ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 27 МАТЕМАТИКИ Выпуск 2
2020

А. А. Елистратов, **Н. В. Никонов**, **В. В. Ларионов**, **З. В. Свистюр** (Москва, ТК 26, Лаб. ТВП)**. О возможности использования внутренних сообщений протокола TLS для проведения паддинг-атак.**

УДК 532.528.2, 532.694.1 DOI https://doi.org/10.52513/08698325_2020_27_2_143

Резюме: Предложена возможность использования внутренних сообщений протокола TLS для проведения паддинг-атак на защищаемые им сообщения прикладного уровня; в этих атаках вместо паддинга используются фиксированные и известные значения полей соответствующих внутренних сообщений.

Ключевые слова: паддинг-атака, TLS.

СПИСОК ЛИТЕРАТУРЫ

1. *Merget R.*, *Somorovsky J.*, *Aviram N.*, *Young C.*, *Fliegenschmidt J.*, *Schwenk J.*, *Shavitt Y.* Scalable scanning and automatic classification of TLS padding oracle vulnerabilities. In: Proceedings of the 28th USENIX Security Symposium. (Santa Clara, CA, August 14–16, 2019.) Berkeley, CA: USENIX Ass., 2019, p. 1029–1046.
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. 534–545. (Ser. Lect. Notes Comput. Sci. V. 2332.)
3. *Бирюков Д. С.*, *Елистратов А. А.*, *Ларионов В. В.*, *Никонов Н. В.*, *Самойлов А. А.* О возможных модификациях временных паддинг-атак на протоколы семейства TLS. — Обозрение прикл. и промышл. матем., 2017, т. 24, в. 5.// *Biryukov D. S.*, *Elistratov A. A.*, *Larionov V. V.*, *Nikonov N. V.*, *Samoilov A. A.* On possible modifications of timing padding attacks on TLS family of protocols. — OP&PM Surv. Appl. Industr. Math., 2017, т. 24, в. 5. (In Russian.)
4. *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.// *Elistratov A. A.*, *Nikonov N. V.*, *Shumilov A. O.* Padding attacks on cryptographic protocols using standard n-tuples block encryption schemes. — OP&PM Surv. Appl. Industr. Math., 2014, v. 21, is. 4, p. 358–360. (In Russian.)
5. *Rizzo J.*, *Duong T.* Here Come The $\oplus$ Ninjas. http://packetstormsecurity.com/files/105499/Browser-Exploit-Against-SSL-TLS.html, 2011.

UDC 532.528.2, 532.694.1 DOI https://doi.org/10.52513/08698325_2020_27_2_143

Elistratov A. A., ***Nikonov N. V.***, ***Larionov V. V.***, ***Svistyur Z. V.*** (Moscow, Technical Committee 26, TVP Laboratories)**. How internal TLS messages in padding attacks can be used**

Abstract: It is suggested to use internal TLS messages in padding-attacks against TLS-protected application layer messages; in these attacks some fixed and known values of internal messages' fields plays the role of padding bytes.

Keywords: padding attack, TLS.