상태 전이 중심 자동화 기법을 통한 MCU 펌웨어 재호스팅 가능성 연구

김상윤[1], 이병영[2]
[1]서울대학교 전기정보공학부 석박사통합과정
[2]서울대학교 전기정보공학부 교수
sangyun.kim@snu.ac.kr, byoungyoung@snu.ac.kr

Exploring State-Transition-Centric Automation for MCU Firmware Rehosting

Sangyun Kim[1], Byoungyoung Lee[2]
[1]Dept. of Electrical and Computer Engineering, Seoul National University
[2]Dept. of Electrical and Computer Engineering, Seoul National University

요 약

사물인터넷(IoT)과 임베디드 시스템의 확산으로 인해 마이크로컨트롤러 유닛(MCU) 펌웨어 보안 분석의 중요성이 커지고 있다. 그러나 펌웨어는 하드웨어에 강하게 종속되어 있어, 실제 장치 없이 재호스팅(rehosting)하기 어렵다는 한계가 존재한다. 기존 연구들은 자동화된 주변장치 모델링을 통해 문제를 해결하고자 하였으나, 단순 기록 재생(replay)이나 제한된 규칙 기반 접근에 머물러 새로운 입력이나 비동기 이벤트(DMA, IRQ 등)에 대한 충실도(fidelity)가 부족하다.

본 논문은 이러한 한계를 보완하기 위한 새로운 방향으로, 상태 전이 중심(state-transition-centric) 자동화 접근을 제안한다. 제안 기법은 펌웨어 실행 과정에서 발생하는 HAL 시퀀스를 입력으로, 그 결과 나타나는 레지스터 상태의 before/after 전이를 출력으로 정의하여 분석한다. 이를 통해 입력 조건과 출력 반응의 관계를 규칙화하고, 새로운 입력에도 반응 가능한 상호작용적 모델을 구성한다. 실험 결과, 기존 방식에서 실패하던 새로운 입력 처리와 반복 인터럽트 재현 상황에서 본 접근이 보다 높은 충실도를 보임을 확인하였다.

1. 서론

사물인터넷(IoT)과 임베디드 시스템의 확산으로 인해, 마이크로컨트롤러 유닛(MCU)을 기반으로 동작하는 펌웨어의 보안성이 점차 중요한 연구 주제로 부상하고 있다. 이러한 펌웨어는 센서, 통신 모듈, 제어 장치 등 다양한 하드웨어 주변장치와 밀접하게 결합되어 동작한다. 따라서 보안 분석을 위해서는 펌웨어를 실제 하드웨어에 의존하지 않고 실행할 수 있는 재호스팅(rehosting)기술이 필수적이다.

그러나 재호스팅은 여러 가지 어려움을 동반한다. MCU 펌웨어는 전용 하드웨어를 대상으로 작성되며, 메모리 맵드 I/O(MMIO), 인터럽트(IRQ), 직접 메모리 접근(DMA) 등 하드웨어 특화 동작을 전제로 하기 때문에, 기존 범용 분석 기법을 적용하기 어렵다. 이에 따라 많은 연구들이 자동화된 주변장치 모델링을 통해 재호스팅 문제를 해결하고자 하였다. 예를 들어, PRETENDER[1]는 펌웨어와 하드웨어 간 상호작용 기록을 기반으로 자동화된 모델을 생성하였으며, Conware[2]는 상태 기계(automata) 기반의 일반화된 모델을 제시하여 재사용성을 높였다. 또한 FlexEmu[3]는 공통 하드웨어 개념을 추상화한 primitive와 의미적 모델링을 도입하여 다양한 MCU 주변장치에 적용 가능한 프레임워크를 제안하였다.

하지만 이러한 기존 접근법들은 공통적으로 몇 가지 한계를 가진다. 첫째, 기록 기반 재생(replay)에 머무르는 경우가 많아 새로운 입력에 대한 반응성이 부족하다. 둘째, DMA나 IRQ와 같은 비동기적 이벤트 처리에서 충실도(fidelity)가 떨어지는 문제가 있다. 셋째, 다양한 MCU 아키텍처와 주변장치의 복잡성을 일반화하기에는 한계가 있다.

