ЭЛВИС-ПЛЮС

Гибридный пост-квантовый обмен ключами в интернет-протоколах

Квантовые компьютеры и современная криптография

ЭЛВИС-ПЛЮС

- Алгоритм **Шора** ([quant-ph/9508027] Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer (arxiv.org))
  - Считается, что представляет практическую угрозу для всех классических алгоритмов с открытым ключом
  - Для практического применения требуется наличие квантового компьютера достаточной размерности (Cryptographically Relevant Quantum Computer - CRQC):
    - число логических кубитов > (1.5 * размер поля)
    - число физических кубитов приблизительно на два порядка больше
- Алгоритм **Гровера** ([quant-ph/9605043] A fast quantum mechanical algorithm for database search (arxiv.org))
  - В настоящее время считается, что не представляет практической угрозы

Практические последствия квантовой угрозы

ЭЛВИС-ПЛЮС

- Атака на конфиденциальность **«Harvest and Decrypt»**: атакующий записывает весь зашифрованный трафик, включая вычисление сеансовых ключей, и расшифровывает его позднее, когда появляются квантовые компьютеры, способные «взломать» вычисление сеансовых ключей
  - Возможно, это уже происходит (Forbes: Leaked NSA Doc Says It Can Collect And Keep Your Encrypted Data As Long As It Takes To Crack It)
- Атаки на аутентификацию в интернет-протоколах неактуальны
  - Оценка реального времени «взлома» – порядка 2 дней для факторизации числа размером 2048 бит и порядка 5 часов для вычисления дискретного логарифма в поле размером 448 бит (Scott Fluhrer: https://mailarchive.ietf.org/arch/msg/ipsec/EC5KPzE4JyuNkgH2N_TmrXCRXaE/ https://mailarchive.ietf.org/arch/msg/ipsec/EuRIUUGYrGro6Yx7n5_big6mK-Q/)

Возможные меры противодействия

ЭЛВИС-ПЛЮС

- Отказ от использования криптографии с открытым ключом при вычислении сеансовых ключей
  - проблемы с масштабированием и отсутствие PFS
- Комбинированные схемы с дополнительным симметричным ключом
  - проблемы с масштабированием
- Квантовое распределение ключей
  - сложная и дорогая инфраструктура, проблемы с размерностью
- Использование пост-квантовых криптографических примитивов при вычислении сеансовых ключей
  - функциональная замена классических криптографических примитивов с открытым ключом для вычисления общего ключа

Проблемы замены примитивов вычисления общего ключа в протоколах на пост-квантовые

ЭЛВИС-ПЛЮС

- Разнообразие пост-квантовых механизмов вычисления общего ключа
  - NIST (Post-Quantum Cryptography | CSRC (nist.gov))
- Недостаточная глубина и широта анализа большинства пост-квантовых механизмов
  - NIST (Post-Quantum Cryptography | CSRC (nist.gov))?
- Использование Key Encapsulation вместо Key Agreement
- Повторное использование ключей (Cryptanalysis of ring-LWE based key exchange with key share reuse (iacr.org))
- Существенно больший размер открытых ключей
  - (EC)DH 64-1024
  - NTRU 699-1138
  - Kyber **(NIST)** 800-1568
  - BIKE 1541-5122
  - HQC 2249-7245
  - FrodoKEM 9616-21520
  - Classic McEliece **(BSI)** 261120-1357824
  - ???? **(ТК26)** ??????-???????

Гибридный пост-квантовый обмен ключами

ЭЛВИС-ПЛЮС

- Гибридный пост-квантовый обмен ключами - метод вычисления общего секрета, при котором используется комбинация классического механизма (EC)DH и одного или нескольких пост-квантовых механизмов вычисления общего секрета, которые комбинируются таким образом, что общий секрет зависит от всех задействованных механизмов (RFC 9370)
  - NIST Post-Quantum Cryptography | CSRC (nist.gov)
  - ETSI TS 103 744 - V1.1.1 - CYBER; Quantum-safe Hybrid Key Exchanges (etsi.org)
- Возможность комбинирования нескольких пост-квантовых механизмов, базирующихся на разных математических принципах (коды исправления ошибок, алгебраические решетки, ~~изогении эллиптических кривых~~) с классическим (EC)DH позволяет снизить риски, связанные с недостаточной глубиной их анализа

Отношение к гибридному пост-квантовому обмену ключами

ЭЛВИС-ПЛЮС

- NSA: “*Even though hybrid solutions may be allowed or required due to protocol standards, product availability, or interoperability requirements, CNSA 2.0 algorithms will become mandatory*” (CSA_CNSA_2.0_ALGORITHMS_.PDF (defense.gov))
- D. J. Bernstein: “*_turn off ECC_ - this is the scary part, since there's a serious risk that the small lattice systems are easier to break than ECC*” (https://mailarchive.ietf.org/arch/msg/cfrg/T3XgKeJr4-PvmPrS5TwVNfW9t_w/)

