ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 30 МАТЕМАТИКИ Выпуск 1
2023

А. А. Елистратов, **Н. В. Никонов** (Москва, Департамент информационной безопасности Банка России; Москва, Федеральное учебно-методическое объединение ВУЗов России по образованию в области информационной безопасности)**. О возможных сценариях атак на протоколы семейства SCP.**

УДК 000.00+000.00 DOI https://doi.org/10.52513/08698325_2023_30_1_1

Резюме: Доклад посвящен обзору возможных атак на криптопротоколы семейства SCP (Secure Channel Protocol), разработанных организацией GlobalPlatform. На основе идеи паддинг-атаки Воденея предлагаются новые сценарии атак, в которых роль дополнения играют предсказуемые значения полей защищаемых APDU-данных. Отмечается, что таким атакам могут быть подвержены протоколы SCP, использующие как режим шифрования CBC, так и режимы аутентифицированного шифрования AEAD.

Ключевые слова: Протоколы защиты канала SCP, организация Global Platform, паддинг-атака, APDU-данные, режим шифрования CBC, режим AEAD.

Протоколы семейства SCP (Secure Channel Protocol) разрабатываются международной организацией GlobalPlatform ([1]). Протоколы версий 0x, 1x являются основными протоколами защиты взаимодействия чиповой карты UICC (Universal Integrated Circuit Card) и внешней по отношению к ней стороны OCE (Off Card Entity). Взаимодействие между OCE и UICC основано на протоколе APDU (Application Protocol Data Unit) и заключается в передаче командных сообщений $C\text{-}APDU = HDR||BODY$ от OCE к UICC и получении от нее ответных сообщений $R\text{-}APDU = BODY||TRAILER$. Для защиты APDU-сообщений удаленного управления используются версии 8x, связанные с различными протоколами передачи данных по технологии Over The Air.

Протоколы семейства SCP позволяют обеспечивать аутентификацию сторон (на основе предварительно распределенных секретов PSK, инфраструктуре открытых ключей PKI на криптосистеме RSA или эллиптических кривых ECC), целостность (с помощью формирования имитовставки MAC) и конфиденциальность (с помощью шифрования ENC) сообщений обмена, но при этом используют различные конструкции защиты для одновременного обеспечения этих свойств (см. табл.).

Таблица

Версия протокола SCP	01	02	03	04-1	04-2	10	11	80	81-1	81-2
Год выхода первой спецификации	2000	2003	2009	2022	2022	2020	2015	2006	2010	2023
Год актуальной спецификации	2011	2018	2020	2023	2023	2020	2021	2022	2023	2023
Протокол передачи данных	APDU	APDU	APDU	APDU	APDU	APDU	APDU	SMS	TCP	TCP
Аутентификация, ключи	PSK	PSK	PSK	PSK	PSK	PKI (RSA)	PKI (ECC)	PSK	PSK	PSK
Конструкция защиты	E&M	E&M	EtM	EtM	AEAD	EtM	EtM	MtE	MtE	AEAD
Режим блочного шифрования	CBC	CBC	CBC	CBC	GCM	CBC	CBC	CBC	CBC	GCM
Дополнение (паддинг)	pad1	pad1	pad1	pad1	нет	pad1	pad1	любой	pad2	нет
Значение вектора инициализации	$\vec{0}$	$\vec{0}$	$IV(\vec{k})$	$IV(\vec{k})$	$IV(\vec{k})$	$\vec{0}$	$IV(\vec{k})$	$\vec{0}$	$\vec{0}$	$IV(\vec{k})$
Возможный сценарий атаки (номер)	1,3,5	1,3,5	-	-	6	1,2,3,4,5	-	1,5	1,3,5	6

Для защиты APDU-данных $BODY$ в SCP0x, 1x используются конструкции:

— E&M — соответствует $ENC(BODY), MAC([HDR]||BODY||[TRAILER])$;

— EtM — соответствует $ENC(BODY), MAC([HDR]||ENC(BODY)||[TRAILER])$,

поле $TRAILER$ присутствует для *R-APDU*, поле HDR — для *C-APDU*.

Для защиты всего $APDU$-сообщения в протоколах SCP8x используется конструкция MtE:

— $ENC(CNTRS||MAC(HDR_{SCP}||CNTRS||APDU)||APDU)$ для SCP80 ([2,3]);

— $ENC(APDU||MAC(HDR_{TLS}||APDU))$ для SCP81-1 на основе TLS_PSK ([4]).

