PoC 시스템 사용설명서

시큐리티플랫폼

문서이력		
2016-11-14	초기작성	강호관

1. 개요

본 문서에서 설명하는 PoC 시스템은 일반 사용자에게 Remote Attestation (이하 RA) 관련 기능에 대한 경험을 제공하는 것을 목적으로 한다.

해당 PoC 시스템은 RA 기능의 서버 역할을 담당하며, 클라이언트 역할을 담당할 장치와 소프트웨어는 사용자가 준비해야 한다. 하지만, 모든 장치와 소프트웨어에 대해 RA 기능을 제공하는 것은 불가능하기 때문에, PoC 시스템에서는 적용 범위를 지정된 장치와 소프트웨어로 한정한다. 이는 PoC 시스템의 제한일 뿐, RA 기능 자체의 제한은 아니다.

본 문서에서는 PoC 시스템 구성 및 설치와 관련된 내용은 언급하지 않는다. 해당 내용들은 별도의 문서에서 다룬다.

2. 라즈베리파이(Raspberry Pi) 설정

PoC 시스템과 연동할 클라이언트는 다음의 절차를 따라 준비한다.

1. 라즈비안(Raspbian) 설치
2. TPM 초기화 & 설정
3. RA 용 kernel 설치

각 단계별 상세한 절차는 GMMP_RA_client/misc/README.raspbian.md 파일을 참조한다.

(git repository 기준: remote_attestation_crypto_lib/_src/remote_attestation 디렉터리에서 찾을 수 있음)

해당 내용은 Cryptolib 과제 산출물을 기반으로 하는 것으로, 차이는 PCR 관련 설정 변경에 따른 kernel 이미지 변경뿐이다.

참고로, 라즈비안 설치 후, 라즈베리파이의 최초 부팅 과정에서 SD 카드에 잔여 공간이 있는 경우, 파티션 조정 작업이 진행되면서 재부팅이 진행되는데, 경우에 따라서는 재부팅이 계속될 수도 있다. 이럴 때는 다른 SD 카드를 이용하여 작업 결과를 비교하는 것을 추천한다. 또한, 무선랜 설정이 계속 실패하는 경우, 해당 무선 공유기의 설정에 문제가 없다면, 다른 AP 에 접속해보는 것을 권장한다.

3. 클라이언트 소프트웨어 빌드

장치에서 RA 진행 요청을 진행할 소프트웨어는 다음의 절차를 따라 빌드한다.

1. $ cd GMMP_RA_client
2. $ ./bootstrap
3. $ ./configure
4. $ make

참고로 빌드를 위해서는 다음의 패키지들이 기본적으로 설치되어 있어야 한다.

- ✓ automake
- ✓ libtool
- ✓ libcurl4-openssl-dev

빌드가 정상적으로 마무리되면, 다음의 프로그램들이 생성된다.

- ✓ GMMP_RA_client/src/tp_attestant – RA 클라이언트 프로그램
- ✓ GMMP_RA_client/src/dummy_gw – 샘플 GMMP 스택
- ✓ GMMP_RA_client/src/show_gw – 장치 관련 ThingPlug 정보 조회/출력

해당 프로그램들은 다음과 같은 항목을 가진 설정 파일을 참조하여 시작해야 한다.

- mId_addr – 프로그램이 접속할 서버의 IP 주소
- mId_port – 프로그램이 접속할 서버의 Port 정보 (서비스 고유 정보)
- svc_id – 서비스 ID, 일명 DomainCode (서비스 고유 정보)
- auth_id – 장치 ID, 일명 GWAuthID, 혹은 AuthID (장치 고유 정보)
- mf_id – 제조사 ID, 일명 GWMFID, 혹은 MFID (장치 식별 정보)
- mesg – 주기 보고 데이터로 사용할 문자열 (특별한 의미는 없음)
- log – 프로그램이 생성할 로그 종류 (error, debug, verbose)

위의 항목들에 대한 RA 서비스의 기본 정보는 GMMP_RA_client/src/gw_0001.conf 파일을 참고한다. 단, 관리 UI 를 통해 ThingPlug 에 장치를 추가하는 경우, mf_id 항목은 관리의 편이를 위해 auth_id 항목 정보 앞에 "MF"를 추가한 형태로 고정했다.

ThingPlug 내에서 장치에 대한 고유 정보인 GW_ID 는, 장치가 최초로 register 과정을 거치면서 결정되기 때문에, 프로그램 시작 단계에서 참조하는 설정 파일에 입력해둘 수는 없다.

