УДК 004.056.55
DOI 10.21685/2587-7704-2020-5-1-1

Open Access RESEARCH ARTICLE

Анализ угроз программной реализации средств криптографической защиты информации

М. С. Коростелев
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

О. В. Липилин
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

Аннотация. В статье рассматриваются угрозы программной реализации средств криптографической защиты информации. Приводится классификация атак, направленных на реализацию угроз, основные методы защиты программных средств криптографической защиты информации.

Ключевые слова: угроза, атака, побочный канал, несанкционированный доступ, программное средство криптографической защиты информации.

Analysis of threats for software implementation of cryptographic information protection facilities

M. S. Korostelev
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

O. V. Lipilin
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

Abstract. The article considers the threats for software implementation of cryptographic information protection facilities. The classification of attacks, aimed at implementing threats, and the key software security methods for cryptographic information protection facilities are given.

Keywords: threat, attack, side channel, unauthorized access, cryptographic information protection software.

Введение

Программная реализация средств криптографической защиты информации (СКЗИ) является самым распространенным способом использования криптографических преобразований для обеспечения свойств защищаемой информации.

Основными достоинствами программной реализации являются:

– низкая стоимость самого программного СКЗИ по сравнению с программно-аппаратной и аппаратной реализацией;

– простота ввода в эксплуатацию и снятия с эксплуатации;

– низкая стоимость эксплуатации.

Среди основных недостатков можно выделить следующие:

– сложность обеспечения защиты СКЗИ и их среды функционирования от несанкционированного доступа;

– доступность исполняемого кода СКЗИ для анализа злоумышленником.

Целью статьи является рассмотрение основных угроз программной реализации СКЗИ и защитных мер, которые должны быть реализованы непосредственно в СКЗИ.

При программной реализации средств криптографической защиты информации можно выделить следующие основные угрозы:

– угрозы, связанные с исследованием исполняемого кода СКЗИ;

– угрозы, связанные с несанкционированным доступом к программному СКЗИ;

– угрозы, связанные с уязвимостями реализованных криптографических преобразований;

– угрозы, связанные с использованием анализа сопутствующей функционированию СКЗИ информации, получаемой по побочным каналам.

Угрозы, связанные с исследованием исполняемого кода СКЗИ

Угрозы, связанные с исследованием исполняемого кода СКЗИ, могут быть реализованы через динамическое исследование процесса выполнения кода с использованием отладчика и статическое исследование кода программы с помощью дизассемблера.

Исследование исполняемого кода СКЗИ в динамическом режиме с использованием отладчика может позволить злоумышленнику получить ключевую информацию и иную информацию, сопутствующую криптографическим преобразованиям, реализованным в СКЗИ. При использовании отладчика может производиться установка точки останова, пошаговая трассировка программы, отслеживание состояния регистров процессора и содержимого оперативной памяти, а также динамическое изменение исполняемого кода.

Защитной мерой, противодействующей угрозе, является отслеживание режима запуска исполняемого кода под отладчиком и остановка выполнения программного СКЗИ. Другим способом защиты от отладки является отслеживание времени выполнения участков кода. В этом случае в исполняемый код СКЗИ включается проверка времени выполнения определенных участков кода. При запуске программного СКЗИ под отладчиком время выполнения операций превысит допустимое, что приведет к завершению работы. Кроме того, для защиты от динамической модификации исполняемого кода СКЗИ в него можно вносить вычисление контрольных сумм от отдельных участков кода и (или) данных в процессе функционирования. В некоторых случаях возможно связать контрольное время выполнения участка кода и его контрольную сумму. Следует учесть, что такие способы защиты от отладки не защищают от эмулирующих отладчиков [1].

Исследование исполняемого кода СКЗИ в статическом режиме с использованием дизассемблера может позволить злоумышленнику получить информацию о логике работы программного СКЗИ. Анализ может позволить определить связанные с ключевой информацией области хранения, найти уязвимости программной реализации и т.д. Поскольку ключевая информация непосредственно не хранится в исполняемом коде СКЗИ, статический анализ кода менее опасен. Защитных мер, позволяющих полностью исключить возможность дизассемблирования исполняемого кода, не существует. Однако можно выделить некоторые защитные меры, позволяющие усложнить исследование кода. Первой защитной мерой является использование зашумления исполняемого кода программы незначащими инструкциями. Второй защитной мерой является зашифрование частей исполняемого кода. Расшифрование кода выполняется непосредственно в процессе функционирования СКЗИ, причем ключ расшифрования не должен храниться в открытом виде в исполняемом коде.

Угрозы, связанные с несанкционированным доступом к программному СКЗИ

Некоторые из угроз, связанные с несанкционированным доступом к СКЗИ, могут быть нейтрализованы корректным применением организационных мер защиты информации. Однако организационные меры защиты информации не в состоянии полностью обеспечить защиту программного СКЗИ в силу специфики его применения, поэтому некоторые защитные меры должны быть реализованы непосредственно в СКЗИ.

