하드웨어를 이용한 자동차 보호 기법 연구

최진명[1], 마틴[2], 백윤흥[3]
[1,2]서울대학교 전기정보공학부 석박사과정
[3]서울대학교 전기정보공학부 교수
jmchoi@sor.snu.ac.kr, kayondo@sor.snu.ac.kr, yhpaek@snu.ac.kr

A Study on Automotive Protection Techniques Using Hardware

Jinmyung Choi[1], Martin Kayondo[2], Yunheung Paek[3]
[1]Dept. of Electrical and Computer Engineering and Inter-University Semiconductor Research Center(ISRC), Seoul National University

요 약

본 연구는 현대 자동차 산업에서 급증하는 사이버 보안 위협에 대응하기 위한 하드웨어 기반 보호 기법들을 종합적으로 분석한다. 특히 하드웨어 보안 모듈(HSM), 신뢰 플랫폼 모듈(TPM), 그리고 ARM TrustZone 기술에 초점을 맞추어, 이들의 기본 개념, 특징, 그리고 자동차 보안 시스템에서의 적용 사례를 살펴본다.

1. 서론

현대 사회에서 자동차 산업은 급속도로 발전하고 있으며, 이는 우리의 일상생활과 경제 전반에 지대한 영향을 미치고 있다. 특히 최근 들어 테슬라와 같은 기업들이 선보이는 자율주행 기술은 자동차 산업의 새로운 지평을 열어가고 있다. 이러한 기술의 발전은 운전자의 편의성과 안전성을 크게 향상시키는 한편, 예상치 못한 새로운 위험 요소들도 함께 대두되고 있다.

자동차 기술이 더욱 복잡해지고 전자화됨에 따라, 사이버 보안 위협 또한 증가하고 있다. 최근 들어 해커들의 자동차 시스템 침입 사례가 빈번히 보고되고 있으며[ref], 이는 단순한 데이터 유출을 넘어 운전자와 탑승자의 생명을 위협할 수 있는 심각한 문제로 대두되고 있다. 예를 들어, 원격으로 자동차의 제동 시스템을 조작하거나 엔진을 정지시키는 등의 공격이 실제로 발생하고 있어, 자동차 보안의 중요성이 그 어느 때보다 강조되고 있다.

이러한 위협에 대응하기 위해, 자동차 산업계와 관련 기관들은 다양한 보안 기술과 표준을 개발하고 있다. 특히 주목할 만한 것은 국제표준화기구(ISO)에서 제정한 ISO 21434 표준이다. 이 표준은 자동차 사이버 보안에 관한 지침을 제공하며, 특히 위협 분석 및 위험 평가(TARA, Threat Analysis and Risk Assessment)를 자동차 개발 과정에 필수적으로 포함시키도록 요구하고 있다. 이는 설계 단계에서부터 보안을 고려하는 "Security by Design" 원칙을 자동차 산업에 적용하는 중요한 이정표가 되고 있다.

본 연구에서는 이러한 배경을 바탕으로, 하드웨어를 이용한 다양한 자동차 보호 기법들을 소개하고 분석하고자 한다. 하드웨어 기반의 보안 솔루션은 소프트웨어 기반의 방식에 비해 더욱 견고하고 신뢰성 있는 보안을 제공할 수 있다는 장점이 있다[11]. 특히 본 논문에서는 다음과 같은 하드웨어들을 중점적으로 다룰 예정이다:

하드웨어 보안 모듈 (HSM, Hardware Security Module), 신뢰 플랫폼 모듈 (TPM, Trusted Platform Module) , ARM TrustZone.

이러한 하드웨어들은 각각 고유한 특성과 장단점을 가지고 있으며, 자동차의 다양한 구성 요소와 시스템에 적용되어 전반적인 보안 수준을 향상시킬 수 있다.

본 논문은 하드웨어를 이용한 자동차 보호 기법에 대한 기술의 작동 원리, 적용 사례, 그리고 향후 발전 방향을 알아보는 것을 목표로 한다.

