부산대학교 정보컴퓨터공학부

마이크로 컨트롤러에서의 안전한 로봇 어플리케이션 수행을 위한 원격 증명 기술 개발

2025 전기 졸업과제 중간보고서

202055506 강승민
202055523 김의준
202055543 박재선

2025-7-17

지도 교수 권동현

목차

Ⅰ. 요구조건 및 제약사항 분석에 대한 수정사항

1. 기존 요구 조건

① Remote Attestation 구조 적용 필요

MCU에서 실행 중인 Micro-ROS 노드의 무결성을 원격지에서 검증하고, DDS 통신 연결 여부를 제어할 수 있는 구조가 필요하다[5].

② TF-M 기반 Root-of-Trust 사용

ARM Cortex-M 계열 MCU에서 사용 가능한 TF-M을 신뢰 기반으로 사용하여 부트 시점 및 런타임의 무결성을 증명한다.

③ Flash 영역 중심의 정적 증거 활용

.text, .rodata 등 변경되지 않는 실행 코드 및 데이터 영역의 해시 값을 이용한 무결성 증명을 위주로 한다.

④ 암호화 및 인증 구조 미비한 DDS (XRCE-DDS) 보완 필요

MITM 방지, 인증 토큰 기반 세션 통제를 통해 안전한 통신이 필요하다[2].

2. 요구 조건 수정사항

① Hybrid Root-of-Trust 구조 도입 :

기존 TF-M 단일 구조에서 → DICE + TF-M, TF-M + MPU, TF-M + TrustZone-M 등의 **복수 구성안**으로 확장하여, 다양한 MCU 보드를 포괄할 수 있도록 설계 유연성 확보하였다.

기존 TF-M 중심에서 다음과 같이 **복수 구조로 확장**하며 아래와 같은 구조에서 진행한다.

- DICE (Device Identifier Composition Engine)
- TF-M + MPU (ARMv7-M 기반)
- TF-M + TrustZone-M (ARMv8-M 기반)

② 증거 수집 방식의 세분화 및 확장

기존에는 flash 기반 정적 무결성 정보만을 사용했으나, 향후 ROP/DOP 등 동적 공격에 대응하기 위해 dynamic 및 continuous evidence 구조로 확장을 계획하였다. 가장 주된 목적은 3가지에서의 레이턴시와 메모리 사용량, 그리고 각각의 장단점을 분석하는 것이다.

기존 Flash 기반 정적 증거에서 다음으로 확장하였다.

- **Discrete Evidence**: .text, .rodata (정적/불변)
- **Continuous Evidence**: control-flow, data-flow 추적 (예: ROP, DOP 대응)

③ TPM 없이 동작 가능한 구조 설계

TPM 기반이 아닌 lightweight 구조를 아래와 같이 도입하였다[3].

- DICE: TPM 없이도 Root-of-Trust 기능 제공
- TF-M PSA API를 통한 토큰 생성 (psa_initial_attest_get_token)

④ Micro-ROS 특성 반영 :

네트워크 연결이 불가능한 MCU 보드에서 serial 통신 기반 구조로 대응. 추후 다양한 물리 인터페이스에서도 확장 가능한 추상화 구조 설계 고려하여 DDS Agent와의 통신 handshake에 remote attestation token을 포함시키는 구조로 변경한다. 인증과정에 Nonce 기반의 freshness 보장 및, 키-채널-플랫폼 바인딩 추가하였고, 인증된 노드만 DDS 세션 연결이 가능하도록 attestation token 기반 handshake 구조 도입한다.

[Client] → Nonce 요청

[MCU] → Token 생성 (TF-M 또는 DICE 기반)

[Client] → Token 검증 후 DDS 세션 허용

3. 제약 사항 분석

구분	제약 내용	대응 방안
하드웨어	TPM 미탑재 MCU가 대부분	DICE, TF-M 등 소프트웨어 기반 Root-of-Trust 도입
리소스 제한	Flash/RAM/연산 성능 부족	경량 암호화 및 서명 알고리즘 사용, 토큰 크기 최적화
통신 구조	Micro-ROS 네트워크 미지원 보드 존재	Serial 통신 대체 적용
보안 요구	MITM 및 replay 공격에 취약한 XRCE-DDS	인증 토큰 바인딩, 키 채널 플랫폼 통합 검증 적용

검증 오버헤드	실시간 제어 시스템과 보안 검증의 충돌	검증 주기 최적화 및 증거 수집 최소화 설계

4. 유스케이스 (Use cases)

