Ежегодная международная научно-практическая конференция
«РусКрипто’2019»

Криптографические механизмы защищенного взаимодействия контрольных и измерительных устройств (МР 26.4.003-2018)

Алексей Нестеренко
к.ф.-м.н, Кафедра компьютерной безопасности МИЭМ НИУ ВШЭ

Области применения

- Гетерогенные сети с различными каналами связи (уровни L2, L3)
  - беспроводные/широковещательные
  - без гарантированной доставки сообщений (IP, UDP)
  - с гарантированной доставкой (TCP)
- Различные методы аутентификации абонентов
  - симметричные ключи аутентификации
  - открытые ключи (PKI) и сертификаты
    - X509, CV и т.п.

- Микропроцессоры с различными техническими/эксплуатационными характеристиками
- Унифицированный механизм для ПО kernel/user space

Базовые технические требования

или какие криптографические примитивы нужно предварительно реализовать

- ГОСТ Р 34.12-2015 - алгоритмы блочного шифрования
- ГОСТ Р 34.11-2012 - функция хеширования
- ГОСТ Р 34.10-2012 - электронная подпись
- ГОСТ Р 34.13-2015 - режимы гаммирования и выработки имитовставки
- Режим аутентифицированного шифрования MGM
  - (дополнительно нужна операция умножения в полях $GF(2^n)$ при n = 64, 128)
- Память для хранения ключевой информации (2,5Кб = 5x512 бит)

МР 26.4.003-2018. Состав документа

- Транспортный протокол
- Протокол выработки общих ключей
- Протокол передачи прикладных данных
  - туннелирование
  - выработка новых ключей аутентификации iPSK

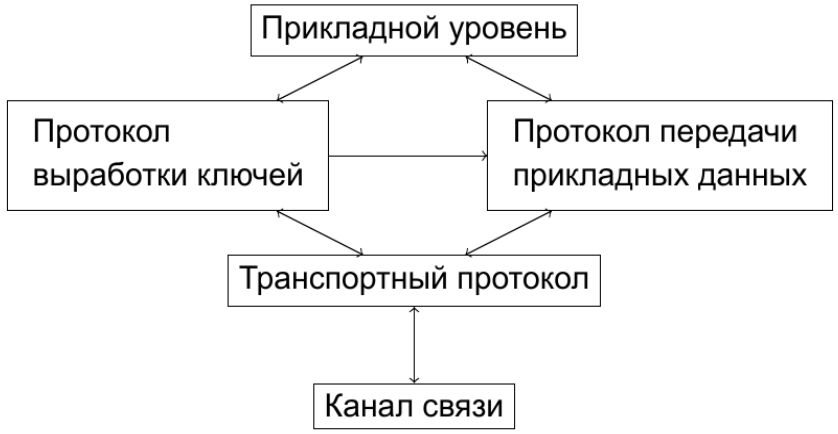
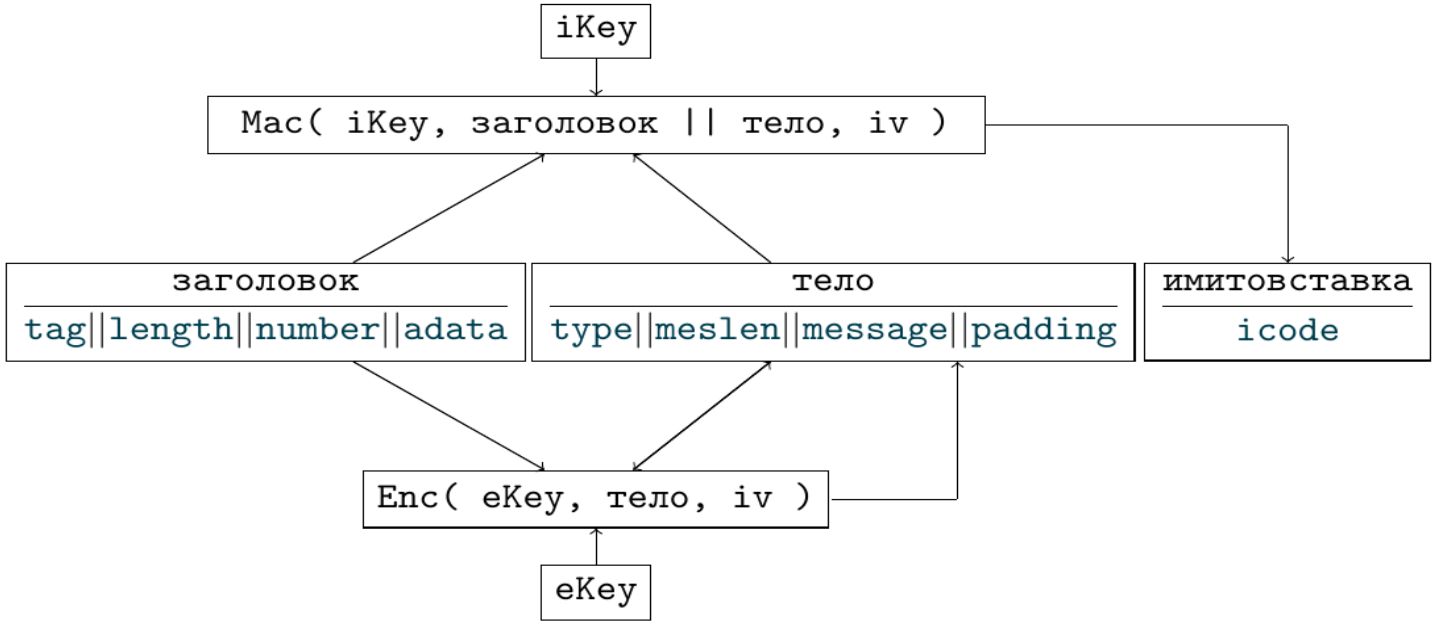


