N. A. Chepik, M. A. Ivanov

Kleptographic Attacks on ECDSA

Keywords: ECCS, kleptography, SETUP Attack

This paper presents secretly trapdoor with universal protection (SETUP) attacks on the elliptic curve digital signature algorithm ECDSA. It allows a malicious manufacturer of black-box cryptosystems to implement these attacks to get access to user's private key. The attacker can obtain user's private key. The way ECDSA can be used for encryption and key exchange is also described.

Н. А. Чепик, М. А. Иванов

АТАКИ НА СХЕМУ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Введение

Эллиптическая криптография – раздел криптографии, который изучает криптосистемы с открытым ключом, основанные на свойствах эллиптических кривых над конечными полями – ECCS. Стойкость ECCS основана на вычислительной неразрешимости задачи дискретного логарифмирования.

Эллиптические кривые

Кривые, использующиеся для шифрования, могут быть определены как в простом конечном поле, так и в расширенном поле с характеристикой 2. Эллиптические кривые над конечными простыми полями определяются уравнением:

$E: y^2 = x^3 + ax + b \bmod \rho$,

где $a, b \in \mathbf{F}(\rho)$ – коэффициенты эллиптической кривой и $4a^3 + 27b^2 \neq 0 \bmod \rho$.

Эллиптические кривые E над конечным полем задаются множеством точек на плоскости. Над точками из $E(\mathbf{F}(\rho))$ определены операции сложения, скалярного умножения и отрицания.

Проблема дискретного логарифмирования на эллиптической кривой (ECDLP)

Возьмем точку P порядка n на эллиптической кривой E над конечным полем $\mathbf{F}(\rho)$ и точку Q на E. ECDLP заключается в том, чтобы найти целое число k, где $0 \leq k \leq n - 1$ и $Q = kP$, если такое число вообще существует.

Вычислительная проблема Диффи – Хеллмана на эллиптической кривой (ECDHP)

Возьмем точку P порядка n на эллиптической кривой E над конечным полем $\mathrm{F}(\rho)$ и две точки kP и lP, где $0 \leq k, l \leq n - 1$. ECDHP заключается в том, чтобы найти точку $k \times lP$.

Схема электронной цифровой подписи на эллиптических кривых (ECDSA)

Пусть m – это сообщение, которое необходимо подписать. Параметры схемы:

- эллиптическая кривая E над конечным полем $\mathrm{F}(\rho)$;
- базовая точка G порядка n;
- секретный ключ d;
- открытый ключ $Q = dG$;
- $h(x)$ – безопасная хеш-функция.

Алгоритм формирования подписи

Входные данные: сообщение m.

Выходные данные: подпись (r, s).

Выберем случайное число $1 \leq k \leq n - 1$, вычисляем

$R = kG = (x_1, y_1)$, $r = x_1 \bmod n$, $s = k^{-1}(h(m) + d \times r) \bmod n$.

Если $s = 0$ или $r = 0$, то (r, s) не принимается для данного сообщения m и вычисления надо повторить заново. В другом случае (r, s) является подписью сообщения.

Алгоритм проверки подписи

Входные данные: подпись (r, s), сообщение m.

Выходные данные: результат проверки подписи (r, s) сообщения m.

Вычисляем $R' = s^{-1}(h(m)G + rQ) = (x_1', y_1')$.

Если $r = x_1' \bmod n$, то подпись (r, s) принимается, в противном случае – отвергается.

Скрытые каналы передачи информации

Это понятие было предложено Симмонсом [3]. Он продемонстрировал, как злоумышленник может узнать секретную информацию, в то время как ее владелец даже не будет подозревать, что происходит утечка информации. Владелец имеет возможность читать все сообщения, но не может прочитать тайное послание, встроенное в сообщение. Симмонс развил эту технику на различные криптоалгоритмы и криптопротоколы.

Клептография

Клептография – это использование криптографии против криптографии с целью получения секретной информации [4, 5]. Клептографические системы содержат безопасные и скрытые каналы утечки информации. Клептографическая атака на задачу нахождения дискретного логарифма была описана Янгом и Юнгом в работе [5]. Они ввели понятие секретной встроенной лазейки с универсальной защитой (SETUP), которая видоизменяет криптографический алгоритм таким образом, чтобы атакующий мог получить секретную информацию пользователя. Лазейка обеспечивает существование скрытого канала передачи информации. Некоторые свойства SETUP описаны ниже.