Единственным поддерживаемым вариантом шифрования ENC всех рассматриваемых версий протоколов SCP является блочное шифрование в режиме CBC (протоколы SCP04-2, SCP81-2 поддерживают режим аутентифицированного шифрования GCM), при котором блоки шифрованных данных Y_i формируются из блоков открытых данных X_i по правилу: $Y_i = ENC(X_i \oplus Y_{i-1}),\ \ i = 1, \ldots, n,$ где вектор инициализации Y_0 либо нулевой $\vec{0}$, либо зависит от ключа $IV(\vec{k})$, а последний неполный блок X_n дополняется байтами дополнения, либо вида $pad1 =' 80', '00', \ldots, '00'$, либо вида $pad2 =' 0X', \ldots, '0X'$, где байт $'0X'$ повторяется $X + 1$ раз.

В работе [5] на основе идеи Дэя [6] описывается сценарий атаки с выбранными открытыми текстами (**атака 1**) на протокол SCP02, в котором по существу используется знание текущего значения Y_0 в режиме CBC, что делает уязвимым к этому сценарию атаки протокол SCP01, SCP10, а также протоколы, построенные по принципу MtE ([7]), к которым относятся SCP80 и SCP81-1.

В работе [8] на основе идеи Блейхенбахера [9] описывается сценарий атаки (**атака 2**) с выбранными шифрованными текстами на протокол SCP10, который использует криптосистему RSA с дополнением по стандарту PKCS#1 v1.5.

В работе [10] на основе идеи Воденея [11] описывается сценарий атаки (паддинг-атаки, **атака 3**) с выбранными шифрованными текстами вида $Y_{i-1} \oplus R \ ||\ Y_i$, $i \geqslant 1$ при перебираемом значении блока R и проверке корректности дополнения после расшифрования, что дает определение как минимум одного байта данных X_i: $DEC(Y_i) \oplus Y_{i-1} \oplus R = \ldots\ '80';\ X_i = \ldots '80' \oplus R$. Существенным для проведения паддинг-атаки является использование небезопасной конструкции защиты E&M (или MtE, [12]) и знание байтов дополнения. Сценарий излагается применительно к протоколу SCP02, однако нетрудно заметить, что SCP01 и SCP81-1 также уязвимы.

Протокол SCP10 использует безопасную конструкцию защиты EtM ([12]), но в отличие от протокола SCP03 (как и построенного на его основе SCP11), поддерживает вариант, при котором обеспечивается только конфиденциальность APDU-данных. В связи с этим по принципу wrap/decrypt-атаки ([13,14]) представляется возможным отбросить байты MAC с корректировкой полей заголовков (**атака 4**) для сведения конструкции защиты EtM к шифрованию данных, что делает ее уязвимой к атаке 3,

которая становится более эффективной за счет исключения проверки MAC.

Авторы настоящих тезисов на основе идеи, сформулированной в [15], предлагают новый сценарий возможной паддинг-атаки (**атака 5**), основанной на проверяемых при расшифровании предсказуемых полях данных, расположенных в блоке с номером j, $j \geqslant 2$ (так как Y_0 не передается), и передаче сообщений вида $Z||Y_{i-1} \oplus R \,||\, Y_i|| \ldots$, $i \geqslant 1$, где Z содержит $j-2$ случайных блоков. Такая возможность может возникнуть:

— при защите APDU-сообщений с использованием протоколов SCP8x, при этом предсказуемыми полями станут HDR для SCP80 начиная с первой команды, а для SCP81-1 — со второй в составе нескольких команд ([1], с. 149; [3], с. 9), поле счетчиков $CNTRS$ для SCP80, начиная со второй команды, $TRAILER$ и другие ([16]);

— при известном содержимом поля $BODY$, например, полей критичных данных $SensData$, не подлежащих предварительному шифрованию. Так, в случае передачи APDU-команды PUT KEY, для ключа Key будет сформирована TLV-структура (от Type, Lenght, Value) вида ([1], с. 184; [4]): $ENC(SensData) = TypeKey||LenKeyData||LenKey||ENC(Key)||LenCheck||CheckVal$ с предсказуемыми полями типа ключа $TypeKey$ и длин $LenKeyData$, $LenKey$, $LenCheck$. Необходимость дополнительной защиты этой TLV-структуры обуславливается хотя бы тем, что при ее передаче можно установить число байтов проверки ключа $LenCheck = '00'$, отбросить байты проверки $CheckVal$, скорректировать поля по аналогии с атакой 4 и навязать карте ложный ключ, изменив $ENC(Key)$.

Зашифрованное значение ключа $ENC(Key)$ вместе с предсказуемыми полями могут стать полем $BODY$ вида $Plaintext||ENC(SensData)||Plaintext$ ADPU-команды, которое затем может быть обработано с применением соответствующей конструкции защиты и получением $ENC(BODY) = Y_1|| \ldots ||Y_n$. Сама атака по нахождению байтов блока $X_i, i \geqslant 1$ может базироваться не на проверке байтов дополнения, а на проверке предсказуемых полей TLV-структуры с кодировкой ASN.1 BER-TLV.