본 논문은 이러한 한계를 보완하기 위해 상태 전이 중심(state-transition-centric) 접근을 기반으로 한 자동화 기법의 가능성을 탐색한다. 제안하는 아이디어는 펌웨어 실행 과정에서 발생하는 주변장치 동작을 단순한 값 재생이 아닌 상태 전이 단위로 분석하여, 새로운 입력에도 반응 가능한 상호작용적

모델을 구성하는 것이다. 이를 통해 기존 연구들이 제시한 자동화 수준을 한 단계 확장하고, 보다 높은 fidelity를 갖는 재호스팅 환경을 제공할 수 있음을 보여주고자 한다.

2. 배경 및 문제 정의

임베디드 펌웨어는 일반적인 소프트웨어와 달리, 실행 환경이 하드웨어에 강하게 종속되어 있다는 특징을 가진다. MCU 기반 시스템은 크게 (1) CPU 코어, (2) 온칩 주변장치(타이머, UART, SPI, GPIO 등), (3) 외부 디바이스(센서, 액추에이터 등)로 구성된다. 이 중 대부분의 펌웨어 동작은 메모리 맵드 I/O(MMIO)를 통해 주변장치 레지스터를 읽거나 쓰는 방식으로 이루어진다. 또한, 펌웨어 실행은 인터럽트(IRQ)나 DMA 이벤트와 같이 비동기적으로 발생하는 하드웨어 신호에 의해 제어 흐름이 크게 달라진다.

이러한 특성은 재호스팅을 어렵게 만든다. 단순히 펌웨어를 QEMU와 같은 범용 에뮬레이터 위에서 실행하는 경우, 대응되는 주변장치 모델이 존재하지 않으면 프로그램이 곧바로 예외를 일으키거나 무한 루프에 빠지게 된다. 따라서 주변장치 동작을 충실히 모델링하는 것이 재호스팅의 핵심 과제가 된다. 기존 연구들은 이를 해결하기 위해 다양한 접근을 시도해왔다.

* **기록 재생(replay) 기반**: PRETENDER[1]와 같은 기법은 실제 하드웨어에서 수집한 로그를 재생하여 모델을 구축한다. 그러나 새로운 입력 상황에서는 반응하지 못하는 한계가 있다.
* **상태 기계(automata) 기반**: Conware[2]는 기록을 일반화하여 재사용 가능한 상태 기계 모델을 생성하였으나, 여전히 복잡한 DMA/IRQ 동작을 완전하게 포착하기는 어렵다.
* **추상 primitive 기반**: FlexEmu[3]는 공통 하드웨어 개념을 추상화하여 다양한 MCU에 적용할 수 있으나, 단순한 동작 규칙 추출에 머무는 경우 fidelity가 떨어질 수 있으며, 주변 장치의 드라이버 소스코드에 의존하였기에, 펌웨어 내부에서 레지스터 값을 변경하는 로직을 모델링하기 어렵다.

결국, 현존 기법들은 (1) 새로운 입력 반응성 부족, (2) 비동기 이벤트 처리 한계, (3) 다양한 MCU 지원의 어려움이라는 공통 문제를 안고 있다.

본 연구는 이러한 한계를 극복하기 위해 상태 전이 중심(state-transition-centric)접근을 도입한다. 즉, 주변장치의 동작을 단순 값 시퀀스가 아닌 전이(Transition)단위로 해석하여, 입력 조건과 출력 반응의 관계를 모델링하는 것이다. 이를 통해 기존 방식보다 상호작용성이 높고 충실도가 높은 재호스팅 환경을 제공할 수 있다.

3. 제안 방법

본 연구는 기존 자동화 기법의 한계를 보완하기 위해 상태 전이 중심(state-transition-centric) 접근을 제안한다. 핵심 아이디어는 펌웨어가 주변장치와 상호작용하는 과정을 단순히 값의 기록을 재생하는 방식이 아니라, 입력과 출력의 전이 관계로 분석하고 모델링하는 것이다. 구체적으로 입력은 펌웨어가 호출하는 HAL sequence이며, 출력은 해당 호출 이후 관찰되는 레지스터 상태 변화(before/after)로 정의된다. 이러한 전이를 중심으로 모델을 구성함으로써, 새로운 입력이 주어지더라도 적절한 출력을 생성할 수 있으며, 인터럽트나 DMA와 같은 비동기 이벤트 역시 전이 단위에서 충실하게 재현할 수 있다.