2. 배경이론

본 섹션에서는 자동차 보안에 활용되는 주요 하드웨어 기반 보안 기술인 하드웨어 보안 모듈(HSM), 신뢰 플랫폼 모듈(TPM), 그리고 ARM TrustZone에 대한 기본적인 개념과 특징을 설명한

다.

2.1 HSM (Hardware Security Module)

하드웨어 보안 모듈(HSM)은 디지털 키를 안전하게 관리하고 암호화 작업을 수행하는 물리적 컴퓨팅 장치이다[1]. HSM은 탬퍼 저항성을 갖추고 있어 물리적 공격에 대한 저항력이 있으며, 장치가 무단으로 열리거나 조작될 경우 저장된 중요 데이터를 자동으로 삭제한다. 또한 암호화 키의 생성, 저장, 백업, 복구 등을 안전하게 수행하며, 대칭키 및 비대칭키 암호화, 해시 함수, 디지털 서명 등의 암호화 작업을 고속으로 처리한다. HSM은 인증된 사용자나 프로세스만이 그 기능을 사용할 수 있도록 엄격한 접근 제어를 제공한다. 자동차 산업에서 HSM은 차량 내 통신의 보안, 펌웨어 업데이트의 무결성 검증, 차량 인증 등 다양한 보안 기능을 제공하는 데 활용된다[2].

2.2 TPM (Trusted Platform Module)

신뢰 플랫폼 모듈(TPM)은 컴퓨터 시스템의 하드웨어 수준에서 보안 기능을 제공하는 전용 마이크로컨트롤러이다[3]. TPM은 시스템에서 사용되는 암호화 키를 안전하게 생성하고 저장하며, 시스템의 현재 상태를 원격지에서 안전하게 확인할 수 있게 하는 원격 검증 기능을 제공한다. 또한 부팅 과정에서 시스템 컴포넌트의 무결성을 측정하고 기록하며, 특정 시스템 상태와 연계하여 데이터를 암호화함으로써 시스템 상태가 변경되면 데이터에 접근할 수 없게 하는 데이터 봉인 기능을 제공한다. 자동차 분야에서 TPM은 차량의 전자제어장치(ECU) 보안, 차량 인증, 안전한 소프트웨어 업데이트 등에 활용될 수 있다[4].

2.3 ARM TrustZone

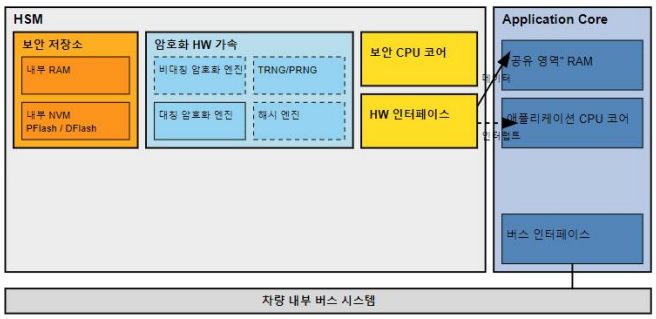
ARM TrustZone은 ARM 프로세서에 내장된 보안 기술로, 하드웨어 수준에서 보안 환경과 일반 환경을 분리하는 기능을 제공한다[5]. TrustZone은 프로세서를 보안 상태와 일반 상태로 분리하여 운영하며, 메모리, 주변장치, 인터럽트 등의 하드웨어 리소스를 보안 상태와 일반 상태 간에 격리한다. 또한 두 상태 간의 전환을 관리하고 제어하는 보안 모니터를 제공하며, 보안이 필요한 애플리케이션을 안전하게 실행할 수 있는 신뢰 실행 환경(TEE, Trusted Execution Environment)을 지원한다. 자동차 산업에서 ARM TrustZone은 인포테인먼트 시스템의 보안, 디지털 키 관리, 보안 부팅 등 다양한 영역에 적용될 수 있다[6].

이러한 하드웨어 기반 보안 기술들은 각각의 특성을 바탕으로 자동차의 다양한 구성 요소와 시스템에 적용되어 전반적인 보안 수준을 향상시키는 데 기여하고 있다.

