электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

 # 01, январь 2016

УДК 004.056

Обзор основных атак по побочным каналам

Чубатая А., *студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»

Ступин Н. С., *студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»

Научный руководитель: Алешин В.А., к.т.н, доцент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»
v.aleshin@bmstu.net

Введение

В последние годы исследователи стали более осведомлены о возможности атак, которые используют определенные свойства реализации и операционной среды. Такие атаки используют утечку информации во время выполнения протокола и не рассмотрены в традиционных моделях обеспечения безопасности. Например, злоумышленник может контролировать потребляемую мощность или электромагнитное излучение, испускаемое смарт-картой, в то время как выполняются операции с закрытым ключом. Злоумышленник может также измерить время, которое требуется, чтобы выполнить криптографическую работу или проанализировать, как криптографическое устройство ведет себя, когда встречается с определенными ошибками. Такие атаки называются атаками по побочным (побочным) каналам (SCA - Side Channel Attack).

Авторы статьи [1] рассматривают криптографический примитив с двух точек зрения: с одной стороны, это абстрактный математический объект; с другой, этот примитив в конечном счете должен быть реализован в программе, которая будет работать на данном процессоре, на данной среде, поэтому будет обладать определенными характеристиками. Первая точка зрения - точка зрения «классического» криптоанализа (рис. 1); вторая - криптоанализа по побочным каналам (рис. 2).

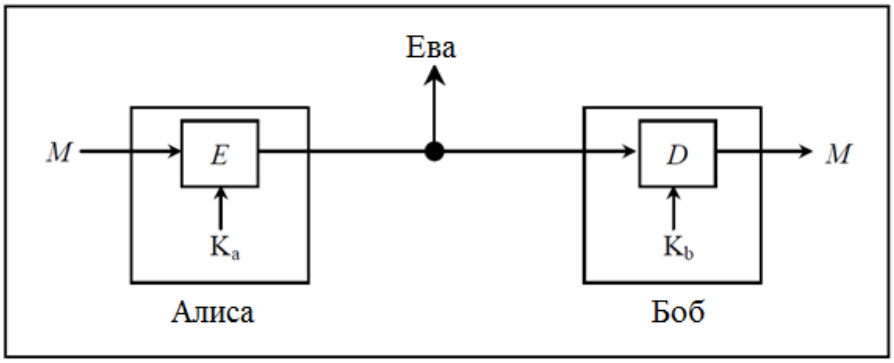


Рис. 1. Традиционная криптографическая модель

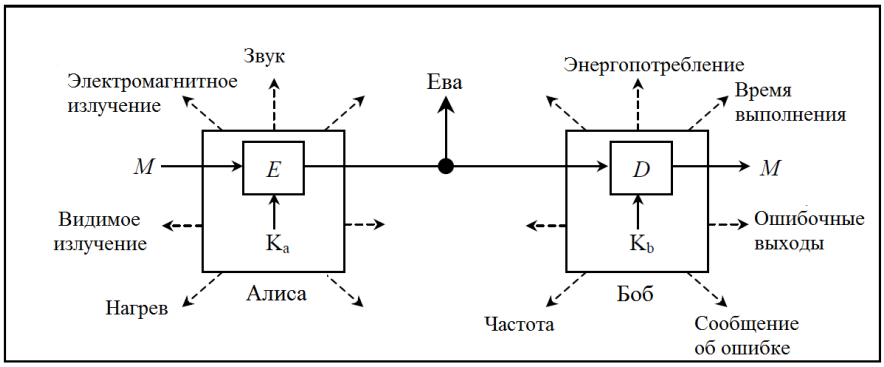


Рис. 2. Криптографическая модель, включающая побочные каналы

Криптоанализ по побочным каналам использует преимущества реализации конкретных характеристик для восстановления ключевых параметров, участвующих в вычислениях.

Классификации атак по побочным каналам

Авторы [1] приводят классификацию атаки по побочным каналам по трем ортогональным признакам:

- Классификация в зависимости от контроля за ходом вычислительного процесса;
- Классификация в зависимости от способа доступа в модуль;
- Классификация в зависимости от метода, используемого в процессе анализа.

В зависимости от контроля за ходом вычислительного процесса злоумышленниками, SCA-атаки можно разделить на две основные категории: пассивные и активные атаки.

