Российское экспертное сообщество в области криптографии и работы в IETF

Смышляев Станислав Витальевич, к.ф.-м.н.,
директор по информационной безопасности

РусКрипто'2018

IETF и российское участие

XVII заседание ТК 26, 26.04.2016

- О важности представительства экспертов ТК 26 в международных профессиональных сообществах разработчиков стандартов.
- В том числе, в IETF.

Цели участия в IETF

- Определение алгоритмов и порядка работы с ними в протоколах в RFC — стандартах одной из основных организаций по стандартизации.
- Обеспечение полноценной совместимости стандартов по протоколам со встраиванием российской криптографии.
- Повышение статуса российских механизмов.

Необходимые условия для возможности использования ГОСТ в международных протоколах

- Собственно международные документы, специфицирующие алгоритмы и параметры.
- Вариабельность алгоритмов и параметров — “crypto agility”.
- Общая архитектура протоколов не должна противоречить российским требованиям по безопасности.

Включение в документы IETF

- Не влечет формальных обязательств по поддержке в ПО.
- Зачастую требуется для фактической совместимости и поддержки (пример: AppStore).
- Открытые стандарты — влечет возможность поддержки в открытых сообществах.
- Необходимо для получения идентификаторов IANA.

Необходимые условия для возможности использования ГОСТ в международных протоколах

- Собственно международные документы, специфицирующие алгоритмы и параметры.
- Вариабельность алгоритмов и параметров — “crypto agility”.
- Общая архитектура протоколов не должна противоречить российским требованиям по безопасности.

Включение в документы IETF

- Не влечет формальных обязательств по поддержке в ПО.
- Зачастую требуется для фактической совместимости и поддержки (пример: AppStore).
- Открытые стандарты — влечет возможность поддержки в открытых сообществах.
- Необходимо для получения идентификаторов IANA.

Состояние в начале 2016 года

Наработки в IETF: предыдущий набор криптографических стандартов (ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001)

- Переводы стандартов: RFC 5830, RFC 5831, RFC 5832.
- Использование российских криптографических стандартов в протоколах: RFC 4357, RFC 4490, RFC 4491, RFC 5933.

Наработки в IETF: новый набор криптографических стандартов (ГОСТ Р 34.11-2012, ГОСТ Р 34.10-2012)

- Переводы стандартов: RFC 6986, RFC 7091.

RFC 7801

Vasily Dolmatov. «GOST R 34.12-2015: Block Cipher “Kuznyechik“».

RFC 7836

Stanislav Smyshlyaev (Ed.), Evgeny Alekseev, Igor Oshkin, Vladimir Popov, Serguei Leontiev, Vladimir Podobaev, Dmitry Belyavsky.
«Guidelines on the Cryptographic Algorithms to Accompany the Usage of Standards GOST R 34.10-2012 and GOST R 34.11-2012».

RFC 8133

Stanislav Smyshlyaev (Ed.), Evgeny Alekseev, Igor Oshkin, Vladimir Popov.
«The Security Evaluated Standardized Password-Authenticated Key Exchange (SESPAKE) Protocol».

RFC 7836

На основе Рекомендаций по стандартизации ТК 26

- «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования»
- «Информационная технология. Криптографическая защита информации. Параметры эллиптических кривых для криптографических алгоритмов и протоколов»
- «Задание параметров скрученных эллиптических кривых Эдвардса в соответствии с ГОСТ Р 34.10-2012»
- «Задание узлов замены блока подстановки алгоритма шифрования ГОСТ 28147-89»

RFC 8133

- Протокол SESPAKE, введенный в Рекомендациях по стандартизации ТК 26 Р 50.1.115-2016, разработан Рабочей группой по сопутствующим криптографическим алгоритмам и протоколам ТК 26.
- Экспертиза в IETF проводилась при участии Йорна-Марка Шмидта — автора требований к протоколам PAKE в CFRG.
- Протокол определен для произвольной эллиптической кривой, хэш-функции и функции HMAC, все приведенные примеры, как и в Рекомендациях ТК 26, в итоговой версии RFC 8133, созданы для ГОСТ Р 34.11-2012, а также HMAC и параметров эллиптических кривых, определенных Рекомендациями по стандартизации ТК 26 Р 50.1.113-2016 (и ранее утвержденным RFC 7836).