3. 하드웨어를 이용한 보호 기법

3.1 HSM

현재 자동차에 HSM이 기본적으로 사용되고 있어서 관련된 연구가 많이 진행되었다.[7,8]. EVITA 프로젝트[7]는 자동차 온보드 네트워크의 보안을 강화하기 위해 설계된 유럽의 연구이다. 해당 연구에서 서술한 HSM에 대한 기준을 소개하겠다. 자동차용 HSM의 일반적인 구조는 그림 1에 나타나 있다. 이 구조에서 HSM은 애플리케이션 CPU 코어와 동일한 칩에 위치한다.



<그림 1> 자동차용 HSM의 일반 구조

HSM의 구성 요소는 필수 구성 요소와 선택적 구성 요소로 나뉜다. 이는 사용 사례에 따라 서로 다른 보안 요구사항을 충족해야 하기 때문이다. 그림 1에서 선택적 구성 요소는 점선으로 표시되어 있다. 비용 효율적인 하드웨어 솔루션을 제공하기 위해, 서로 다른 보안 요구를 충족하는 세 가지 EVITA HSM 변형을 명시한다:

FULL HSM: 이 HSM은 V2X 통신의 보안 취약점으로부터 차량 내부 도메인을 보호하는 데 중점을 둔다. 이를 위해 전자 서명의 생성과 검증이 필요하다. 성능 요구사항을 만족시키기 위해 매우 효율적인 비대칭 암호화 엔진이 필요하다. FULL HSM은 모든 HSM 변형 중 최대 수준의 기능성, 보안성, 성능을 제공한다.

MEDIUM HSM: 이 HSM은 차량 내 통신의 보안에 중점을 둔다. 비대칭 암호화 블록과 약간 낮은 성능의 CPU(예: 100MHz 대신 25MHz)를 제외하면 MEDIUM HSM은 FULL HSM과 유사하다. MEDIUM HSM은 하드웨어에 비대칭 암호화 블록이 없지만, 공유 비밀 설정과 같은 시간에 민감하지 않은 일부

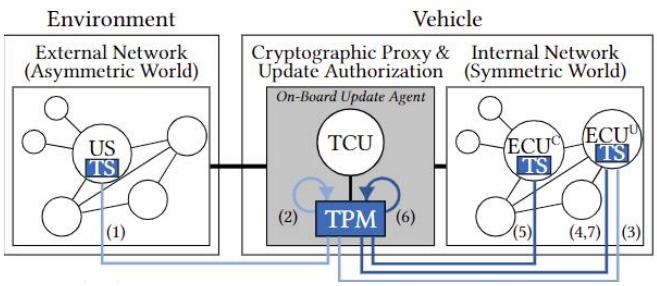
비대칭 암호화 작업을 소프트웨어로 수행할 수 있다. 효율성과 비용 측면에서 거의 모든 내부 통신 보호가 대칭 암호화 알고리즘을 기반으로 하기 때문에, 비대칭 암호화 엔진을 제외하는 것이 비용과 하드웨어 크기를 절감하는 데 합리적이다.

LIGHT HSM: 이 HSM은 보안 ECU와 센서 및 액추에이터 간의 상호 작용을 보호하는 데 중점을 둔다. 대칭 암호화 엔진과 이에 상응하는 기능적으로 축소된 하드웨어 인터페이스만 포함하면 된다. 따라서 LIGHT HSM은 센서와 액추에이터에 전형적인 엄격한 비용 및 효율성 요구사항(예: 메시지 크기, 타이밍, 프로토콜 제한 또는 프로세서 소비 관련)을 충족할 수 있다. 필요한 공유 비밀은 제조 과정에서의 사전 구성, 자체 초기화(예: 물리적 복제 방지 함수 기반) 또는 연결된 애플리케이션 프로세서에서 소프트웨어로 키 설정 프로토콜을 실행하는 등 다양한 방법으로 설정할 수 있다.

이러한 HSM 변형들은 다양한 보안 요구사항과 비용 제약을 가진 자동차 시스템에 유연하게 적용될 수 있어, 전반적인 차량 보안을 향상시키는 데 크게 기여한다.

