КРИПТОАНАЛИЗ НА ОСНОВЕ АТАК ПО ПОБОЧНЫМ КАНАЛАМ

Олейников Р.В., Минаков А.Г.
АО "Институт информационных технологий"
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина 14, каф. безопасности информационных технологий
тел.(057) 702-14-25,
E-mail: ROliynykov@gmail.com, minakov13@gmail.com

This work describes the state situation in the area of side-channel attacks. It describes the various side channel known cryptanalysis methods available from the public literature. These attacks pose a serious threat to the security of cryptographic modules in the specific model with physical access o the attacking devic. In consequence, cryptographic implementations have to be evaluated for their resistivity against such attacks and the incorporation of different countermeasures has to be considered.

Информационно-телекоммуникационные системы активно применяются в современном мире, в том числе в критически важных системах. Информация, циркулирующая в них, нуждается в надёжной защите. При построении современных КСЗИ широко используются криптографические алгоритмы и протоколы, обладающие высоким уровнем стойкости к различным методам, основанным на математическом анализе свойств преобразований.

Тем не менее, для осуществления атак на криптографические примитивы было предложено использование так называемых побочных каналов, появляющихся в результате практической реализации математического алгоритма. Утечка данных через такие каналы чаще всего не предусматривается в классической модели безопасности протокола. Атаки по побочным каналам (Side Channel Attack) - это класс атак на криптосистему, которые, в отличие от теоретического криптоанализа, пытаются получить информацию о ключе или исходном тексте не на основании исследования описания криптографического алгоритма, а на основании данных, полученных в результате наблюдения за физическим процессом работы криптографического модуля, реализующего данный алгоритм.

Атаки по побочным каналам классифицируют по двум типам.

Инвазивные — неинвазивные. Инвазивные атаки требуют наличия прямого доступа к чипу или устройству. Типичным примером является подключение к шине данных для перехвата передаваемой информации. Неинвазивные атаки используют только информацию доступную извне: время работы устройства, потребляемая мощность, побочное электромагнитное излучение, звук работы системы. В некоторых источниках встречается термин полуинвазивные атаки. Эти атаки специфичны тем, что требуют наличия прямого доступа к поверхности чипа, но не требуют электрического контакта с металлической поверхностью.

Активные — пассивные. Активные атаки мешают должному функционированию оборудования (fault-injection attacks пытаются внести ошибки в вычисления). Пассивные атаки наблюдают за обработкой информации в устройстве, не нарушая его работу.

Перечень основных атак по побочным каналам и возможные методы защиты представлены ниже.

Probing attacks.

В данном типе атак для получения информации устройство вскрывается и исследуется каждый проводник, по которому передаются данные, или же с помощью электронного микроскопа исследуется состояние ячеек памяти. Эта задача может быть выполнена с использованием зондирующей станции, состоящей из микроскопа с микроманипуляторами.

Timing attacks.

Обычно, время работы программы рассматривается как параметр, который должен быть сокращён программистом. Однако известен факт, что время работы криптографического алгоритма также может являться информационным каналом для злоумышленника.

Время выполнения каждой логической операции может различаться в зависимости от входных данных (например, открытого текста или ключа). Это является следствием оптимизации производительности и других причин. При многократном измерении времени отклика системы на разные входные данные эта информация может оказаться исчерпывающей. Таким образом, атакующая сторона может произвести высокоточные измерения времени, за которое шифратор выполняет некоторые операции, и получить информацию о ключе (точнее, о его фрагментах).

В работе [1] приведена следующая классификация используемых в криптографических алгоритмах операций по степени их подверженности атакам по времени выполнения:

- не подвержены атакам по времени выполнения (т.е. выполняются за одинаковое число тактов на всех платформах): операции табличной замены, сдвига на фиксированное число битов, а также логические операции;
- в ряде случаев атаки по времени выполнения могут быть проведены против алгоритмов, в которых присутствуют операции модульного сложения или вычитания;
- наиболее проблемными с данной точки зрения являются операции умножения, деления, возведения в степень, а также сдвиги на переменное число битов.