Use Case	**설명**
부팅 시점 무결성 검증 (Discrete Attestation)	부트 시점에 .text, .rodata 영역 해시 생성 후 토큰화 -> DDS handshake 시 전달
연속 무결성 검증 (Continuous Attestation)	런타임 중 control-flow, data-flow trace 기반 증거 수집 → 주기적 토큰 전송
다양한 MCU 구조 적용	DICE만 사용 가능한 저사양 보드부터 TrustZone 지원 보드까지 범용 적용 가능
XRCE-DDS 기반 보안 세션 연결	Nonce 기반 handshake → 인증 성공 시 세션 연결 허용, 실패 시 차단
공식 검증 기반 보안 증명	Tamarin Prover 등을 활용하여 handshake 프로토콜의 기계적 증명 수행 계획

Ⅱ. 설계 상세화 및 변경 내역

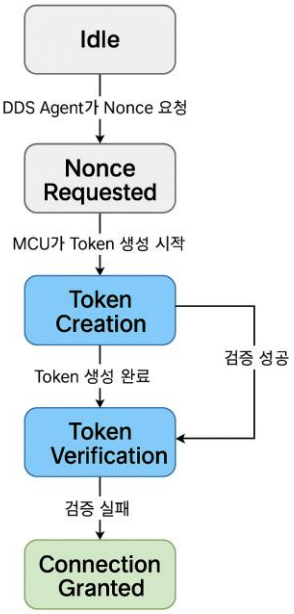
1. 핵심 변경 개요

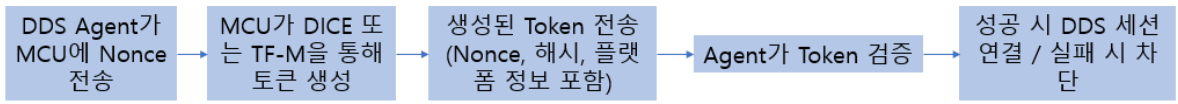
항목	**착수 보고서(기존 설계)**	**중간 보고서(변경 후 설계)**
Root-Of-Trust 방식	TF-M 기반 단일 구조	DICE, TF-M+MPU, TF-M+TZ-M의 복수 구성안 제안
증거 유형	정적 (부팅 시점)	정적 + 연속(런타임) 증거 수집
인증 구조	단순 무결성 검증	Nonce 기반 handshake + 인증된 DDS 세션 연결
통신 방식	Micro-ROS 네트워크 기반	serial 기반 대체 통신 적용
증명 기법 적용 방식	TF-M 직접 호출 및 구조 통합	DICE/TF-M 통합 구현 시나리오 세분화
검증 대상 확장	.text, .rodata 중심	향후 .data, .bss, control/data-flow 포함 고려

2. 설계 구조 변경 요약

- 기존 설계 흐름 (부트 시점 단일 무결성 검증 구조) :

- 변경된 설계 흐름 (XRCE-DDS 통합 handshake 구조) :





-> 토큰에는 **디바이스 식별 정보, 부트 해시, 인증 서명** 등이 포함되어 있다.

-> 키-채널-플랫폼 바인딩을 통해 보안성을 강화한다.

3. 세부 구성 요소별 변경 사항

항목	변경 전	변경 후
Token 생성	TF-M 내부 구조 직접 구현	psa_initial_attest_get_token() API 활용, DICE 사용 가능성 열림
통신 모듈	micro-ROS WiFi 또는 Ethernet 기반	보드에 따라 Serial (UART) 통신 기반으로 전환
보안 프로토콜 적용	DDS Security 외부 연계 미고려	XRCE-DDS 내부 handshake 구조 통합 설계

실험 비교 대상	TF-M 기반 단일 방식	DICE / TF-M + MPU / TF-M + TZ-M 성능 비교 실험 계획 포함
Formal Verification	적용 고려 없음	Tamarin Prover 등 모델링 검증 도구 활용 계획 포함

4. 설계 시나리오별 적응 전략

적용 설계안	보드 종류	특징
DICE	TrustZone MCU가 아닌 보드	경량 MCU (ARM Cortex-M3)
TF-M + MPU	ARMv7-M(MPU 지원)	보안 격리는 없지만 접근 제어 가능
TF-M + TZ-M	ARMv8 (TrustZone 지원)	Secure/Non-Secure 분리, 고보안

5. 핵심 설계 목표

과제의 설계 방향은 다음의 세 가지 Root-of-Trust 구조에 대한 독립적 실현과, 그 구조들이 부팅 시점 Remote Attestation에 어떻게 적용될 수 있는지를 정량적으로 비교하는 것이다.

