Petro Davydov

Рев'ю на тему:

Проектування та валідація квантової системи управління ключами для побудови квантового криптографічного зв'язку KREONET

1. Вступ

Автори статті**:**

Kyu-Seok Shim - науковий співробітник з докторською степеню, KISTI, Daejeon, Korea

Yong-hwan Kim - старший дослідник, KISTI, Korea

IlKwon Sohn - старший дослідник, KISTI, Daejeon, Korea

Eunjoo Lee - науковий співробітник з докторською степеню, KISTI, Daejeon, Korea

Kwang-il Bae - старший дослідник, KISTI, Daejeon, Korea

Wonhyuk Lee - головний дослідник, KISTI, Daejeon, Korea

Стаття присвячена розробці та валідації Quantum Key Management System (QKMS) - системи управління квантовими ключами, яка має забезпечити фізичний рівень безпеки для наступного покоління комунікаційної мережі KREONET**.**

Питання яке досліджувалося в цій праці, це - чи можливо створити масштабовану, стандартизовану та інтегровану систему управління квантовими ключами, яка буде сумісна з існуючими протоколами (наприклад, IPsec) і чи буде вона працювати в реальному середовищі національної дослідницької мережі?

Ціль яку переслідували дослідники спроектувати QKMS, яка відповідає архітектурі KREONET.

Провести симуляцію та валідацію QKMS у декілька етапів.

Забезпечити інтеграцію з протоколами безпеки.

Підготувати систему до реального впровадження у національну інфраструктуру.

Корисне посилання для вивчення: https://kreonet.net/eng/.

2. Методологія

У дослідженні застосовано поетапний підхід до проектування та валідації QKMS, який охоплює чотири послідовні фази. Методологія базується на симуляціях, моделюванні інтерфейсів, структурному аналізі компонентів, а також на валідації взаємодії з протоколами безпеки (взято як приклад IPsec).

Етап 1 - Архітектура інтерфейсів

- ✓ Розроблено структуру взаємодії між QKD-модулями, QKMS та передавальним обладнанням.
- ✓ Інтерфейси спроектовано згідно зі стандартами ETSI та ITU-T.

Етап 2 - Моделювання управління мережею

- ✓ QKMS розділено на чотири рівні: керування мережею, керування обладнанням, QKD-рівень, транспортний рівень.
- ✓ Визначено ролі компонентів, події (Alarm, Fault, Run), показники продуктивності та структуру бази даних.

Етап 3 - Гетерогенна структура управління ключами

- ✓ Впроваджено розділення об'єктів QKD та QKMS згідно зі стандартом TTA.
- ✓ Розроблено структуру «relay-mode» для передачі ключів через довірені вузли.
- ✓ Проведено симуляцію з використанням M101 повідомлень, OTP-KEY та QKMS логіки.

Етап 4 - Інтеграція з IPsec

- ✓ Валідація взаємодії QKMS з IKEv2 протоколом.
- ✓ Ініціатор отримує ключ через GetKey, передає Key-ID у nonce.
- ✓ Респондент виконує GetKeyWithID, обидві сторони конфігурують SAD з однаковим ключем.

Методи збору даних

- ➢ Логи ініціатора та респондента IPsec.
- ➢ Вивід QKMS-модуля (Master/Slave).
- ➢ Візуалізація relay-процесів та SAD конфігурацій.

Основна увага в дослідженні приділяється функціональній валідації, синхронізації ключів та сумісності пов'язаній з інтерфейсами(можемо сказати інтерфейсна сумісність).

3. Результати

У результаті поетапної валідації було підтверджено, що запропонована архітектура QKMS відповідає вимогам до безпечного розподілу квантових ключів у національній дослідницькій мережі KREONET. Основні результати охоплюють симуляцію, функціональну інтеграцію з IPsec, а також виявлення критичних точок для подальшого вдосконалення.

Етап 1 - «Інтерфейсна модель»

- Визначено структуру взаємодії між QKD, QKMS і передавальним обладнанням.
- Інтерфейси були сумісні зі стандартами ETSI/ITU-T.
- Встановлено канали для управління ключами та передачі даних.