Пассивные атаки - те, которые незаметно вмешиваются в работу целевой системы; злоумышленник получает некоторую информацию о работе целевой системы, но система ведет себя точно так же, как если бы никакой атаки не происходило. С другой стороны, в

активной атаке злоумышленник оказывает некоторое влияние на поведение целевой системы. В то время как активно атакованная система может либо обнаружить такое влияние, либо нет, то посторонний наблюдатель мог бы заметить разницу в работе.

Авторы статьи [1] ссылаются на работы Андерсона [2], который разделил атаки по побочным каналам по способу получения доступа к модулю на следующие классы: агрессивные, полуагрессивные и неагрессивные.

Агрессивная атака включает в себя распаковку, для получения прямого доступа к внутренним компонентам криптографических модулей или устройств. Типичным примером является то, что атакующие могут открыть дыру в пассивирующем слое криптографического модуля и поместить иглу зондирования в шину данных, чтобы видеть передачу данных.

Понятие полуагрессивной атаки впервые разработали Скоробогатов и Андерсон [3]. Этот вид атаки включает в себя доступ к устройству, но не повреждает пассивирующий слой или устанавливая электрический контакт только с санкционированной поверхностью. Например, в вызванной отказом атаке, атакующий может использовать лазерный луч, чтобы ионизировать устройство, для изменения некоторых участков его памяти и таким образом изменить вывод этого устройства.

Неагрессивная атака включает в себя тщательное наблюдение или манипулирование процессами устройства. Эта атака использует только внешне доступную информацию, которая часто неумышленно пропускается.

В зависимости от методов, используемых в процессе анализа выбранных данных, атаки SCA могут быть разделены на простую атаку по побочным каналам (SSCA - Simple Side Channel Attack) и дифференциальную атаку по побочным каналам (DSCA - Differential Side Channel Attack).

SSCA использует отношения между выполняемыми инструкциями и выводом побочного канала. То есть информация о побочном канале, связанная с атакованными инструкциями (сигналами), должна быть больше, чем информация о побочном канале, связанная с несвязанными инструкциями (шумами).

С другой стороны, когда SSCA не представляется возможной из-за большого количества шумов в измерениях, применяют DSCA с использованием статистических методов. DSCA использует корреляцию между обработанными данными и выводом побочного канала. В атаке DSCA в основном используют выход побочного канала в зависимости от выполняемых данных. Как правило, используется много трассировок, а затем используются статистические методы для того, чтобы определить возможные секретные ключи. В связи с этим можно утверждать, что DSCA более мощны, чем SSCA.

До сих пор атаки SCA успешно использовались, чтобы повредить аппаратные средства или реализации программного обеспечения многих криптографических систем включая блочные шифры, поточные шифры, шифры с открытым ключом, чтобы повредить реализации схем подписи, схемы кода аутентификации сообщений, реализацию криптографических протоколов, реализацию криптографических систем, и даже повредить сетевые системы.

Атаки SCA используют характеристики аппаратных и программных элементов, а также структуру реализации криптографического примитива. Поэтому, в отличие от анализа математической структуры и свойств криптографических примитивов, только анализ побочного канала также включает реализацию.

Атака по времени

Реализации криптографических алгоритмов часто выполняют вычисления за различное время из-за оптимизации производительности. Если такие операции затрагивают секретные параметры, то эти временные вариации могут пропустить некоторую часть информации и, если под рукой достаточно знаний о реализации, тщательный статистический анализ может даже привести к полному восстановлению этих секретных параметров. Эта идея была представлена Кохером [4], в которой на практике проводилась атака по времени против современной реализации смарт-карты RSA.

Атака по времени - это способ получения конфиденциальной информации некоторого пользователя, тщательно измеряя время, которое требуется пользователю, чтобы выполнить криптографические операции. Принцип этой атаки очень прост: использовать различные временные дисперсии в работе.

Основные положения временного анализа:

1. Время выполнения криптографической операции зависит в некоторой степени от ключа. С существующими аппаратными средствами это так, но существуют различные предложения эффективных аппаратных средств сделать атаку временным анализом менее выполнимой через "шумовую инжекцию". Подходы программного обеспечения, чтобы сделать атаку временным анализом неосуществимой основываются на идее, что вычисления в двух ответвлениях условного выражения должны занять то же количество времени ("коррекция ответвления").
2. Достаточно большое количество кодировок может быть выполнено, и за это время ключ не изменится. Протокол вызов-ответ идеален для атак по времени.

