О необходимости реализации мер защиты от атак по побочным каналам для алгоритмов, основанных на использовании функции хэширования

Матвеев С.В.

Пензенский филиал ФГУП «НТЦ «Атлас»

РусКрипто'2020

Необходимость реализации мер защиты

Рекомендации по стандартизации Р 1323565.1.012-2017

> СЗКИ **должны** противостоять атакам, использующим технические каналы распространения информативных сигналов

Меры защиты:

- Технические меры
- Алгоритмические меры
  - Ограничение объема материала обрабатываемого на одном ключе

Криптоалгоритмы в стандартизированных протоколах

- блочные шифры (ГОСТ Р 34.12-2015) и режимы их использования (ГОСТ Р 34.13-2015)
- Схема ЭЦП ГОСТ (Р 34.10-2012)
- Сопутствующие криптографические алгоритмы (Р 50.1.113 - 2016):
  - HMAC
  - VKO
  - PRF
  - KDF
  - ...

Криптоалгоритмы в стандартизированных протоколах

- блочные шифры (ГОСТ Р 34.12-2015) и режимы их использования (ГОСТ Р 34.13-2015)
- Схема ЭЦП ГОСТ (Р 34.10-2012)
- Сопутствующие криптографические алгоритмы (Р 50.1.113 - 2016):
  - **HMAC**
  - VKO
  - PRF
  - KDF
  - ...

HMAC

$$HMAC(K, T) = H(K \oplus opad \parallel H(K \oplus ipad \parallel T))$$

- K – ключ
- T – данные
- $opad$, $ipad$ – константы

Уроза - многократное обращение к ключу

Сравниваем с алгоритмом «Кузнечик»
При шифровании 4 Кбайт – 256 $= 2^8$ обращений к ключу

Обращения к ключу при одном вызове HMAC

- 2 вызова хэш-функции $H(\cdot)$
- для каждого вызова

  $g_N(h, k \oplus pad) = E(LPS(h \oplus N, K \oplus pad) \oplus h \oplus K \oplus pad)$

  Итого – 4 обращения

HMAC в различных конструкциях

Алгоритм/ Обращение к	PRF_{TLS} PRF_{IPSEC}	KDF	$KDF-Expand$ $PRFPLUS^*$	$TLSTREE$ $IKETREE$ $ESPTREE$
HMAC	V	1	V	V
H	$2V$	2	$2V$	$2V$
ключ K	$4V$	4	$4V$	$4V$

V – количество формируемых ключей

* - для данных алгоритмов $V \leqslant 255$

TLS 1.2

$TLSTREE(K, i) = Divers(Divers(Divers(K, ...), ...), ...) =$
$Divers(Divers(K_2, ...), ...) = Divers(K_3, ...)$
где $Divers = KDF$

- TLS_GOSTR341112_256_WITH_MAGMA_CTR_OMAC
  - $K - V = 1$
  - $K_2 - V = 2^7$
  - $K_3 - V = 2^{13}$
- TLS_GOSTR341112_256_WITH_KUZNYECHIK_CTR_OMAC
  - $K_1 - V = 2^{32}$
  - $K_2 - V = 2^{13}$
  - $K_3 - V = 2^{13}$

PRF

- $V \leqslant 7$

TLS 1.3

$TLSTREE(K, i)$

- TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_L
  - $K_1 - V = 2^5$
  - $K_2 - V = 2^{23}$
  - $K_3 - V = 2^{23}$
- TLS_GOSTR341112_256_WITH_MAGMA_MGM_L
  - $K_1 - V = 2^{11}$
  - $K_2 - V = 2^{23}$
  - $K_3 - V = 2^{23}$
- TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_S
- TLS_GOSTR341112_256_WITH_MAGMA_MGM_S
  - $K_1 - V = 2^{13}$
  - $K_2 - V = 2^{13}$
  - $K_3 - V = 2^{13}$

HKDF-Extract

- $V \leqslant 2^8$

IKEv2

- функция PRFPLUS

  исходя из конструкции
  - $V \leqslant 255$

  при формрировании $SK_d, SK_{ai}, SK_{ar}, SK_{ei}, SK_{er}, SK_{pi}, SK_{pr}$
  - $V \leqslant 7$
- функция PRF

  при формировании SKEYSEED
  - $V = 1$
- ключ защиты сообщения
  $K_{msg} = IKETREE(K, i_1, i_2, i_3) = KDF(KDF(KDF(K, ...), ...), ...) = KDF(KDF(K_2, ...), ...) = KFD(K_3, ...)$
  - для K – $V \leqslant 2^8$
  - для K_2 – $V \leqslant 2^{16}$
  - для K_3 – $V \leqslant 2^{16}$

ESP

$$K_{msg} = ESPTREE(K, i_1, i_2, i_3) =$$
$$= KDF(KDF(KDF(K, ...), ...), ...) =$$
$$= KDF(KDF(K_2, ...), ...) = KFD(K_3, ...)$$

- для $K - V \leqslant 2^8$
- для $K_2 - V \leqslant 2^{16}$
- для $K_3 - V \leqslant 2^{16}$

Меры защиты

- Промужуточные ключи должны формироваться однократно
- Ограничение количества обращений к секретному ключу
- Алгоритмические меры защиты, применимые к алгоритму «Кузнечик» (маскирование,..)

Спасибо за внимание!

Вопросы?