포스트 양자(post-Quantum) 보안을 위해 지금 준비

(2021.12.28., 양자정보연구지원센터)

□ 미, 기존 암호화 방식 깨는 양자 컴퓨터 등장 대비

○ 많은 암호화 방법 해독할 강력한 양자컴퓨터 등장에 대비

- 양자 방어(Quantum-proof) 보안 추구 목표
- 국립표준기술원(NIST)이 양자 방어 암호화 알고리즘 초기 표준 발표 예정(2022년)
- 국토안보부(DHS)는 기업이 새로운 표준 채택하도록 준비 도움 지원

○ 양자 위험 예측

- 양자 컴퓨팅의 발전은 디지털 통신에서 신용카드 결제까지 암호화 위협, DHS는 양자 방어 암호화로 긴 전환 과정 예상
- NIST, 양자-내성(Quantum-resistant) 암호화 알고리즘 같은 새로운 암호화 방법 찾기 위해 노력

○ 인식 제고

- 올해 출시된 DHS 로드맵 및 자원은 다가오는 양자 내성 알고리즘 전환 준비를 돕기 위함
- 고전 암호화에 대한 양자 컴퓨팅의 위협은 주 정부 우선순위가 높지 않음

○ 지금 계획 세우기

- DHS 지침은 모든 조직이 새로운 표준으로 업데이트해야 할 시스템 및 데이터 세트 평가 시작을 촉구
- 대칭 키 기반 암호화는 고급 양자 컴퓨팅에 강력한 성능 유지하는 반면, 여러 비대칭(또는 공개키) 암호화 시스템은 취약
- 가장 위험하거나 중요하거나 민감한 시스템 같은 우선순위가 가장 높은 시스템을 먼저 전환

ㅇ 공정한 채택은 가능한가

- 주 및 지방 정부가 업데이트할 사항을 확인하면, 민간 소프트웨어 공급업체들이 새로운 암호화 방법을 제품에 통합, 안전한 서비스 제공을 보장하는 것
- 연방 정부는 잠재적 자본 격차 상황 분석, 더 작고 덜 성숙한 플레이어가 제한된 자원을 사용하지 않고 더 큰 플레이어와 함께 양자 저항 암호화로 마이그레이션 하도록 보장
- NIST가 고려하는 알고리즘은 오픈소스이지만, 알고리즘의 구현은 라이선스 또는 특허가 될수 있음

(원문)

1. https://www.govtech.com/computing/state-local-govt-can-prepare-now-for-post-quantum-security