Етап 2 - Мережева модель

- Успішно реалізовано багаторівневу структуру QKMS.
- Визначено ролі компонентів, події та показники продуктивності.
- Побудовано модель бази даних для зберігання ключів і логів.

Етап 3 - Relay-mode симуляція

- Relay-вузол отримав, дешифрував і передав ключ через OTP-KEY.
- Master і Slave QKMS підтвердили однакові ключі через GetKey та GetKeyWithID.
- Всі пристрої отримали синхронізовані ключі.

Етап 4 - Інтеграція з IPsec

- Ініціатор отримав ключ через GetKey, передав Key-ID у nonce.
- Респондент виконав GetKeyWithID, отримав той самий ключ.
- SAD був сконфігурований на обох сторонах, тунель IPsec успішно встановлено.
- Логи підтвердили отримання ключа, конфігурацію SA та завершення сесії.

Також у одній з таблиць наведено приклад виявлення проблем кодування, розмірів ключів, UUID, хешування, CLI/GUI, та запропоновано рішення, що до використання в цьому випадку Base64, SHA2, REST, генерацію UUID з KDK-Pair-ID.

4. Ключові інсайти

1. *Інтеграція QKMS з IPsec через IKEv2 nonce*

Чому важливо: Це дозволяє використовувати квантові ключі в існуючих VPN-протоколах без зміни базової архітектури.

Користь: Можна адаптувати до корпоративних тунелів без втрати сумісності.

2. *Relay-mode передача ключів через довірені вузли*

Чому важливо: Забезпечує багатоступеневу передачу ключів у великих мережах.

Користь: Можна моделювати захищені маршрути в розподілених інфраструктурах.

3. *Використання OTP-KEY для шифрування ключових повідомлень*

Чому важливо: OTP забезпечує криптографічну безпеку.

Користь: Можна застосувати для критичних повідомлень у системах управління.

4. *Генерація UUID з KDK-Pair-ID для унікальної ідентифікації ключів*

Чому важливо: Уникнення конфліктів між гетерогенними пристроями.

Користь: Можна стандартизувати ідентифікацію ключів у мультидоменних системах.

5. *Використання SHA2 для хешування UUID згідно RFC4122*

Чому важливо: Забезпечує криптографічну стійкість.

Користь: Можна інтегрувати в системи перевірки автентичності ключів.

6. *Модульна структура QKMS з чітким розділенням шарів*

Чому важливо: Полегшує масштабування та обслуговування.

Користь: Можна адаптувати до різних типів мереж, від локальних до глобальних.

7. *Симуляція QKMS перед фізичним впровадженням*

Чому важливо: Дозволяє виявити помилки до виробництва.

Користь: Можна створити тестові середовища для перевірки безпеки.

8. *CLI/GUI інтероперабельність через JSON/REST*

Чому важливо: Забезпечує гнучкість для адміністраторів і розробників.

Користь: Можна інтегрувати в DevOps-процеси та CI/CD пайплайни.

9. *Валідація через логи IPsec ініціатора та респондента*

Чому важливо: Підтверджує реальну роботу системи.

Користь: Можна використовувати для аудиту та моніторингу безпеки.

10. *Визначення чотирьох типів інтерфейсів для управління*

Чому важливо: Стандартизує взаємодію між компонентами.

Користь: Можна створити шаблони для інтеграції з іншими системами.

5. Висновок

Наукова публікація «*Проектування та валідація квантової системи управління ключами для побудови квантового криптографічного зв'язку KREONET*» - є важливим внеском у розвиток квантово-захищених комунікаційних систем. Автори які працюють у, або з KISTI використали та продемонстрували системний підхід до проектування, моделювання та валідації QKMS, який відповідає вимогам національної дослідницької мережі KREONET.

Основні внески дослідження які можна відмітити, це:

- Створення багаторівневої архітектури QKMS з *чітким* розділенням функцій.
- Інтеграція з існуючими протоколами безпеки, наприклад IPsec через IKEv2.
- Розробка relay-mode логіки для передачі ключів через довірені вузли.
- Визначення критичних точок для вдосконалення, зокрема UUID, хешування, інтерфейси.

