Quantum-safe 마이그레이션 과정 및 적용사례

https://youtu.be/HNwKaEvS-tc

IT융합공학부 송경주

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

참고 문서

- ETSI, “Quantum Safe Cryptography; Case Studies and Deployment Scenarios” [internet], https://www.etsi.org/deliver/etsi_gr/qsc/001_099/003/01.01.01_60/gr_qsc003v010101p.pdf

- ETSI, “CYBER; Migration strategies and recommendations to Quantum Safe schemes” [internet], https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf

- 두 문서를 참고하여 발표를 준비하였습니다.

Quantum-safe 마이그레이션 과정 및 적용사례

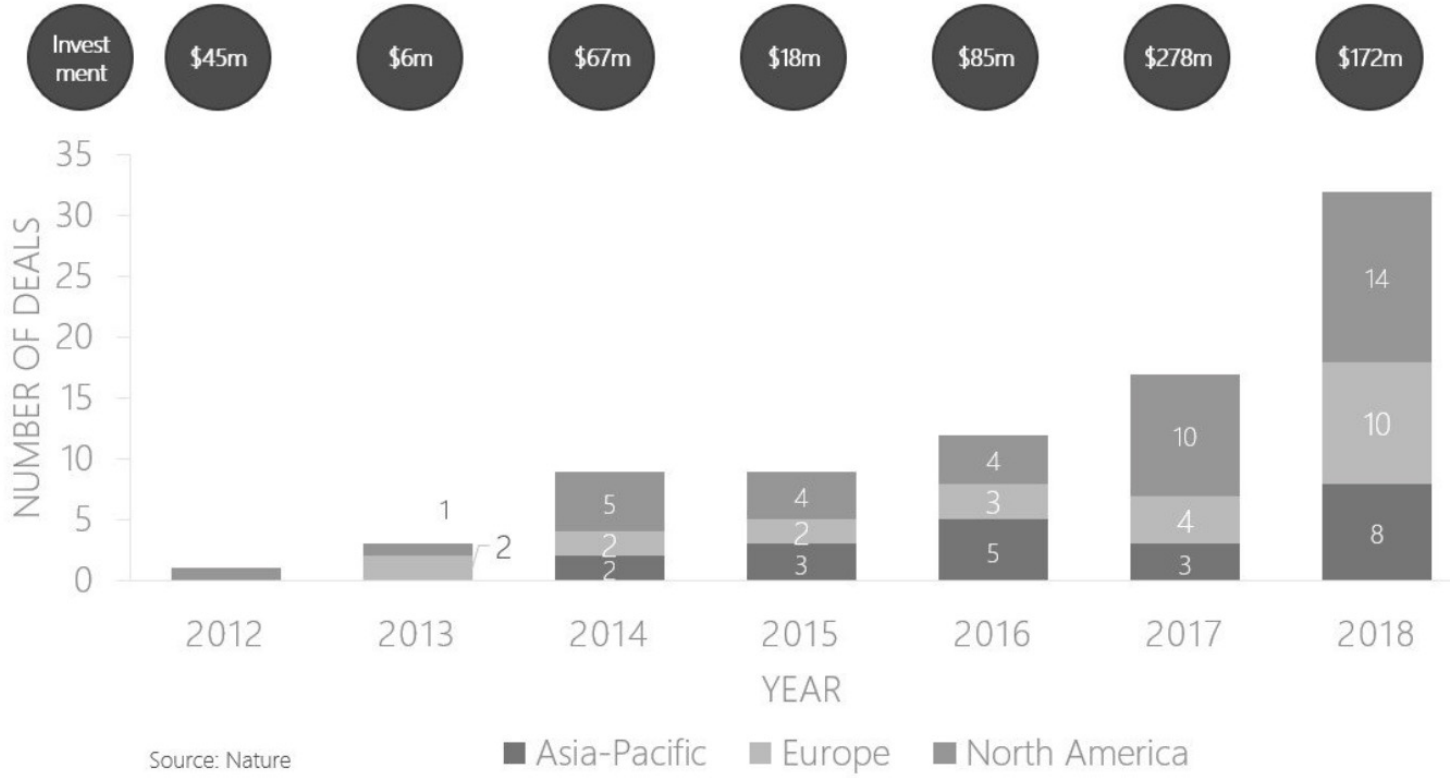
- 정보화 시대로 바뀌면서 데이터들이 클라우드 및 데이터 베이스 등에 전자적으로 저장되어 관리되고 있음
  → 이에 따라 암호화의 중요성은 더욱 커짐

