ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 24 МАТЕМАТИКИ Выпуск 5
2017

Д. С. Бирюков, А. А. Елистратов, Н. В. Никонов, А. А. Самойлов, В. В. Ларионов (Москва, ФУМО ВО ИБ). **О возможных модификациях временных паддинг-атак на протоколы семейства TLS.**

Протоколы семейства TLS (от англ. Transport Layer Security) являются основными криптопротоколами для осуществления безопасной передачи данных при обращении к веб-ресурсам. При установлении TLS-сессии стороны проходят аутентификацию и вырабатывают необходимые ключи для обеспечения конфиденциальности и целостности передаваемых данных прикладного уровня. Шифрование данных может происходить с использованием блочной шифрсистемы в режиме CBC. При этом сначала от открытых данных формируется MAC-код, происходит добавление паддинга в соответствии с PKCS#5 для выравнивания границ последнего неполного блока, а затем происходит зашифрование данных вместе с MAC-кодом и паддингом.

В работе [1] теоретически показано, что такая последовательность преобразований не является безопасной. В подтверждение этого факта в [2] была предложена общая идея всех паддинг-атак с выбранными шифрованными текстами вида $y_{j-1} \oplus r \| y_j$ (знак $\|$ разделяет блоки, r — случайный блок) для нахождения байтов открытого блока x_j, а в [3, 4] описаны различные ее реализации.

Атаки [3, 4] относятся к классу временных паддинг-атак, в которых по существу используется разница во времени ΔT формирования и передачи ошибки bad_record_mac от сервера при проверке MAC-кода при корректном и некорректном паддинге. Атака Lucky13 ([4]) может быть реализована и в случае неприменимости атаки [3], то есть когда используется защита (см. RFC 5246), при которой MAC-код вычисляется и при некорректном паддинге. Для ее более эффективной реализации предлагается использовать сценарий Beast-атаки ([5]), позволяющий через внедренный на стороне клиента javascript располагать разными способами неизвестные куки-данные клиента в блоках перед их зашифрованием. В любом случае величина будет небольшой и определяться отношением τ числа применений сжимающей функции при подсчете MAC-кода: при использовании криптонабора AES-CBC-SHA1 $\tau = 4/5$.

В предположении возможности проведения сценария Beast-атаки в [6] была предложена модификация временной паддинг-атаки в направлении увеличения разницы ΔT за счет использования длинного паддинга и при том же криптонаборе $\tau = 4/8$.

В 2015 году соавторами данной работы был предложен способ дальнейшего увеличения величины ΔT за счет использования паддинга максимальной длины в 256 байтов и такого расположения неизвестных байтов куки-данных $\dots x_{-1}, x_0, \dots, x_b$ в блоках длины b байтов перед шифрованием:

$$\|x_0, \dots, x_{b-1}\| x_b, 255, \dots, 255 \| \mathrm{Pad}_1,$$

Pad_1 — 15 блоков со значением 255 в каждом байте, при котором в случае корректного паддинга MAC-код не может быть проверен из-за нехватки числа соответствующих байтов. В соответствии с RFC 5246 это должно приводить к ошибке decode_error без проверки MAC-кода, поэтому при том же криптонаборе можно считать, что $\tau = 0/8$.

Идея с нехваткой байтов для проверки MAC-кода при корректном паддинге была закреплена за Юраем Соморовски как CVE-2016-2107. Также им был предложен способ различения ошибок по их типам, а не по времени.

Авторы отмечают возможность отдельно выделить случай, когда MAC-код будет считаться от пустого фрагмента, передача которого может быть запрещена, что приведет к формировании различных типов ошибок и вместе с тем — увеличению ΔT. Например, в случае криптонабора AES-CBC-SHA1 можно использовать следующее расположение байтов куки-данных:

$$\|x_{-4}, \ldots, x_{b-5}\|x_{b-4}, \ldots x_b, 251, \ldots, 251\| \operatorname{Pad}_2,$$

Pad_2 — 15 блоков со значением 251 в каждом байте.

