A. B. Levina, M. G. Korovkin

Combined Side Channel Attacks: breaking COMP128

Keywords: side channel attacks, cryptography, COMP128

Different variants of combined side channel attacks (SCA) on authentication protocol COMP128 are analyzed in the article, paper. Main attack presented in the paper is partitioning attack. In the result, combined SCA increasing breaking of cipher are shown in the research.

А. Б. Левина, М. Г. Коровкин

КОМБИНИРОВАННЫЕ АТАКИ ПО СТОРОННИМ КАНАЛАМ: ВЗЛОМ COMP128

Введение

В последние 20 лет активно развивается новое направление криптоанализа, называемое Side Channel Attacks (SCA), или атаки по сторонним каналам [1–9]. Основная идея данного подхода заключается в том, что шифрующее устройство рассматривается не только как математический аппарат, но и как конкретная его реализация на практике. Классический криптоанализ рассматривает криптоалгоритм с точки зрения математики — как некоторую функцию от входных данных, на выходе которой зашифрованный текст. Новая концепция рассматривает криптоалгоритм вместе с его материальной реализацией, обладающей определенными физическими свойствами, такими как время выполнения алгоритма, потребляемая при шифровании мощность, электромагнитное излучение от шифрующего устройства и другие.

В настоящее время SCA являются более результативным вариантом криптоанализа, нежели его классический вариант. С развитием SCA многие известные реализации используемых алгоритмов шифрования были взломаны, что побудило криптографов к созданию мер защиты от этой угрозы.

В данной статье будет рассмотрена одна из таких атак по сторонним каналам — «распределенная атака» на COMP128, который является базовой реализацией для аутентификации пользователей в сетях GSM. В нем используется секретный ключ, зашитый в SIM-карте телефона. Узнав этот ключ, злоумышленник может совершать звонки за счет настоящего владельца SIM-карты, а также прослушивать его разговоры.

Комбинированные атаки

Атаки по сторонним каналам очень многообразны. Как уже упоминалось ранее, можно использовать такие сторонние каналы, как время шифрования [2], мощность потребления [3], электромагнитное излучение от шифратора [4, 5]. Помимо этого, можно использовать яркость света, излучаемого монитором и отраженного от стены [6]. Можно достать секретную информацию даже по звукам, издаваемым внутренними компонентами электронного шифратора [7]. Существуют также различные атаки, воздействующие на шифратор и создающие в нем ошибки, по которым потом восстанавливается ключ [8, 9].

В связи с этим многообразием возникла идея о возможности проведения комбинированной атаки по сторонним каналам. Суть заключается в комбинировании нескольких атак для того, чтобы вскрыть какой-то алгоритм быстрее, чем это может сделать каждая из атак по отдельности. Также возможно сочетать несколько атак для получения большего количества секретных сведений, это даст результат, лучший, чем если бы использовалась одна из атак или обе, но по отдельности.

Следует отметить, что противодействие комбинированным side channel атакам состоит в том, чтобы противодействовать составляющим атакам. Это является основным недостатком комбинированных SCA, поскольку сложность защиты от них равна сложности защиты от одной из составляющих атак, причем именно той, которой легче всего противодействовать.

Распределенная атака на COMP128

В 2002 г. в работе "Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards" («Распределенные атаки, или Как быстро клонировать GSM-карты») [1] авторы рассказали, как можно реализовать атаку по потребляемой мощности (Simple Power Analysis – SPA) на SIM-карту. Данная атака позволяет получать секретный ключ всего за пару минут. При этом авторы использовали около 1000 случайных запросов и доказали, что можно использовать всего 255 заранее подготовленных запросов (атака с выбором открытого текста). Более того, атаку можно усовершенствовать до 8 приспосабливающихся запросов, что позволяет проводить вскрытие секретного ключа за несколько секунд. Предыдущая известная атака на COMP128 – BGW (Briceno, Goldberg, Wagner – по фамилиям авторов) – требовала примерно 150000 запросов.

