IoT platform security enhancements

IT 보안팀 조성규

2016. 6. 23.

Remote attestation

- **주요 이슈**
  - Milestone
    - Toy system (7월초) – toy system 수준? (이후 어떤 step으로 진행할지)
    - GMMP(client) integration (??)
    - ThingPlug(server) integration (??)
- 필요사항

Remote attestation

- **이슈 논의사항**
  - Milestone
    - Toy system 수준은 privacy CA, attestator, attestant 간의 기본적인 통신내용을 확인하는 수준
      - 즉, 실제 tpm에서 연산하는 각 measurements 의 데이터 등 단말 사이드에서의 실 데이터는 아님
      - 단말 사이드에서의 실 데이터는 현 단계 이후에 진행 예정
  - 기타사항
    - privacy CA 와 attestator 의 보안성(DDoS 등) 에 대해서는 현 시점에서 논외
    - GMMP integration 을 위한 필요사항은 현 단계 이후에 추가 논의 예정

HW Crypto Lib

- **주요 이슈**
  - (Not a scope of this project) Authorization
  - Key type (binding keys for symmetric key, signature keys for asymmetric key) : But is signature key valid? How can the server trust it?
  - Key spec
  - API sets : How to revoke keys?

HW Crypto Lib

- **이슈 논의사항**
  - Key type 에 따른 기본적인 spec. 정의 진행 필요
  - 암호 알고리즘 spec. 정의 진행 필요
  - API spec. 정의 진행 필요