3.2 TPM

TPM을 사용하여서 내부와 외부 사이에 안전한 프록시처럼 작동하도록 연구한 내용들이 많다.[9,10]



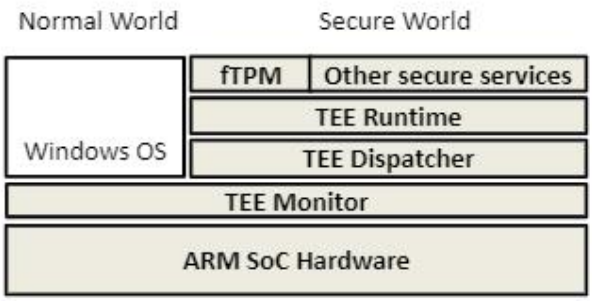
<그림 2> TPM을 이용한 안전한 자동차 시스템

기존 업데이트에서는 자동차에 있는 모든 ECU들이 각각 외부와 연결하여서 업데이트를 하였지만 보안적인 취약점이 많아지기에 안전한 업데이트를 위해 TPM을 사용하였다. 본 연구에서 제안된 Over-the-Air (OTA) 소프트웨어 업데이트 시스템은 연결된 차량 환경에서의 보안성과 효율성을 동시에 달성하는 것을 목표로 한다. 해당 연구는 비대칭 및 대칭 암호화 기법을 결합한 하이브리드 암호화 방식을 채택하여 통신의 기밀성과 무결성을 보장한다. 시스템 아키텍처는 그림2와 같이 중앙 서버, 차량의 텔레매틱스 제어 장치(Telematics Control Unit, TCU), 그리고 다수의 전자 제어 장치(Electronic Control Units, ECUs) 간의 보안 통신을 기반으로 구성되었다. 차량별 고유 암호화 키를 사용하여 개별화된 보안을 제공함으로써 대규모 보안 사고의 위험을 최소화하였다. 또한, 업데이트 실패 시 시스템을 이전 상태로 복원하는 롤백 메커니즘을 구현하여 시스템의 안정성을 보장하였다. 이러한 종합적인 접근 방식을 통해, 본 연구에서 제안된 기술은 현대 자동차 산업의 복잡한 소프트웨어 업데이트 요구사항을 효과적으로 충족시키는 것으로 평가된다.

3.3 Trust Zone

예전까지는 ARM Cortex-M 시리즈에서는 HSM만 있고 trustzone 은 ARM Cortex-A 에서만 있었다. 하지만 ARMv8-M 시리즈부터 tustzone-M 이 나오게되어서 Cortex-M 시리즈에서 사용하던 제품의 보안성이 더 향상되게 되었다. 자동차뿐 아니라 핸드폰 같은 IOT제품에서 정보를 지켜야하는 에플리케이션을 secure world에 실행하여 보호 및 인증을 할 수 있다. 자체적인 기능을 활용하는 것 뿐아니라 기존 HW 기능을 소프트웨어적으로 구현하여 활요한 기술도 있다.[[12]

fTPM 연구는 신뢰할 수 있는 플랫폼 모듈의 소프트웨어 기반 구현인 fTPM(Firmware TPM)을 제안한다. 기존의 하드웨어 기반 TPM 칩이 가지는 비용 및 구현 복잡성 문제를 해결하고자, ARM 프로세서의 TrustZone 기술을 활용하여 소프트웨어로만 구성된 TPM 솔루션을 개발하였다.



<그림 3> fTPM 의 구조

연구진은 fTPM의 설계 및 구현 과정에서 안전한 비휘발성 저장소의 구현, 암호화 연산의 최적화, 하드웨어 TPM과 동등한 수준의 보안 보장을 하였다. fTPM은 TrustZone의 보안 환경 내에서 동작하며, 암호화 키와 중요 데이터를 안전하게 저장하고 관리한다. 비휘발성 저장소의 구현을 위해 eMMC 저장장치의 신뢰할 수 있는 파티션을 활용하였으며, 암호화

연산의 성능 향상을 위해 하드웨어 가속기를 적극 활용하였다.

성능 평가 결과, fTPM은 대부분의 TPM 2.0 명령어에 대해 하드웨어 TPM과 유사하거나 더 우수한 성능을 보였다. 특히, 비대칭 키 생성 및 서명 검증 작업에서 fTPM이 하드웨어 TPM보다 현저히 빠른 처리 속도를 나타냈다.