Авторы «распределенной атаки» воспользовались тем фактом, что на первом раунде шифрования используется замена по таблице T0, которая содержит 512 элементов. То есть для индексации по ней необходимо использовать 9-битовые значения, в то время как в SIM-карте используется лишь 8-битовая архитектура. Тогда авторы предположили, что таблица должна быть разбита на 2 подтаблицы размером по 256 элементов. Анализируя энергопотребление SIM-карты при различных запросах, исследователи смогли определить, к какой части таблицы T0 был адресован запрос. Таким образом, замеряя энергопотребление запросов при изменении входных данных, они смогли вычислить секретный ключ.

В данной статье будет представлено, как можно улучшить полученные ранее результаты и уменьшить количество необходимых входных текстов, применив другие атаки по сторонним каналам.

Варианты комбинированных атак на COMP128

«Распределенная атака» на COMP128, разработанная в 2002 г., является простой атакой по потребляемой мощности. Чтобы улучшить ее результаты, необходимо скомбинировать эту атаку с другими атаками. Для комбинации рассмотрим атаку по времени, атаку на основе зондирования и атаку на основе генерируемых ошибок.

Комбинация с атакой по времени

Комбинация с атакой по времени является хорошим вариантом комбинированной атаки, поскольку и атака по потребляемой мощности, и атака по времени являются неинвазивными и пассивными. Данная комбинация удобна, поскольку в этом сочетании не нужно дополнительных активных воздействий, а требуется лишь «прослушивание» шифрующего устройства (пассивность). Обнаружить такую атаку после ее совершения было бы крайне трудно, поскольку обе ее составляющие никак не воздействуют на SIM-карту (неинвазивность).

Рассмотрим операции, из которых состоит исследуемый алгоритм шифрования, и проанализируем, насколько они подвержены атакам по времени. Сложение в формуле вычисления индексов для таблиц замены всегда одинаковое и никак не зависит ни от ключа, ни от входного значения:

$$\left.\begin{aligned} m &= l + k*2^{(5-j)} \\ n &= m + 2^{(4-j)} \end{aligned}\right\}, \quad (1)$$

где переменные l, k и j – порядковые индексы, обозначающие номера определенных стадий шифрования. Сложение в формуле вычисления индексов для таблицы замены зависит непосредственно от байтов, полученных на предыдущем раунде:

$$\left.\begin{aligned} y &= (X[m] + 2*X[n]) \bmod 2^{(9-j)} \\ z &= (2*X[m] + X[n]) \bmod 2^{(9-j)} \end{aligned}\right\}, \quad (2)$$

где m и n — индексы, полученные из формулы (1), а X[] — массив из 32 байт, с которым работает алгоритм. Здесь тоже не видится возможности для атаки, поскольку складываются одинаковые по размеру величины, а результатом вычисления является лишь индекс, по которому на следующем шаге будет взят определенный элемент таблицы. В конце каждого из раундов также происходит перестановка битов.

Получается, что COMP128 использует следующие операции: сложение, модульное деление (по модулю, являющемуся степенью двойки), умножение на 2, табличные замены и перестановки битов — операции, не подверженные атаке по времени. Отсюда можно сделать вывод, что на данный алгоритм провести такую атаку довольно сложно.

Комбинация с атакой на основе зондирования

Комбинация с атакой на основе зондирования теряет те преимущества, которые имела комбинация атаки по потребляемой мощности и атаки по времени, поскольку зондирование является инвазивной атакой, то есть потребуется «вскрывать» SIM-карту. Обнаружить такую атаку после ее осуществления становится проще. Однако зондирование дает куда большую свободу в выборе анализируемых данных, поскольку с его помощью можно наблюдать за практически любым местом шифрующего алгоритма.

В COMP128 можно наблюдать за последними 16 байтами массива X[] на каждом из 8 раундов, а не только на первом:

