38 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

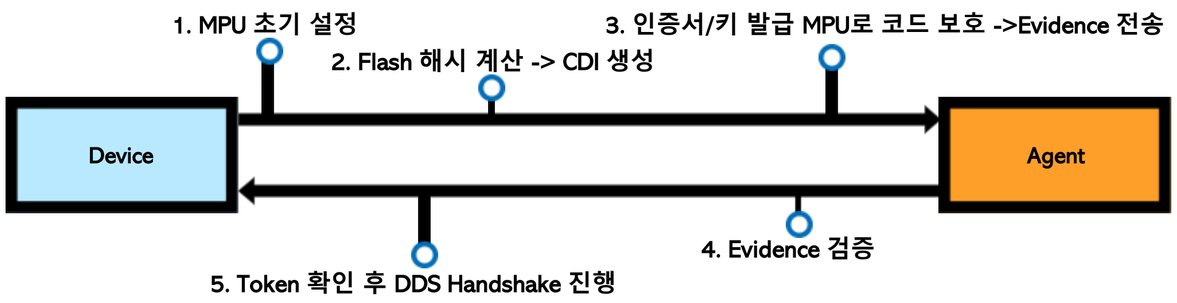
⇒ 자원 제약 환경에 최적화된 경량 무결성 검증 기술 필요

연구 개요

DDS HandShake에 부팅시점 Remote Attestation 추가

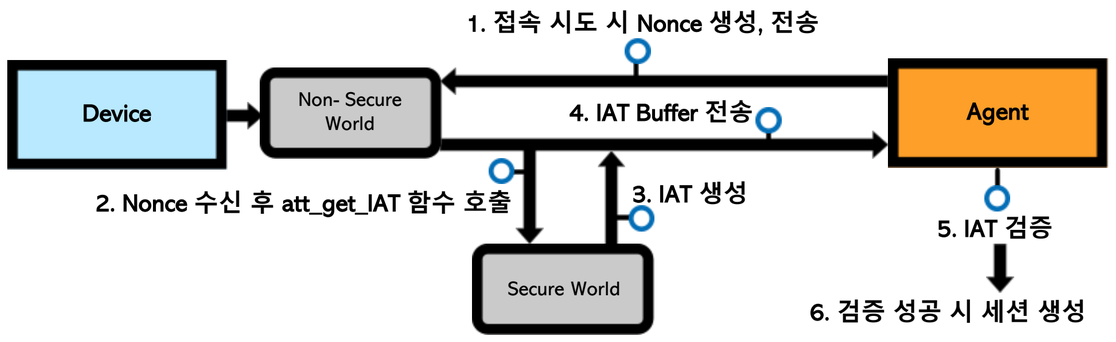
DICE + MPU

TPM이 실용적이지 않거나 실행할 수 없는 환경에서 보안 기능 제공



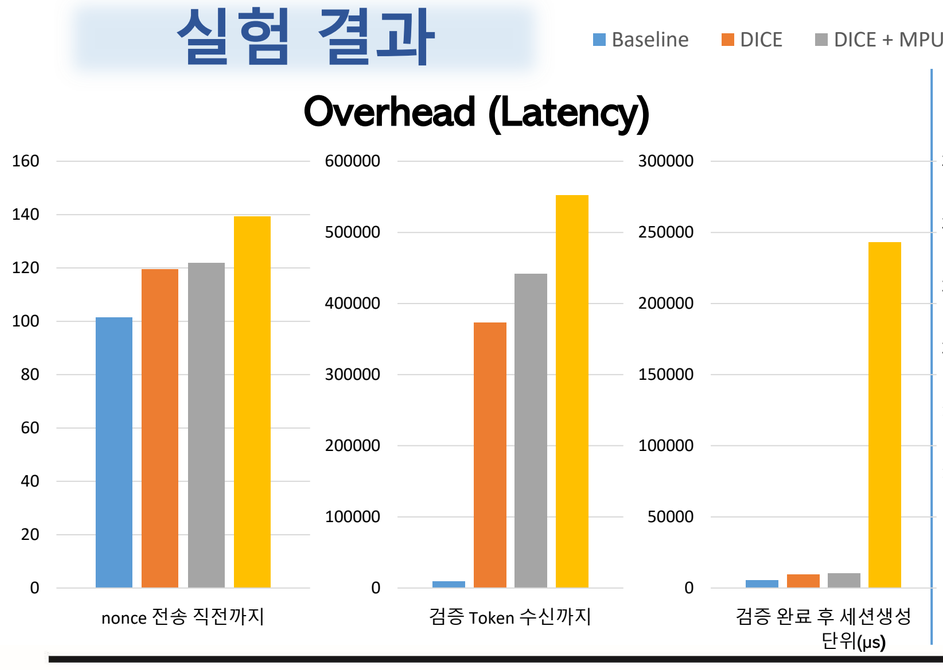
