ЭЛВИС-ПЛЮС

Международные стандарты протоколов сетевой безопасности: как они влияют на нас и как мы влияем на них

Валерий Смыслов

Преимущества использования международных стандартов протоколов при разработке продуктов сетевой безопасности

- Разработка нового протокола «с нуля» - сложная и трудоемкая задача
- Принятие международных стандартов сопровождается их скурпулезным анализом
- Международные стандарты охватывают широкий спектр возможных сценариев использования
- Опора на международные стандарты позволяет добиться совместимости с продуктами других производителей
- В конечном счете снижается стоимость и время разработки продукта

© АО «ЭЛВИС-ПЛЮС», 2019 | elvis.ru

Всегда ли международные стандарты протоколов полностью удовлетворяют наши потребности?

- Международные стандарты пишутся без оглядки на требования российских сертифицирующих органов
- Стандартные протоколы не всегда предусматривают необходимой для Росии параметризации
- Иногда местные особенности эксплуатации выявляют слабые стороны стандартных решений
- Как результат – международные стандарты как правило требуют адаптации

© АО «ЭЛВИС-ПЛЮС», 2019 | elvis.ru

Работа по адаптации международных стандартов в ТК26

- ТК26 – Технический Комитет по стандартизации «Криптографическая защита информации»
- Одно из направлений деятельности ТК26 – гармонизация международных стандартов и российских криптоалгоритмов
- ЭЛВИС-ПЛЮС участвует в работе ТК26 с **2006** года
- Специалисты ЭЛВИС-ПЛЮС принимали участие в обсуждении технических спецификаций по использованию российских криптоалгоритмов ГОСТ в протоколе IKEv1
- В настоящее время ЭЛВИС-ПЛЮС в качестве головной организации участвует в разработке стандартов по использованию российских криптоалгоритмов ГОСТ в протоколах ESP и IKEv2

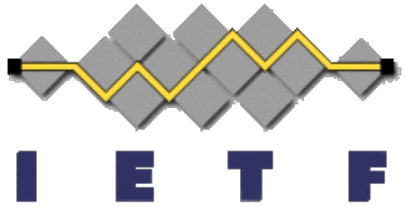
© АО «ЭЛВИС-ПЛЮС», 2019 | elvis.ru

Простая адаптация международных стандартов – это улица с односторонним движение, мы стремимся сделать ее двухсторонней путем активного участия в их разработке

- Стандартизация в международных организациях специфичных для России сущностей (например криптоалгоритмов)
- Учет российской специфики при разработке стандартов
- Вовлеченность в разработку базовых (неспецифичных для России) международных стандартов

© АО «ЭЛВИС-ПЛЮС», 2019 | elvis.ru

IETF –международная организация, занимающаяся стандартизацией протоколов работы в IP-сетях



- Образована в 1986
- Основная задача – разработка технических стандартов определяющих работу сети Интернет
- Формальное членство отсутствует; основная работа ведется через почтовые списки рассылки; любой подписавшийся автоматически становится членом IETF
- Конференции три раза в год в различных частях мира (более 1000 участников)
- Принципы – открытость, вовлеченность, компромисс и работающий код
  - «**Be conservative in what you send and liberal in what you accept**» (Jon Postel)

© АО «ЭЛВИС-ПЛЮС», 2019 | elvis.ru

Участие российских специалистов в работе IETF

- За все время существования IETF в его работе участвовало **38** авторов из России (КриптоПро, КриптоКом, Яндекс, Qrator Labs, ЭЛВИС-ПЛЮС и другие)
- ЭЛВИС-ПЛЮС участвует в работе IETF с **1998** года
- Все вместе российские авторы опубликовали **22** RFC, из них **6**, имеющих статус стандарта, из них **4** за авторством/соавторством ЭЛВИС-ПЛЮС
- В настоящий момент у всех активных авторов из России в совокупности в IETF находятся в работе **18** документов, из них **8** у ЭЛВИС-ПЛЮС
- Сейчас ЭЛВИС-ПЛЮС – один из самых активных членов рабочей группы ipsecme (занимающейся развитием протоколов IPsec)

Источник http://www.arkko.com/tools/docstats

© АО «ЭЛВИС-ПЛЮС», 2019 | elvis.ru

Участие ЭЛВИС-ПЛЮС в работе IETF: разработка международного стандарта по фрагментации сообщений IKEv2

- Проблема «NAT и IKEv2»
  - Протокол IKEv2 является ключевой частью IPsec, обеспечивая аутентифицированный обмен ключами
  - IKEv2 использует UDP в качестве транспортного протокола, при этом IKEv2 в процессе работы может посылать достаточно большие сообщения, которые разбиваются на несколько фрагментов на уровне IP протокола
  - Некоторые Трансляторы Сетевых Адресов (NAT, Network Address Translator) не пропускают фрагментированные IP пакеты
    - Неполнофункциональные SOHO (Small Office/Home Office) маршрутизаторы
    - В CGN (Carrier Grade NAT) обработка фрагментов может быть отключена
  - Результат – пользователь не может установить защищенное соединение из кафе/гостиницы или если его провайдер использует NAT с отключенной обработкой IP фрагментов
- Проблема стала заметной в мире начиная с 2010 г.

