in main(), get\_text\_size(), get\_num\_sections(), get\_sym\_entries().

4. In analyzer.c in get\_text\_size().

16. Backdoor is in main(). Have to hit ‘q’ on keyboard.