Ежегодная международная научно-практическая конференция
«РусКрипто’2021»

Об участии российских специалистов в развитии протокола IPsec в IETF

Валерий Смыслов
Архитектор системы, ЭЛВИС-ПЛЮС

IETF (Internet Engineering Task Force)

- Образована в 1986
- Основная задача – разработка технических стандартов определяющих работу сети Интернет (TCP/IP)
- Формальное членство отсутствует; основная работа ведется через почтовые списки рассылки; любой подписавшийся автоматически становится членом IETF
- Конференции трижды в год в различных частях мира, в 2020-21 онлайн (более 1000 участников)
- Принципы – открытость, вовлеченность, компромисс и работающий код

Be conservative in what you send and liberal in what you accept

Jon Postel

Протокол IPsec (IP security)

Обеспечивает защиту TCP/IP трафика на сетевом уровне, состоит из:

- Протокола защиты данных ESP (Encapsulating Security Payload)
  - ESPv1: RFC 1827 (1995), ESPv2: RFC 2406 (1998), **ESPv3**: RFC 4303 (2005)
- Протокола управления ключами IKE (Internet Key Exchange)
  - IKEv1: RFC 2409 (1998), статус на сегодняшний день - «устаревший»
  - **IKEv2:** RFC 4306 (2005), RFC 5996 (2010), RFC 7296 (2014)
  - Разработано множество расширений IKEv2, имеющих статус стандарта:
    RFC 5685, 5723, 5998, 6290, 6311, **7383**, 7427, **7619**, **7791**, **8019**, 8229, 8598, 8750, **8784** …

*RFC, выделенные **синим** цветом, разработаны целиком или при участии ЭЛВИС-ПЛЮС*

Текущее состояние и перспективы развития IPsec

https://datatracker.ietf.org/wg/ipsecme/documents/

Текущие направления работы группы по IPsec в IETF:

- **Управление групповыми ключами с использованием IKEv2**
- **Гибридный ключевой обмен в IKEv2**
- Агрегирования и фрагментации IP-пакетов для скрытия параметров трафика
- Метки безопасности в IPsec
- **Обновление RFC 8229 (инкапсуляция IKE и ESP в TCP)**

Перспективные направления:

- **Конфигурирование защищенного DNS посредством IKEv2**
- Оптимизация обновления ключей в IKEv2
- **Устранение ограничения на размер секции в IKEv2 в 64K**
- **Анонсирование методов аутентификации в IKEv2**
- **…**

*ЭЛВИС-ПЛЮС участвует в работах, выделенных **синим** цветом*

IKE фрагментация (RFC 7383)

Расширение IKEv2, позволяющее избежать фрагментации на уровне IP при передачи больших сообщений IKEv2

- IKEv2 использует UDP в качестве транспорта
- UDP плохо поддерживается сетевыми трансляторами адресов (NAT) в случае, если пакет фрагментирован на уровне IP

- Внесено как предложение в рабочую группу IPsec в IETF в 2012г.
- В 2013г. принято как основной вариант решения проблемы
- Опубликовано в качестве стандарта в ноябре 2014г. (RFC 7383)
- На настоящий момент реализовано у всех ведущих производителей IPsec

Разработано ЭЛВИС-ПЛЮС

Реализовано в продуктах ЭЛВИС-ПЛЮС, strongSwan, Cisco Systems, Apple, INSIDE Secure, libreswan, Microsoft, …

Классическое противодействие квантовой угрозе в IKEv2 (RFC 8784)

Расширение IKEv2, позволяющее использовать дополнительный симметричный ключ в дополнение к DH обмену

- Переводит квантовую атаку на IKEv2 с алгоритма Шора на алгоритм Гровера
- Является временным решением до появления постквантовых алгоритмов ключевого обмена
- Позволяет защитить трафик в ситуации, когда злоумышленник сохраняет его и расшифровывает позднее, когда появится полноразмерный квантовый компьютер

- Разработано с учетом возможного использования с алгоритмами ГОСТ
- Опубликовано в качестве стандарта в июне 2020г. (RFC 8784)

Совместная разработка Cisco Systems и ЭЛВИС-ПЛЮС

Реализовано у ЭЛВИС-ПЛЮС, libreswan, Apple

Гибридный ключевой обмен в IKEv2

Расширение IKEv2, позволяющее использовать постквантовые примитивы обмена ключами

- Постквантовые примитивы имеют большой размер публичного ключа, что создает сложности в случае IP-фрагментации сообщений IKE
- Постквантовые примитивы недостаточно хорошо изучены, поэтому используется комбинация нескольких примитивов (гибридный ключевой обмен)

- Использует новый т.н. «промежуточный» обмен протокола IKEv2, разработанный ЭЛВИС-ПЛЮС
- Публикация в качестве стандарта ожидается в 2021г.

Разрабатывается совместно Post-Quantum, Quantum Secret, Cisco Systems, ISARA, Philips, ЭЛВИС-ПЛЮС

Несколько экспериментальных реализаций

Устранение ограничения на размер секции IKEv2 в 64 Кбайт

Расширение IKEv2, позволяющее использовать примитивы обмена ключами с открытыми ключами > 64 Кбайт

- Актуально для некоторых постквантовых алгоритмов обмена ключами (Classic McEliece)
- Возможно будет актуально для постквантовых примитивов, разрабатываемых в ТК26

Разрабатывается совместно Post-Quantum, genua, ЭЛВИС-ПЛЮС

Управление групповыми ключами с использованием IKEv2 (G-IKEv2)

Расширение IKEv2, позволяющее управлять групповыми ключами и т.о. защищать широковещательный (multicast) IP трафик

- Базируется на IKEv2, имеет собственное название: G-IKEv2
- Глубокая переработка базового протокола
- На замену протоколу GDOI, базировавшемуся на IKEv1

- Помимо защиты IP трафика, G-IKEv2 предполагается использовать для передачи групповых ключей в стандарте IEEE 802.15.9 (управление ключами для 802.15.4)

В разное время в разработке участвовали Cisco Systems, CheckPoint, Dell EMC.

На данный момент разрабатывается преимущественно ЭЛВИС-ПЛЮС

Передача параметров защищенного DNS посредством IKEv2

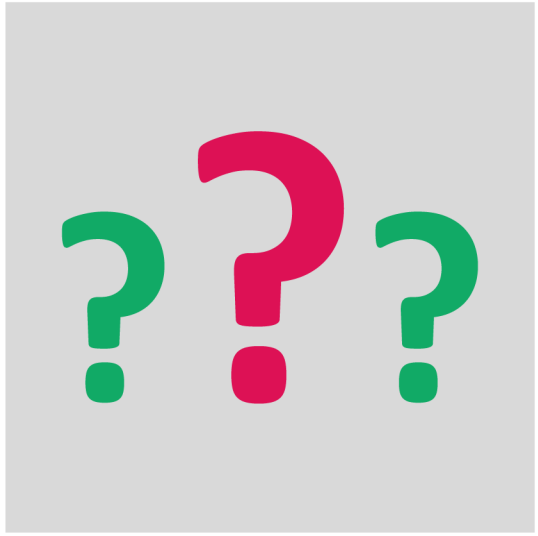
Расширение IKEv2, позволяющее передавать на IPsec клиенты параметры защищенных DNS серверов

- Позволяет защищенным образом передавать информацию о DNS серверах
- Поддерживаются DoT (DNS over TLS), DoH (DNS over HTTPS) и DoQ (DNS over QUIC)

- Использование защищенного DNS является современной тенденцией в плане повышения защищенности в Интернет

Разрабатывается совместно Orange, McAfee, Citrix, ЭЛВИС-ПЛЮС

Вопросы



Контактная информация

Электронная почта:

info@elvis.ru

svan@elvis.ru

Телефон:

+7 495 276-02-11

Сайт:

www.elvis.ru