КРИПТО ПРО

ПРОТИВОДЕЙСТВИЕ АТАКАМ НА ПРОТОКОЛ TLS

Гилязов Руслан Раджабович
Леонтьев Сергей Ефимович
Смышляев Станислав Витальевич

Содержание

- Описание проблематики
- Метод Барда
- Метод Воденея
- Результаты Кравчика
- Изменения в новых версиях TLS
- Предлагаемый метод
- Обход уязвимостей

Описание проблематики

- Сентябрь 2011 года, конференция Ekoparty в Аргентине: работа Дуонга и Риззо, посвященная практической реализации атаки Барда на SSL/TLS.
- 2004 год: работа Барда о теоретической уязвимости SSL/TLS к атакам с выбором открытого текста.
- 2002 год: заметка Дэя о теоретической уязвимости некоторого класса протоколов при использовании режима CBC блоковых шифров.
- 2002 год, Eurocrypt: работа Воденея о теоретической уязвимости SSL/TLS к атакам с выбором шифртекста.
- 2001 год, CRYPTO: работа Кравчика о методологии использования алгоритмов шифрования и обеспечения аутентификации в протоколах.

Метод Барда

Модель нарушителя:

•Угроза: IND, различение гипотез о равенстве либо неравенстве фиксированному блоку M* некоторого блока M_i открытого текста $M=(M_1|M_2|\ldots|M_m)$, соответствующего известному для нарушителя шифртексту $C=(C_1|C_2|\ldots|C_m)$, полученному в режиме CBC работы некоторого блокового шифра.

•Атака: CPA, с выбором открытого текста при заранее известном IV.

Метод Барда

Метод:

•Отправителю навязывается зашифрование некоторого сообщения, начальный блок которого равен $M'=C_{i-1}\oplus IV\oplus M^*$.

•Первый блок шифртекста равен

$$C'=E_K(M\oplus IV) = E_K(C_{i-1}\oplus IV\oplus M^*\oplus IV) = E_K(C_{i-1}\oplus M^*).$$

•Гипотеза о равенстве M_i и M^* верна тогда и только тогда, когда блок шифртекста C' в точности равен C_i.

Метод Воденея

Модель нарушителя:

•Угроза: нахождение части блока M_i открытого текста $M=(M_1|M_2|\ldots|M_m)$, соответствующего известному для нарушителя шифртексту $C=(C_1|C_2|\ldots|C_m)$, полученному в режиме CBC работы некоторого блокового шифра.

•Атака: CCA*, с наличием доступа к оракулу, вычисляющему предикат о корректности паддинга открытого текста, соответствующего поданному на вход шифртексту.

Метод Воденея

Построение оракула:

Требуется различать следующие события:

1.Вычисление имитовставки производится (TRUE).
2.Вычисления имитовставки после расшифрования не производится (FALSE).

Различать данные события возможно
•По коду ошибки
•По времени обработки

Метод Воденея

Метод:

•Случайным образом выбирается порядка 2^8 блоков T_{i-1}^j, j=1,2,...

•Для каждого из T_{i-1}^j, j=1,2,... на вход оракулу подается строка $(C_0|C_1|...|C_{i-2}|T_{i-1}^j|C_i)$. Если при некотором j для T_{i-1}^j оракул возвращает TRUE, C^*_{i-1} полагается равным T_{i-1}^j.

•С использованием информации о том, что в блоке $P_i = C^*_{i-1} \oplus D_K(C_i)$ содержится корректный PKCS#5 паддинг, находится длина паддинга: перебираются сообщения

$C^*_{i-1}(1)=C^*_{i-1} \oplus (00|00|...|00|01)$,
$C^*_{i-1}(2)=C^*_{i-1} \oplus (00|...|00|01|00)$,
...
$C^*_{i-1}(b)=C^*_{i-1} \oplus (01|00|...|00|00)$,
затем на вход оракулу O_K подаются строки
$(C_0|C_1|...|C_{i-2}|C(j)|C_i)$, j=b,b-1,..., 1.

Метод Воденея

Метод:

•В случае, если ответ FALSE впервые появится от оракула при j=j*, становится известно, что в сообщении, получаемом расшифрованием на ключе K из шифртекста ($C_0|C_1|...|C_{i-2}|T^*_{i-1}|C_i$), в конце находится j* байтов со значением j*.