Одним из наиболее показательных алгоритмов, против которых может быть проведена атака по времени выполнения, является алгоритм RC5. Среди других алгоритмов, подверженных данной атаке, в [2] упоминаются такие известные алгоритмы, как IDEA, Blowfish и DES.

В качестве противодействия атакам по времени выполнения предлагается следующее [2]:

1. обеспечить выполнение шифратором операций строго за одно и то же количество тактов процессора независимо от значений операндов, что сопряжено с техническими сложностями; кроме того, уменьшает быстродействие алгоритма, поскольку время выполнения операций в этом случае будет приведено к максимально возможному;
2. различным образом маскировать время выполнения операций: использовать случайные временные задержки, выполнять произвольные зашумляющие операции, внедрять в алгоритм различные случайные величины;
3. устранить условные переходы в реализации алгоритма.

Все это также приводит к уменьшению быстродействия алгоритма, поэтому наилучшим вариантом противодействия таким атакам является отсутствие в алгоритме шифрования операций, время выполнения которых зависит от обрабатываемых данных.

Power analysis attacks.

Как и время выполнения, энергопотребление криптографического устройства может предоставить дополнительную информацию о выполняемых операциях и входных параметрах. Суть данной атаки состоит в том, что в процессе работы шифратора злоумышленник с высокой точностью измеряет потребляемую мощность устройства. Современные лаборатории располагают оборудованием, способным производить измерения на исключительно высоких частотах (более 1 ГГц) и с высокой точностью (ошибка менее 1%).

Атаки по потребляемой мощности могут быть разделены на простые (Simple Power Analysis) и разностные (Differential Power Analysis). Простой анализ мощности представляет собой атаку по побочным каналам, которая включает в себя визуальный осмотр графиков текущего энергопотребления устройства. Изменение потребляемой мощности происходит в устройстве при выполнении различных математических операций. Цифровой осциллограф позволяет увидеть даже малые изменения в потребляемой мощности. Целью SPA является получение информации о конкретных выполняемых инструкциях в системе и о конкретных обрабатываемых данных. В общем случае SPA может дать как сведения о работе устройства, так и информацию о ключе. Для осуществления этой атаки криптоаналитик должен располагать точными данными о реализации устройства. Дифференциальный анализ мощности представляет собой атаку по побочным каналам, кото-

рая включает в себя статистический анализ потребляемой мощности. Эта атака применяется, если измерения содержат слишком много шума для простого анализа мощности. Более того, DPA зачастую не нуждается в данных о конкретной реализации и в качестве альтернативы использует статистические методы анализа. Дифференциальный анализ мощности – одно из самых мощных средств для проведения атак, использующих побочные каналы, причём эта атака требует сравнительно небольших затрат.

Основным методом борьбы с этим видом атак является балансировка потребляемой мощности. Следует добавить неиспользуемые (с точки зрения алгоритма) регистры и вентили, на которых выполняются бесполезные операции для того, чтобы сделать уровень потребляемой энергии постоянным значением. Такие методы, с помощью которых энергопотребление остаётся постоянным и не зависит от битов входа и ключа, предотвращают все виды атак по каналу энергопотребления.

Fault-injection attacks.

Суть рассматриваемой атаки заключается в осуществлении различного воздействия на криптографическое устройство с целью возникновения искажения информации на некоторых этапах шифрования. Это даёт возможность узнать входные параметры или некоторые части ключа. Наиболее распространённые методы воздействия:

- увеличение напряжения питания криптосистемы (выше максимально допустимого значения);
- изменение конструкции шифратора(нарушение электрических контактов);
- изменение тактовой частоты шифрующего устройства;
- помещение устройства в электромагнитное поле;
- повышение температуры некоторых частей криптографического устройства.

Подробный анализ может сравнивать данные на выходе до и после внесения изменений, таким образом, постепенно получая части ключа. Например, можно подобрать определённую интенсивность воздействия на алгоритм шифрования, чтобы происходила генерация одной ошибки за то время, которое тратится на шифрование одного блока. После каждого раунда шифрования находится секретный параметр, что в итоге приводит к полностью известному ключу.