Рисунок 1. Схема информационного обмена.

- Типовые схемы аутентификации
- Механизмы формирования предварительно распределенных ключей
- Точные значения криптографических параметров для всех классов СКЗИ

Транспортный протокол

Формат передаваемых данных



- Формат пакетов данных ориентирован на сети с потерей данных

Транспортный протокол

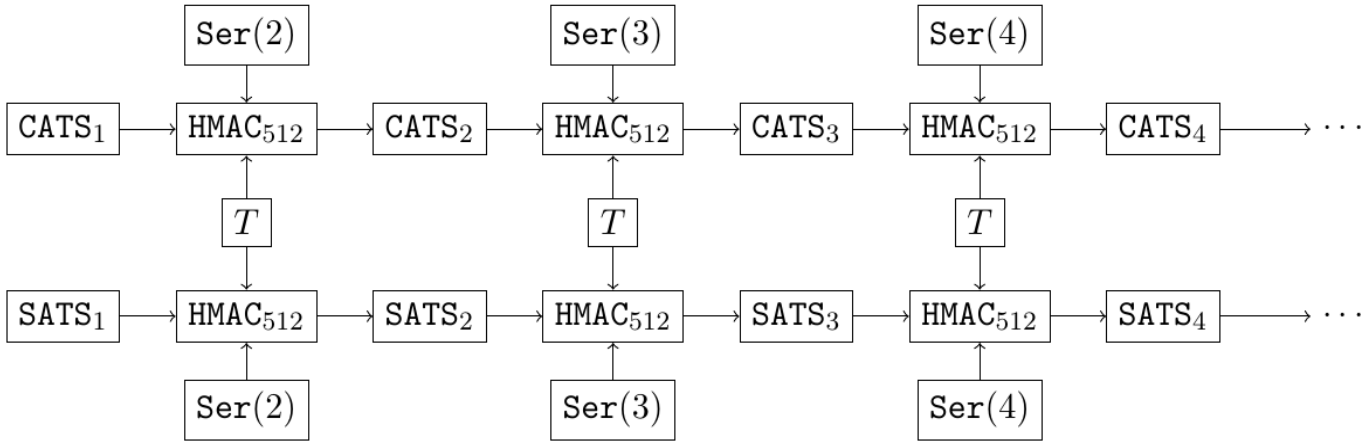
Криптографические механизмы обеспечения конфиденциальности и целостности