Существует C – криптосистема с объявленной спецификацией, SETUP-механизм – это такая модификация криптоалгоритма C в алгоритм C_1, что:

- параметры входа C_1 согласуются с входными параметрами C;
- параметры выхода C_1 соответствуют параметрам выхода C, но при этом выход C_1 содержит секретные биты, которые легко извлекаются разработчиком;
- по выходам алгоритмы C_1 и C полиномиально неразличимы для всех, кроме разработчика;
- выход C_1 эффективно вычисляется с использованием встроенной в C_1 функции шифрования E;
- секретная функция расшифрования D, обратная к E, не содержится в C_1 и известна только разработчику;
- после обнаружения в реализации алгоритма SETUP-механизма ни пользователи, ни злоумышленники (иначе говоря, никто за исключением разработчика) не могут определить использованные секретные ключи пользователя.

SETUP-атака на ECDSA

Пусть v – закрытый ключ атакующего и $V = vG$ – его открытый ключ. Хеширование точки эллиптической кривой определим как хеширование ее x-координаты. Устройство работает следующим образом.

Алгоритм формирования цифровой подписи с SETUP

Входные данные: сообщение m.

Выходные данные: подпись (r, s).

1) Выбираем целое число $1 \le k_1 \le n - 1$.

Вычисляем

$R_1 = k_1G = (x_1, y_1)$; $r_1 = x_1 \bmod n$; $s_1 = k_1^{-1}(h(m_1) + d \times r_1) \bmod n$.

Сохраняем k_1 в энергонезависимой памяти.

2) Вычисляем

$Z = a \times k_1 G + b.k_1 V + h \times jG + e \times uV$,

где $a, b, h, e < n$ – фиксированные целые числа; $j, u \in \{0, 1\}$ — случайные.

Вычисляем

$k_2 = h(Z)$; $R_2 = k_2 G = (x_2, y_2)$; $r_2 = x_2 \bmod n$; $s_2 = k_2^{-1}(h(m_2) + d \times r_2) \bmod n$.

Сохраняем k_2 в энергонезависимой памяти.

Каждый может проверить подпись в любое время с помощью открытого ключа Q. Злоумышленник может получить d и сообщение с помощью (r_1, s_1) и (r_2, s_2).

Алгоритм расшифрования SETUP

Входные данные: (r_1, s_1), (r_2, s_2), m_2.

Выходные данные: секретный ключ d.

Если предположить, что полученные подписи действительны, используем уравнение кривой E над конечным полем $F(p)$ для расчета возможных точек R_1' на кривой, чьи координаты x удовлетворяют соотношению $x \bmod n = r_1$. Существуют две такие точки. Для каждой возможной точки R_1' выполняем следующие действия:

{

$Z_1 = aR_1' + b \times vR_1' = a \times k_1' G + b \times v \times k_1' G = a \times k_1' G + b \times k_1' V$

Для каждого возможного значения j, u вычисляем:

{

$Z_2 = Z_1 + h \times jG + e \times uV$

$k_2' = h(Z_2)$

$R_2' = k_2' G = (x_2', y_2')$

$r_2' = x_2' \bmod n$

Если $r_2' = r_2$, тогда $k_2' = k_2$, и выходим из цикла

}

}

$d = (s_2 k_2 - h(m_2)) \times r_2^{-1} \bmod n$

Таким образом вычисляется секретный ключ d, что позволяет атакующему подделывать подписи и расшифровывать сообщения.

Безопасность

SETUP-атака безопасна в том смысле, что пользователь, не зная случайного числа k_1, не может рассчитать секретный ключ k_2 (проблема ECDHP). Кроме того, противник, не знающий закрытого ключа атакующего, не может рассчитать Z и, следовательно, не может рассчитать k_2. Поэтому SETUP-атаки обладают универсальным свойством защиты. Однако ее можно назвать неустойчивой, потому что пользователь, который знает собственный секретный ключ, может восстановить выбранное k и обнаружить SETUP. Случайные значения j и u используются в качестве меры предосторожности, если случайный параметр k доступен для пользователя. Благодаря этим параметрам пользователь не сможет обнаружить SETUP в устройстве даже после многократного использования.

