Использование алгоритмов ГОСТ в протоколе DTLS

Дмитрий Белявский, ТЦИ

РусКрипто

22-25 марта 2016

Коротко о протоколе DTLS

- RFC 6347 специфицирует DTLS 1.2
- DTLS = TLS over UDP
  - Нет гарантии доставки пакетов
  - Нет гарантии порядка доставки
- Область применения: VoIP, online-игры

Базовые требования к криптографии

- RFC 6347, раздел 3.1
  - Зависимость между отдельными TLS Records (потоковые шифры)
    Запрет потоковых шифров
- Защита от повторов и переупорядочивания
  - Неявный номер пакета используется при вычислении MAC
    Вводится явный номер пакета

ГОСТ в TLS

Проблемы с текущими шифронаборами:

- Key meshing (1024 байта для «Магмы»)
- Вычисление MAC от конкатенации пакетов

Необходимо специфицировать новые шифронаборы, универсальные или специально для DTLS.

Нумерация пакетов

- Номер пакета – 64 бита:
  - 16 бит – номер «эпохи»
    Увеличивается при отправке ChangeCipherSpec
  - 48 бит – sequence number
- Можно применить двухуровневый KDF Tree для модификации ключей
  - «Использование криптографических алгоритмов, сопутствующих применению стандартов ГОСТ Р 34.10-2012 И ГОСТ Р 34.11-2012», раздел 5.5

KDF Tree

KDF_TREE(Kin,label,seed,R) = K(1) | K(2) | K(3) |...
где K(i) = HMAC256(Kin,[i]2|label|0x00|seed|[L]2),i≥1

- R от 1 до 4
- Kin – ключ диверсификации,
- L –битовая длина вырабатываемого ключевого материала, в битах
- [L]2 – байтовое представление L в сетевом порядке байт
- i –счетчик числа итераций
- [i]2–байтовое представление счетчика числа итераций длиной R байт
- label, seed – константы протокола

Прочие отличия от TLS

- При ошибке не разрываем сессию
  - Ошибочные пакеты игнорируются, при этом атаки типа Oracle не получается.
- Необходимость защиты от DDoS
  - Cookie

Выводы

- Нужны DTLS-совместимые ciphersuites

- Требуется:
  - KDF для шифрования и для MAC
  - Блочный режим или AEAD-режим
  - Способ выработки Cookies

Вопросы?

Пишите на beldmit@tcinet.ru