IoT 및 엣지 디바이스를 위한 ARM TrustZone 기반 보안 기법 조사

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

Survey of ARM TrustZone-based Security Techniques for IoT and Edge Devices

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 논문에서는 IoT 및 엣지 디바이스를 위한 ARM TrustZone 기반 보안 기법인 TEECheck, TrustedGateway, TeeFilter를 조사하였다. 이 기법들은 각각 차량 내 통신, 게이트웨이 라우터, IoT 네트워크 필터링이라는 다른 도메인에서 하드웨어 격리를 통해 운영체제가 손상되더라도 네트워크 보안을 유지한다.

1. 서론

최근 몇 년간 사물인터넷(IoT) 기기의 폭발적인 증가와 함께 엣지 컴퓨팅 인프라의 중요성이 커지고 있다. 연구기관 Transforma Insights에 따르면 2022년 약 131억 개의 IoT 기기가 존재했으며, 2030년에는 약 264억 개로 증가할 것으로 예상된다 [1]. 이러한 기기들은 에너지 생산, 운송, 의료 등 중요 인프라의 일부로 자리 잡고 있으며, 네트워크 운영자들은 IoT와 클라우드 사이의 연결고리 역할을 하는 컴퓨팅 자원을 갖춘 지능형 네트워크 요소를 배포하고 있다 [2].

그러나 이러한 발전과 함께 보안 위협도 증가하고 있다. Mirai 봇넷은 60만 개 이상의 IoT 기기를 감염시켰으며 [3], Hajime 봇넷은 최소 6만 5천 개의 IoT 기기를 감염시켰다 [4]. 이러한 대규모 감염 사례는 공격자들이 IoT 및 엣지 인프라를 표적으로 삼는 잠재력을 이해하고 있음을 보여준다. 또한 Ripple20, Amnesia:33과 같은 최근 발견된 취약점은 네트워크 스택에 대한 공격이 실제로 가능하며 매우 위험하다는 것을 증명하고 있다. 이러한 취약점들은 스마트 콘센트부터 산업용 제어 시스템, 의료 장비에 이르기까지 다양한 기기에 영향을 미친다.

네트워크 필터는 악성 소프트웨어의 결과를 완화하기 위한 잘 알려지고 널리 사용되는 기술이다. 악의적인 소스에서 들어오는 트래픽을 차단하면 초기 감염을 방지할 수 있고, 나가는 트래픽을 제한하면 감염을 억제하고 추가 피해를 방지할 수 있다. 그러나 일반적으로 네트워크 필터는 리눅스의 netfilter와 같은 운영 체제의 네트워크 스택에 통합되어 있다. 보안 관점에서 이는 문제가 될 수 있는데, 장치 드라이버, 인터넷 프로토콜, 시스템 데몬, 소프트웨어 라이브러리를 포함하는 네트워크 스택은 네트워크 기반 공격자에게 상당한 공격 표면을 제공하기 때문이다.

이러한 보안 문제를 해결하기 위해 ARM TrustZone과 같은 신뢰 실행 환경(TEE)을 활용한 보안 기법이 주목받고 있다 [5]. TEE는 하드웨어 지원 격리 기능을 통해 민감한 코드와 데이터를 보호하는 메커니즘을 제공한다. 특히 ARM TrustZone은 IoT 및 엣지 디바이스에 널리 사용되는 ARM 프로세서에 내장된 보안 기능으로, 시스템을 일반 세계(Normal World)와 보안 세계(Secure World)로 분리하여 보안 세계에서 실행되는 코드와 데이터를 일반 세계의 악의적인 소프트웨어로부터 보호할 수 있다 [6].