4. 결론

본 연구를 통해 하드웨어 기반 자동차 보안 기술의 중요성과 다양한 적용 가능성을 확인하였다. HSM, TPM, ARM TrustZone 등의 기술은 각각의 고유한 특성을 바탕으로 자동차 시스템의 다양한 보안 요구사항을 효과적으로 충족시킬 수 있음을 보여주었다. 특히 EVITA 프로젝트에서 제안한 다양한 수준의 HSM 구현 방식은 비용 효율성과 보안성을 동시에 고려한 유연한 접근 방식을 제시하였다. TPM을 활용한 안전한 소프트웨어 업데이트 시스템은 자동차의 OTA 업데이트 과정에서의 보안을 크게 향상시킬 수 있는 가능성을 보여주었다. 또한, ARM TrustZone을 이용한 fTPM의 구현은 소프트웨어 기반 솔루션으로도 하드웨어 수준의 보안을 제공할 수 있음을 입증하였다.

5. Acknowledgement

이 논문은 2024년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (RS-2023-00277326). 이 논문은 2024년도 BK21 FOUR 정보기술 미래인재 교육연구단에 의하여 지원되었음. 이 논문은 2024년도 정부(과학기술정보통신부)의 재원으로정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2021-0-00528, 하드웨어 중심 신뢰계산기반과 분산 데이터보호박스를 위한 표준 프로토콜 개발),이 논문은 2024년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (IITP-2023-RS-2023-00256081). 본 연구는 반도체 공동연구소 지원의 결과물임을 밝힙니다. 이 논문은 2024년도 정부(산업통상자원부)의 재원으로 한국산업기술기획평가원의 지원을 받아 수행된 연구임.(No. RS-2024-00406121, 자동차보안취약점기반위협분석시스템개발(R&D)). 이 논문은 2024년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구 결과임 (No.RS-2024-00438729, 익명화된 기밀실행을 이용한 전주기적 데이터 프라이버시 보호 기술 개발)

참고문헌

[1] NIST SP 800-57 Part 1 Rev. 5, "Recommendation for Key Management"

[2] G. Escherich et al., "SHE – Secure Hardware Extension Functional Specification"

[3] Trusted Computing Group, "TPM 2.0 Library Specification"

[4] M. Wolf and T. Gendrullis, "Design, Implementation, and Evaluation of a Vehicular Hardware Security Module"

[5] ARM Limited, "ARM Security Technology: Building a Secure System using TrustZone Technology"

[6] J. Jang et al., "A Study on the Application of Automotive Security Technology based on ARM TrustZone“

[7] Apvrille, Ludovic, et al. "Secure automotive on-board electronics network architecture." FISITA 2010 world automotive congress, Budapest, Hungary. Vol. 8. 2010.

[8] Nasser, A. M., & Ma, D. (2020). SecMonQ: An HSM based security monitoring approach for protecting AUTOSAR safety-critical systems. Vehicular Communications, 21, 100201.

[9] Plappert, C., & Fuchs, A. (2023, December). Secure and Lightweight Over-the-Air Software Update Distribution for Connected Vehicles. In Proceedings of the 39th Annual Computer Security Applications Conference (pp. 268-282).

[10] Plappert, C., & Fuchs, A. (2023, December). Secure and Lightweight ECU Attestations for Resilient Over-the-Air Updates in Connected Vehicles. In Proceedings of the 39th Annual Computer Security Applications Conference (pp. 283-297).

[11] Plappert, C., Lorych, D., Eckel, M., Jäger, L., Fuchs, A., & Heddergott, R. (2023). Evaluating the applicability of hardware trust anchors for automotive applications. Computers & Security, 135, 103514.

[12] Raj, H., Saroiu, S., Wolman, A., Aigner, R., Cox, J., England, P., ... & Wooten, D. (2016). {fTPM}: A {Software-Only} Implementation of a {TPM} Chip. In 25th USENIX Security Symposium (USENIX Security 16) (pp. 841-856).