•Для нахождения последних j* байтов M_i вычисляется значение выражения $T^*_{i-1} \oplus C_{i-1} \oplus (00|00|...|j^*|j^*|...|j^*)$ (j* ненулевых байтов) и берутся его последние j* байтов.

Результаты Кравчика

- В случае использования просто устроенного паддинга методам криптоанализа, аналогичным методу Воденея, подвержен не только режим CBC работы блоковых шифров, но и все режимы, при которых расшифрование каждого блока производится с помощью наложения гаммы: CFB, OFB, CNT.
- Использование паддинга, вносящего существенную дополнительную энтропию, в некоторых случаях также не является препятствием для построения аналогичных атак (см. работу Климы и Роши, 2003 г.).
- CRYPTO 2001, Хьюго Кравчик: результаты об отсутствии, в общем случае, IND-CCA стойкости криптосистем с секретным ключом, работающих по принципу «аутентификация, затем шифрование» (и всяких криптосистем с секретным ключом, в которых шифрованию предшествует дополнение ОТ отрезком текста с малой энтропией), даже в случае IND-CPA стойкости используемой непосредственно для шифрования криптосистемы.

Изменения в новых версиях TLS

Для ликвидации уязвимости к аналогичным атаке Воденея атакам принят ряд контрмер, связанных с порядком вычисления имитовставки при неправильном паддинге.

•В пункте 6.2.3.2 RFC 5246 (описание протокола TLS версии 1.2) присутствует следующий аспект: указано, что лучшим методом защиты от временных атак, аналогичных атаке Воденея, является вычисление значения имитовставки даже в случае некорректного паддинга, например, вычисление значения имитовставки по всему полученному после расшифрования фрагменту, полагая отсутствие паддинга.

•При ошибке расшифрования (некорректный паддинг/имитовставка) соединение разрывается, производится смена ключа.

Изменения в новых версиях TLS

- Предлагаемые меры оставляют временной канал утечки информации, связанный с наличием разницы по времени вычисления имитовставки в случае сообщения с корректным паддингом и модифицированного сообщения с некорректным паддингом.

- В пункте 6.2.3.2 указано, что паддинг может иметь любую длину, не превосходящую 255 байт, обеспечивающую должное выравнивание..

Изменения в новых версиях TLS

- Таким образом, при размере блока алгоритма выработки имитовставки в 16 байт сообщение длиной, например, 16 байт, дополненное 240 байтами вида 0xF0, будет считаться дополненным корректным паддингом и при проверке корректности сообщения будет вычисляться имитовставка на 1 блок.

- В случае контролируемой модификации конечных блоков данного открытого текста паддинг будет приниматься как некорректный и имитовставка будет вычисляться на 16 блоков, обеспечивая, таким образом, существенную разницу во времени вычисления, создающую потенциальный канал утечки информации.

Предлагаемый метод

Идея метода

Модель нарушителя (для идейного описания):

•Угроза: нахождение последнего байта блока M_i открытого текста $M=(M_1|M_2|\ldots|M_m)$, соответствующего известному для нарушителя шифртексту $C=(C_1|C_2|\ldots|C_m)$, полученному в режиме CBC работы некоторого блокового шифра.

•Атака: CTA*, с выбором открытого текста и IV и наличием доступа к оракулу, вычисляющему предикат о корректности паддинга открытого текста, соответствующего поданному на вход шифртексту.

Предлагаемый метод

Построение оракула:

Требуется различать следующие события:

1. Вычисляется имитовставка сообщения длины ≤2b байтов.
2. Вычисляется имитовставка сообщения длины 256 байтов.

Предлагаемый метод

Метод (идейно):

•Положить s=256-b+1, навязать зашифрование отправителем сообщения (s|s|…|s) длины 256-b на используемом ключе <u>при IV, равном C_i</u>, положить Q равным полученному шифртексту.

•Перебором (порядка 256 попыток) установить значение блока C'_0 такое, что оракул на входе $(C'_0|C_i|Q)$ выдаст TRUE.

•Вычислить последний байт блока M_i, полагая его равным последнему байту $C'_0 \oplus C_{i-1} \oplus (\ldots|s)$.