3. Время может быть измерено с известной ошибкой. Чем меньше ошибка, тем меньше временных измерений требуется.

Один простой подход к защите заключается в том, чтобы сделать рабочие параметры независимыми от входных данных. Возможность этого подхода зависит от функционирования. Другой, более простой подход к защите заключается в разработке аппаратных средств, которые принимают постоянное время для каждой операции, независимо от того, какие были данные.

Атака на основе сбоев

Предполагается, что большинство устройств, которые выполняют различные криптографические операции, работают надежно. Несмотря на это предположение, сбои оборудования и ошибки, возникающие во время работы криптографического модуля, фактически продемонстрировали серьезное влияние на безопасность.

Атаки на основе сбоев (ошибок) в криптографических алгоритмах изучались с 1996, и с тех пор почти все криптографические алгоритмы были повреждены при помощи таких видов атак. Атаки на основе сбоев предлагают атакующему много возможностей атаковать криптографическую систему. Способы использования ошибочного результата очень отличаются от одного алгоритма к другому. Выполнимость атаки на основе сбоя зависит от возможностей противника и типа сбоев, которые она может вызвать. Обычно модель сбоя должна определить следующие аспекты:

- Точность, которую атакующий может достигнуть при выборе времени и места, на котором сбой происходит во время выполнения криптографического модуля.
- Длина данных, затронутая сбоем; например, только один бит или один байт.
- Постоянство ошибки; переменная ли ошибка или постоянная.
- Тип сбоя, такие как инверсия одного бита, инверсия одного бита, но только в одном направлении (например, от 1 до 0); байт изменился на неизвестное значение; и т.д.

Есть два главных вида побочных каналов сбоя. Первые - каналы, которые вызваны вычислительными сбоями, происходящими во время криптографического вычисления в атакованном модуле. Эти сбои могут быть или случайными, или намеренными, вызванные, например, с помощью точного манипулирования напряжения. Вторые виды побочных каналов сбоя - те, которые провоцируют, отправив преднамеренно поврежденные входные данные в атакованный модуль. Для модуля это означает нестандартную ситуацию, которая должна быть обработана специальным образом.

Вообще говоря, успешная атака на основе сбоя на криптографические модули или устройства требует двух шагов: внесение неисправности и ошибочное эксплуатирование шагов. Эти два шага проиллюстрированы на рисунке 3.

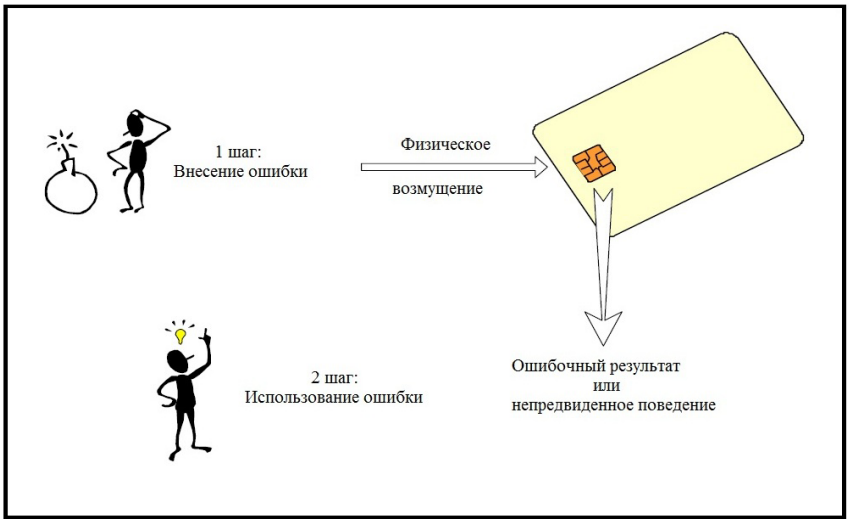


Рис. 3. Атака на основе сбоя на смарт-карту

Одна из контрмер, чтобы защищать алгоритмы с открытым ключом от некоторых определенных атак сбоя, должна проверить целостность секретного ключа в конце вычисления подписи. Другие общие приемы независимо от конкретных алгоритмов также были предложены, в том числе контрольные суммы, рандомизация выполнения, счетчики ратификации и приманки, повторные обновления.