- Заголовок пакета (*имитозащита*)
  - длины заголовка (6 бит) и всего пакета (16 бит), уникальный номер пакета, при необходимости, дополнительные идентифицирующие отправителя данные
- Тело пакета (*шифрование данных + имитозащита*)
  - тип, длина, данные + случайное дополнение
- Режимы AEAD
  - гаммирование + имитовставка согласно ГОСТ Р 34.13-2015 или режим MGM
  - имитозащита всегда; шифрование, при необходимости
  - различные ключи шифрования и имитозащиты (ключевая пара)
  - алгоритм развертки производных ключей

Транспортный протокол

Механизмы развертки ключевой информации

- Исходная ключевая информация CATS и SATS + общий секрет T
  - Размер каждого вектора: по 512 бит
  - Различные данные для направления клиент/сервер (CATS) и сервер/клиент (SATS)
- Два уровня ключевого «дерева» с различной трудоемкостью
  - Верхний «тяжелый» с использованием HMAC (Р 50.1.113-2016)

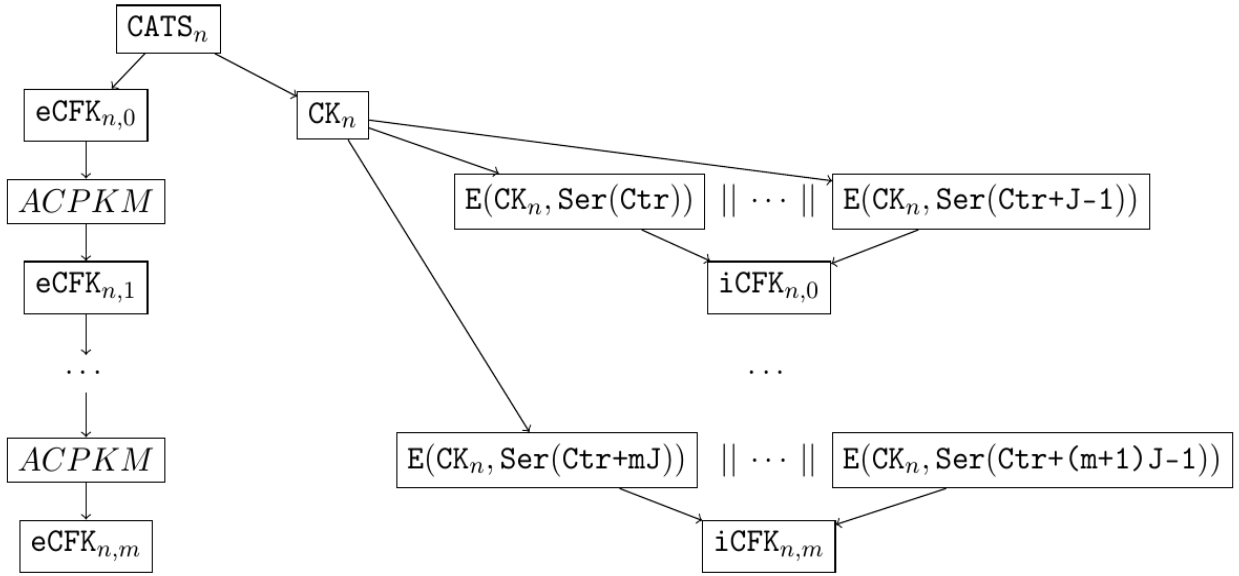


Транспортный протокол

Механизмы развертки ключевой информации, часть II

- Два уровня ключевого «дерева» с различной трудоемкостью
  - Нижний «легкий» с использованием блочного шифрования (Р 1323565.1.017-2018)

$$\mathtt{K}_m = ACPKM(\mathtt{K}_{m-1}) = \mathtt{E}(\mathtt{K}_{m-1}, D_1)|| \cdots ||\mathtt{E}(\mathtt{K}_{m-1}, D_J),$$



  - Значения индексов n, m + порядковый номер пакета входят в его заголовок

Протокол выработки общих ключей

Основные характеристики и свойства

- В основе схема Р 1323565.1.004-2017 (Эхинацея, Сигма) с тремя пересылками
  - используются эллиптические кривые в форме Вейерштрасса или Эдвардса
  - шифрование и имитозащита на уровне транспортного протокола
  - разная ключевая информация для протокола и передачи данных

$$\xrightarrow{\texttt{ClientHello} = R_c, k_c P}$$

$$\xleftarrow{\begin{cases} \texttt{ServerHello} = R_s, k_s P, \\ \texttt{Certificate}_s, \\ \texttt{VerifyMessage}_s = \texttt{Sign}_s(\texttt{ClientHello}, \texttt{ServerHello}, \texttt{Certificate}_s) \end{cases}}$$

$$\xrightarrow{\begin{cases} \texttt{Certificate}_c, \\ \texttt{VerifyMessage}_c = \texttt{Sign}_c(\texttt{ClientHello}, \texttt{ServerHello}, \texttt{Certificate}_s, \\ \qquad\qquad \texttt{VerifyMessage}_s, \texttt{Certificate}_c) \end{cases}}$$

  - три схемы аутентификации: включая, PKI и симметричные ключи (ePSK или iPSK)

Протокол выработки общих ключей

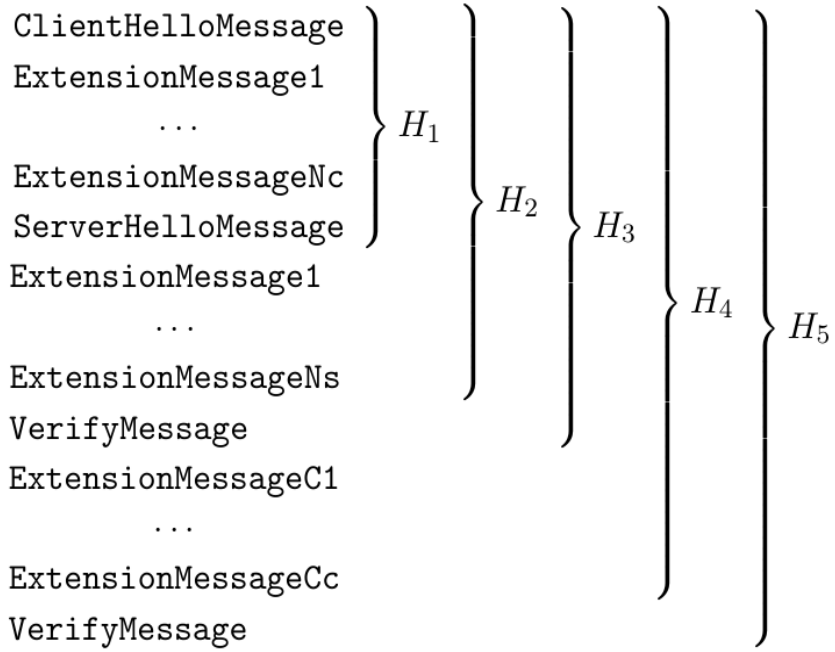
Основные характеристики и свойства, часть II

- Обеспечиваемые свойства безопасности:
  - Обязательная генерация уникальных ключей для каждого сеанса
  - Стойкость при компрометации сеансовых ключей
  - Защита от чтения вперед/назад (Perfect Forward Secrecy)
  - Подтверждение ключевой информации
  - Аутентификация абонентов: односторонняя или взаимная
  - Защита от навязывания ключевых значений
  - Защита от имперсонализации (защита от UKS-атак)
  - Анонимность клиента
- Текст обоснования доступен на сайте ТК 26

