IoT 상에서의 양자 내성 원격 증명 연구 동향

한성대학교 김원웅

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

서론

관련 연구

연구 동향

서론

- **사물 인터넷(Internet of Things. IoT)은 생활 전반에 걸쳐 대중화**

  → 그러나, IoT 디바이스가 손상될 경우 오작동을 일으키거나 생명과 직결된 문제 발생

  → 이 때 IoT 장치의 무결성을 제공하기 위해 **"원격 증명"** 시용

- **기술의 발전**

  1. Shor Algorithm
  2. 양자 컴퓨팅

  → 이를 위해, IoT 디바이스에 대한 **"양자 내성 원격 증명"**을 통해 기존의 프로토콜 대체

서론

- **원격 증명**

  → 장치의 **무결성**을 검증하는 수단

  → 디바이스의 내부 상태(현재 펌웨어, 하드웨어 또는 소프트웨어)에 대한 증거를 다른 사용자에게 전송

- **문제점**

  - RSA 또는 ECC 기반의 비대칭 암호 기법 사용

    → **양자 공격에 대한 취약점** 존재

양자 내성 원격 증명 솔루션 요구

관련 연구

- **원격 증명**
  - 다른 시스템의 플랫폼 **무결성을 검증**하기 위해 사용
  - IoT 상에서, IoT 디바이스의 하드웨어 및 펌웨어가 위변조되었는지 검증하기 위해 사용

    → 리소스가 제한된 IoT 디바이스의 특성상 **경량화 요구**
  - **Challenge-Response 방식** 사용
    - 클라이언트가 서버에 대한 하드웨어 및 소프트웨어 구성을 인증하는 방식

    1. 증명을 시작하기 위해 검증자(Verifier)는 증명자(Prover)에게 챌린지 전송
    2. 증명자는 검증자에게 특정 증명 요청에 따른 대상(펌웨어의 해시 또는 메모리 세그먼트)에 **서명** 후 전송

연구 사례 (1)

- Román et al. [1]
  - RoTMR(Root of Turst for Measurement and Reporting) 기법 제안

    → PUF(Phsically Unclonable Function) + A-ROM(Attestation Read-Only Memory)
  - **해시 기반 디지털 서명** 사용

    → **해시 함수의 단방향성에 의존하기 때문에 양자 저항성 만족**
  - 외부의 비휘발성 메모리에 있는 애플리케이션 코드를 실행하는 마이크로 컨트롤러를 기반으로 하는 IoT 장치를 대상으로 함
  - 디지털 서명에 필요한 비밀키를 장치에 저장하지 않고 PUF를 통해 재구성
  - A-ROM에는 증명 프로토콜이 포함되어 있으며, 내용이 변경될 수 없어 해당 프로토콜이 수정없이 순차적으로 실행될 수 있도록 보장
  - OTS(One-Time Signature) 생성 및 MTS(Many-Time Signature) 검증을 통해 경량 장치에 적합하고 MTS 방식이 검증자 애플리케이션 컨텍스트에 적합

    → OTS 기법으로 (Winternitz One-Time Signature) 기법을 사용하여 수십 밀리초 안에 서명 작업 수행

    → OTS 기법은 다른 양자 내성 솔루션에 비해 작은 서명을 사용하기 때문에 통신 대역폭 측면에서도 효율적

연구 사례 (2)

- Liu et al. [2]
  - 매우 가벼운 일회성 **해시 기반 서명** 작업만을 수행하는 원격 증명 프로토콜 제안

    → **해시 함수의 단방향성에 의존하기 때문에 양자 저항성 만족**
  - 일회성 키를 여러 증명에 사용할 수 있도록 키 재구성 기술 제안
  - 제 3자에 의존하지 않는 다중 해시 기반 서명 방식을 통한 실행 구조 제시
  - **보안 특성**
    - 해시 기반 서명을 통해 무결성과 신뢰성 보장
    - OTS 기반 체계를 통해 DoS 공격에 대한 내성 제공
  - 해시 기반 서명을 사용하므로 클래식 및 양자 내성 요구 사항을 모두 지원

    → 즉, **기존 보안 매개변수를 사용하는 장치에 프로토콜을 배포하는 것이 가능**

연구 사례 (3)

- **Ghosh et al. [3]**
  - IoT 기술의 end-to-end 보안을 유지할 수 있는 **양자 내성 공개 키 서명/검증**을 위한 경량 솔루션 제안
  - **경량 해시 기능을 갖춘 XMSS 체계 기반**
  - Grover 공격에 대한 128비트 사전 이미지 저항성을 제공하는 동시에 IoT 모트에 대한 XMSS 체계의 허용 가능한 성능을 달성하기 위해 XOF(eXtended Output Function) 모드의 Keccak-400 해시함수 사용

    → **양자 보안성 달성 및 IoT 보안을 위한 적합한 XMSS 매개변수 선택**
  - 리소스가 제한된 IoT 모트에서의 경량 XMSS 방식을 구현하기 위해 지연 시간이 최적화된 HW-SW 하이브리드 아키텍쳐 제공

참고문헌

- [1] Román, Roberto, Rosario Arjona, and Iluminada Baturone. "A lightweight remote attestation using PUFs and hash-based signatures for low-end IoT devices." Future Generation Computer Systems (2023).
- [2] Liu, Xiruo, Rafael Misoczki, and Manoj R. Sastry. "Remote attestation for low-end prover devices with post-quantum capabilities." Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy. 2018.
- [3] Ghosh, Santosh, Rafael Misoczki, and Manoj R. Sastry. "Lightweight post-quantum-secure digital signature approach for IoT motes." Cryptology ePrint Archive (2019).

Q & A