TF-M + TrustZone - M

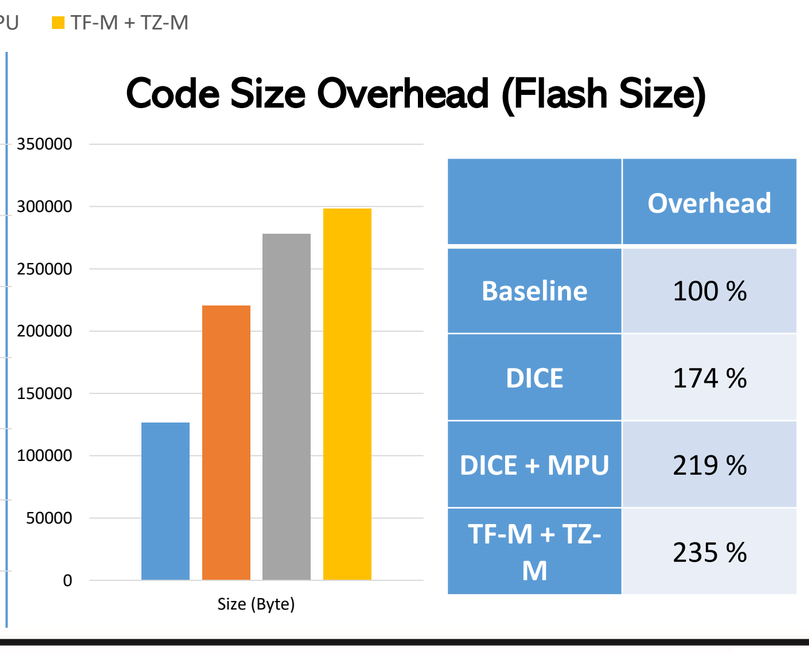
Trusted Firmware 와 TrustedZone을 융합하여 사용



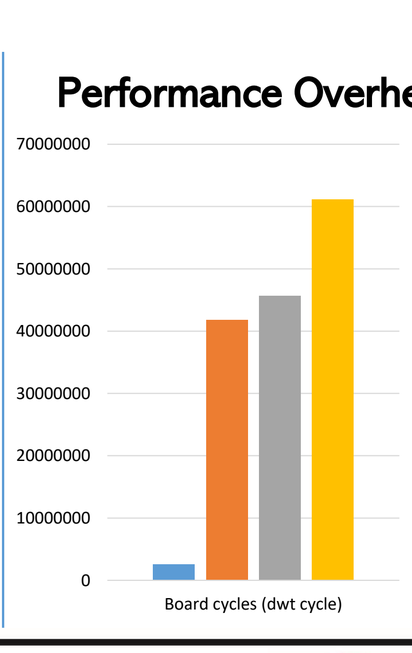
실험 내용

실험 결과





	Overhead
Baseline	100 %
DICE	174 %
DICE + MPU	219 %
TF-M + TZ-M	235 %



	Overhead
Baseline	100 %
DICE	1646 %
DICE + MPU	1799 %
TF-M + TZ-M	2408 %