Ми бачимо, що квантова криптографія може бути інтегрована в реальні інфраструктури без порушення існуючих стандартів. Вона також відкриває перспективи для подальших досліджень у напрямку:

- Впровадження QKMS у фізичні пристрої.
- Розширення підтримки протоколів безпеки.
- Створення тестових середовищ для перевірки стійкості до атак у квантовому середовищі.

У сфері кібербезпеки ця робота є джерелом практичних рішень, які можна адаптувати до сучасних викликів починаючи з захисту VPN до побудови квантово-захищених мереж.

*подальші розділи є спробою розширити горизонти досліджень у напрямку використання знань здобутих у цьому розділі.

6. Модулі з HackTheBox

Після ретельного аналізу, включно з використанням AI, доступних навчальних матеріалів HackTheBox, *не було знайдено спеціалізованих модулів*, присвячених *Quantum Key Management System (QKMS) або Quantum Key Distribution (QKD)***.** Проте, існують загальні модулі, які охоплюють *IPsec*, що є частиною інтеграції, описаної в публікації.

Корисні модулі:

1. *Introduction to Networking* - базове розуміння VPN, тунелювання, обміну ключами.
2. *VPN Enumeration & Exploitation* - охоплює IPsec, IKE, SA, ESP, що прямо пов'язано з інтеграцією QKMS у IPsec.
3. *IKEv2/IPsec VPN Attacks* - практичні вправи з аналізу SA, nonce, та ключових обмінів.

Нажаль, ці *модулі не охоплюють квантову криптографію*, але ***можуть бути використані для моделювання класичних частин інтеграції***, описаної у статті.

Словник

QKMS (Quantum Key Management System) - Система управління квантовими ключами, яка забезпечує генерацію, розподіл, зберігання та валідацію ключів у квантово-захищених мережах.

QKD (Quantum Key Distribution) - Метод розподілу криптографічних ключів, що базується на принципах квантової механіки, з гарантією виявлення перехоплення.

KREONET - Корейська національна дослідницька мережа, яка використовується для наукових комунікацій і тестування нових технологій.

IKEv2 (Internet Key Exchange version 2) - Протокол для встановлення захищених з’єднань у IPsec, який підтримує обмін ключами та автентифікацію.

IPsec (Internet Protocol Security) - Набір протоколів для захисту IP-комунікацій через шифрування та автентифікацію.

SAD (Security Association Database) - База даних, яка зберігає параметри безпеки, включаючи ключі, алгоритми та час життя сесії.

SPD (Security Policy Database) - База даних, яка визначає політики безпеки для вхідного та вихідного трафіку.

Nonce - Одноразове випадкове число, яке використовується для запобігання повторним атакам у криптографічних протоколах.

UUID (Universally Unique Identifier) - Унікальний ідентифікатор, який використовується для маркування ключів, пристроїв або сесій.

SHA2 / MD5 - Хеш-алгоритми, які використовуються для генерації цифрових відбитків даних або UUID.

OTP-KEY (One-Time Pad Key) - Ключ, який використовується один раз і забезпечує ідеальну криптографічну безпеку.

Relay-mode - Модель передачі ключів через довірені вузли, яка дозволяє масштабування у великих мережах.

Інтероперабельність - Здатність різних систем, пристроїв або програмного забезпечення ефективно взаємодіяти між собою без потреби в додаткових адоптаціях. У контексті QKMS це забезпечує узгоджену роботу між QKD, передавальним обладнанням та протоколами безпеки.

Стандарти ETSI та ITU-T - Міжнародні технічні стандарти, що регулюють телекомунікаційні протоколи, інтерфейси та безпеку. *ETSI* (Європейський інститут стандартів зв'язку) і *ITU-T* (Міжнародний союз електрозв'язку) використовуються для узгодження архітектури QKMS з глобальними нормами.

Стандарт TTA - Корейський національний стандарт, який визначає технічні вимоги до телекомунікаційних систем. У QKMS він застосовується для розділення об'єктів QKD і KMS та побудови гетерогенної структури управління ключами.

M101 повідомлення - тип повідомлення, що використовується в моделі relay-mode для передачі ключів між QKMS через довірені вузли. Воно містить зашифровану інформацію про ключ, що передається через OTP-KEY.