- 양자컴퓨터는 암호의 특정 수학적 문제 해결에 효율성을 가진다는 것이 입증됨 (공개키 암호: Shor's algorithm, 대칭키 암호: Grover's algorithm)

  - 하지만 현재 소형 양자 컴퓨터로 암호화 문제를 해결하기는 어려움 (다항시간 내에 동작 불가, 자원부족)
  - 그러므로 현재의 소형 양자 컴퓨터는 아직 보안에 위협이 되지 않지만 향후 대규모 양자 컴퓨터 개발 시 보안에 위협이 됨

Quantum-safe 마이그레이션 과정 및 적용사례

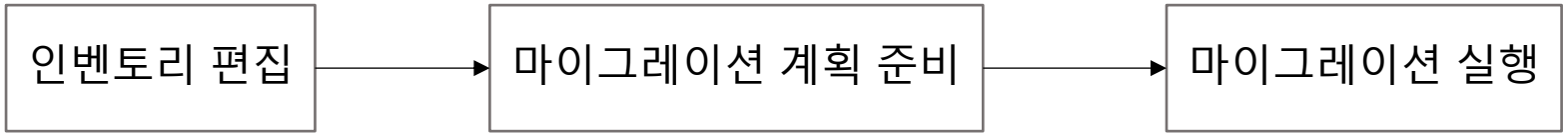
- 최근 양자컴퓨터는 개발이 빠르게 진행되고 있음
- 국제적인 기업들 및 각 정부는 양자 컴퓨터 연구에 집중하고 있으며 투자 경향으로 이를 확인할 수 있음



빠른속도로 증가되고 있는 양자 컴퓨터 투자 경향 (2018년까지만 나타났지만 그 이후로도 빠르게 상승했을 것이라 예상 가능)

Quantum-safe cryptography(QSC) 마이그레이션 과정

- Non quantum-safe한 상태에서 Fully Quantum Safe Cryptographic State(FQSCS) 환경으로 마이그레이션이 필요함
  → 여기서 마이그레이션은 non-QSC에서 QSC로 전환하는데 필요한 일련의 프로세스, 절차 및 기술을 의미
- Non-QSC에서 QSC로 전환하기 위해서는 정해진 절차와 절차에 따른 고려사항을 따라야 함



<3단계 마이그레이션 plan>

1) 단계 - 인벤토리 편집(Inventory compilation)

- 먼저, 시스템에서 암호화 자산 및 프로세스를 식별함 (여기서 자산은 하드웨어or 소프트웨어)
- 마이그레이션 대상의 암호화를 제공하는 엔티티 및 기능을 선별
- 인벤토리에서 식별된 많은 자산에 대한 신뢰 관리 및 자격증명 관리 프레임워크가 필요
- 신뢰에 의존하는 엔티티(조직의 통제 밖의 것 의미)는 자산에 대한 신뢰 기반 식별이 포함되어야 함

Quantum-safe cryptography(QSC) 마이그레이션 과정

2) 단계 - 마이그레이션 계획 작성(Creation of the migration plan)

공개키 및 대칭키 암호로 암호화된 자산은 각각 마이그레이션 이후에도 동일한 방식으로 암호화 됨

[1단계-인벤토리 편집]를 완료해야 [2단계-마이그레이션 계획 작성] 진행 가능

- 마이그레이션 계획에 포함되어야 하는 것 : 자산의 전체 목록, 각 자산에 대한 정보 (즉. 지정된 자산이 마이그레이션 되는지의 여부를 포함해야 함)

