3 마이크로 컨트롤러에서의 안전한 로봇 어플리케이션 수행을 위한 원격증명기술 개발

소속 정보컴퓨터공학부

분과 D

팀명 응답하라 지휘본부

참여학생 강승민, 김의준, 박재선

지도교수 권동현

과제 개요

기존 연구

- TF-M 기반 단일 Root-of-Trust와 부팅 시점의 정적 증거에 의존 다양한 MCU 적용과 런타임 공격 방어에 한계 & TPM 부재 환경에서 활용 어려움
- MITM·Replay 공격에 취약한 DDS 통신

연구의 필요성

- IoT와 로봇 기술에서 MCU는 자율주행·스마트팩토리 등 핵심 시스템을 제어하는 두뇌
- MCU 소프트웨어 변조는 물리적 피해와 인명 사고로 이어질 수 있음
- 연산 능력과 메모리 한계로 강력한 보안 기능 적용이 불가능
- ⇒ 자원 제약 환경에 최적화된 경량 무결성 검증 기술 필요

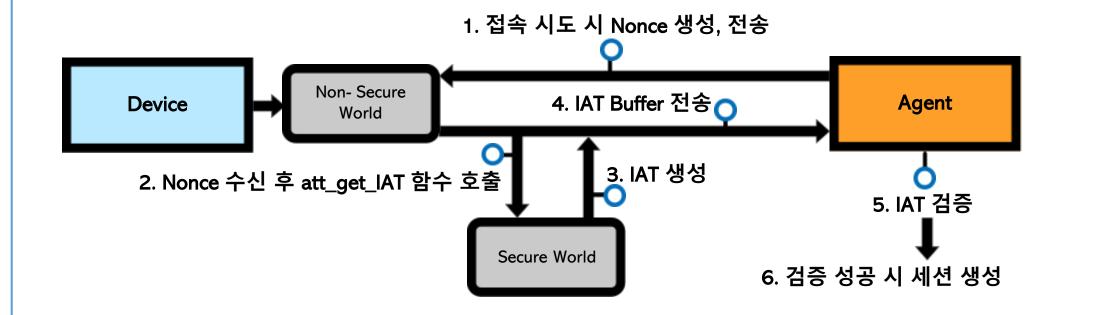
연구 개요

DDS HandShake에 부팅시점 Remote Attestation 추가 Attestation Token 생성 Device Attestation Token 검증 완료 후 HandShake 진행

DICE + MPU TPM이 실용적이지 않거나 실행할 수 없는 환경에서 보안 기능 제공 1. MPU 초기설정 3. 인증서/키 발급 MPU로 코드 보호 -> Evidence 전송 2. Flash 해시 계산 -> CDI 생성 Agent 4. Evidence 검증 5. Token 확인 후 DDS Handshake 진행

TF-M + TrustZone - M

Trusted Firmware 와 TrustedZone을 융합하여 사용



실험 내용

실험 결과 DICE ■ DICE + MPU ■ TF-M + TZ-M Code Size Overhead (Flash Size) Overhead (Latency) 160 350000 140 Overhead 300000 500000 250000 120 250000 400000 200000 100 % Baseline 100 200000 300000 150000 DICE 174 % 150000 200000 100000 100000 DICE + MPU 219 % 100000 50000 20 50000 TF-M + TZ-235 % M nonce 전송 직전까지 검증 Token 수신까지 검증 완료 후 세션생성 Size (Byte) 단위(µs)