본 논문에서는 ARM TrustZone을 활용한 세 가지 주요 보안 기법인 TEECheck [7], TrustedGateway [8], TeeFilter [9]를 조사하고 분석한다. TEECheck

는 차량 내 통신을 위한 고보증 네트워크 필터링 엔진으로, 자동차 내부 통신의 보안을 강화한다. TrustedGateway는 라우팅 및 방화벽 정책을 보호하기 위한 TEE 기반 솔루션으로, 게이트웨이 라우터의 핵심 네트워킹 기능을 보호한다. TeeFilter는 고급 IoT 및 엣지 디바이스를 위한 고보증 네트워크 필터링 엔진으로, 운영 체제가 손상된 경우에도 네트워크 트래픽을 효과적으로 필터링할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 IoT 및 엣지 컴퓨팅의 보안 위협과 ARM TrustZone 기술에 대한 배경 지식을 제공한다. 3장에서는 TEECheck, TrustedGateway, TeeFilter의 설계, 구현 및 평가에 대해 상세히 살펴보고, 이들 접근법을 다양한 측면에서 비교 분석한다. 마지막으로 4장에서는 연구 결과를 요약하고 향후 연구 방향에 대해 논의한다.

2. 배경 지식

2.1 보안 세계(Secure World)와 일반 세계(Normal World)

TrustZone의 핵심 개념은 시스템을 보안 세계(Secure World)와 일반 세계(Normal World)라는 두 개의 격리된 실행 환경으로 분리하는 것이다 [6]. 일반 세계에서는 일반 운영체제(Rich OS)와 애플리케이션이 실행되며, 보안 세계에서는 보안에 민감한 코드와 데이터가 실행된다. 보안 세계는 일반 세계의 자원에 접근할 수 있지만, 일반 세계는 보안 세계의 자원에 접근할 수 없다 [5].

각 세계는 자체적인 특권 레벨을 가지고 있다. ARMv8-A 아키텍처에서는 Exception Level(EL)이라는 개념을 사용하며, EL0는 가장 낮은 권한을 가진 애플리케이션 레벨, EL1은 운영체제 레벨, EL2는 하이퍼바이저 레벨, EL3는 가장 높은 권한을 가진 시큐어 모니터 레벨이다 [6]. 보안 세계와 일반 세계는 각각 EL0와 EL1을 가지며, EL3는 두 세계 간의 전환을 관리하는 시큐어 모니터가 실행된다.

2.2 신뢰 실행 환경(TEE)의 역할

TrustZone을 기반으로 구축된 신뢰 실행 환경(TEE)은 보안 세계에서 실행되는 소프트웨어 스택으로, 보안 애플리케이션의 실행을 위한 안전한 환경을 제공한다 [5]. TEE는 일반적으로 TEE OS(보안 운영체제)와 TA(신뢰 애플리케이션)로 구성된다. TEE OS는 보안 세계에서 실행되는 경량 운영체제로, TA는 보안에 민감한 연산을 수행하는 애플리케이션이다 [6]. 대표적인 TEE OS로는 OP-TEE, Trustonic Kinibi, Qualcomm QSEE 등이 있다 [5].

2.3 TrustZone-A와 TrustZone-M의 차이점

ARM TrustZone은 Cortex-A(TZ-A)와 Cortex-M(TZ-M) 계열 프로세서에 대해 서로 다른 구현을 가지고 있다 [5][6]:

- 아키텍처적 차이: TZ-A는 ARMv8-A와 같은 고성능 애플리케이션 프로세서를 위한 것으로, 복잡한 메모리 관리 및 가상화 기능을 지원한다. TZ-M은 ARMv8-M과 같은 마이크로컨트롤러를 위한 것으로, 더 단순하고 자원 효율적인 구현을 제공한다 [6].
- 메모리 보호: TZ-A는 TZASC를 통해 동적인 메모리 분할을 지원하는 반면, TZ-M은 정적인 메모리 분할을 제공하며 구현 정의 속성 유닛(IDAU)이라는 하드와이어드 컨트롤러 로직을 사용한다 [5].
- 컨텍스트 스위칭: TZ-A는 SMC를 통해 세계 간 전환이 이루어지며 상대적으로 오버헤드가 크지만, TZ-M은 보안 게이트웨이(SG) 명령어를 사용하여 더 빠른 전환을 제공한다 [6].
- 인터럽트 처리: TZ-A에서는 인터럽트가 발생하면 일반 세계에서 보안 세계로 전환 시 모든 정보가 보안 스택에 저장되고 레지스터가 초기화되는 반면, TZ-M은 더 효율적인 인터럽트 처리 메커니즘을 제공한다 [5].

