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	УТВЕРЖДАЮ Академический руководитель образовательной программы «Программная инженерия» профессор, канд. техн. наук
_____ А.Д. Брейман «___» _____ 2020 г.	_____ 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
Программа и методика испытаний

ЛИСТ УТВЕРЖДЕНИЯ
RU.17701729.02.13-01 51 01-1-ЛУ

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

Москва 2020

Утверждено
RU.17701729.02.13-01 51 01-1

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

Программа и методика испытаний

RU.17701729.02.13-01 51 01-1

Листов 15

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

Москва 2020

Изм.	Лист	№ докум.	Подп.	Дата
RU.17701729.02.13-01 51 01-1				
Инв. № подл.	Подп. и дата	Взам. Инв. №	Инв. № дубл.	Подп. и дата

Содержание

1. Объект испытаний

1.1. 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»).

1.2. Область применения программы

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

2. Цель испытаний

Цель проведения испытаний – проверка соответствия характеристик разработанной программы функциональным требованиям и отдельным требованиям к надёжности, изложенным в документе Техническое задание к данной программе.

3. Требования к программе

3.1. Требование к функциональным характеристикам

3.1.1. Требования к составу выполняемых 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.

3.1.2. Требования к интерфейсу

- Программа должна получать через аргументы командной строки значения следующих параметров:
  - Имена входных файлов;
  - Тип архитектуры исполняемого файла;
  - Размер стека вызовов.
- Программа должна считывать входные данные и выводить результат через указанные в аргументах командной строки файлы.

3.1.3. Требования к формату входных данных

- Программа должна получать через аргументы командной строки значения следующих параметров:
  - Имена входных файлов;
  - Тип архитектуры исполняемого файла;
  - Размер стека вызовов.
- Программа должна считывать входные данные из указанного в аргументах командной строки файла для ввода.

3.1.4. Требования к выходным данным

- Программа должна выводить результат в указанный в аргументах командной строки файл для вывода.

3.2. Требования к надёжности

При любом вводе пользователя программа не должна завершаться аварийно. При неправильном формате вводимых данных программа должна завершаться с сообщением о некорректных входных данных.

3.3. Условия эксплуатации

3.3.1. Климатические условия

Климатические условия эксплуатации, при которых должны обеспечиваться заданные характеристики, должны удовлетворять требованиям, предъявляемым к персональным компьютерам.

Персональный компьютер предназначен для работы в закрытом отапливаемом помещении со стабильными климатическими условиями согласно [2].

1) влажность от 20% до 70%;

2) температура от 5°C до 30°C;
3) атмосферное давление — от 84 до 106,7 кПа (от 630 до 800 мм рт. ст.).

3.3.2. Требования к квалификации оператора

Не требует специального обслуживания. Требуемая квалификация – продвинутый пользователь.

3.4. Требования к составу и параметрам технических средств

Минимальные требования программы для работоспособности.

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

3.5. Требования к информативной и программной совместимости

- 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

3.6. Требования к маркировке и упаковке

При хранении на физическом носителе на нём должны быть указаны ФИО Исполнителя, название продукта и год окончания разработки.

3.7. Требования к транспортировке и хранению

Программное изделие может храниться и транспортироваться на флэш-носителе и распространяться через облачное хранилище.

4. Требования к программной документации

4.1. Состав программной документации

В рамках данной работы должна быть разработана следующая программная документация в соответствии с ГОСТ ЕСПД:

- «Программа для защиты исполняемого файла от уязвимости переполнения буфера на стеке путём переноса стека вызовов в кучу». Техническое задание (ГОСТ 19.201-78) [1];
- «Программа для защиты исполняемого файла от уязвимости переполнения буфера на стеке путём переноса стека вызовов в кучу». Программа и методика испытаний (ГОСТ 19.301-79) [3];
- «Программа для защиты исполняемого файла от уязвимости переполнения буфера на стеке путём переноса стека вызовов в кучу». Текст программы (ГОСТ 19.401-78) [4];
- «Программа для защиты исполняемого файла от уязвимости переполнения буфера на стеке путём переноса стека вызовов в кучу». Пояснительная записка (ГОСТ 19.404-79) [5];
- «Программа для защиты исполняемого файла от уязвимости переполнения буфера на стеке путём переноса стека вызовов в кучу». Руководство оператора (ГОСТ 19.505-79) [6].