Атака по энергопотреблению

В дополнение к своим времени выполнения и ошибочному поведению системы, потребляемая мощность криптографического устройства может предоставить много информации об операциях, которые происходят и соответствующих параметрах. Это и есть сама идея атаки анализа энергопотребления. Данная атака особенно эффективна и успешно зарекомендовала в атаках на смарт-карты или другие специальные встраиваемые системы, хранящие секретный ключ.

В основном атака анализа энергопотребления может быть разделена на Простой Анализ Энергопотребления (SPA - Simple Power Analysis) и Дифференциальный Анализ Энергопотребления (DPA - Differential Power Analysis). В атаках SPA цель состоит в том, чтобы по существу предположить какая определенная инструкция выполняется в определенное время и что имеется на оцениваемых входах и выходах. Поэтому злоумышленник должен точно знать реализацию, чтобы осуществить такую атаку. С

другой стороны, для атаки DPA не нужно знание деталей реализации и альтернативного использования статистических методов в аналитическом процессе. DPA - одна из самых мощных атак SCA, но она может быть установлена при помощи очень малого количества ресурсов. Также существует более усовершенствованный дифференциальный анализ энергопотребления, который смотрит на тонкие статистические корреляции между секретными битами и потребляемой мощностью.

Защита против дифференциальной атаки анализа энергопотребления трудна, так как она в основном только уменьшает сигнал, который противник считывает, вместо того, чтобы устранить его. Интересно, что эффективный метод рандомизации, используя некоторые случайные переменные в операции сложения точки, был также предложен как возможная контрмера против атаки DPA.

Атака по электромагнитному излучению

Как электрические устройства, компоненты компьютера часто генерируют электромагнитное излучение как часть их операций. Злоумышленник, который может наблюдать эти излучения и может понять их причинно-следственную связь с базовыми вычислениями и данными, в состоянии вывести удивительное количество информации об этом вычислении и данных.

Подобно атакам анализа энергопотребления, атаки по электромагнитному излучению (EMA - ElectroMagnetic Analysis) могут также быть разделены на две основных категории: Простой Анализ Электромагнитного Излучения (SEMA - Simple ElectroMagnetic Analysis) и Дифференциальный Анализ Электромагнитного Излучения (DEMA - Differential ElectroMagnetic Analysis).

Контрмеры против атак EM на определенные реализации делятся на две большие категории: снижение мощности сигнала и снижение объема информации сигнала. Методы для сокращения мощности сигнала включают модернизацию схемы [8], чтобы уменьшить непреднаменные излучения и использование экранирования и физически защищенных зон, чтобы уменьшить силу ущерба сигналов, доступных противнику относительно окружающего теплового шума. Методы для снижения объема информации сигнала полагаются на использование рандомизации и/или частого ключевого обновления в вычислении, чтобы существенно уменьшить эффективность статистических атак, используя доступные сигналы.

Атаки по видимому излучению

Одной из рассмотренных атак также стала атака по видимому излучению. Одна выдающаяся характеристика этой атаки - то, что физический доступ не требуется. Кун [5] демонстрировал (с помощью сложного анализа и с помощью прямого эксперимента), что средняя яркость диффузного отражения ЭЛТ от стены может быть достаточно, чтобы восстановить сигнал, выведенный на экран на ЭЛТ (так что экранирование ЭЛТ для защиты от утечки информации через электромагнитное излучение может оказаться недостаточно). Он также размышлял, что те же методы одинаково применимы к сигналам LED. Даже без угла обзора, злоумышленник может быть в состоянии считать сигналы, которые платформа доверительных вычислений оптических каналов выхода испускают.

Атака, основанная на кэше

Основная идея атаки состоит в том, что если ЦП обращается к данным, которые не сохранены в кэше (промах кэша), то будет произведена задержка, так как целевые данные должны быть загружены из основной памяти в кэш. Измерение этой задержки может позволить злоумышленникам определить вхождение и частоту промахов кэша. Существует множество контрмер для уменьшения атак на основе кэша, таких как ограничение доступа к кэшу, выключение очистки кэша, использование специфических алгоритмов маскировки, принятие разделенной аппаратной структуры кэша и др.

Частотная атака

В статье [1] дается ссылка на работу Лиу [6], который предложил частотную атаку, направленную против мобильных устройств, таких как смартфоны, телефоны и пейджеры. Его метод эффективен даже при смещении следов, в то время как ранее предложенная DEMA не справилась с задачей в таких условиях. В дополнение, десинхронизирующая контрмера (которая вставляла случайные задержки) не действует на частотную атаку Луи.