- 마이그레이션 계획 시 고려사항

1. PKI의 엔티티 기능 및 제한사항 고려 – quantum safe는 더 큰 공개키 및 서명을 포함하므로 QSC를 처리할 수 없는 경우 교체
2. Quantum safe 암호로 업그레이드 된 PKI에 quantum safe 서명이 포함된 새로운 인증서 필요
3. PKI 업그레이드와 이에 의존하는 응용프로그램 업그레이드 간의 상호작용 고려
4. PKI의 업데이트 된 엔티티에 대한 cryptographic agility(암호 민첩성) 고려 – 추후 quantum safe 알고리즘의 취약점이 발견되면 다른 quantum safe 알고리즘으로 완전히 전환하거나 매개변수 강도를 수정하여 취약점 해결 가능

Quantum-safe cryptography(QSC) 마이그레이션 과정

- 마이그레이션 중 키 관리

키 관리는 모든 암호화 응용프로그램의 중요한 요소, 마이그레이션 중 키 관리도 중요함

- Key Management System (KMS)은 다양한 형식으로 배포될 수 있으므로 x.509를 사용한다고 가정
- Quantum Safe 알고리즘에 해당 알고리즘 ID가 있고 CA가 public key 인코딩 방법을 알고 있는 경우 최종 엔티티 인증서의 Subject Key Info 필드에 Quantum Safe 공개 키를 쉽게 포함 시킬 수 있음

- 마이그레이션 중 신뢰 관리

- 1단계에서 식별한 것을 따라 신뢰 infrastructure을 식별함
- 신뢰 및 키 관리 infrastructure의 역할과 관계는 변하지 않지만 기술 작업을 수행하는 수단이 변경될 수 있음

- 마이그레이션 중 격리 접근 관리

모든 시스템이 동시에 업데이트 되는 것이 아니므로 가능한 한 하위 시스템은 개별 보안 도메인으로 격리해야 함 → 보안 도메인은 Quantum safe VPN과 같은 Quantum safe 경로를 통해 상호 연결 가능

Quantum-safe cryptography(QSC) 마이그레이션 과정

- 마이그레이션 후 non-QSC 보호 리소스에 대한 액세스

이전에 암호화된 자산을 quantum-safe 상태로 마이그레이션하는 것이 경제적으로 불가능할 경우가 있음, 이러한 경우 외부 공격으로부터 방어하기 위해 QSC가 아닌 리소스를 격리하는 단계가 포함됨

→ 마이그레이션되지 않은 모든 non-QSC 보호 자산은 격리 영역으로 물리적으로 이동되고 격리 영역 내에서 위험이 관리됨

- 비즈니스 프로세스 요구사항

1. 마이그레이션 관리자 지정
   - 전체 비즈니스/조직에 대한 지식이 있는 마이그레이션 실행을 담당하는 단일 관리자를 지정해야 함
   - 마이그레이션의 각 이해관계자는 자신의 역할에 대해 인식하고 브리핑 받을 수 있어야 함
2. 마이그레이션을 위한 예산 할당
   - 마이그레이션할 자산을 식별하는 작업에서 3)단계- 마이그레이션 실행 예산(시간, 재정, 시설) 확인
3. “down time” 관리
   - 개발할 때 조직의 일부를 폐쇄하거나 일시 중지해야 할 수 있으므로 이것이 가능한지 승인 여부 확인

Quantum-safe cryptography(QSC) 마이그레이션 과정

3) 단계 – 마이그레이션 실행

1,2) 단계에서 계획한 것을 구현하는 단계

- Mitigation(완화) 관리

계획의 실행 가능성을 결정하기 위해 마이그레이션을 시뮬레이션하고 테스트 수행

→누락된 인벤토리 요소를 발견할 수 있으므로 중요한 단계

- 비즈니스 프로세스 요구사항
  1. 마이그레이션 관리자가 프로세스를 주도하고 책임져야 함
  2. 마이그레이션 관리자는 재정 및 조직적 지원을 받아야 함
  3. 마이그레이션 관리자는 마이그레이션 계획 단계의 중간에서 중단하면 안됨