© АО «ЭЛВИС-ПЛЮС», 2019 | elvis.ru

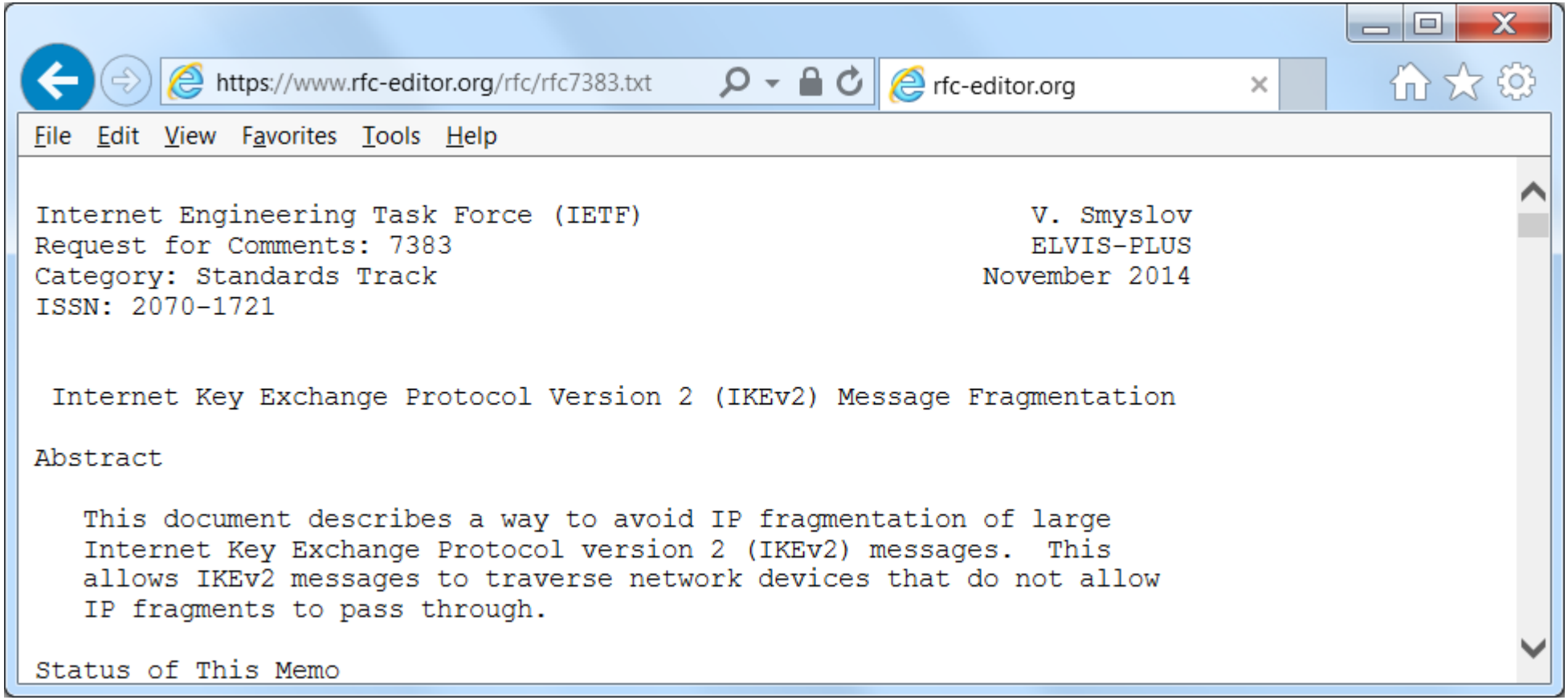
Участие ЭЛВИС-ПЛЮС в работе IETF: разработка международного стандарта по фрагментации сообщений IKEv2

- Рабочая группа ipsecme в IETF занялась поиском решения летом 2012
- Было предложено несколько вариантов решения проблемы:
  - использование короткоживущих TCP соединений (CheckPoint)
  - фрагментация пакетов на уровне IKE без криптографической защиты фрагментов (Microsoft, Cisco)
  - фрагментация пакетов на уровне IKE с криптографической защитой каждого фрагмента (ЭЛВИС-ПЛЮС)
- Летом 2013 вариант предложенный ЭЛВИС-ПЛЮС после длительного обсуждения был окончательно принят как основной
- В течении 2013-2014 проект стандарта дорабатывался с учетом замечаний рабочей группы

© АО «ЭЛВИС-ПЛЮС», 2019 | elvis.ru

Участие ЭЛВИС-ПЛЮС в работе IETF: разработка международного стандарта по фрагментации сообщений IKEv2

В ноябре 2014 вышел RFC 7383 «Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation», имеющий статус стандарта