Документ CFRG по механизмам смены ключей

- На заседании CFRG на встрече IETF 97 по поручению руководителей CFRG было принято решение о разработке документа CFRG по механизмам смены ключей.
- После доклада на IETF 97 председателями CFRG было решено поручить руководство разработкой документа С.В. Смышляеву.
- К работе были подключены, в том числе:
  - Михир Белларе (University of California);
  - Расс Хассли (Vigil Security);
  - Скотт Флюрер (Cisco);
  - Дэниел Франке (Akamai);
  - Шей Герон (University of Haifa);
  - Дороти Кули (АНБ США);
  - Йоав Нир (Checkpoint);
  - Джим Шаад (August Cellars);
  - Пол Хоффман (ICANN).

CRYPTOPRO

Документ CFRG по механизмам смены ключей

- Кроме прочего, документ определяет механизмы смены ключей, введенные в утвержденном на XX заседании ТК 26 проекте Рекомендаций по стандартизации.
- В рамках IETF 98 руководителями CFRG было организовано отдельное совещание CFRG, посвященное работам по документу, продолжительностью один час.
- Документ в конце 2017 года успешно прошел этап экспертизы со стороны членов совета Crypto Review Panel.
- Документ в феврале 2018 года успешно прошел этап обсуждения в рамках CFRG (RG Last Call).

Важность обсуждения общих архитектурных решений с учетом, в том числе, и российских требований

- Строгие требования к ограничению нагрузки на ключ (пример: NIST, ограничение материала на 3DES до 8 МБ только в 2017 году) — процедуры смены ключей.
- Резервный источник случайности на случай сбоев основного пула (С.В. Смышляев).
- Стратегии развития постквантовой криптографии (Г.Б. Маршалко, С.В. Смышляев).
- Оптимизация работы IPsec (В.А. Смыслов).
- Подходы к работе с PKI (Д.М. Белявский).
- Соответствие протоколов и их модельных версий в обоснованиях — пример с TLS, влияние на разрабатываемые в CFRG PAKE (Е.К. Алексеев).
- Экспертиза документов по криптографии — выработка общих подходов, согласованных с позицией РФ.

CRYPTOPRO

Работы по IPsec (В.А. Смыслов)

- Активное содействие Скотту Флюреру по теме дополнения процесса согласования ключей в IKEv2 симметричными ключами, распределенными по квантовому каналу, документ «Postquantum Preshared Keys for IKEv2» — адаптация IPsec для обеспечения стойкости в случае появления полномасштабного квантового компьютера.
- Работы над документом «Group Key Management using IKEv2», посвященным протоколу управления ключами в группе, сопряженному с IKEv2 — протокол распределения ключей на базе IKE для многоадресной передачи.
- Адаптация IPsec для ресурсоограниченных устройств (IoT).
- В.А. Смыслов: соруководство РГ uta.

Работы в процессе: по линии IPsec (Валерий Смыслов)

RFC 7791

Daniel Migault (Ed.), Valery Smyslov. «Cloning the IKE Security Association in the Internet Key Exchange Protocol Version 2 (IKEv2)»

IPSECME IETF 97, 15 ноября 2016

Доклад Валерия Смыслова «Compact representation of IKEv2 payloads» (draft-smyslov-ipsecme-ikev2-compact).

IPSECME IETF 97, 15 ноября 2016

Доклад Валерия Смыслова «PSS vs PKCS1 v1.5 interop issues».

Работы по CLP (Д.М. Белявский)

- Начата работа над проектом документа по ограничению использования сертификатов (CLP) после инцидента с Google и Symantec.
- Разработка механизмов тонкой настройки доверия к сертификатам от тех или иных УЦ.
- Цель: получить возможность криптографически защищённого отчуждаемого представления списка ограничений.