Проблемы использования гибридного пост-квантового обмена ключами

ЭЛВИС-ПЛЮС

1. Согласование использования гибридного пост-квантового обмена в протоколах
2. Передача нескольких открытых ключей
3. Комбинирование Key Agreement и Key Encapsulation
   - эмуляция Key Agreement через Key Encapsulation
4. Получение общего секрета из отдельные компонентов (**combiner**)
   - XOR
   - Конкатенация
   - Dual-PRF (Practical (Post-Quantum) Key Combiners from One-Wayness and Applications to TLS (iacr.org))
5. Проблема больших открытых ключей
   - DoS атаки
6. Проблема повторного использования ключей
   - IND-CCA2
   - использование преобразования Фудзисаки-Окамото

Варианты применения гибридного пост-квантового обмена ключами в протоколах

ЭЛВИС-ПЛЮС

- **Композитный протокол** – сохраняется формат сообщений и обменов исходного протокола, классический (EC)DH обмен ключами заменяется на комбинированный
  - минимальные изменения в протоколе, существенные изменения в криптобиблиотеках
  - возможные комбинации механизмов жестко заданы
    - как правило гибридный обмен ключами включает в себя (EC)DH и один пост-квантовый механизм
- **Некомпозитный протокол** – исходный протокол модифицируется для возможности дополнительных пост-квантовых обменов ключами помимо классического (EC)DH обмена
  - существенные изменения в формате сообщений и/или обменов протокола, возможные изменения в криптобиблиотеках
  - возможные комбинации механизмов определяются локальной политикой

Гибридный пост-квантовый обмен ключами в интернет-протоколах

ЭЛВИС-ПЛЮС

- SSH:
  - Experimental
  - Amazon, University of Waterloo
  - Первая версия - ноябрь 2022
  - Work in progress
- TLS 1.3:
  - Informational
  - Cisco Systems, University of Waterloo, University of Haifa and Amazon Web Services
  - Первая версия - март 2019
  - Work in progress
- IKEv2:
  - Standard
  - Post-Quantum, Quantum Secret, Cisco Systems, ISARA Corporation, Philips, ELVIS-PLUS
  - Первая версия - июль 2017
  - RFC (2023)

SSH

ЭЛВИС-ПЛЮС

- draft-kampanakis-curdle-ssh-pq-ke - Post-quantum Hybrid Key Exchange in SSH (ietf.org)
- Композитный протокол
- Гибридные обмены:
  - x25519 + kyber512
  - nistp256 + kyber512
- Передача открытых ключей: конкатенация
- Combiner: конкатенация
- Вычисление сеансовых ключей: без изменений
- Размер открытого ключа: TCP-based протокол, размер сообщений ограничен 32 Кбайт, механизмы с ключами большего размера не рассматриваются
- Угроза DoS атак: игнорируется

TLS 1.3

ЭЛВИС-ПЛЮС

- draft-ietf-tls-hybrid-design - Hybrid key exchange in TLS 1.3
- Композитный протокол
- Гибридные обмены:
  - x25519 + kyber768
  - secp384r1 + kyber768
  - x25519 + kyber512
  - secp256r1 + kyber512
- Передача открытых ключей: конкатенация
- Combiner: конкатенация
- Вычисление сеансовых ключей: без изменений
- Размер открытого ключа: TCP-based протокол, размер сообщений с открытым ключом ограничен 64 Кбайт, механизмы с ключами большего размера не рассматриваются
- Угроза DoS атак: игнорируется

IKEv2

ЭЛВИС-ПЛЮС

- RFC 9370 - Multiple Key Exchanges in IKEv2
- Некомпозитный протокол
- Гибридные обмены:
  - до 8 механизмов, без ограничения типов (не обязательно пост-квантовые)
- Передача открытых ключей: в отдельных обменах IKEv2
- Размер открытого ключа: ограничен 64 Кбайт форматом сообщений
  - UDP + IKE Fragmentation (RFC 7383) – до нескольких Кбайт (кроме первого обмена)
  - TCP – до 64 Кбайт
  - TCP + draft-tjhai-ikev2-beyond-64k-limit - Beyond 64KB Limit of IKEv2 Payloads (ietf.org) – до нескольких Мбайт (в теории до 4 Гбайт)
- Угроза DoS атак: учитывается

IKEv2 – начальные обмены при создании IKE SA

ЭЛВИС-ПЛЮС

При создании защищенного соединения используется новый обмен IKE_INTERMEDIATE, посредством которого проводятся дополнительные обмены ключами

```
Initiator                                                                    Responder
-------------------------------------------------------------------------------------
HDR(IKE_SA_INIT), SA, Ni, KEi, N -->                    <-- HDR(IKE_SA_INIT), SA, Nr, KEr, N
HDR(IKE_INTERMEDIATE), SK {KEi(1)} -->                  <-- HDR(IKE_INTERMEDIATE), SK {KEr(1)}
HDR(IKE_INTERMEDIATE), SK {KEi(2)..KEi(2)} --> <-- HDR(IKE_INTERMEDIATE), SK {KEr(2)..KEr(2)}
HDR(IKE_AUTH), SK {IDi, AUTH, TSi, TSr} -->       <-- HDR(IKE_AUTH), SK {IDr, AUTH, TSi, TSr}
```