TrustZone 기술은 다양한 보안 응용 분야에서 활용되고 있으며, 특히 키 관리, 생체 인증, 디지털 권한 관리, 모바일 결제, 그리고 네트워크 필터링과 같은 응용에서 널리 사용되고 있다 [5][6].

3. ARM TrustZone을 활용한 보호 기법

3.1 TEECheck: 차량 내 통신을 위한 보안 솔루션

TEECheck는 ARM TrustZone을 활용하여 차량 내 통신(In-Vehicle Communication)을 보호하기 위한 메커니즘으로, 전자제어장치(ECU) 간의 통신을 보호한다. 현대 자동차에는 수많은 ECU가 장착되어 있으며, 이들은 CAN(Controller Area Network) 버스를 통해 통신한다. 그러나 CAN 버스는 인증 및 암호화 기능이 없어 공격자가 ECU를 침해하면 전체 차량 네트워크가 위험에 노출될 수 있다.

TEECheck는 ARM TrustZone을 기반으로 ECU 시스템 아키텍처를 재설계하여, CAN 컨트롤러와 네트워크 스택의 중요 부분을 보안 세계에 배치함으로써 이러한 문제를 해결한다. TEECheck의 주요 구성 요소는 다음과 같다:

- 메시지 발신 검증(Source Verification): HMAC(Hash-based Message Authentication Code)를 사용하여 메시지 발신자를 검증한다. 이를 통해 공격자가 다른 ECU를 가장하는 것을 방지한다.
- 메시지 전송률 제한(Rate Limiting): 각 작업의 메시지 전송 빈도를 제한하여 DoS(Denial of Service) 공격을 완화한다.
- 메시지 정보 유출 방지(Snoop Prevention): 의도하지 않은 수신자가 메시지에 접근하는 것을 차단한다.

TEECheck는 ECU의 Trust Computing Base(TCB)를 최소화하기 위해 메시지 필터링 및 인증 메커니즘만을 보안 세계에 배치한다. 실험 결과, TEECheck는 메시지 생성부터 전송까지 약 477µs의 오버헤드를 보이며, 이는 일반적인 ECU 처리 시간에 비해 매우 낮은 수준이다.

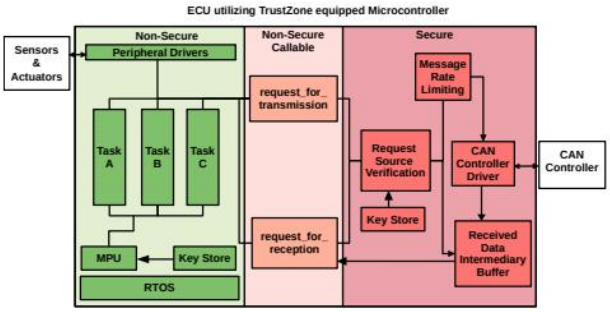

그림 1 TEECHECK 아키텍처

3.2 TrustedGateway: 라우팅 및 방화벽 정책 보호

TrustedGateway는 ARM TrustZone을 활용하여 게이트웨이 라우터의 핵심 네트워킹 기능(라우팅 및 방화벽)을 보호하는 시스템이다. 게이트웨이 라우터는 서브네트워크를 상호 연결하고 방화벽 정책을 사용하여 접근 제어를 수행하는 중요한 역할을 담당한다. 그러나 최근 연구에 따르면 많은 라우터가 보조 서비스(웹 UI, VoIP, 파일 공유 등)의 취약점으로 인해 공격에 노출되어 있다.