К таким мерам относятся [2]:

– аутентификация субъектов доступа СКЗИ;

– разграничение прав пользователей СКЗИ;

– ассоциирование аутентифицируемого процесса с субъектом, от имени которого он выполняется;

– ограничение числа неудачных попыток аутентификации;

– встроенный механизм контроля целостности ключевой информации и исполняемого кода;

– механизм гарантированного затирания областей памяти, используемой для хранения и обработки защищаемой, ключевой и криптографически опасной информации.

Угрозы, связанные с уязвимостями реализованных криптографических преобразований

Реализуемые в программных СКЗИ криптографические преобразования обладают практической стойкостью к атакам криптоаналитика [3]. Для того чтобы предельно снизить вероятность проведения атак на криптографические преобразования, необходимо выполнение требований к качеству формируемых псевдослучайных последовательностей и ресурсу использования ключа.

В программных СКЗИ должны быть учтены требования к реализации криптографических преобразований, в частности:

– проверка в автоматическом режиме статистического качества инициализирующей последовательности датчика псевдослучайных чисел;

– периодическая смена инициализирующей последовательности;

– использование различной ключевой информации для различных криптографических преобразований;

– сигнализация и (или) блокировка при истечении срока действия ключей.

Угрозы, связанные использованием анализа сопутствующей функционированию СКЗИ информации, получаемой по побочным каналам

Атака по побочному каналу реализуется злоумышленником на основе информации, доступной ему на основании наблюдения за выполнением криптографических операций в технических устройствах.

Программная реализация СКЗИ наиболее подвержена разновидности таких атак, называемой атакой по времени выполнения [4]. Атака основана на том, что на некоторых аппаратных платформах для выполнения различных операций требуется различное количество тактов процессора. Результатом является различное время выполнения операций. Криптоаналитик путем высокоточного замера времени может сделать предположения о значении ключа. В криптографических преобразованиях используются операции различного типа, как арифметические, так и битовые примитивы. Операции по устойчивости к атаке по времени выполнения подразделяются на следующие виды:

– неподверженные, особенностью которых является одинаковые временные затраты на выполнение на любой вычислительной платформе. К ним относятся операции табличной замены, сдвига и логические побитовые операции;

– ограниченно подверженные, для которых время выполнения может зависеть от операнда при определенных условиях. К ним относятся операции сложения и вычитания;

– подверженные, время выполнения которых определяется какой-либо зависимостью от размера операндов. К ним относятся операции умножения, деления, возведения в степень и переменные сдвиги.

Защитными мерами, предназначенными для противодействия атаке по времени выполнения, являются:

– рандомизация времени выполнения операций, когда вместе с операциями, реализующими преобразование, вводятся дополнительные незначащие операции со случайными значениями аргументов, либо произвольные временные задержки выполнения. В результате время выполнения даже одинаковых операций будет сильно различаться, что не позволит сопоставить выполняемые операции и значения операндов. Защитная мера позволяет снизить вероятность успешной реализации атаки по времени, однако не исключает ее полностью. Кроме того, рандомизация снижает производительность программного СКЗИ;

– выравнивание времени выполнения, когда время выполнения каждой операции выбирается максимально возможным, независимо от значений аргументов. Защитная мера позволяет полностью исключить атаку, однако сильно снижает производительность программного СКЗИ.

Заключение

Криптографические преобразования защищаемой информации не могут обеспечить свойств защищаемой информации, если при их реализации не рассматривать СКЗИ как объект защиты. В статье были рассмотрены основные угрозы программной реализации СКЗИ, к которым относятся угрозы исследования исполняемого кода, несанкционированного доступа к СКЗИ, угрозы криптографическим преобразованиям и угрозы утечки информации по побочным каналам. Также были рассмотрены основные защитные меры, нейтрализующие рассмотренные угрозы.

Библиографический список

1. Касперски, К. Искусство дизассемблирования / К. Касперски, Е. Рокко. – Санкт-Петербург : БХВ-Петербург, 2008. – 896 с.
2. Р 1323565.1.012-2017 Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации. – Москва : Стандартинформ, 2018.
3. Алферов, А. П. Основы криптографии : учеб. пособие / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. – Москва : Гелиос АРВ, 2005. – 480 с.
4. Панасенко, С. П. Алгоритмы шифрования. Специальный справочник / С. П. Панасенко. – Санкт-Петербург : БХВ-Петербург, 2009. – 567 с.

Образец цитирования:

Коростелев, М. С. Анализ угроз программной реализации средств криптографической защиты информации / М. С. Коростелев, О. В. Липилин // Инжиниринг и технологии. – 2020. – Vol. 5(1). – С. 1–4. – DOI 10.21685/2587-7704-2020-5-1-1.