Использование ECDSA для шифрования и обмена ключами

Янг и Юнг описали использование DSA для шифрования и обмена ключами [6].

Опишем эту возможность для ECDSA. Пусть d_A и Q_A — закрытый и открытый ключи пользователя A, соответственно d_B и Q_B — закрытый и открытый ключи пользователя B.

Пользователь A шифрует секретное сообщение m, чтобы только пользователь B мог его получить:

выбирает случайное число $k \le n - 1$;

вычисляет

$Z = kQ_B = (x_z, y_z)$; $m_2 = E_{xz}(m_1)$, где $E_{xz}(m_1)$ — результат зашифрования сообщения m_1 на ключе x_z; $R = kG = (x_1, y_1)$; $r = x_1 \bmod n$; $s = k^{-1}(h(m_2) + d_A \times r) \bmod n$;

формирует (r, s).

Когда пользователь B получит m_2 и подпись (r, s), он проверит подпись с помощью открытого ключа A, чтобы убедиться, что это сообщение действительно от A, а затем может извлечь m_1 следующим образом:

$R' = s^{-1}(h(m_2)G + rQ_A) = (x_1', y_1')$;

если $r = x_1' \bmod n$, то подпись (r, s) принимается, в другом случае отвергается.

$Z' = d_B R' = (x_z', y_z')$; $x_z' = x_z$; $m_1 = D_{xz}(m_2)$,

где $D_{xz}(m_2)$ — результат расшифрования m_2 на ключе x_z (D_{xz} — функция, обратная E_{xz}).

Выводы

Продемонстрирована возможность клептографической атаки на схему электронной цифровой подписи на эллиптических кривых, в результате которой вычисляется секретный ключ d, что позволяет атакующему подделывать подписи и расшифровывать сообщения.

СПИСОК ЛИТЕРАТУРЫ:

1. *Cohen H., Frey G., Avanzi R., Doche C., Lange T., Nguyen K., and Vercauteren F.* Handbook of Elliptic and Hyperelliptic Curve Cryptography. Chapman & Hall/CRC. 2000.
2. *Hankerson D., Menezes A., Vanstone S.* Guide to Elliptic Curve Cryptography. Springer-Verlag, 2004.
3. *Simmons G. J.* The Prisoner's Problem and the Sublimianal Channel, Advances in Cryptology: Proceedings of CRYPTO '83, Plenum Press, 1984. P. 364–378.
4. *Young A., Yung M.* Kleptography: Using Cryptography against Cryptography, Advances in Cryptology — EUROCRYPT '97 Proceedings, Springer-Verlag, 1997. P. 62–74.
5. *Young A., Yung M.* The Prevalence of Kleptographic Attacks on Discrete-Log Based Cryptosystems, Advances in Cryptology — CRYPTO '97 Proceedings, Springer-Verlag, 1997. P. 264–276.
6. *Young A., Yung M.* Malicious Cryptography: Exposing Cryptovirology. Wiley Publishing. 2004.

REFERENCES:

1. *Cohen H., Frey G., Avanzi R., Doche C., Lange T., Nguyen K., and Vercauteren F.* Handbook of Elliptic and Hyperelliptic Curve Cryptography. Chapman & Hall/CRC. 2000.
2. *Hankerson D., Menezes A., Vanstone S.* Guide to Elliptic Curve Cryptography. Springer-Verlag, 2004.
3. *Simmons G. J.* The Prisoner's Problem and the Sublimianal Channel, Advances in Cryptology: Proceedings of CRYPTO '83, Plenum Press, 1984. P. 364–378.
4. *Young A., Yung M.* Kleptography: Using Cryptography against Cryptography, Advances in Cryptology — EUROCRYPT '97 Proceedings, Springer-Verlag, 1997. P. 62–74.
5. *Young A., Yung M.* The Prevalence of Kleptographic Attacks on Discrete-Log Based Cryptosystems, Advances in Cryptology — CRYPTO '97 Proceedings, Springer-Verlag, 1997. P. 264–276.
6. *Young A., Yung M.* Malicious Cryptography: Exposing Cryptovirology. Wiley Publishing. 2004.