구조 유형	설명
DICE 기반	TPM이 없는 MCU 환경에서 디바이스 고유 정보 기반으로 증명 수행
TF-M + MPU	ARMv7-M 기반, Memory Protection Unit을 활용한 영역 보호 가능
TF-M + TrustZone-M	ARMv8-M 기반, Secure/Non-secure 실행 환경 분리로 높은 보안성 제공

각 구조는 동일한 attestation 시나리오를 바탕으로 설계되며, 부팅 시점 단일 펌웨어 무결성 검증을 수행한 뒤, DDS (XRCE-DDS) handshake에 통합되어 신뢰 기반 세션 연결을 제어하게 된다.

6. Control-Flow Integrity(CFI) 적용 방향

본 과제는 부팅 시점 무결성 검증에 중점을 두어 향후 런타임 CFI 확장 가능성을 고려하여 코드 구조를 유연하게 설계하였다. 현재는 lightweight firmware attestation을 중심으로, 추후 data-flow/control-flow trace 수집 기반 구조로의 확장 가능성을 기술적 옵션으로 남긴다[1].

Ⅲ. 갱신된 과제 추진 계획

1. 추진 방향의 명확화

본 과제의 추진 계획은 다음의 세 가지 핵심 흐름을 중심으로 재정비되었다:

① 부팅 시점 단일 펌웨어 무결성 검증 구조 구현
→ 시스템이 ROS 네트워크에 연결되기 전, 단 한 번의 attestation 으로 신뢰를 검증하는 구조 설계를 한다.

② 세 가지 Root-of-Trust 구조에 대한 독립적 구현
→ 각 구조마다 개별 MCU 보드에 적합한 attestation 환경을 구축한다.
→ 비교 대상:

DICE 기반 구조

TF-M + MPU (ARMv7-M)

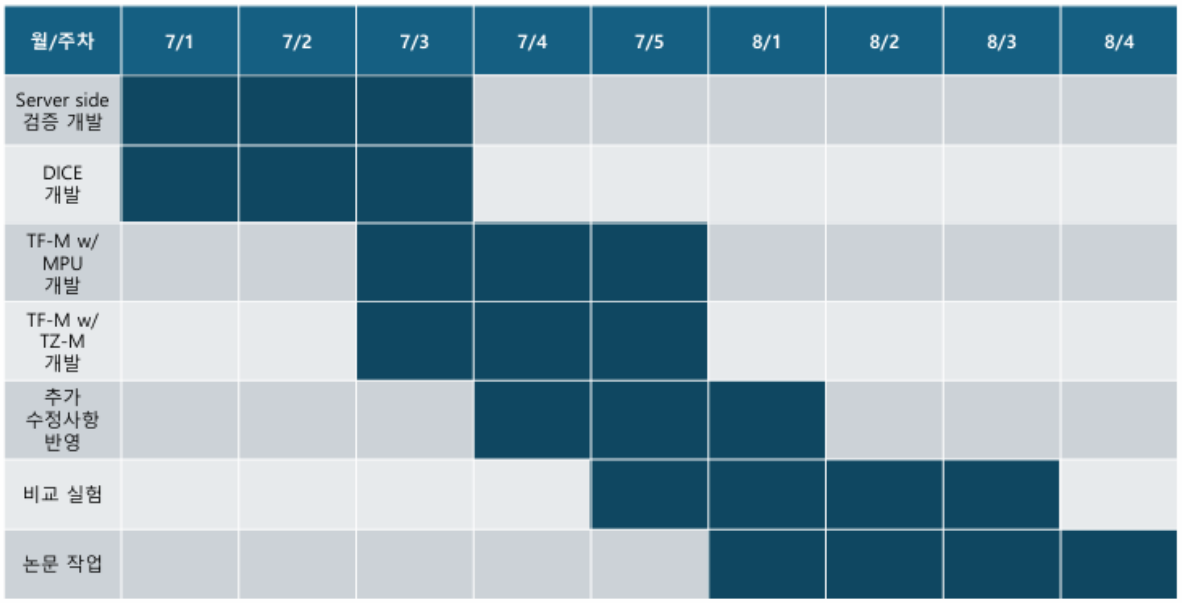
TF-M + TrustZone-M (ARMv8-M)

③ 구조별 비교 실험 및 정량적 분석
→ latency, flash 메모리 소비량 측정한다.
→ 각 구조의 장단점 기술 및 적합성 비교한다.