따라서, ThingPlug 에 등록하지 않은 장치들은 RA 서버의 UI 를 통한 장치 등록 과정을 먼저 거친 후에 클라이언트 프로그램을 실행한다.

4. RA 서버 설정 (일반 사용자)

RA 설정은 UI 를 통하여 이루어지며, 접근 권한에 따라 일반 사용자 작업 메뉴와 관리자 작업 메뉴로 구분된다. 이 단락에서는 일반 사용자 작업 메뉴에 대해 설명한다.

1. UI 는 브라우저로 접속하며, URL 은 다음과 같다.
   A. http://223.39.121.20:8000/
2. ThingPlug 에 장치 등록
   A. 이미 ThingPlug 의 다른 서비스에 등록된 장치는 기존 등록 정보를 삭제해야 한다. 삭제 작업은 해당 서비스에서 정의한 절차를 따른다.
   B. "ThingPlug 에 등록" 메뉴에서 "Register device to ThingPlug" 항목을 이용한다. 여기서 입력하는 "MAC Address"는 실제 MAC 주소나, 이동 전화 번호 형식의 정보면 된다. 해당 정보는 이후 장치에 대한 AuthID 정보로 설정된다. "Add This Device" 버튼을 누르면, 실행 결과는 브라우저 하단의 "Result" 윈도에 표시된다. "201"이 표시되면 성공적으로 등록된 것이다.
   C. 장치 등록만 진행된 경우, GW_ID 정보는 없으며, 해당 장치가 register 과정을 거쳐야만 할당된다. 앞서 설명한 클라이언트 프로그램을 실행하여 GW_ID 정보를 파악한다.
3. RA 대상에 장치 등록
   A. ThingPlug 에 등록된 장치는 "RA 장치 목록" 메뉴에서 "새 장치 등록" 항목을 선택하여 RA 대상으로 등록한다.
      i. Gateway ID – GW_ID 정보 입력
      ii. Device ID – 입력하지 않음 (현재 장치는 게이트웨이 장치)
      iii. PCR Index To RA – 장치에게 요청할 Measurement List 설정 정보
      iv. Firmware Version – 배포 대상 source code 에 해당하는 버전
   B. 등록된 장치에 대한 RA 진행 상황은 "RA 진행 상황" 메뉴에서 확인한다.

i. "RA 검증" 항목은 클라이언트 프로그램이 전달한 정보에 대한 유효성 검사 결과

ii. "NONCE" 항목은 RA 서버가 보냈던 nonce 정보와의 일치 점검 결과

iii. "PCR 해시 값" 항목은 클라이언트 프로그램이 보낸 정보가 RA 서버가 보관하고 있는 정답과 일치하는지 표시

5. RA 서버 설정 (관리자)

RA 서버 UI 는 관리자가 수행할 작업을 지원하기 위한 관리자 mode 를 제공한다.

주의: 해당 mode 에서 수행하는 작업은 RA 진행 전반에 영향을 미치는 것이므로 관련 정보의 배포와 공유에 주의를 기울여야 한다.

- 관리자 mode 로 전환
  - http://223.39.121.20:8000/admin/
  - 접속 정보: skadmin / SKTadmin1!
    - 접속 정보 관련 설정은 별도의 문서(주석으로 입력)를 참조
- 정답지 등록과 제거
  - "PCR 정답지 등록" 메뉴에서 등록
  - "펌웨어 별 PCR 정답 값 등록" 항목을 선택하여 진행
    - 항목별 정보는 GetAnswerbyTPMQuote2 프로그램 실행하여 수집
    - 해당 프로그램은 TPM 이 장착된 Raspberry Pi 에서 실행해야 함
    - Source code 의 위치는 OMP_RA_server/tools/gen_pcr_answer/
  - 등록된 값들은 목록 형태로 표시되며, 함께 표시된 "삭제" 버튼으로 제거
- RA 대상에서 장치 제거
  - 관리자 mode 상태에서 "RA 장치 목록" 메뉴 진입하면 장치 마다 "삭제" 버튼이 표시되며, 이를 이용하여 RA 대상에서 제거 가능
  - RA 대상에서 제거해도 ThingPlug 에서 해당 장치가 RA 서비스와 완전히 분리되는 것은 아니며, 이를 위해서는 "ThingPlug 에 등록" 메뉴의 "Delete device from ThingPlug" 항목을 이용해야 함
    - 해당 항목에서 요구하는 정보 중, "Gateway ID"와 "Auth Key" 정보는 해당 장치가 ThingPlug 에 register 과정을 거쳐야만 존재하는 정보임.