Основные идеи этой методики были представлены в работе [3]. Предложенный подход был существенно развит в статье [4], где был описан дифференциальный анализ сбоев (differential fault analysis, DFA). Этот метод состоит в изучении результата работы алгоритма шифрования в нормальных условиях и при наличии сбоев при одном и том же входе (открытом тексте). Сбои обычно получаются созданием ошибки в процессе (кратковременная ошибка) или перед началом (постоянная ошибка) работы.

Противодействие атакам на основе сбоев. Не существует какой-либо универсальной защиты от воздействия на шифратор. Однако в [5] предлагается усложнение проведения атак на основе сбоев против аппаратного шифратора следующими способами:

- внедрение в шифратор детекторов различных воздействий (например, детекторов изменения напряжения, частоты питания и/или синхронизации, освещённости и т.д.), которые при обнаружении воздействия выполняли бы блокировку шифратора;
- различного рода пассивное экранирование шифратора, устранение которого приводило бы к выходу шифратора из строя;
- различные виды дублирования вычислений со сравнением результатов.

Для программных шифраторов также предлагаются методы защиты:

- использование контрольного суммирования фрагментов данных с периодической проверкой в процессе вычислений или различные контрольные вычисления;
- дублирование вычислений со сравнением результатов;
- внедрение в программу случайных избыточных вычислений.

Ясно, что подобные методы приводят к удорожанию шифратора и/или снижению его быстродействия, однако это необходимые методы при наличии у злоумышленника физического доступа к шифратору.

Electromagnetic analysis attacks.

В процессе функционирования средств вычислительной техники в конструктивных элементах и кабельных соединениях циркулируют электрические токи информативных сигналов, в результате чего формируются электромагнитные поля, уровни которых могут быть достаточными для приема сигналов и извлечения информации с помощью специальной аппаратуры. Катушка индуктивности помещается вблизи чипа, после чего измеряется электромагнитное поле. Возможно построение трёхмерных карт электромагнитного поля путём изменения положения катушки относительно чипа. Если добавить сюда изменение поля во времени, то получаем четырёхмерную модель. Анализ этих данных, как и в случае с изучением потребляемой мощности, может быть как простым, так и дифференциальным. Противодействием данному виду атак является надежное физическое экранирование или применение активных зашумляющих устройств.

Cache-based attacks.

В современных компьютерах для ускорения обработки информации при вычислениях используется кэш между процессором и оперативной памятью. Когда процессор обращается к информации, которая находится в оперативной памяти, то возникает задержка, так как необходимые данные должны быть загружены в кэш. Суть атаки заключается в анализе этих задержек и частоты появления кэша в вычислениях.

Таким образом, современные атаки по побочным каналам демонстрируют, что при наличии физического доступа к криптографическому устройству злоумышленник может значительно упростить криптоанализ. Известные методы защиты предполагают достаточно серьезное усложнение программной или аппаратной реализации, при этом не обеспечивая гарантий полной блокировки действий криптоаналитика. В дальнейших исследованиях целесообразно получить оценку верхней границы сложности и обоснование эффективности таких методов.

Литература:

1. Nechvatal J., Barker E., Dodson D., Dworkin M., Foti J., Roback E. Status report on the first round of the development of the advanced encryption standard // http://csrc.nist.gov — National Institute of Standards and Technology.
2. Kocher P. C. Timing Attacks on Implementation of Diffie-Hellman, RSA, DSS, and Other Systems // http://citeseer.ist.psu.edu — 1999 — Cryptography Research, Inc., San Francisco, CA, USA.
3. Boneh D., DeMillo R. A., Lipton R. J. On the Importance of Checking Cryptografic Protocols for Faults // http://citeseer.ist.psu.edu — Bellcore, Morristown, NJ.
4. Biham E., Shamir A. Differential Fault Analysis of Secret Key Cryptosystems // http://citeseer.ist.psu.edu — Technion — Israel Institute of Technology, Haifa, Israel — 1997.
5. Bar-El H., Choukri H., Naccache D., Tunstall M., Whelan C. The Sorcer's Apprentice Guide to Fault // http://citeseer.ist.psu.edu.
6. Панасенко С. П. Алгоритмы шифрования. Специальный справочник. - СПб.: БВХ-Петербург, 2009. - 576 с.: ил.
7. YongBin Zhou, DengGuo Feng. Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing.