УДК 681.3.06

А.А. Смирнов, канд. техн. наук
Кировоградский национальный технический университет

Метод обеспечения защиты информации в автоматизированных системах управления противодействием временной атаке

Предложен метод обеспечения защиты информации в АСУ противодействием криптографической атаке, на основе замера времени выполнения операций, при формировании цифровой подписи в группе точек эллиптических кривых
цифровая подпись, эллиптические кривые, временная атака

На современном этапе развития информационных технологий, при работе с данными, циркулирующими в открытых сетях и системах, активно применяется цифровая подпись. Цифровые подписи, сформированные на основе применения аппарата эллиптических кривых, являются наиболее стойкими.

В [1-5] проведено исследование методов криптоанализа, определяющих стойкость цифровой подписи, основанной на преобразованиях в группе точек эллиптических кривых. Были определены две основных группы атак: атаки, основанные на анализе криптографических преобразований, и атаки, основанные на решении задачи нахождения дискретного логарифма. В первой группе одно из лидирующих мест занимает атака, основанная на замере времени выполнения операций при формировании цифровой подписи.

Целью данной статьи является разработка метода противостояния временной атаке на алгоритм формирования цифровой подписи.

Наиболее очевидный путь предотвращения атак временным анализом состоит в том, чтобы все действия занимали точно одно и то же время. Это часто бывает трудно. Создание программного обеспечения, особенно платформо-независимого, таким образом, чтобы оно выполнялось в фиксированное время, весьма трудно, потому что оптимизация компилятора, попадания в программный кэш, время выполнения инструкций и другие факторы могут внести неожиданные колебания во время исполнения. Если для задержки возвращаемых результатов до определенного времени используется таймер, то факторы типа "отклика системы" или энергопотребления могут служить признаками фактического окончания операции. Более того, реализации с фиксированным временем будут медленными; большинство оптимизаций не сможет быть использовано, так как все действия должны занимать время, исполнения самой медленной операции.

Другой подход состоит в том, чтобы сделать измерения времени настолько неточными, чтобы атака стала невыполнимой. Случайные задержки, добавленные к процессу, увеличат необходимое количество шифрованного текста для нападающего, но он сможет преодолеть это увеличением числа измерений. Требуемое число значений грубо оценивается как квадрат шума. К счастью, имеется и лучшее решение. Методы, используемые для скрытия подписей, могут быть приспособлены, чтобы предотвратить знание атакующего входных данных к модульной функции возведения в степень[1]. Следовательно, максимум того, что атакующий может узнать – общее распределение времени для действий умножения точки на число. Практически, эти распределения

близки к нормальным и 2^w экспонент нельзя различить. Однако специально разработанная функция умножения точки на число могла бы теоретически иметь распределение с острыми пиками, соответствующими битам экспоненты, и в этом случае скрытие, вероятно, не предотвратит временной анализ [2, 3].

Атаку можно трактовать как проблему распознавания сигналов [4]. "Сигнал" состоит из вариаций измерения времени для известных бит, "шум" - из погрешностей измерения времени и вариаций измерения времени для неизвестных бит. Свойства "сигнала" и "шума" определяют количество замеров времени, требуемых для атаки. Пусть получено j сообщений $y_0, y_1, ..., y_{j-1}$ и им соответствующие измерения времени $T_0, T_1, ..., T_{j-1}$. Вероятность того, что предположение x_b для первых b бит правильно, пропорциональна $P(x_b) \propto \prod_{i=0}^{j-1} F(T_i - t(y_i, x_b))$, где $t(y_i, x_b)$ – время, требуемое для первых b итераций цикла вычисления произведения точки на число (основная операция при формировании цифровой подписи [5]) с использованием бит x_b, F – ожидаемая функция распределения вероятности $T - t(y, x_b)$ по всем значениям y и правильному x_b. Т.к. F определена как распределение вероятности $T_i - t(y_i, x_b)$, если x_b правильно, то это – лучшая функция для предсказания $T_i - t(y_i, x_b)$. Измерения времени и промежуточные значения s могут использоваться для улучшения оценки F.

