

IoT platform security enhancements

IT 보안팀 조성규
2016. 6. 7.

Goal

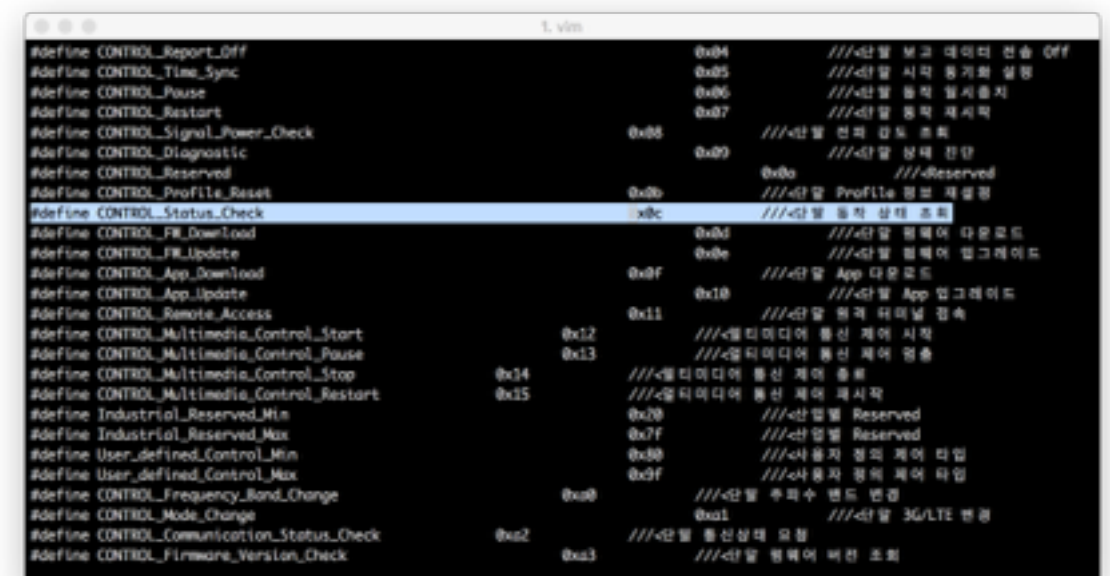
- 과제 목표

- IoT 기기(Hub급)에서 활용할 수 있는 보안기능 - Remote attestation, HW crypto lib.
- ‘특정 조건’을 만족하면 기타 IoT 기기에서 활용할 수 있는 ‘이식 가능한 형태’의 산출물 일체
 - HW 요구사항 - HW 설계사양, TPM (가격, version 등)
 - SW 조건 - 필요한 코드 (부트로더, 커널 등)
 - 각각의 요구조건에 대한 상세한 가이드(소스코드, 라이브러리 및 API documentation) 일체를 thing plug 홈페이지에 게시

Discussions

- Remote attestation

- ThingPlug 의 하나의 spec. 으로 활용 예정
- (CLIENT) 상태 점검(CONTROL_Status_Check) :TPM 모듈 장착 및 정상 동작 여부 확인 후, measurement list 를 서버로 전송
- (SERVER) 검증 작업 후, 이상유무를 DB에 timestamp 와 함께 기록



```
#define CONTROL_Report_Off 0x04 ///<안정 보고 데이터 전송 Off
#define CONTROL_Time_Sync 0x05 ///<안정 시작 동기화 설정
#define CONTROL_Pause 0x06 ///<안정 동작 일시중지
#define CONTROL_Restart 0x07 ///<안정 동작 재시작
#define CONTROL_Signal_Power_Check 0x08 ///<안정 전파 강도 조회
#define CONTROL_Diagnostic 0x09 ///<안정 상태 진단
#define CONTROL_Reserved 0x0a ///Reserved
#define CONTROL_Profile_Reset 0x0b ///<안정 Profile 정보 재설정
#define CONTROL_Status_Check 0x0c ///<안정 동작 상태 조회
#define CONTROL_FW_Download 0x0d ///<안정 펌웨어 다운로드
#define CONTROL_FW_Update 0x0e ///<안정 펌웨어 업그레이드
#define CONTROL_App_Download 0x0f ///<안정 App 다운로드
#define CONTROL_App_Update 0x10 ///<안정 App 업그레이드
#define CONTROL_Remote_Access 0x11 ///<안정 원격 제어 연결
#define CONTROL_Multimedia_Control_Start 0x12 ///<멀티미디어 통신 제어 시작
#define CONTROL_Multimedia_Control_Pause 0x13 ///<멀티미디어 통신 제어 일시중지
#define CONTROL_Multimedia_Control_Stop 0x14 ///<멀티미디어 통신 제어 종료
#define CONTROL_Multimedia_Control_Restart 0x15 ///<멀티미디어 통신 제어 재시작
#define Industrial_Reserved_Min 0x20 ///<산업용 Reserved
#define Industrial_Reserved_Max 0x7f ///<산업용 Reserved
#define User_defined_Control_Min 0x80 ///<사용자 정의 제어 다입
#define User_defined_Control_Max 0xff ///<사용자 정의 제어 다입
#define CONTROL_Frequency_Band_Change 0x80 ///<안정 주파수 밴드 변경
#define CONTROL_Mode_Change 0x81 ///<안정 3G/LTE 변경
#define CONTROL_Communication_Status_Check 0x82 ///<안정 통신상태 요청
#define CONTROL_Firmware_Version_Check 0x83 ///<안정 펌웨어 버전 조회
```

Discussions

- Remote attestation
 - (Q) Secure boot의 필요성?
 - (Q) Attestation 주기 설정은 어떻게?
 - (Q) Attestation 항목(libc, kernel, ...)은 무엇으로?
 - (Q) Attestation protocol 과 ThingPlug protocol 간의 조화는 어떻게?
 - (Q) ECC 적용 가능성?

Expecting output

- Remote attestation & HW crypto lib.
 - Library (*.a)
 - Debug mode와 release mode로 나누어서 log 출력 필요 (기기/개인정보 출력 여부 분기 필요)
 - static linking 형태로 구성하여 해당 라이브러리를 다른 어플리케이션에서 쉽게 import 할 수 있는 방안 필요
 - ARM, MIPS 등 대표 instruction set 을 선정하여 해당 컴파일러로 빌드/링크 방법 제공
 - Documentation
 - HW 및 SW 사양 (requirements)
 - system (bootloader 및 kernel 등) 필요사항 및 code snippet
 - Build & compile 방법 (원본 GMMP daemon 과 link)
 - API documentation 및 sample code
 - DEMO
 - Web UI, demo 용 시나리오 및 환경 등

Expecting output

- TPM management(Remote attestation)
 - Private CA
 - 인증서 specification documents
 - 인증서 발급/갱신/폐기 (?)
 - TPM 및 Private CA 연동 tool (CSR exporting tool, CA signing tool, etc.)
 - API documentation 및 sample code (For B2B/B2G target)
 - DEMO
 - Web UI, demo 용 시나리오 및 환경 등

Expecting output

- HW Crypto lib.
 - 3 개의 API set 필요
 - Encrypt/Decrypt
 - Signing/Verify
 - Key generation / revocation
 - 상기 API를 application(executable daemons)에서 호출하여 데이터 보호
 - GMMP 관련 데이터를 실제로 암호/복호화 하여 back-end 서버로 전송하는 sample code
 - 사용자/기기 인증 데이터 등 중요 데이터 보호
 - setkey() 함수에 대한 customization (서버 공개키로 대칭키 암호화 하여 키 전송)