2. 추후 CFI(Control-Flow Integrity) 적용 방향

- 기존에는 런타임 연속 무결성 검증을 목표로 했으나, 현시점에서 자원 제약과 현실적 구현 범위를 고려해 Control-Flow Integrity (CFI)를 제외한 부팅 시점 무결성 검증으로 방향을 수정함.
- 향후 확장 계획으로 CFI 기반 lightweight runtime extension 또는 event-driven integrity checks 에 대한 가능성은 남겨둠.

3. 재정비된 과제 수행 일정



4. 핵심 실험 및 평가 항목

평가 요소	목적
Latency	각 구조에서 attestation token 생성 및 검증까지 걸리는 시간 측정
Memory Usage (Flash / RAM)	보안 모듈이 MCU 자원에 미치는 영향 평가
구조별 장단점 분석	기능성, 이식성, 보안성, 개발 난이도 등 종합적인 비교

5. 최종 산출 목표

- XRCE-DDS handshake에 부팅 시점 Remote Attestation 통합

- 세 가지 구조에 대한 성능 및 보안 분석 보고서 작성

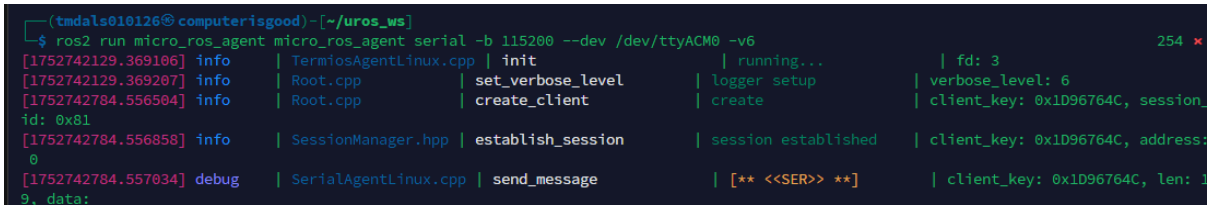
- 최종적으로 세가지 구조와 관련해서 속도와 보안성을 비교한 논문을 작성해 학회에 투고

IV. 구성원별 진척도

이름	구성원별 진척도
강승민	zephyr RTOS와 Micro-ROS 개발 환경 구축 및 TF-M 기반 검증 token 생성 개발
김의준	ROS2 와 Micro-ROS 통합 개발 환경 구축 및 서버측 검증 코드 개발
박재선	zephyr RTOS와 Micro-ROS 통합 개발 환경 구축 및 DICE 기반 검증 token 생성 개발

V. 보고 시점까지의 과제 수행 내용 및 중간 결과

- Tytan, DDS Security+, SMART 등 관련 선행 연구를 분석하여 기반 지식을 구축함[1-5].
- MCU 기반 RTOS 를 조사하고 실습 환경을 구축하여 관련 기술에 대한 이해도를 높임
- DICE, Trusted Firmware-M, TrustZone-M 을 조사하고 실제 코드를 분석하여 동작 원리를 파악함. 라이브러리 기반의 구현도 가능함.
- ROS2 의 통신 구조를 이해하고, 이를 검증하기 위한 코드를 직접 구현할 수 있음.
- 실험을 위한 개발 환경 구성을 마치고, 세 가지 방식의 차이를 비교할 수 있는 템플릿을 완성함.



그림은 같이 Micro-ROS 와 zephyr 를 통합하여 ROS2 agent 와 연결한 모습.

- 자문의견서를 바탕으로 검토한 결과 런타임 무결성을 확보하기 위해 성능을 희생하는 접근보다는 다양한 무결성 검증 방식을 비교·분석하는 것이 보다 실용적이고 의미 있는 방향이라고 판단하였습니다. 이에 따라 과제의 목표를 일부 조정하였음.

VI. Reference

[1] BRASSER, Ferdinand, et al. TyTAN: Tiny trust anchor for tiny devices. In: *Proceedings of the 52nd annual design automation conference*. 2015. p. 1-6.

[2] WAGNER, Paul Georg; BIRNSTILL, Pascal; BEYERER, Jürgen. Dds security+: Enhancing the data distribution service with tpm-based remote attestation. In: *Proceedings of the 19th International Conference on Availability, Reliability and Security*. 2024. p. 1-11.

[3] ELDEFRAWY, Karim, et al. Smart: secure and minimal architecture for (establishing dynamic) root of trust. In: *Ndss*. 2012. p. 1-15.

[4] WANG, Qian; LEE, Brian; QIAO, Yuansong. Support Remote Attestation for Decentralized Robot Operating System (ROS) using Trusted Execution Environment. In: *2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2024. p. 693-695.

[5] DENG, Gelei, et al. On the (in) security of secure ros2. In: *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*. 2022. p. 739-753.