GS LABS
GS GROUP

Публичный - L0

DRE Advanced Encryption Service

Общее описание

Индекс	2004-DREAdvancedEncryptionService-GD
Секретность	Публичный - L0
Ревизия	1.0
Статус	Согласован
Подразделение	ДПРСУД
Компания	GS Labs

Содержание

1. Аннотация

Документ содержит общее описание системы "DRE Advanced Encryption Service" и предназначен для широкого круга специалистов. Подробнее работа системы описана в других документах по продукту.

2. Термины и сокращения

Термин	Определение
Транспортный поток (TS)	Набор объединенных элементарных потоков, используемый для передачи аудио, видео и других данных в системах цифрового вещания. Структура транспортного потока определена в стандарте ISO/IEC 13818-1.
Элементарный поток	Поток данных одного типа, передающийся в составе транспортного потока. Примеры: аудиодорожка, видео, телетекст, служебная информация.
Скремблер (Scrambler)	Устройство шифрования транспортного потока, входящее в состав головного оборудования. В терминологии стандарта DVB-Simulcrypt обозначает функциональный логический блок, ответственный за шифрование MPEG2 транспортного потока. Конкретная функциональность зависит от реализации.

Сокращение	Расшифровка
ADEC	(ADvanced EnCryption) - система шифрования транспортного потока, применяемая в дополнение к стандартному алгоритму шифрования (CSA).
MPEG	(от Moving Picture Experts Group – Группа Экспертов по Движущемуся Изображению) – название системы кодирования набора сжатых цифровых телевизионных видеосигналов, звуковых сигналов и данных пользователя телевизионной информации в поток цифровых пакетов
IP	(Internet Protocol) – протокол передачи данных по сети Интернет
PID	Идентификатор пакетов, относящихся к одному элементарному потоку. Уникален в пределах транспортного потока.
TS	Transport Stream, Транспортный поток (см. таблицу терминов)
TSoIP	(TS over IP) – передача транспортного потока цифрового телевидения по протоколу IP
GbE (GigE)	(Gigabit Ethernet) - технология передачи данных по сети Ethernet со скоростью до 1 гигабит /сек

3. Назначение и структура системы

3.1. Общее описание

Программа DRE Advanced Encryption Service (далее - ADECScrambler или Система) обеспечивает возможность дополнительной защиты контента при вещании в спутниковой и IP сетях. Для поддержки этой функциональности доступны следующие возможности:

- Возможность выбора каналов для включения дополнительной защиты из списка каналов входящего транспортного потока.
- Возможность выбора различных алгоритмов дополнительной защиты, включая алгоритм S17.
- Предоставление набора метрик для мониторинга бесперебойной работы.

Входной (открытый) поток может быть захвачен из следующих источников:

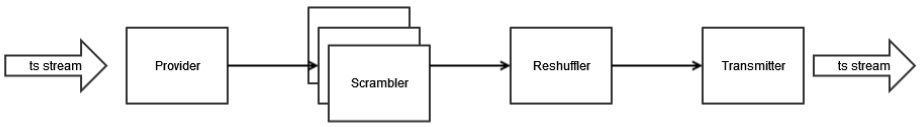
- udp unicast socket
- udp multicast socket

Результирующий (шифрованный) поток передается в один из следующих приемников:

- udp unicast socket
- udp multicast socket

3.2. Логическая структура

Структурная схема ADECScrambler представлена на рисунке:



ADECScrambler представляет собой конвейер с последовательной обработкой на каждом из узлов входного потока. Конвейер состоит из следующих компонентов:

- Provider - обеспечивает забор данных из источника и парсинга их в структуру ts-пакета.
- Scrambler - обеспечивает шифрование ts-пакета заданным алгоритмом.
- Reshufler - обеспечивает выстраивание ts-пакетов в правильном порядке следования после шифрования.
- Transmitter - обеспечивает передачу данных к приемнику.

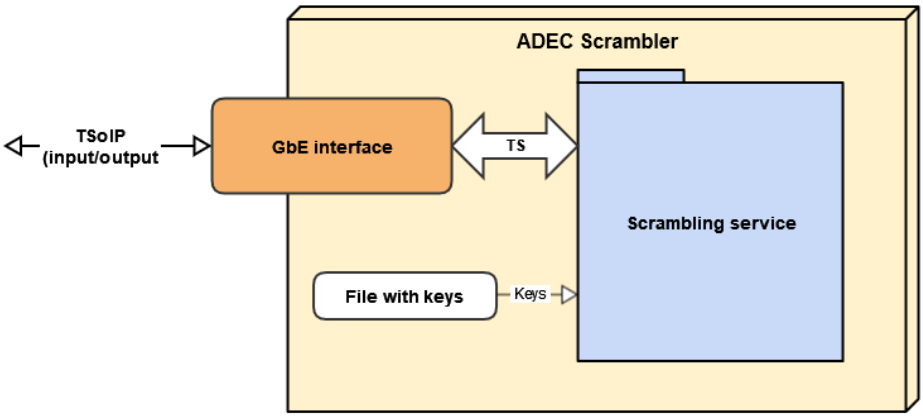
⚠ **Обратите внимание!** Описанное выше деление на компоненты - это логическое деление в рамках одного исполняемого файла adec_scrambler_go, т.е физически запускается одна служба.

3.3. Общая структура взаимодействия

ADECScrambler представляет собой выделенный сервер на ОС Debian 8 64 бит, снабженный интерфейсом Gigabit Ethernet. Входной и и выходной потоки поступают по IP, через сетевую плату.

Используемые для скремблирования ключи могут храниться в зашифрованном виде, для их применения нужно знать пароль.

Взаимодействие частей Системы представлено на рисунке:



3.3.1. Взаимодействие ADECScrambler с приемной стороной

Настройка взаимодействия передающей и приемной стороны заключается в уведомлении приемной стороны об использовании дополнительного шифрования и настройках его режима.

3.4. Функциональные возможности

Основные задачи, выполняемые ADECScrambler:

- высокоскоростное шифрование транспортных потоков, получаемых из следующих источников:
  - через порт Gigabit Ethernet (порт Ethernet находится непосредственно на сетевой плате)
- сигнализация об ошибках
- возможность прямой передачи потока со входа на выход (отключение/включение скремблирования)

ADECScrambler обладает следующими характеристиками:

1) Основные:

- возможность одновременного скремблирования нескольких PID
- любой PID может быть привязан к любому ключу
- поддержка следующих алгоритмов шифрования: TDES, S17
- вывод потока осуществляется на один IP-порт

2) Входные и выходные интерфейсы:

- Gigabit Ethernet:
  - Вход/выход: транспортные потоки по протоколу IP

3) Мониторинг:

- в логах указываются изменения в работе служб шифрования, ошибки, остановки, перезапуски и т.п.

  ⚠ Чтобы посмотреть логи, надо выполнить команду *docker logs container_name*

- собирает статистику о своей работе. Показатели, по которым собирается статистика (например, количество успешно зашифрованных байт), задаются так называемыми "метриками".

4) Безопасность:

- от неавторизованного доступа скремблер защищается средствами ОС
- набор ключей хранится в отдельном файле. Для шифрования файла используется специальная утилита (предоставляется по запросу заказчика).