При правильном предположении для x_{b-1} имеются два возможных значения для x_b. Вероятность того, что x_b - является правильным, а x_b' - неправильным, может быть найдена следующим образом:

$$\frac{\prod_{i=0}^{j-1} F(T_i - t(y_i, x_b))}{\prod_{i=0}^{j-1} F(T_i - t(y_i, x_b)) + \prod_{i=0}^{j-1} F(T_i - t(y_i, x_b'))}. \qquad (1).$$

На практике эта формула не очень полезна, т.к. поиск F потребует слишком больших усилий. Однако возможно упростить временную атаку уходом от вычисления F. Каждое наблюдение времени состоит из $T = e + \sum_{i=0}^{w-1} t_i$, где t_i - время требуемое для сложения бита i, а e включает ошибку измерения, время на инкремент цикла и т.п. Имея предположение x_b, нападающий может вычислить $\sum_{i=0}^{b-1} t_i$ для каждого значения y. Если x_b правильно, то, вычитая это время из T, получим $e + \sum_{i=0}^{w-1} t_i - \sum_{i=0}^{b-1} t_i = e + \sum_{i=b}^{w-1} t_i$. Т.к. время модульного сложения не зависит друг от друга и от ошибки измерения, то дисперсия $e + \sum_{i=b}^{w-1} t_i$ по всем наблюдаемым значениям, будет равна $D(e) + (w-b)D(t)$. Однако, если только первые $c < b$ бит угаданы правильно, ожидаемая дисперсия будет $D(e) + (w - b + 2c)D(t)$. Итерации с правильными предположениями уменьшают ожидаемую дисперсию на $D(t)$, каждая итерация после неправильного предположения увеличивает дисперсию на $D(t)$. Вычислять дисперсии легко, и это обеспечивает хороший способ идентификации правильного бита.

Теперь возможно оценить число значений, требуемых для атаки. Предположим, что нападавший имеет j точных времен измерения и два предположения относительно

первых b бит w-битного значения, одно правильное и другое - неправильное с первой ошибкой в бите c. Для каждого предположения время измерения может быть сверено с $\sum_{i=0}^{b-1} t_i$. Если такая сверка имеет меньшую дисперсию, то это - правильное предположение.

Возможно аппроксимировать t_i с использованием независимых стандартных нормальных переменных. Если $D(e)$ незначительно, ожидаемая вероятность правильности предположения равна:

$$P\left(\sum_{i=0}^{j-1}\left(\sqrt{w-b}X_i+\sqrt{2(b-c)}Y_i\right)^2 > \sum_{i=0}^{j-1}\left(\sqrt{w-b}X_i\right)^2\right) = \\ = P\left(2\sqrt{2(b-c)(w-b)}\sum_{i=0}^{j-1}X_iY_i + 2(b-c)\sum_{i=0}^{j-1}Y_i^2 > 0\right), \quad (2),$$

где X и Y - нормальные случайные переменные с законом (0, 1). Т.к. j – относительно большое, $\sum_{i=0}^{j-1} Y_i^2 \approx j$ и $\sum_{i=0}^{j-1} X_iY_i$ приблизительно нормальны с законом $(0,\sqrt{j})$.

Отсюда:

$$P\left(2\sqrt{2(b-c)(w-b)}(\sqrt{j}Z)+2(b-c)j>0\right)=P\left(Z>\frac{\sqrt{j(b-c)}}{\sqrt{2(w-c)}}\right) \quad (3),$$

где Z - стандартная нормальная случайной переменной. Интегрирование для нахождения вероятности правильного предположения дает $\Phi\left(\frac{\sqrt{j(b-c)}}{\sqrt{2(w-c)}}\right)$, где $\Phi(x)$ – область под стандартной нормальной кривой от $-\infty$ до x. Требуемое число значений j, таким образом, пропорционально длине экспоненты w. Число измерений может быть уменьшено, если нападающий может выбирать такие входные данные, чтобы иметь экстремумы времени в тех битах экспоненты, которые его интересуют.