Авторы допускают, что протоколы SCP на основе аутентифицированного шифрования AEAD с распараллеливанием вычислений ENC и MAC могут также стать уязвимыми к паддинг-атаке при наличии промежуточных проверок получаемых при расшифровании данных (что допускается в [1], с. 149). Так, при использовании в AEAD режима шифрования CTR: $Y_i = X_i \oplus ENC(IV_i)$ ([15]), не требующего наличия дополнения, атака может быть основана на передаче сообщений вида $Y'_1|| \ldots ||Y'_{i-1}||Y_i \oplus R|| \ldots$ с корректировкой необходимых полей заголовков и зашифрованных длин данных: $Y' = Y \oplus L$. При наличии процедуры проверки содержимого полей, расположенных в блоке $DEC(Y_i \oplus R)$ APDU-сообщения (в составе одного или нескольких сообщений), до проверки MAC, получаем значения байтов X_i (**атака 6**).

Данные о возможных сценариях атак на протоколы SCP занесены в табл.

СПИСОК ЛИТЕРАТУРЫ

1. GlobalPlatform Technology. Card Specification. Version 2.3.1. March 2018.
2. ETSI TS 102 225: "Smart Cards; Secured packet structure for UICC based applications". June 2020.
3. ETSI TS 102 226: "Smart Cards; Remote APDU structure for UICC based applications". September 2011.
4. GlobalPlatform Card. Card Specification. Remote Application Management over HTTP – Amendment B v1.2. March 2022.
5. *Sabt M., Traore J.* Cryptanalysis of globalplatform secure channel protocols. — In International Conference on Research in Security Standardization. Springer, 2016, p. 62–91.
6. *Dai W.* An attack against ssh2 protocol. — February, 2002. ftp://ftp.ietf.org/ietf-mail-archive/secsh/2002-02.mail.

7. *Bard G. V.* A challenging but feasible blockwise-adaptive chosen-plaintext attack on ssl. — In: Proc. of the International Conference on Security and Cryptography. — SECRYPT'06, INSTICC Press. 2006, p. 7–10.
8. *Braga D. de A.*, *Fouque P.-A.*, *Sabt M.* The Long and Winding Path to Secure Implementation of GlobalPlatform SCP10. — 2020, p. 196–218.
9. *Bleichenbacher D.* Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS# 1. — In Annual International Cryptology Conference. Springer, 1998, p. 1–12.
10. *Avoine G.*, *Ferreira L.* Attacking GlobalPlatform SCP02-compliant Smart Cards Using a Padding Oracle Attack. — IACR Transactions on Cryptographic Hardware and Embedded Systems. May 2018, p. 149–170.
11. *Vaudenay S.* Security Flaws Induced by CBC Padding – Applications to SSL, IPSEC, WTLS... — EUROCRYPT'02. LNCS 2332, Springer, 2002, p. 534–545.
12. *Krawczyk H.* The Order of Encryption and Authentication for Protecting Communications (or: How Secure Is SSL?). — Advances in Cryptology. LNCS 2139. Springer, 2001, p. 310–331.
13. *Bond M.* Attacks on Cryptoprocessor Transaction Sets. CHES'01. — LNCS 2162. Springer, 2001, p. 220–234.
14. *Clulow J.* On the security of PKCS#11. CHES'03. — LNCS 2779. Springer, 2003, p. 411–425.
15. *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.* About padding attacks on cryptographic protocols using standard n-bit block encryption modes. — OP&PM Surv. Appl. Ind. Math., Moscow, 2014, v. 21, is. 4, p. 358–360. (In Russian.)
16. *Елистратов А. А.*, *Никонов Н. В.*, *Ларионов В. В.*, *Свистюр З. В.* О возможности использования внутренних сообщений протокола TLS для проведения паддинг-атак. — Обозрение прикл. и промышл. матем., 2020, т. 27, в. 2, с. 143–145. // *Elistratov A. A.*, *Nikonov N. V.*, *Larionov V. V.*, *Svistyur Z. V.* About the possibility of using internal messages TLS protocol for padding attacks. — OP&PM Surv. Appl. Ind. Math., Moscow, 2020, v. 27, is. 2, p. 143–145. (In Russian.)

Поступила в редакцию
14.XII.2023

UDC DOI https://doi.org/10.52513/08698325_2023_30_1_1

Elistratov A. A., ***Nikonov N. V.*** (Moscow, Information Security Department Bank of Russia; Moscow, Federal educational and methodological association Russian universities for education in the field of information security)**. On the possible attack scenarios on SCP family.**

Abstract: This paper provides a review of possible attacks on GlobalPlaform's SCP (Secure Channel Protocol) family. Based on Vaudenay's idea of padding oracle attack the new attack scenarios are proposed used predictable fields of protected APDU-data as padding. It is stressed that such attacks may have affect against not only CBC but also AEAD encryption modes implemented in some versions of SCP protocols.

Keywords: SCP, GlobalPlatform, padding oracle attack, APDU, CBC, AEAD.