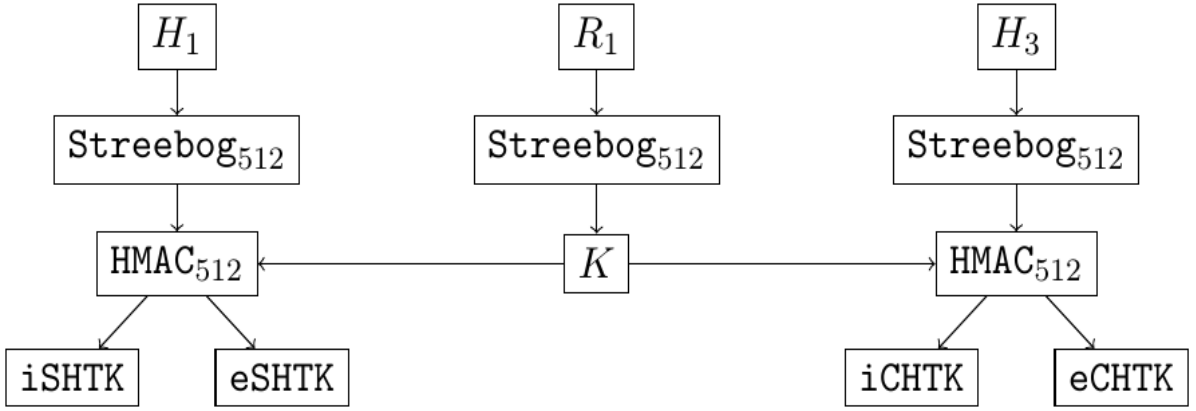
Протокол выработки общих ключей

Дополнительные возможности

- Зависимость ключевой информации от всех переданных сообщений
  - выработка ключей для шифрования данных *в ходе выполнения протокола*



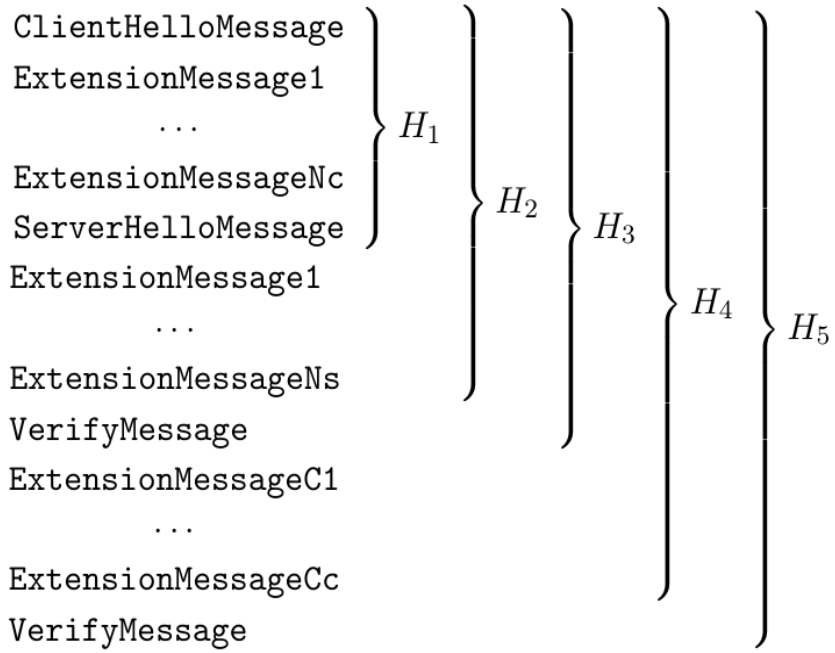
$$R_1 = x(Q)||\texttt{iPSK*}||\texttt{ePSK*}$$



