Российская криптография в свободном ПО

OpenSSL, OpenVPN, XMLSec и все-все-все

Дмитрий Белявский
ООО «Криптоком»

Пятнадцатая конференция разработчиков свободных программ
Калуга, 28-30 сентября 2018 года

Кто мы, где мы, куда мы идём - I

- Я - Дмитрий Белявский
- В 2004-2006 годах и с 2018 года работаю в ООО «Криптоком» http://www.cryptocom.ru
- Автор ряда патчей к OpenSSL
- Мейнтейнер проекта gost-engine https://github.com/gost-engine/engine

Кто мы, где мы, куда мы идём -II

- Компания «Криптоком» http://www.cryptocom.ru специализируется на выпуске СКЗИ и широко использует свободное ПО
- Флагманский продукт — СКЗИ «МагПро Криптопакет»
  - OpenSSL
  - OpenVPN
  - Stunnel
- Наши патчи приняты в:
  - OpenSSL
  - XMLSec
  - Несколько Perl-овых модулей
  - Продолжение следует

OpenSSL и gost engine: история

- Gost engine — реализация криптоалгоритмов ГОСТ и сопутствующих стандартов
- В версиях 1.0.* — часть поставки
- Начиная с версии 1.1.0 — отдельный продукт https://github.com/gost-engine/engine

OpenSSL и gost engine: сейчас

- OpenSSL 1.0.2
  - Шифр ГОСТ89, хеш 1994 года, подпись 2001 года
  - Есть патчи: +хеш и подпись 2012
- OpenSSL 1.1.0
  - Шифры ГОСТ89, Магма, Кузнечик, хеши 1994/2012, подпись 2001/2012, TLS, S/MIME.
- OpenSSL 1.1.1
- OpenSSL master
  - В разработке

OpenSSL: в работе

- Новая волна стандартизации
  - X.509 - в процессе
  - CMS - в процессе
  - TLS - выпущены рекомендации
- В разработке: TLS
  - Спецификация: https://tools.ietf.org/html/draft-smyshlyaev-tls12-gost-suites-01
  - Реализация: https://github.com/beldmit/openssl/tree/GOST_TLS_12_2018

OpenSSL: немного про API

- Исторический API
  - SHA_do_something, RSA_do_something, AES_do_something
- Универсальный API
  - EVP_Cipher_op, EVP_Digest_op, EVP_PKEY_CTX_op
  - Плохо ложится MAC
  - X509_op
- Подпись: все алгоритмы равны, но некоторые равнее
  - RSA, EC, DH
  - ГОСТ - только через engine
- По мелочи: списки

Приложения: всякое бывает

- Универсальный API: EVP, X.509...
  - Патч для версии 1.0.2 и младше:
    OPENSSL_config()
  - Патч для версии 1.1.*
    OpenSSL_add_all_algorithms()
    флаг сборки -DOPENSSL_LOAD_CONF
- «Мы знаем про RSA»
  - Шифры и хеши: EVP API
    Init/Update/Final
  - Асимметричные алгоритмы: много специфичных функций
    Пример — библиотека XMLSec

Приложения: свой протокол

- Пример — OpenVPN
  - TLS-подобный handshake
  - Собственный протокол обмена данными

- Решение: вдумчивый анализ кода
  - PRF (pseudo-random function) по ГОСТ
  - MAC по ГОСТ

Приложения: не всё так просто

- cURL https://curl.haxx.se/
  - Опции сборки ./configure --with-ssl --enable-openssl-auto-load-config
  - Не загружаются внешние engine => нет поддержки ГОСТ

- Windfly-openssl http://wildfly.org/
  - Плохо знаем Java
  - Надо добавить ряд констант

Зачем это сообществу?

- Редкие сценарии использования
  - Тестирование механизма engine
  - Баги в математике эллиптических кривых
  - Исчерпание стека в TLS handshake
- Универсальные механизмы
  - Национальную специфику — в отдельные структуры
- Не только криптография
  - Усовершенствованная поддержка Unicode

Вопросы?

Пишите на beldmit@cryptocom.ru