Основываясь на идее временной атаки [3] и сценария Beast-атаки [5] можно предложить новый вариант расположения неизвестных куки-данных в блоках для формирования ошибок различных типов и увеличения ΔT :
— при использовании AES-CBC-SHA1:

$$Z\|x_{-4}, \ldots, x_{b-5}\|x_{b-4}, \ldots, x_b, b-5, \ldots, b-5\|,$$

— в общем случае при $t = s \cdot b$, $s \geqslant 2$:

$$Z\|r_1\| \ldots \|r_{s-1}\|x_0, \ldots, x_{b-1}\|x_b, b-1, \ldots, b-1\|,$$

t — размер хеш-значения, Z — произвольный набор байтов максимально возможной длины (в соответствии с RFC 5246, 6066 — max_fragment_length+1024), $r_1, \ldots, r_{s-1}$ — произвольные блоки. В этом случае, при корректном паддинге MAC-код будет проверяться от большого числа блоков с формированием ошибки bad_record_mac, а при некорректном — должна возникать ошибка record_overflow.

Что касается использования режимов гаммирования, то идея паддинг-атак для них тоже верна (см. [7]), при этом в случае сценария Beast-атаки «паддингом» могут являться известные поля кросс-доменного запроса, которые должны проверяться на предмет их корректности перед проверкой MAC-кода.

СПИСОК ЛИТЕРАТУРЫ

1. *Krawczyk H.* The order of encryption and authentication for protecting communications (or: How secure is SSL?). In: Advances in Cryptology – CRYPTO 2001. 21st Annual International Cryptology Conference (Santa Barbara, CA, August 19–23, 2001). Proceedings. / Ed. by J. Kilian. Heidelberg etc.: Springer, 2001, p. 310–331. (Ser. Lecture Notes Comput. Sci. V. 2139.)
2. *Vaudenay S.* Security flaws induced by CBC padding — Applications to SSL, IPSEC, WTLS ... In: Advances in Cryptology – EUROCRYPT 2002. International Conference on the Theory and Applications of Cryptographic Techniques (Amsterdam, April 28–May 2, 2002). Proceedings./ Ed. by L. R. Knudsen. Heidelberg etc.: Springer, 2002, p. 547–545. (Ser. Lecture Notes Comput. Sci. V. 2332.)
3. *Canvel B.*, *Hiltgen A. P.*, *Vaudenay S.*, *Vuagnoux M.* Password Interception in a SSL/TLS Channel. In: Advances in Cryptology – CRYPTO 2003. 23rd Annual International Cryptology Conference (Santa Barbara, CA, August 17–21, 2003.) Proceedings./ Ed. by D. Boneh. Heidelberg etc.: Springer, 2002, p. 583–599. (Ser. Lecture Notes Comput. Sci. V. 2729.)
4. *Al Fardan N. J.*, *Paterson K. G.* Lucky Thirteen: Breaking the TLS and DTLS Record Protocols. In: 2013 IEEE Symposium on Security and Privacy SP 2013 (San Francisco, CA, 19–22 May, 2013). Proceedings./ Ed. by W. Lee et al. Los Alamitos, CA: IEEE Computer Soc., 2013, p. 526–540.

5. *Rizzo J.*, *Duong T.* Browser Exploit Against SSL/TLS. 2011. In: Ekoparty security conference – 2011 (Buenos Aires, September 21–23, 2011). http://packetstormsecurity.com/files/download/105499/Beast-SSL.rar/
6. *Леонтьев С. Е.*, *Попов В. О.*, *Смышляев С. В.* Противодействие атакам на протокол TLS. — Системы высокой доступности, 2012, т. 8, № 2, с. 109–115.
7. *Елистратов А. А.*, *Никонов Н. В.*, *Шумилов А. О.* О паддинг-атаках на криптографические протоколы, использующие стандартные n-разрядные блочные режимы шифрования. — Обозрение прикл. и промышл. матем., 2014, т. 21, в. 4, с. 358–360.