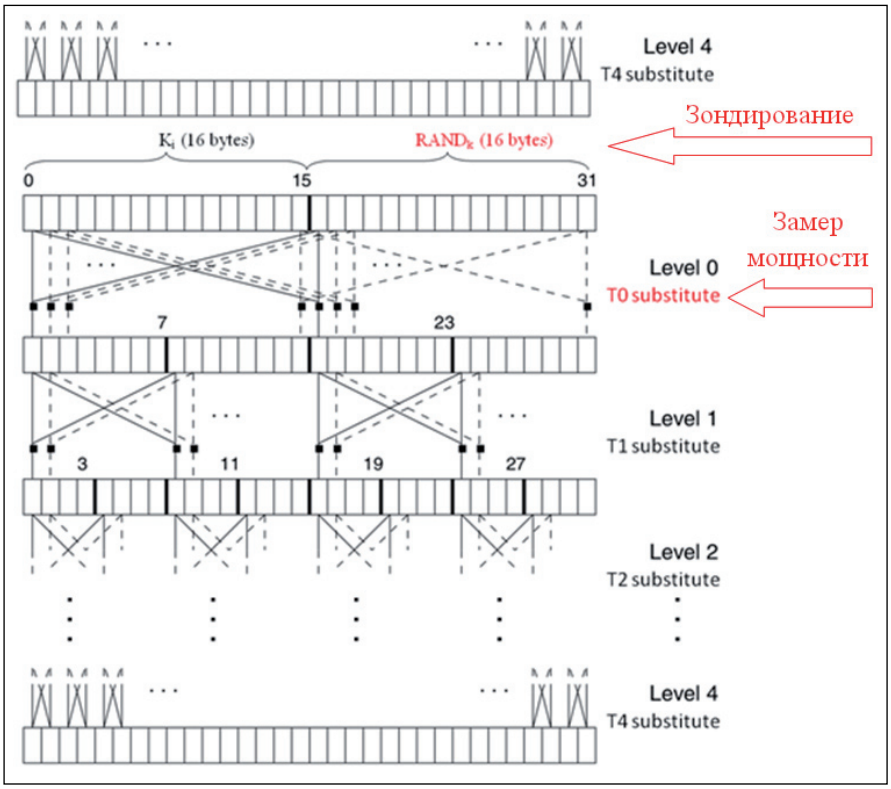

Рис. 1. Замеры по мощности с помощью зондирования на каждом из 8 раундов

Это даст выигрыш в скорости в 8 раз. Таким образом, «распределенную атаку» с выбранными входными значениями можно провести за 255:8 = 64 попытки, а атаку со случайными входными значениями за 1000:8 = 125 попыток.

Комбинация с атакой на основе генерируемых ошибок

Комбинация с атакой на основе генерируемых ошибок является чем-то средним между двумя представленными вариантами атак. Это сочетание уже не дает пассивную атаку, как комбинация с атакой по времени, поскольку генерация ошибок является ярко выраженным примером активной атаки. Это позволяет изменять ход алгоритма, внося туда ошибки, в результате чего получается более широкий спектр данных для анализа по потребляемой мощности. С другой стороны, генерация не такой мощный инструмент, как зондирование, поэтому ее применение не столь разностороннее и всеохватывающее. В то же время атака с генерацией ошибок, как правило, не требует столь дорогого оборудования.

Аналогично предыдущей атаке, можно вносить ошибку в начале каждого раунда в последние 16 байт. COMP128 записывает в эти 16 байт перемешанные биты, полученные на предыдущем раунде шифрования. Если вносить ошибку, которая записывает в последние 16 байт массива X[] нужные нам значения, то замеры по потребляемой мощности возможно проводить не только на первом раунде шифрования. Например, на каждом раунде (кроме первого) требуется записывать в последние 16 байт значения R[], полученные от базовой станции, увеличенные на 1 по сравнению с предыдущим раундом:

X[16] = R[0]
X[17] = R[1]
…
X[31] = R[15]
} на 1-м раунде шифрования

X[16] = R[0] + 1
…
X[31] = R[15] + 1
} на 2-м раунде шифрования

Тогда можно получить результаты по потребляемой мощности для табличной замены T0 для значений от x до x + 7, что раньше можно было сделать только за 8 различных попыток. А это значит, что количество необходимых запросов сокращается в 8 раз.

Заключение

В данной статье рассмотрены различные варианты комбинации атак по сторонним каналам на алгоритм аутентификации COMP128 в сетях GSM. Комбинированные атаки с атакой на основе зондирования и с атакой с генерацией ошибок способны дать выигрыш в скорости в 8 раз.

Статья показывает, как комбинированные SCA могут вскрывать шифры быстрее по сравнению с составляющими SCA атаками. На практике защита от данного вида атак сводится к защите от одной из составляющих ее частей.