TrustedGateway는 다음과 같은 주요 구성 요소를 포함한다:

- NetTrug: 보안 세계에서 실행되는 신뢰할 수 있는 네트워킹 코어로, 네트워크 I/O와 트래픽 처리를 담당한다.
- VNIC(Virtual Network Device): 신뢰할 수 없는 서비스와 네트워크 접근을 공유하면서도 통제할 수 있게 해주는 가상 네트워크 장치.
- ConfigService: 신뢰할 수 있는 원격 관리자만이 정책을 업데이트할 수 있도록 하는 구성 서비스.

TrustedGateway는 NIC(Network Interface Card)를 보안 세계에 할당하고, 네트워크 트래픽 처리를 위한 신뢰할 수 있는 I/O 프레임워크를 구현한다 [8]. 이를 통해 일반 세계의 시스템 수준 공격자가 라우팅 및 방화벽 정책을 우회하거나 조작하는 것을 방지한다. 또한, TZ의 높은 컨텍스트 스위칭 오버헤드를 극복하기 위해 효율적인 I/O 스케줄링 메커니즘을 설계하였다.

성능 평가 결과, TrustedGateway는 기존 시스템 대비 62.6%~103.5%의 네트워크 처리량을 유지하면서도 보안을 크게 강화하였다.

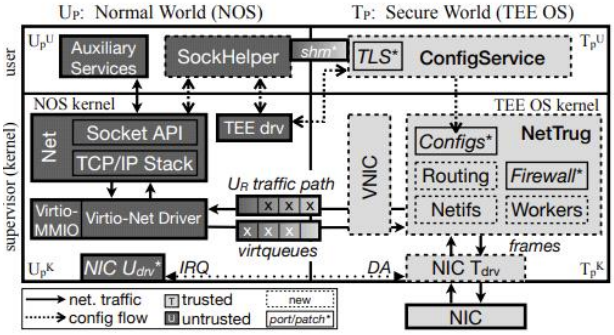

그림 2 TrustedGateway 아키텍처

3.3 TeeFilter: IoT 장치를 위한 네트워크 필터링 엔진

TeeFilter는 ARM TrustZone을 활용하여 고급 IoT 및 엣지 장치를 위한 고보증 네트워크 필터링 엔진을 제공한다. 최근 IoT 멀웨어는 단순히 약한 패스워드와 잘못 구성된 시스템을 공격하는 것뿐만 아니라, 소프트웨어 취약점을 악용하는 경향이 증가하고 있다. TeeFilter는 운영체제가 손상되더라도 네트워크 트래픽을 효과적으로 필터링할 수 있는 메커니즘을 제공한다.

TeeFilter의 핵심 설계 요소는.다음과 같다:

- 선택적 네트워크 스택 실행: 네트워크 스택의 일부분만을 보안 세계에서 실행하여 TCB를 최소화한다.
- eBPF(Extended Berkeley Packet Filter) 인터프리터: 필터링 규칙의 정확성과 보안을 분리하기 위해 eBPF 기반 인터프리터를 사용한다.
- 섀도우 디스크립터 링(Shadow Descriptor Ring): NIC와 내부 데이터 구조에 대한 접근을 제어하기 위해 섀도우 페이지 테이블 개념을 응용한다.

TeeFilter는 NIC를 보안 세계에 할당하고, 일반 세계에서의 NIC 레지스터 접근 시도를 포착하여 처리

한다. 이를 통해 필터링 규칙을 우회하거나 네트워크 트래픽을 조작하는 것을 방지한다. 또한, 필터링 규칙은 LLVM 호환 프로그래밍 언어로 작성하여 eBPF 코드로 컴파일할 수 있다.

