**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**  **Пояснительная записка**  **ЛИСТ УТВЕРЖДЕНИЯ**  **RU.17701729.02.13-01 81 01-1-ЛУ**  Исполнитель  Студент группы БПИ 184  \_\_\_\_\_\_\_\_\_\_\_/Новак В.А./  «\_\_\_»\_\_\_\_\_\_\_\_\_\_2020 г.  **Москва 2020** | |  |

Утверждено  
RU.17701729.02.13-01 81 01-1

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | 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**  **Пояснительная записка**  **RU.17701729.02.13-01 81 01-1**  **Листов 11**  **Москва 2020**  Содержание  [1. Введение 3](#_Toc40550615)  [1.1. Наименование программы: 3](#_Toc40550616)  [1.2. Основания для разработки 3](#_Toc40550617)  [2. Назначение разработки и область применения 4](#_Toc40550618)  [2.1. Назначение 4](#_Toc40550619)  [2.1.1. Функциональное назначение 4](#_Toc40550620)  [2.1.2. Эксплуатационное назначение 4](#_Toc40550621)  [2.2. Краткая характеристика области применения 4](#_Toc40550622)  [3. Технические характеристики 5](#_Toc40550623)  [3.1. Постановка задачи на разработку программы 5](#_Toc40550624)  [3.2. Описание алгоритма и функционала программы 5](#_Toc40550625)  [3.2.1. Описание алгоритма защиты от переполнения стекового буфера 5](#_Toc40550626)  [3.3. Описание и обоснование выбора метода организации входных и выходных данных 5](#_Toc40550627)  [3.4. Описание и обоснование выбора технических и программных средств 5](#_Toc40550628)  [3.4.1. Технические средства 5](#_Toc40550629)  [3.4.2. Программные средства 6](#_Toc40550630)  [4. Ожидаемые технико-экономические показатели 7](#_Toc40550631)  [4.1. Предполагаемая потребность 7](#_Toc40550632)  [4.2. Экономические преимущества разработки по сравнению с отечественными и зарубежными аналогами 7](#_Toc40550633)  [5. Список литературы 8](#_Toc40550634)  [6. Приложение 1. Описание и функциональное назначение классов 9](#_Toc40550635)  [7. Приложение 2. Описание и функциональное назначение функций программы. 10](#_Toc40550636)  [8. Лист регистрации изменений 11](#_Toc40550637) |  |

# Введение

## **Наименование программы:**

Наименование программы: «Программа для защиты исполняемого файла от уязвимости переполнения буфера на стеке путём переноса стека вызовов в кучу» («Program for protecting an executable file from stack buffer overflow vulnerability by moving call stack to heap»).

## **Основания для разработки**

Основанием для разработки является приказ декана факультета компьютерных наук НИУ ВШЭ И.В. Аржанцева от 11.12.2019 г. № 2.3-02/1112-04.

# Назначение разработки и область применения

## **Назначение**

## **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.

## **Эксплуатационное назначение**

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

## **Краткая характеристика области применения**

Программа может быть использована при разработке программ с использованием компиляторов для C/C++ GNU Compiler Collection.

# Технические характеристики

## **Постановка задачи на разработку программы**

Программа должна реализовывать требования к функциональным характеристикам и соответствовать требованиям к надёжности, описанным в пп. 4.1 - 4.2 Технического задания [1].

## **Описание алгоритма и функционала программы**

## **Описание алгоритма защиты от переполнения стекового буфера**

Программа производит защиту от данной уязвимости следующим образом:

* Перед кодом самой программы добавляется код, выделяющий память в куче для хранения адресов возврата.
* Каждый вызов функции из обрабатываемого кода с помощью инструкции «call» заменяется на сохранение адреса возврата в выделенную память в куче и безусловный переход к началу функции.
* Каждый выход из функции в обрабатываемом файле, кроме точки входа с помощью инструкции «ret» заменяется на извлечение адреса возврата из памяти в куче и безусловному переходу по нему.