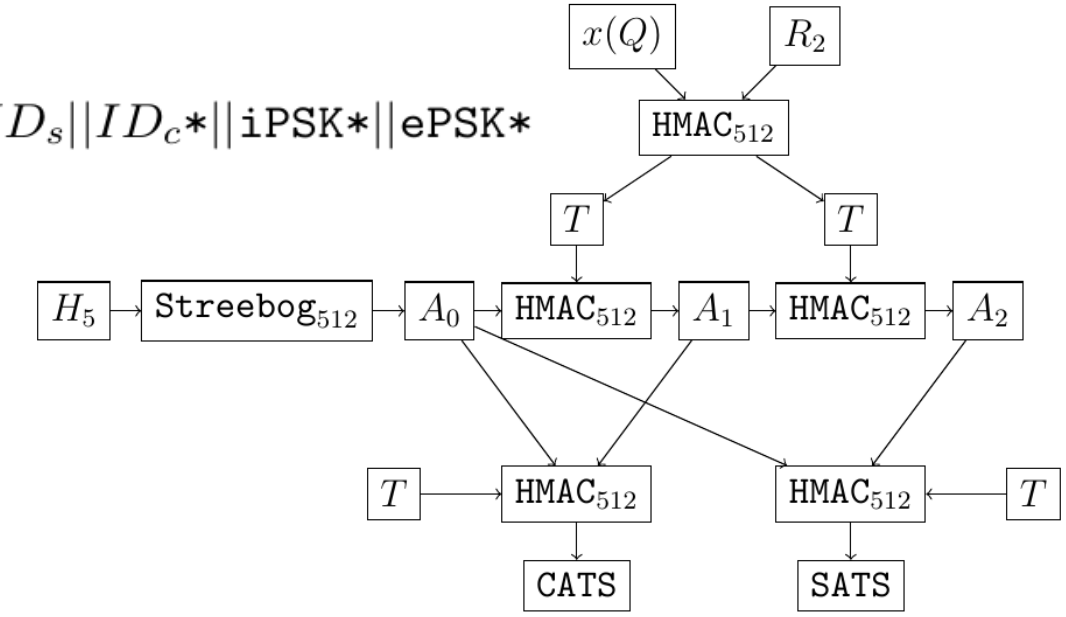
Протокол выработки общих ключей

Дополнительные возможности

- Зависимость ключевой информации от всех переданных сообщений
  - выработка ключей для шифрования *прикладных данных* (P 50.1.113-2016)



$$R_2 = ID_s||ID_c*||\texttt{iPSK*}||\texttt{ePSK*}$$



Протокол выработки общих ключей

Дополнительные возможности

- Согласование криптографических примитивов в ходе протокола
  - блочный шифр, режим AEAD, эллиптическая кривая
- Обмен данными только после завершения протокола
- Допускаются расширения
  - запрос сертификатов и/или идентификаторов
  - контроль используемых криптографических механизмов
- Допустимые объемы обрабатываемых данных (нагрузка на ключ)
  - три группы средств: не попадающие под ПКЗ-2005; средства классов КС1-КС3 и КВ-КА
  - зависимость от длин пакетов
  - общий объем одного сеанса, например, для КС3, шифр Магма, равен 32ТБ.

МР 26.4.003-2018. Резюме

- Что можно отнести к достоинствам:
  - универсальное решение для различных каналов связи
  - различные ключевые системы для аутентификации абонентов
  - обоснованная стойкость/статус рекомендаций ТК 26
  - ориентация на применение в СКЗИ различных классов
  - большой объем трафика для одного сеанса связи
- Что можно отнести к недостаткам
  - инкапсуляция добавляет, минимально, 20 байт
  - большой объем хранимой ключевой информации
  - последовательная процедура выработки производных ключей

Спасибо за внимание! Вопросы?

Контактная информация

Электронная почта:

anesterenko@hse.ru

Сайт:

www.miem.hse.ru