© АО «ЭЛВИС-ПЛЮС», 2019 | elvis.ru

Участие ЭЛВИС-ПЛЮС в работе IETF: разработка международного стандарта по фрагментации сообщений IKEv2

- В настоящее время RFC 7383 реализован у всех ведущих мировых производителей, имеющих отношение к IPsec:

ЭЛВИС-ПЛЮС	**VPN/FW ЗАСТАВА**	**2013 (до выхода RFC!)**
StrongSwan	v5.2.1	2015
Apple	iOS 9, OS X El Capitan	2015
Cisco Systems	IOS 15.5(2)T, ASA 9.6(1)	2015
INSIDE Secure	QuickSec IPsec Toolkit	2015
Microsoft	Windows 10 (v1803), Windows Server 2019	2018

- RFC 7383 стал одним из «базовых» расширений IKEv2: новые расширения разрабатываются в предположении, что его поддержка есть «везде», то есть в любой современной реализации IPsec

© АО «ЭЛВИС-ПЛЮС», 2019 | elvis.ru

Участие ЭЛВИС-ПЛЮС в работе IETF: разработка международного стандарта по защите IKEv2 от распределенных атак отказа в обслуживании

- IKEv2 имеет встроенный механизм защиты от DoS атак исчерпания памяти на шлюзе путем отсылки запросов с «фейковых» IP адресов, основанный на механизме COOKIE
- Механизм COOKIE в паре с фильтрацией IP успешно работают при защите от одиночных DoS атак, но неэффективен в случае распределенных атак отказа в обслуживании (Distributed Denial of Service – DDoS)
- DDoS атака производится с использованием ботнетов – сетей зараженных компьютеров, контролируемых злоумышленником

© АО «ЭЛВИС-ПЛЮС», 2019 | elvis.ru

Участие ЭЛВИС-ПЛЮС в работе IETF: разработка международного стандарта по защите IKEv2 от распределенных атак отказа в обслуживании

- Для защиты IKEv2 от DDoS атак рабочей группой ipsecme в IETF в 2014 г. был предложен новый механизм – PUZZLE, основанный на принципе **Proof-of-Work** (используемом также в BLOCKCHAIN)
- При опасности исчерпания ресурсов шлюз всем новым клиентам начинает выдавать «загадки» (PUZZLE), которые требуют существенной затраты вычислительных ресурсов на решение, что снижает интенсивность атаки
- В октябре 2014 г. - первый рабочий документ IETF по PUZZLE в IKEv2
  - первоначальное авторство было у CheckPoint
  - в марте 2015 г. ЭЛВИС-ПЛЮС стал соавтором документа
- В ноябре 2016 г. вышел окончательный стандарт – RFC 8019 «Protecting Internet Key Exchange Protocol Version 2 (IKEv2) Implementations from Distributed Denial-of-Service Attacks»
- В 2016 г. этот механизм был реализован в VPN/FW ЗАСТАВА

© АО «ЭЛВИС-ПЛЮС», 2019 | elvis.ru

Участие ЭЛВИС-ПЛЮС в работе IETF сегодня: защита от атак с использованием квантовых компьютеров

- В IETF готовится к публикации в качестве стандарта документ по защите IPsec соединений от возможных атак с использованием квантовых компьютеров
  - предполагаемый срок публикации – весна-лето 2019
  - ЭЛВИС-ПЛЮС является соавтором (вместе с Cisco Systems)
  - реализован в VPN/FW ЗАСТАВА
- В работе в IETF находится пакет документов по адаптации IKEv2 к использованию примитивов постквантовой криптографии
  - предполагаемый срок публикации – после 2020
  - авторы Post-Quantum, Cisco Systems, ISARA Corporation, Philips, ЭЛВИС-ПЛЮС

© АО «ЭЛВИС-ПЛЮС», 2019 | elvis.ru

Стандарты IPsec в VPN/FW ЗАСТАВА

Стандарт	Год принятия	В ЗАСТАВЕ
RFC 2409 The Internet Key Exchange	1998 (по 2005!)	2000-2018
RFC 7296 The Internet Key Exchange Version 2 (IKEv2)	2005-2014	с 2012
RFC 7383 IKEv2 Message Fragmentation	2014	с 2013
RFC 6290 A Quick Crash Detection Method for IKEv2	2011	с 2014
RFC 6311 High Availability of IKEv2/IPsec	2011	с 2014
RFC 5723 IKEv2 Session Resumption	2010	с 2015
RFC 5685 Redirect Mechanism for the IKEv2	2009	с 2016
RFC 8019 Protecting Internet IKEv2 from DDoS Attacks	2016	с 2016
RFC 4555 IKEv2 Mobility and Multihoming (MOBIKE)	2006	с 2017
RFC 8229 TCP Encapsulation of IKE and IPsec Packets	2017	с 2018
RFC XXXX Postquantum Preshared Keys for IKEv2	готовится	с 2018

БЛАГОДАРИМ ЗА ВНИМАНИЕ

Валерий Смыслов (svan@elvis.ru)

© АО «ЭЛВИС-ПЛЮС», 2019 | elvis.ru