IoT platform security enhancements

IT 보안팀 조성규

2016. 7. 21.

Crypto Lib. 제안 검토

- **제안사항 (Security Platform)**
  - 상세 crypto 수준의 API 가 아닌, 한 단계 추상화된 형태의 API 제공
    - 디바이스 인증 (sign/verify)
    - 파일 암호화, 통신 암호화 (encrypt/decrypt, MAC(keyed hash), sign/verify)
- 개발자들이 실제로 뭘 써야 하는지를 모르는데, encrypt/decrypt, sign/verify 등의 API 도 효용성이 적을 것이라는 내용

Crypto Lib. 제안 검토

- **검토 의견 (SKT)**
  - 전체적인 방향성은 absolutely agree (w/ IoT Tech Lab.)
    - API set (단말인증, 파일/통신 암호화) 도 적절한 것으로 판단됨
    - 사용자 인증은 현재 시스템 환경 및 시나리오 상 불필요한 부분으로 판단됨
  - 단, 상기 3가지 기능에 대한 제약사항 발생
    - Assumption) 서버 쪽 코드는 현재시점에서는 수정하지 않는 방향
    - 따라서 단말 내부에서의 동작(파일 암호화)은 상기 API 에서 가능하나, 서버 코드 수정작업이 필요한 아래 두 개 기능은 현 시점에서는 불가능
      - 단말 인증: 인증서 기반의 단말 인증 사용 시, 이를 서버에서 verification 해야 함
      - 통신 암호화: key management/sharing/agreement 와 관련된 동작, decryption 동작이 서버에서 필요함
    - 따라서, 우선은 애초에 목표했던 encrypt/decrypt, sign/verify, hash, init/revoke 등의 API 를 구성하고
    - 파일 암호화 관련사항은 진행하되, 단말인증/통신암호화는 IoT Tech Lab. 과 8월 중순 이후에 협의 후 진행