Quantum-safe cryptography(QSC) 실제 사례

- **사례 1. Network security protocols**

두 대상이 네트워크를 통해 안전하고 인증된 통신 링크를 설정하려고 할 때, 한쪽 혹은 양쪽은 통신하고자 하는 상대방의 Public Key Infrastructure(PKI)에서 서명된 인증서를 얻는 방식

(*PKI : 통신 상대의 ID와 공개키가 포함됨)

- 하지만 대부분의 공개키를 기반으로 한 통신은 대규모 양자컴퓨터에 의해 취약해질 수 있음

- 그 결과 양자에 안전한(quantum-safe) 공개키 기반 handshake protocol에 대한 연구가 집중되고 있음

- 인증서의 유효성 및 신원을 확인한 후, 공개키 기반의 handshake protocol을 사용하여 두 대상만 알고 있는 secret session key을 설정하고 이후 통신을 암호화 하는데 사용함

Quantum-safe cryptography(QSC) 실제 사례

<TLS cryptography>

: 키 설정 및 인증 서비스를 위해 PKI가 지원하는 공개 키 암호를 광범위하게 사용함 (e.g. 인수분해, RSA, DH, DSA, ECDH ECDSA) → quantum-safe를 위해 이러한 [기본 요소 (e.g)] 를 업그레이드 해야함

- TLS가 널리 사용되기 때문에 현재 PKC (Public Key Cryptographic) 프로토콜에 안전하고 효율적인 quantum-safe 한 최신 [기본 요소]를 배포해야 함

- TLS는 공개키 암호 뿐만 아니라 대칭키 암호도 사용함 (데이터 암호화: AES, 디지털 서명 및 인증서 확인: SHA)

but ! 대칭키 암호는 block size나 key 길이를 늘려 quantum-safe로 쉽게 바꿀 수 있으므로 공개키에 초점을 맞춤

- 양자 내성을 적용한 방법으로 Drop-in replacement, Hybrid scheme, Re-engineering 등이 있음

Quantum-safe cryptography(QSC) 실제 사례

- **사례 2. Internet of Things**

: Internet of Things(IoT)은 "스마트 개체"의 연결성의 증가를 의미함(e.g 전구, 스위치 등 장치들이 로컬 무선 네트워크를 형성)

<IoT cryptography>

: IoT 네트워크의 전반적인 보안을 개선하기 위해 PKC(공개 키 암호화)를 배포하려는 노력이 있음

→ IoT는 리소스 제한이 많아 PKC기반이 적합하지 않음

Quantum-safe cryptography(QSC) 실제 사례

- **사례 3. Authentication(인증)**

< 요구사항 및 적용 사례>

- Internet-based application 인증

: 많이 사용되는 ECDSA 및 RSA 서명을 quantum safe drop in replacement로 전환하는 방법이 있음

- 오프라인 파일 인증

: 중요한 정보가 포함된 파일은 오랜 기간 동안 원본으로 유지해야하므로 이 경우에도 ECDSA 및 RSA 서명을 quantum safe drop in replacement로 전환하는 방법이 적합 → 속도 및 대역폭 요구사항이 온라인보다 프리하므로 hash-tree 서명이 잠재적 대안으로 제안됨

- broadcast 통신 인증

: 명확히 사용한 사례는 자동차 및 운송 인프라가 주변 엔티티에서 데이터를 broadcast하는 V2X가 있음

→ 초당 최대 10회 전송되는 서명과 최대 2회의 공개 키 인증서를 권장하며 이러한 요구사항을 만족하는 우수한 quantum safe drop in replacement PKC는 없지만 HFE를 기반으로 하는 짧은 서명이 유망해 보임

Q & A