Crypto Review Panel

CFRG IETF 95 (8 апреля 2016), CFRG IETF 96 (20 июля 2016)

- Объявлено о создании централизованного экспертного совета по криптографии в IETF.
- Цели: квалифицированная экспертиза криптографических механизмов в RFC, единые регламенты и критерии.
- Опасения: усугубление проблем с продвижением рос. криптографии (заблокированный TLS с ГОСТ; трудности с RFC 7836...).
- Отбор на конкурсной основе.
- Требования:
  - Публикации в международных рецензируемых журналах.
  - Авторство в утвержденных стандартах IETF.
  - Широкий опыт в области прикладной криптографии.
  - Опыт экспертизы в области криптографии.
  - Наличие рекомендаций от криптографов с международным признанием.

Crypto Review Panel

CFRG IETF 97 (14 ноября 2016, Сеул)

- Конкурсный отбор завершен, утвержден состав совета.
- Срок полномочий — 2 года.
- Состав:
  - Scott Fluhrer
  - Pierre-Alain Fouque
  - Russ Housley
  - Tibor Jager
  - Yaron Sheffer
  - Stanislav Smyshlyaev
  - Bjoern Tackmann
- Согласовываны принципы экспертизы и порядок работы.
- Начало функционирования совета — декабрь 2016.

Текущий статус экспертного совета IETF по криптографии

- С декабря 2016 года новые проекты документов IETF в области криптографии направляются в экспертный совет.
- Проведены работы по экспертизе 9 документов в области криптографии, поступивших в IETF.
  - „Schnorr NIZK Proof: Non-interactive Zero Knowledge Proof for Discrete Logarithm“;
  - „J-PAKE: Password Authenticated Key Exchange by Juggling“;
  - „ChaCha20 and Poly1305 for IETF Protocols“.
  - „The memory-hard Argon2 password hash and proof-of-work function“;
  - „Hash-Based Signatures“;
  - „SCA Extensions For OpenPGP“;
  - „SM2 Digital Signature Algorithm“;
  - „SM3 Hash function“;
  - „The SM4 Block Cipher Algorithm And Its Modes Of Operations“.

Направления развития российской системы стандартизации

- После принятия CMS с ГОСТ — формировать RFC на замену RFC 4490 (CMS с ГОСТ Р 34.10-2001).
- TLS 1.3 с ГОСТ, TLS 1.2 с ГОСТ в IETF.
- Развитие анализа в современных моделях безопасности.
- Устранение областей отставания (пример: AEAD),
- Требуется формирование RFC по IPsec с ГОСТ — важен AEAD.

Перспективы, задачи

- Постквантовая криптография: алгоритмы и модификации протокольных решений.
- Приложения криптопротоколов: DNSSEC, DPRIVE, ACME.
- Разработка AEAD-режима — MGM.
- Продвижение MGM в IETF, несмотря на трудности из-за CAESAR (запланирован доклад на IETF 102 в Монреале).
- TLS 1.3 и DTLS 1.3 — порядок использования российских алгоритмов.
- IPsec — MGM как возможный путь продвижения.

Итоги

- Полный спектр российских базовых алгоритмов из разработанных в ТК 26 стандартов — в RFC.
- Все основные механизмы и протокольные решения из разработанных ТК 26 Рекомендаций по стандартизации — в RFC.
- Высокие шансы на стандартизацию решений из утвержденного проекта Рекомендаций по стандартизации по сопутствующим алгоритмам для ГОСТ Р 34.12-2015.
- Для TLS 1.3 должна быть возможность как минимум специфицировать российские криптонаборы.
- Российский эксперт в составе Crypto Review Panel.
- Участие в ряде работ, определяющих архитектурные решения.

CRYPTOPRO

Спасибо за внимание!

Вопросы?

- Материалы, вопросы, комментарии:
  - svs@cryptopro.ru