Программно-аппаратные средства обеспечения информационной безопасности (ПАСО ИБ)

Тема 2. Сертификация средств защиты и защита программ и данных

Занятие 2/11. Лабораторная работа

Тема:

Разработка элементов защиты программ от отладки и дизассемблирования

Учебные вопросы:

1. Исследование защиты программ от отладчика
2. Исследование защиты программ от дизассемблера
3. Анализ алгоритмов функционирования программ

Литература

Основная

1. Программно-аппаратные средства обеспечения информационной безопасности. В 2 ч. Ч. 1. Защита от разрушающих программных средств : пособие / А. Г. Мацкевич, С. В. Снигирев, Д. А. Свечников. – Орёл : Академия ФСО России, 2011. – 141 с.

2. Программно-аппаратные средства обеспечения информационной безопасности. В 2 ч. Ч. 2. Методы и средства локальной защиты ПЭВМ / А. В. Козачок [и др.]. – Орёл : Академия ФСО России, 2015. – 143 с.

3. Методы и протоколы аутентификации: пособие: в 2 ч. Ч. 1 / Д. Е. Шугуров [и др.]. – Орел : Академия ФСО России, 2013. – 219.

Дополнительная

1. Защита программ и данных: учеб. пособие для студ. учреждений высш. проф. образования / В. Г. Проскурин. – М.: Издательский центр «Академия», 2011. – 208 с. – (Сер. Бакалавриат).

2. В.Г. Проскурин и др. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: Учеб. Пособие для ВУЗов. – М.: Радио и связь, 2000. – 168 с.

Цели занятия

- Закрепить практические навыки разработки внедряемых механизмов защиты в программное обеспечение
- Закрепить навыки исследования системы защиты программного обеспечения

Контроль готовности к занятию

1. Классификация методов исследования (анализа) ПО.
2. Классификация методов мониторинга функционирования процессов.
3. Дать определение: статический метод исследования ПО, его достоинства и недостатки.
4. Дать определение: динамический метод исследования ПО, его достоинства и недостатки.
5. Пояснить в чем заключается метод маяков и принцип метода защиты (обнаружения) от данного метода.
6. Пояснить в чем заключается метод Step-Trace и принцип метода защиты (обнаружения) от данного метода.
7. Дать определения: дизассемблер, эмулирующий отладчик.
8. Дать определения: отладчик, эмулятор.
9. Привести 2-3 примера методов защиты от отладчика (динамического анализа ПО).
10. Привести 2-3 примера методов защиты от дизассемблирования (статического анализа ПО).

Учебные вопросы

1. Исследование защиты программ от отладчика
2. Исследование защиты программ от дизассемблера
3. Анализ алгоритмов функционирования программ

Варианты заданий на лабораторную работу № 2

№ п/п	Вариант 1	Вариант 2	Вариант 3
1	**Реализовать экзотическую проверку значения регистра на нулевое значение на основе**		
	контроля ввода правильности логина	контроля ввода правильности пароля	контроля ввода правильности регистрационного кода
2	**Реализовать привязку на основе команды CPUID к**		
	расширенному семейству (extended family) и модели (model) ЦП	семейству (family) и расширенной модели (extended model) ЦП	семейству (family) и типу (type) ЦП
3	**Защита от отладчика** • метод временных меток • на основе потери трассировочного прерывания		
4	**Реализовать защиту от дизассемблирования методом шифрования**		
	кода защиты от отладчика на основе потери трассировочного прерывания	кода считывания характеристик аппаратного окружения	кода экзотической проверки значения регистра на нулевое значение
	Алгоритм шифрования		

	`x =(BYTE x) + № п/п)`
	`x = rol (x, 5)`
	`x = x XOR № п/п`
		`x =(BYTE x) - № п/п)`
		`x = rol (x, 3)`
		`x = x XOR № п/п`
			`x = x xor № п/п`
			`x = not (BYTE x)`
			`x = rol (x, 7)`

5	**Реализовать контроль целостности**		
	кода расшифровщика	кода блока сравнения	кода шифровщика
6	**Восстановить алгоритм, реализованный в выданной преподавателем программе**		

Дополнительные задания (+ 1 балл)

Разработать программную реализацию средств защиты от изучения машинного кода на основе:

- Использования относительной адресации при обращении к зашифрованному участку кода
- Выявление факта работы под эмулятором (например, используя инструкцию cpuid)
- Формирования ключа расшифрования кода на основе значения контрольной суммы критического участка программы
- Использования SEH для воздействия на отладчик
- Полиморфного кода критического участка программы (например, на основе изменения ключа или алгоритма шифрования/расшифрования)
- Обфускации потока управления:
  - создание эквивалентных ветвей, выполняемых в случайном порядке
  - разбитие алгоритма на независимые блоки и исполнения в случайном порядке
- Применения помехоустойчивого программного кода (например, на

Отчетные материалы, сроки их представления и защиты

1. Задание на лабораторную работу
2. Листинг разработанного приложения

Срок защиты лабораторной работы – в течение недели после её проведения

ВОПРОСЫ ПО ЗАНЯТИЮ?

ЗАДАНИЕ НА САМОСТОЯТЕЛЬНУЮ ПОДГОТОВКУ

1. Подготовить отчет по лабораторной работе
2. Повторить пройденный материал по теме № 2, изучить рекомендованную литературу
3. Защитить результаты лабораторной работы в установленные сроки

Тема 2. Сертификация средств защиты и защита программ и данных

Занятие 2/11. Лабораторная работа

Тема:

Разработка элементов защиты программ от отладки и дизассемблирования

Учебные вопросы:

1. Исследование защиты программ от отладчика
2. Исследование защиты программ от дизассемблера
3. Анализ алгоритмов функционирования программ