TeeFilter는 정확성과 메모리 안전성을 보장하기 위해 대부분의 코드를 정형 검증하였다. 성능 평가 결과, TCP 네트워크 처리량은 기존 시스템의 66.86%를 유지하며, 네트워크 지연 시간은 1.21% 증가하는 데 그쳤다. 이는 TeeFilter가 실용적인 성능 오버헤드로 높은 수준의 보안을 제공할 수 있음을 보여준다.

4. 결론 및 향후 연구 방향

본 논문에서는 ARM TrustZone을 활용한 세 가지 주요 보안 기법인 TEECheck, TrustedGateway, TeeFilter를 분석하였다. 이 기법들은 각각 차량 내 통신, 게이트웨이 라우터, IoT 및 엣지 디바이스라는 서로 다른 도메인에서 네트워크 보안을 강화하는 메커니즘을 제공한다.

향후 연구 방향으로는 이러한 기법들을 다양한 ARM 프로세서 환경(특히 ARMv8-M)으로 확장하고, 실시간 시스템과의 호환성을 높이며, 다양한 네트워크 프로토콜에 적용하는 방안을 고려할 수 있다. 또한 이러한 보안 기법들의 형식 검증을 더욱 확장하고, 하드웨어 기반 보안과 소프트웨어 기반 보안을 결합한 하이브리드 접근법을 탐구하는 것도 중요한 연구 주제가 될 것이다.

5. ACKNOWLEDGEMENT

이 논문은 2025년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (RS-2023-00277326). 이 논문은 2025년도 BK21 FOUR 정보기술 미래인재 교육연구단에 의하여 지원되었음."이 논문은 2025년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2021-0-00528,하드웨어 중심 신뢰계산기반과 분산 데이터보호박스를 위한 표준 프로토콜 개발)" 이 논문은 2025년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (IITP-2023-RS-2023-00256081) 본 연구는 반도체 공동연구소 지원의 결과물임을 밝힙니다. 이 논문은 2025년도 정부(산업통상자원부)의 재원으로 한국산업기술기획평가원의 지원을 받아 수행된 연구임.(No. RS-2024-00406121, 자동차보안취약점기반위협분석시스템개발(R&D)).

참고문헌

[1] Transforma Insights, "Number of IoT connected devices worldwide 2016-2021, with forecasts to 2030," 2022.

[2] K. Cao, Y. Liu, G. Meng, and Q. Sun, "An Overview on Edge Computing Research," IEEE Access, vol. 8, pp. 85714-85728, 2020.

[3] M. Antonakakis et al., "Understanding the Mirai Botnet," in Proc. 26th USENIX Security Symposium, 2017, pp. 1063-1110.

[4] S. Herwig, K. Harvey, G. Hughey, R. Roberts, and D. Levin, "Measurement and Analysis of Hajime, a Peer-to-peer IoT Botnet," in Proc. Network and Distributed System Security Symposium, 2016.

[5] S. Pinto and N. Santos, "Demystifying ARM TrustZone: A Comprehensive Survey," ACM Computing Surveys, vol. 51, no. 6, pp. 130:1-130:36, 2019.

[6] ARM Limited, "ARM Security Technology: Building a Secure System using TrustZone Technology," ARM White Paper, 2006.

[7] T. Mishra, T. Chantem, and R. Gerdes, "TEECheck: Securing Intra-Vehicular Communication Using Trusted Execution," in Proc. 28th International Conference on Real-Time Networks and Systems, 2020, pp. 1-11.

[8] F. Schwarz, "TrustedGateway: TEE-Assisted Routing and Firewall Enforcement Using ARM TrustZone," in Proc. 25th International Symposium on Research in Attacks, Intrusions and Defenses, 2022, pp. 56-71.

[9] J. Röckl, N. Bernsdorf, and T. Müller, "TeeFilter: High-Assurance Network Filtering Engine for High-End IoT and Edge Devices based on TEEs," in Proc. ACM Asia Conference on Computer and Communications Security, 2024, pp. 1568-1583.