Предлагаемый метод

Модель нарушителя:

•Угроза: нахождение блока M_i открытого текста $M=(M_1|M_2|\ldots|M_m)$.

•Атака: CTA’, с возможностью зашифрования модифицированного справа от блока M_i текста M на текущем ключе и наличием доступа к оракулу, вычисляющему предикат о корректности паддинга открытого текста, соответствующего поданному на вход шифртексту.

Предлагаемый метод

Метод:

•Для каждого t=1,2,…,b:

- Положить для всякого t, t=1,2,…,b, s_t=256-2b+t.
- Перед шагом попытки нахождения байта b-(t-1) навязать зашифрование отправителем на текущем ключе любого сообщения вида (…|M_i) | (s_t | s_t |…| s_t), где длина второй части равна 256-2b байтов.
- Положить ($w^t_{b-(t-2)}|w^t_{b-(t-1)}|\ldots|w^t_b$) | C_t | Q_t равным полученному шифртексту, где Q_t имеет длину 256-2b байтов, C_t – длину b байтов, w – отдельные байты.

Предлагаемый метод

Метод:

•Для каждого t=1,2,…,b:

- Положить для всякого j=b-(t-2), b-(t-1),…,b байт блока C'_t с номером j равным $r^t_j \oplus w^t_j \oplus w^{t-1}_j \oplus s_t \oplus s_{t-1}$.
- Установить (с вероятностью 1/256) значение (b-(t-1))-го байта блока C'_t, такое, что оракул на входе $(C'_t|C_t|Q_t)$ выдаст TRUE.
- Положить $(r^{t+1}_{b-(t-1)}, r^{t+1}_{b-(t-2)},\ldots, r^{t+1}_b)$ равными последним t байтам блока C'_t.

• Вычислить блок M_i, полагая его равным

$$C'_b \oplus (w^b_1|\, w^b_2|\ldots|w^b_b) \oplus (s_b|\, s_b|\ldots|s_b).$$

Обход уязвимостей

Вышеописанные типы атак используют следующие три проблемных аспекта:

•Потенциальная возможность бесключевого чтения при повторном/навязанном использовании синхропосылки.
•Уязвимость к навязыванию шифртекста.
•Непродуманное использование алгоритмов проверки паддинга и алгоритмов проверки имитовставки.

Обход уязвимостей

Аутентификация сообщений вместе с паддингом. Каждое принимаемое сообщение обязано проходить проверку аутентичности с использованием режима выработки имитовставки блокового шифра ГОСТ 28147-89, что делает невозможным навязывание сообщений. Сквозная имита вместе с защитой имитой номера пакета и заголовка позволяет предотвратить перестановку пакетов.

Выработка имитовставки на сообщение вместе с паддингом позволит предотвратить атаки, связанные с различием в реакции на навязанное сообщение. Заметим, что в стандарте SSL v2 аутентификация сообщений производится вместе с паддингом. Это позже было изменено, что привело к появлению описанных выше атак.

Отказ от использования паддинга. Использование режима CNT работы блокового шифра, не требующего использования паддинга делает невозможными любые атаки, использующие вносимую алгоритмами паддинга избыточность.

Обход уязвимостей

Случайный выбор синхропосылки. Обработка каждого пакета должна предваряться отдельным запуском генератора случайных чисел для порождения новой, никак не зависящей от предыдущих данных в канале, синхропосылки. Благодаря этому невозможны любые атаки, использующие уязвимости, связанные с повторным использованием синхропосылок либо с использованием в качестве синхропосылок ранее присутствовавших в канале блоков шифртекста.

Таким образом, для ликвидации уязвимости ко всем описанным типам атак на TLS предлагается использовать следующие сюиты: TLS_GOSTR341094_WITH_28147_CNT_IMIT, TLS_GOSTR341001_WITH_28147_CNT_IMIT.

КРИПТО ПРО

СПАСИБО ЗА ВНИМАНИЕ!

КРИПТО-ПРО – ключевое слово в защите информации

http://www.cryptopro.ru
lse@cryptopro.ru
svs@cryptopro.ru
rubin@cryptopro.ru

Тел./факс:
+7 (495) 780-48-20
+7 (495) 660-23-30