ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

Факультет компьютерных наук

Департамент программной инженерии

СОГЛАСОВАНО
Приглашенный преподаватель
департамента программной инженерии,
к.т.н., доцент.

_____ А.Д. Брейман
«___» _____ 2020 г.

УТВЕРЖДАЮ
Академический руководитель
образовательной программы
«Программная инженерия»
профессор, канд. техн. наук

_____ В.В. Шилов
«___» _____2020 г.

Подп. и дата

Инв. № дубл.

Взам. Инв. №

Подп. и дата

Инв. № подл.

Программа для защиты исполняемого файла от уязвимости переполнения буфера на стеке путём переноса стека вызовов в кучу
Руководство оператора

ЛИСТ УТВЕРЖДЕНИЯ
RU.17701729.02.13-01 34 01-1-ЛУ

Исполнитель
Студент группы БПИ 184
_____/Новак В.А./
«___»_____2020 г.

Москва 2020

Утверждено
RU.17701729.02.13-01 34 01-1

Программа для защиты исполняемого файла от уязвимости переполнения буфера на стеке путём переноса стека вызовов в кучу

Руководство оператора

RU.17701729.02.13-01 34 01-1

Листов 8

Подп. и дата	
Инв. № дубл.	
Взам. Инв. №	
Подп. и дата	
Инв. № подл.	

Москва 2020

Содержание

1. Назначение программы

1.1. Функциональное назначение

Программа модифицирует поданный на вход файл ассемблерного кода, созданный компилятором GCC, так что получаемый в результате дальнейшей сборки исполняемый файл при вызовах подпрограмм будет использовать кучу для хранения адресов возврата.

1.2. Эксплуатационное назначение

Программа может быть использована для защиты исполняемых файлов от внедрения вредоносного кода путём изменения адреса возврата через эксплуатацию уязвимости буфера на стеке.

1.3. Состав функций

Программа должна позволять пользователю:

- Изменять в зависимости от выбранного пользователем значения из поддерживаемых программой следующие параметры:
  - Имена входных файлов;
  - Тип архитектуры исполняемого файла;
  - Размер стека вызовов.

2. Условия выполнения программы

2.1. Минимальный состав программных и технических средств

Список программных средств для надёжной и бесперебойной работы программы:

- Windows 7 или более поздняя версия операционной системы (32-разрядные или 64-разрядные) либо операционная система на основе ядра Linux (32-разрядные или 64-разрядные).
- Компилятор языка C/C++ из GNU Compiler Collection.

Список технических средств для надёжной и бесперебойной работы программы:

- Процессор архитектуры AMD или Intel с частотой не менее 2,10 ГГц;
- Не менее 150мб ОЗУ;
- Не менее 80мб на жёстком диске;
- Клавиатура.

2.2. Требования к пользователю

Не требует специального обслуживания. Требуемая квалификация – продвинутый пользователь.

3. Выполнение программы

3.1. Установка программы

Установка программы не требуется.

3.2. Запуск программы

Для запуска программы необходимо последовательно выполнить следующие действия:

1. Скомпилировать файлы исходного кода с помощью компилятора GCC без сборки (ключ -S) и использования встроенного защитника стека (ключ -fno-stack-protector).
2. Исполнить файл protect.exe для ОС Windows или protect.out для ОС Linux,передав ему все файлы, полученные на предыдущем шаге и указав необходимые опции в аргументах командной строки.
3. Завершить компиляцию файлов, полученных на первом шаге, с помощью компилятора GCC.

3.3. Выбор архитектуры обрабатываемой программы

Для выбора 32-битной архитектуры в аргументах командной строки следует указать ключ -x86. Для выбора 64-битной архитектуры в аргументах командной строки следует указать ключ -x64 (вариант по умолчанию). Данные две опции являются взаимоисключающими.

3.4. Выбор размера стека вызовов для обрабатываемой программы

Размер стека вызовов для обрабатываемой программы указывается в байтах в следующем аргументе после ключа -s.

4. Сообщения оператору

Все нижеперечисленные сообщения выводятся в стандартный поток ошибок программы в виде строки «Error: » и следующего за ней текста сообщения.

- При отсутствии входных файлов выводится сообщение «No input files»
- При невозможности открыть входной файл на чтение или запись выводится сообщение «Cannot open file *имя_файла*», где вместо «*имя_файла»* указано имя первого входного файла, который не удалось открыть.
- При повторном использовании какого-либо ключа выводится сообщение «Key *ключ* is used more than once», где вместо «*ключ*» указан первый найденный повторяющийся ключ.
- При одновременном использовании ключей для разных архитектур выводится сообщение «More than one architecture is specified».
- При указании некорректного размера стека (должен быть натуральным числом) выводится сообщение «Call stack size must be a natural number».

5. Список литературы

1. ГОСТ 19.201-78 Техническое задание. Требования к содержанию и оформлению. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
2. ГОСТ 15150-69 Машины, приборы и другие технические изделия. Исполнения для различных климатических районов. Категории, условия эксплуатации, хранения и транспортирования в части воздействия климатических факторов внешней среды. – М.: Изд-во стандартов, 1997.
3. ГОСТ 19.301-79 Программа и методика испытаний. Требования к содержанию и оформлению. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
4. ГОСТ 19.401-78. ЕСПД. Текст программы. Требования к содержанию и оформлению. – М.: ИПК Издательство стандартов, 2001.
5. ГОСТ 19.404-79. ЕСПД. Пояснительная записка. Требования к содержанию и оформлению. – М.: ИПК Издательство стандартов, 2001.
6. ГОСТ 19.505-79. ЕСПД. Руководство оператора. Требования к содержанию и оформлению. – М.: ИПК Издательство стандартов, 2001.

7. Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	№ документа	Входящий № сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	Новых	аннулированных					

Изм.	Лист	№ докум.	Подп.	Дата
RU.17701729.02.13-01 34 01-1				
Инв. № подл.	Подп. и дата	Взам. Инв. №	Инв. № дубл.	Подп. и дата