Большинство вариаций времени в модульном умножении обычно вызывает сокращение модульных операций. Умножение реализуемое алгоритмом Монтгомери устраняет необходимость сокращения $\bmod p$ и, в результате, имеет тенденцию уменьшать значимость временных характеристик. Однако некоторые вариации все же остаются. Если оставшийся "сигнал" не затмевается ошибками измерения, дисперсия в t_b и дисперсия $\sum_{i=b+1}^{w-1} t_i$ будут сокращены пропорционально и атака сработает. Однако, если ошибка измерения e большая, то требуемое число значений увеличится пропорционально $\frac{1}{D(t_i)}$.

Китайская теорема об остатках часто используется, чтобы оптимизировать операции при нахождении порядка эллиптической кривой. Эти шаги могут быть уязвимыми для временных атак. В некоторых случаях возможно улучшить атаку на цифровую подпись основанную на преобразованиях в группе точек эллиптической кривой с китайской теоремой об остатках, если использовать известный (не выбранный) шифрованный текст, сокращая число требуемых сообщений. Сокращение модульных операций выполняется вычитанием нескольких модулей сразу, и вариации

времени, которые можно использовать, возникают за счет разного количества шагов "сравнения-вычитания". Временной анализ может быть использован для определения старших цифр p. Например, полный перебор по всем возможным значениям для старших двух цифр p (или более эффективные методы) может установить значение, для которого наблюдаемое время коррелирует наиболее близко с ожидаемым количеством действий вычитания. Как только одна цифра p будет найдена, измерения времени могут многократно использоваться, чтобы найти последующие цифры. Еще не известно, может ли быть приспособлен временной анализ, чтобы непосредственно нападать на умножение точки на число по модулю p и q, выполняемых с помощью китайской теоремы об остатках.

Предложенный в работе метод скрытия времени выполнения операций, позволяет эффективно противостоять временной атаке. Однако, даже используя скрытие, распределение будет отражать среднее время операции, что можно использовать, для нахождения хеммингского веса экспоненты. Если важна анонимность, то экспонента может быть умножена на случайную последовательность $\varphi(n)$ перед каждым умножением точки на число. При этом необходимо убедиться, что процесс умножения не имеет временных характеристик, которые могут раскрыть $\varphi(n)$. Такой метод может быть полезен и в предотвращении криптоатак, которые используют утечку информации в процессе умножения точки на число из-за электромагнитных излучений, колебаний в производительности системы, изменений в потреблении энергии и т.д., вплоть до изменения бит экспоненты в каждой операции.

Список литературы

1. M. Wiener, R. Zuccherato “Faster attacks on elliptic curve cryptosystem”, Selected Areas in Cryptography // Lecture Notes in Computer Science, 1556 (1999), Springer-Verlag 252-266.
2. Joye M., and Quisquater J.-J. Hessian elliptic curves and side-channel attacks. In Cryptographic Hardware and Embedded Systems // CHES 2001 [Pre-]Proceedings (2001), C. K. Koc, D. Naccache, and C. Paar, Eds., pp. 412–420.
3. Kocher, P. C. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems // Advances in Cryptology – CRYPTO '96 (1996), N. Koblitz, Ed., vol. 1109 of Lecture Notes in Computer Science, pp. 104-113.
4. Kocher P. C., Jaffe J., and Jun B. Differential power analysis // Advances in Cryptology – CRYPTO '99 (1999), M. Wiener, Ed., vol. 1666 of Lecture Notes in Computer Science, pp. 388-397.
5. Смирнов А.А. Метод противодействия атаке на реализацию цифровой подписи // Збірник наукових праць інституту проблем моделювання в енергетиці ім. Г.Є. Пухова, вип 22, Київ: НАНУ, 2003, С. 188-192.

Запропоновано метод забезпечення захисту інформації в АСУ протидією атаці на основі виміру часу виконання операцій при формування цифрового підпису в групі точок еліптичних кривих

The method defense of information counteraction is offered cryptographic attack, on the basis gauging time of performance operations, at formation digital signature in group points of elliptic curves