Атаки, основанные на сканировании

Тест, основанный на сканировании, является очень мощным инструментом проверки. Однако он в равной степени может стать и мощным инструментом для атаки. В 2004 году Ян [7] использовал сканирование цепей, как побочный канал для восстановления секретных ключей из аппаратной части DES (Data Encryption Standard). При использовании одной встроенной схемы для тестирования, внутренний статус

криптографического чипа не будет просканирован, таким образом можно избежать атак основанные на сканировании.

Контрмеры

В настоящее время существует множество стратегий (как в области аппаратного, так и программного обеспечения), среди которых авторы выделили три основных направления:

- де-коррелирование отдельных выходных параметров (например, путем введения случайных временных сдвигов и состояний ожидания, вставляя фиктивные инструкции, хаотизации выполнения операций и т.п.);
- замена критических инструкций ассемблера теми, чьи ключи трудно анализировать, или модернизировать критическую схему, которая выполняет арифметические операции или передачу данных в память;
- сделать алгоритмические изменения в криптографических примитивах, так что атаки становятся неэффективны на полученной реализации, например, маскируя данные и ключ со случайной маской, генерируемой в каждом цикле.

Заключение

Мы рассмотрели атаки по побочным каналам и соответствующие контрмеры. Широкий спектр контрмер против атак по побочным каналам были разработаны исследователями для обеспечения защиты. Мы считаем, что ясное понимание атак, а также компромиссы, связанные с развертыванием контрмер позволят разработать действительно безопасную систему.

Широта диапазона возможных направлений атаки усложняет задачу их решения. В настоящий момент были полностью или частично исследованы по крайней мере десять видов побочных каналов. Таким образом, разработка реализации криптографического модуля или системы требует хорошей осведомленности о потенциальных слабостях реализации, которые становятся недостатками безопасности, и тщательного рассмотрения безопасности всех аспектов архитектуры, аппаратного обеспечения, а также разработки программного обеспечения процессов.

Есть также много интересных тем для исследователей. В частности, строгие модели безопасности атак по побочным каналам, которые до сих пор плохо изучены. Не стоит также забывать, что есть еще некоторые побочные каналы, которые ждут своего открытия.

Список литературы

[1] Zhou Y. B., Feng D. G. Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing. Cryptology ePrint Archive. 2005. Available at: http://eprint.iacr.org/2005/388.pdf, accessed 16.02.2015.

[2] Anderson R., Bond M., Clulow J., Skorobogatov S. Cryptographic Processors - A Survey // Proceedings of the IEEE. 2006. Vol. 94. No. 2. P. 357–369. DOI: 10.1109/JPROC.2005.862423.

[3] Skorobogatov S., Anderson R. Optical Fault Induction Attacks // In Proceedings of Cryptographic Hardware and Embedded Systems (CHES 2002). Springer-Verlag, London, UK, 2003. Vol. 2523 of Lecture Notes in Computer Science (LNCS). P. 2–12.

[4] Kocher P. Timing attacks on implementations of Diffie-Hellmann, RSA, DSS, and other systems // In Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO ’96). Springer-Verlag, London, UK, 1996. Vol. 1109 of Lecture Notes in Computer Science (LNCS). P. 104–113.

[5] Kuhn M. Optical Time-Domain Eavesdropping Risks of CRT Displays // Proceedings of the 2002 IEEE Symposium on Security and Privacy. Berkeley, California, 2002. P. 3–18. DOI: 10.1109/SECPRI.2002.1004358.

[6] Tiu C.C. A New Frequency-Based Side Channel Attack for Embedded Systems. Master degree thesis: Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada, 2005.

[7] Yang B., Wu K., Karri R. Scan-based Side-Channel Attack on Dedicated Hardware Implementations of Data Encryption Standard // In Proceedings of the International Test Conference on International Test Conference (CCS ’05). New York, USA, 2005. P. 139-146.

[8] Maistri P., Leveugle R., Bossuet L., Aubert A., Fischer V., Robisson B., Moro N., Maurine P., Dutertre J.-M., Lisart M. ElectroMagnetic Analysis and Fault Injection onto Secure Circuits // 22nd IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC 2014). Playa del Carmen, Mexico, 2014. P. 1-6.