4.2. Специальные требования к программной документации

Документы к программе должны быть выполнены в соответствии с ГОСТ 19.106-78 и ГОСТами к каждому виду документа (см. п. 5.1);

Пояснительная записка должна быть загружена в систему «Антиплагиат» через LMS «НИУ ВШЭ». Лист, подтверждающий загрузку пояснительной записки, сдается в учебный офис вместе со всеми материалами не позже, чем за день до защиты курсовой работы;

Вся документация также воспроизводится в печатном виде, она должна быть подписана исполнителем и руководителем разработки и утверждена академическим руководителем образовательной программы 09.03.04 «Программная инженерия» перед сдачей курсовой работы в учебный офис не позже одного дня до защиты;

Документация и программа также сдается в электронном виде в формате .pdf или .docx. в архиве формата .zip или .rar;

За один день до защиты комиссии все материалы курсового проекта:

– техническая документация,

– программный проект,

– исполняемый файл,

– отзыв руководителя

должны быть загружены одним или несколькими архивами в проект дисциплины «Курсовой проект 2019-2020» в личном кабинете в информационной образовательной среде LMS (Learning Management System) НИУ ВШЭ.

5. Средства и порядок испытаний

5.1. Технические средства, используемые во время испытаний

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

5.2. Программные средства, используемые во время испытаний

- 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.

5.3. Порядок проведения испытаний

Испытания должны проводиться в следующем порядке:

1) Проверка выполнения требований к программной документации
2) Проверка выполнения требований к интерфейсу
3) Проверка выполнения требований к функциональным характеристикам
4) Проверка выполнения требований к надёжности

5.4. Условия проведения испытаний

5.4.1. Климатические условия

Климатические условия эксплуатации, при которых должны обеспечиваться заданные характеристики, должны удовлетворять требованиям, предъявляемым к персональным компьютерам.

Персональный компьютер предназначен для работы в закрытом отапливаемом помещении со стабильными климатическими условиями согласно [2].

1) влажность от 20% до 70%;
2) температура от 5°C до 30°C;
3) атмосферное давление — от 84 до 106,7 кПа (от 630 до 800 мм рт. ст.).

5.4.2. Требования к квалификации оператора

Не требует специального обслуживания. Требуемая квалификация – продвинутый пользователь.

6. Методы испытаний

Испытания проводятся в порядке, указанном в п. 5.3 настоящего документа

6.1. Испытание выполнения требований к программной документации

Проверка соответствия программной документации требованиям проводится путём просмотра программной документации.

6.2. Испытание выполнения требований к интерфейсу

Проверка выполнения требований к интерфейсу проводится путём проверки сообщений пользователю, описанных в п. 4 Руководства оператора.

6.3. Испытание выполнения требований к функциональным характеристикам

Проверка выполнения требований к функциональным характеристикам осуществляется путём выполнения перечисленных ниже действий и проверки соответствия результата требованиям к функциональным характеристикам, описанным в п. 3.1.1 настоящего документа.

6.3.1. Проверка корректности обработки программы

Для проверки корректности обработки необходимо подать на вход программе тестовую программу (представлена в п. 1.4 Текста программы), после чего запустить полученный исполняемый файл и убедиться в корректности его работы, т.е. убедиться, что:

- Отсутствовали ошибки времени выполнения;
- Программа вывела строку, переданную в качестве аргумента командной строки, в стандартный вывод. Длина строки должна быть меньше 20 символов.

6.3.2. Проверка защиты от переполнения буфера

Для проверки корректности обработки необходимо подать на вход программе тестовую программу, после чего запустить полученный исполняемый файл. При этом следует убедиться в отсутствии уязвимости переполнения стекового буфера, т.е. при передаче в качестве аргумента строку, которая содержит некоторый исполняемый машинный код для устройства, на котором производится тестирование, и при переполнении буфера перезаписывает адрес возврата на стеке на начало этого машинного кода, вышеупомянутый машинный код не исполняется.

6.3.3. Проверка параметра «размер стека вызовов»

Для проверки данного параметра необходимо подать на вход программе тестовую программу, и убедиться, что полученный в результате исполняемый файл выделяет в куче объём памяти, не меньший указанного.

6.4.Испытание выполнения требований к надёжности

Проверка соответствия программы требованиям к надёжности проводится путём проверки работоспособности программы на протяжении испытания выполнения требований к функциональным характеристикам согласно п. 6.3 настоящего документа.

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.

8. 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 51 01-1				
Инв. № подл.	Подп. и дата	Взам. Инв. №	Инв. № дубл.	Подп. и дата