где, например:

KE	- ECDH
KE(1)	- Kyber
KE(2)	- Classic McEliece

IKEv2 – ключи IKE SA

ЭЛВИС-ПЛЮС

После каждого дополнительного обмена ключами происходит обновление текущих ключей IKE SA:

```
SKEYSEED(n) = prf(SK_d(n-1), KE(n) | Ni | Nr)

{SK_d(n) | SK_ai(n) | SK_ar(n) | SK_ei(n) | SK_er(n) | SK_pi(n) | SK_pr(n)} =
prf+ (SKEYSEED(n), Ni | Nr | SPIi | SPIr)
```

Ключи SK_*, полученные после последнего промежуточного обмена, используются как сеансовые ключи IKE SA

Combiner: итеративное применение prf

IKEv2 – аутентификация IKE SA

ЭЛВИС-ПЛЮС

Дополнительные обмены учитываются при аутентификации IKE SA в соответствии с RFC 9242:

```
InitiatorSignedOctets = RealMsg1 | Nr | prf(SK_pi, IDi) | IntAuth
ResponderSignedOctets = RealMsg2 | Ni | prf(SK_pr, IDr) | IntAuth

IntAuth = IntAuth_iN | IntAuth_rN | IKE_AUTH_MID

IntAuth_i1 = prf(SK_pi1, IntAuth_i1A [| IntAuth_i1P])
IntAuth_i2 = prf(SK_pi2, IntAuth_i1 | IntAuth_i2A [| IntAuth_i2P])
IntAuth_i3 = prf(SK_pi3, IntAuth_i2 | IntAuth_i3A [| IntAuth_i3P]) ...
IntAuth_iN = prf(SK_piN, IntAuth_iN-1 | IntAuth_iNA [| IntAuth_iNP])

IntAuth_r1 = prf(SK_pr1, IntAuth_r1A [| IntAuth_r1P])
IntAuth_r2 = prf(SK_pr2, IntAuth_r1 | IntAuth_r2A [| IntAuth_r2P])
IntAuth_r3 = prf(SK_pr3, IntAuth_r2 | IntAuth_r3A [| IntAuth_r3P]) ...
IntAuth_rN = prf(SK_prN, IntAuth_rN-1 | IntAuth_rNA [| IntAuth_rNP])
```

где

`IntAuth_[i/r](n)A` ~ AAD n-го сообщения

`IntAuth_[i/r](n)P` ~ содержимое n-го сообщения до его зашифрования

`IKE_AUTH_MID` - MID первого обмена IKE_AUTH

IKEv2 – создание IPsec SA / обновление ключей

ЭЛВИС-ПЛЮС

При создании защищенных соединений IPsec или обновлении ключей IPSec SA / IKE SA используется новый обмен IKE_FOLLOWUP_KE, посредством которого проводятся дополнительные обмены ключами

```
Initiator                                                                    Responder
-------------------------------------------------------------------------------------
HDR(CREATE_CHILD_SA), SK {SA, Ni, KEi} -->       <--  HDR(CREATE_CHILD_SA), SK {SA, Nr, KEr }

HDR(IKE_FOLLOOWUP_KE), SK {KEi(1)} -->                <-- HDR(IKE_FOLLOOWUP_KE), SK {KEr(1)}

HDR(IKE_FOLLOOWUP_KE), SK {KEi(2)..KEi(2)} --> <-- HDR(IKE_FOLLOOWUP_KE), SK {KEr(2)..KEr(2)}
```

где, например:

KE	- ECDH
KE(1)	- Kyber
KE(2)	- Classic McEliece

IKEv2 –ключи IPsec SA / обновление ключей

ЭЛВИС-ПЛЮС

При создании дополнительных IPsec SA или при обновлении ключей IPsec SA:

```
KEYMAT = prf+ (SK_d, KE(0) | Ni | Nr | KE(1) |  ... KE(n))
```

При обновлении ключей IKE SA:

```
SKEYSEED = prf (SK_d, KE(0) | Ni | Nr | KE(1) | ... KE(n))
```

Combiner: конкатенация

Практические реализации

ЭЛВИС-ПЛЮС

ЭЛВИС-ПЛЮС: ЗАСТАВА 8

- включает в себя возможность комбинирования нескольких обменов ключами в соответствии с RFC 9370
- без фиксации конкретных пост-квантовых механизмов, для тестов использовались:
  - библиотека liboqs
  - библиотека PQLR компании QApp
- продукт сертифицируется

ЭЛВИС-ПЛЮС

Благодарю за внимание!

Смыслов Валерий Анатольевич

svan@elvis.ru
+7 (495) 276-0211