СПИСОК ЛИТЕРАТУРЫ:

1. *Rao J., Rohatgi P., Scherzer H., Tinguely S. Partitioning Attacks*: Or How to Rapidly Clone Some GSM Cards // IEEE Symposium on Security and Privacy. 2002. P. 31–41.
2. *Kocher P. C.* Timing attacks on implementations of Diffie-Hellmann, RSA, DSS, and other systems // Advances in Cryptology. CRYPTO'96. 1996. P. 104–113. URL: http://www.cryptography.com/public/pdf/TimingAttacks.pdf (дата обращения: 07.12.2013).
3. *Kocher P., Jaffe J., Jun B.* Differential Power Analysis // Proceedings of Advances in Cryptology. 1999. P. 388–397. URL: http://www.cryptography.com/public/pdf/DPA.pdf (дата обращения: 20.03.2014).
4. *Quisquater J.-J., Samyde D.* ElectroMagnetic Analysis (EMA): Measures and Counter-measures for Smart Cards // E-SMART'01 Proceedings of the International Conference on Research in Smart Cards: Smart Card Programming and Security. 2001. P. 200–210.
5. *Gandolfi K., Naccache D., Paar C., Karine G. , Mourtel Ch., Olivier F.* Electromagnetic Analysis: Concrete Results // Proceedings of the Third International Workshop on Cryptographic Hardware and Embedded Systems. Springer-Verlag. 2001. P. 251–261.

6. *Kuhn M. G.* Optical time-domain eavesdropping risks of CRT displays // Proceedings of IEEE Symposium on Security and Privacy. 2002. P. 3–18. URL: http://www.cl.cam.ac.uk/~mgk25/ieee02-optical.pdf (дата обращения: 12.02.2014).
7. *Shamir A., Tromer E.* Acoustic cryptanalysis: On nosy people and noisy machines. 2011. URL: http://tau.ac.il/~tromer/acoustic/ (дата обращения: 10.04.2014).
8. *Boneh D., DeMillo R. A., Lipton R. J.* On the importance of checking cryptographic protocols for faults // Advances in Cryptology. EUROCRYPT'97. 1997. P. 37–51.
9. *Biham E., Shamir A.* Differential Fault Analysis of Secret Key Cryptosystems // Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO'97). Springer-Verlag, 1997. P. 513–525.

REFERENCES:

1. *Rao J., Rohatgi P., Scherzer H., Tinguely S.* Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards // IEEE Symposium on Security and Privacy. 2002. P. 31–41.
2. *Kocher P. C.* Timing attacks on implementations of Diffie-Hellmann, RSA, DSS, and other systems // Advances in Cryptology — CRYPTO '96. 1996. P. 104–113. URL: http://www.cryptography.com/public/pdf/TimingAttacks.pdf.
3. *Kocher P., Jaffe J., Jun B.* Differential Power Analysis // Proceedings of Advances in Cryptology.1999. P. 388–397. URL: http://www.cryptography.com/public/pdf/DPA.pdf.
4. *Quisquater J.-J., Samyde D.* ElectroMagnetic Analysis (EMA): Measures and Counter-measures for Smart Cards // E-SMART '01 Proceedings of the International Conference on Research in Smart Cards: Smart Card Programming and Security. 2001. P. 200–210.
5. *Gandolfi K., Naccache D., Paar C., Karine G., Mourtel C., Olivier F.* Electromagnetic Analysis: Concrete Results // Proceedings of the Third International Workshop on Cryptographic Hardware and Embedded Systems. Springer-Verlag, 2001. P. 251–261.
6. *Kuhn M. G.* Optical time-domain eavesdropping risks of CRT displays // Proceedings of IEEE Symposium on Security and Privacy. 2002. P. 3–18. URL: http://www.cl.cam.ac.uk/~mgk25/ieee02-optical.pdf
7. *Shamir A., Tromer E.* Acoustic cryptanalysis: On nosy people and noisy machines. 2011. URL: http://tau.ac.il/~tromer/acoustic/
8. *Boneh D., DeMillo R. A., Lipton R. J.* On the importance of checking cryptographic protocols for faults // Advances in Cryptology — EUROCRYPT '97.1997. P. 37–51.
9. *Biham E., Shamir A.* Differential Fault Analysis of Secret Key Cryptosystems // Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO '97). Springer-Verlag, 1997. P. 513–525.