## **Описание и обоснование выбора метода организации входных и выходных данных**

Параметры программы подаются с помощью аргументов командной строки в следующем виде:

* Размер стека вызовов в байтах – следующий аргумент после ключа «-s», число. По умолчанию 65536;
* Архитектура – ключи «-x86» для 32-битной архитектуры и «-x64» для 64-битной. По умолчанию используется 64-битная архитектура;
* Все остальные аргументы командной строки воспринимаются программй как входные файлы.

Программы для обработки считывается из файлов. Результат обработки каждого файла записывается в тот же файл.

## **Описание и обоснование выбора технических и программных средств**

## **Технические средства**

Минимальные требования программы для работоспособности.

* Процессор архитектуры AMD или Intel с частотой не менее 2,10 ГГц;
* Монитор с разрешением 1280х768 точек и более;
* Не менее 150мб ОЗУ;
* Не менее 2мб на жёстком диске;
* Клавиатура.

Выбор параметров процессора обусловлен отсутствием устройств с меньшими характеристиками и, как следствие, невозможностью убедиться в работоспособности программы при меньших требованиях. Выбор остальных параметров основан на оценке необходимых характеристик для возможности выполнения всех требуемых функций.

## **Программные средства**

* 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).
* Обрабатываемая программа должна быть скомпилирована с помощью компилятора для языка C/C++ из GNU Compiler Collection.

Выбор набора операционных систем обусловлен тем, что этот набор покрывает большинство устройств, под которые производится разработка на языках C и C++. Выбор компилятора обрабатываемых программ обусловлен тем, что вышеупомянутый компилятор является свободным программным обеспечением и имеет открытый исходный код, что упрощает разработку под него.

# Ожидаемые технико-экономические показатели

В рамках данной работы расчет экономической эффективности не предусмотрен.

## **Предполагаемая потребность**

Данная программа будет полезна при разработке на языках C и C++.

## **Экономические преимущества разработки по сравнению с отечественными и зарубежными аналогами**

На момент начала разработки найдены следующие аналоги:

* GCC StackGuard;
* Компилятор Microsoft Visual Studio (имеет встроенную защиту от описанной уязвимости).

Данная программа использует принципиально другой способ защиты. Представленные варианты используют «канареек» - значения в конце кадра стека, по изменениям которых можно определить повреждение данных на стеке. Это ограничение можно умышленно обойти, подобрав данные для перезаписи так, чтобы «канарейка» не была изменена [7].

# 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. Exploit Mitigation Techniques – Stack Canaries – Exploit Development [Электронный ресурс] – Блог. – Режим доступа:  
   https://0x00sec.org/exploit-mitigation-techniques-stack-canaries/5085/1 (дата обращения 04.12.2019)

# Приложение 1. Описание и функциональное назначение классов

Программа написана без использования классов, поэтому в таблице присутствуют только типы перечислений (enum).

|  |  |
| --- | --- |
| **ENUM** | **ОПИСАНИЕ** |
| ArgError | Результат обработки аргументов командной строки |
| Arch | Архитектура обрабатываемого файла |

# Приложение 2. Описание и функциональное назначение функций программы.

|  |  |  |
| --- | --- | --- |
| **Имя** | **Тип** | **Назначение** |
| startswith | bool | Проверка того, что строка начинается с заданного префикса |
| isFuncName | bool | Проверка того, что данная строка может быть именем функции на данной архитектуре |
| isMainName | bool | Проверка того, что данная функция является точкой входа в приложение на данной архитектуре |
| getMallocCall | const char\* | Возвращает вызов функции malloc в ассемблерном коде на данной архитектуре |
| parseArgs | ArgError | Обработка аргументов командной строки |
| parseFiles | void | Построчно считывает входные файлы и находит в них все функции |
| processFiles | void | Обработка считанных входных файлов |

# Лист регистрации изменений

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