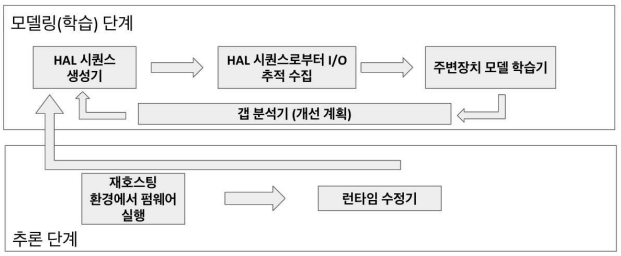

그림 1. 상태 전이 중심 자동화 접근의 학습 및 추론 과정 개요

제안하는 접근은 다음과 같은 과정으로 이루어진다. 먼저, 펌웨어 실행 과정에서 발생하는 HAL API 호출 시퀀스를 입력으로 수집한다. 각 호출은 주변장치와의 상호작용을 트리거하며, 이에 따라 레지스터 값이 변한다. 이때 레지스터의 상태 변화를 before/after 쌍으로 기록하여 출력으로 정의한다. 이후 이러한 입력-출력 쌍을 기반으로 하여, 동일한 입력이 주어졌을 때 어떠한 레지스터 전이가 발생하는지를 규칙으로 정리한다. 또한, 이 과정에서 자동화를 높이기 위해 LLM을 활용하여 before/after 쌍으로부터 주변장치 전이 규칙을 추출하는 가능성을 탐색한다. 마지막으로, 이렇게 도출된 전이 규칙들을 일반화하여 상태 전이 기반의 주변장치 모델을 구성

하고, 이를 에뮬레이터(QEMU 등)에 통합한다.

이와 같은 접근은 기존 방식과 비교해 몇 가지 장점을 갖는다. 첫째, 단순한 로그 재생이 아니라 HAL 호출과 레지스터 상태 변화를 직접적으로 연결하기 때문에, 기록되지 않은 입력에도 반응할 수 있어 상호작용성이 강화된다. 둘째, DMA나 인터럽트와 같은 비동기적 이벤트도 레지스터 전이 형태로 포착할 수 있어 충실도를 높인다. 셋째, before/after 전이 규칙을 자동으로 도출할 수 있는 가능성을 통해 다양한 MCU 플랫폼에 대한 적용성을 확장할 수 있다. 결과적으로, 기존 연구들이 단순 시퀀스 재생이나 제한적인 규칙 추출에 머물렀다면, 본 접근은 HAL sequence에서 레지스터 전이라는 구조적 일반화를 통해 새로운 입력 상황에도 적응 가능한 모델을 제공한다는 점에서 차별성을 가진다.

4. 실험 및 관찰

본 연구에서는 제안한 상태 전이 중심 접근의 가능성을 확인하기 위해 STM32F4 MCU(Nucleo 보드)를 대상으로 실험을 수행하였다. 실험에는 UART 송수신 예제와 Timer 주기 인터럽트 예제를 펌웨어로 활용하였다. 이 두 예제는 MCU 주변장치와의 상호작용이 명확하게 드러나며, DMA 및 IRQ 이벤트가 포함되어 있어 검증 대상으로 적합하다.

비교는 기존의 단순 기록 기반 재생(replay) 방식과 본 논문에서 제안한 상태 전이 중심 자동 모델링 방식을 기준으로 이루어졌다. UART 예제에서 기존 방식은 드라이버 소스코드에 명시되어 있지 않은 새로운 입력 패턴이 주어졌을 때 대응하지 못하고 busy-loop에 빠지는 문제가 발생하였다. 반면, 제안 방식은 입력 - 출력 전이를 규칙으로 일반화함으로써 새로운 입력 상황에서도 정상적인 응답을 유지하였다. 특히 busy-loop에 빠진 경우에도, LLM을 활용하여 해당 상황을 추론하고 부족한 전이를 자동으로 보강함으로써 모델을 업데이트할 수 있음을 확인하였다.

Timer 예제에서도 유사한 차이가 관찰되었다. 기존 방식은 특정 주기 이후 인터럽트 처리를 재현하지 못해 펌웨어가 deadlock 상태에 진입하였으나, 제안 방식은 “카운터 증가 → 주기 도달 → IRQ 발생”이라는 전이를 규칙화하여 반복 주기를 충실하게 재현하였다. 더 나아가, HAL 입력과 그에 따른 레지스터 before/after 상태를 기반으로 LLM이 정보 공백(information gap)을 식별하는 경우, 필요한 HAL 시퀀스를 스스로 요청하여 모델을 확장할 수 있다는 가능성도 확인하였다.

이러한 결과는 상태 전이 중심 접근이 기존 방식보다 새로운 입력에 대한 상호작용성과 비동기 이벤트 처리 충실도 측면에서 우수하다는 점을 보여준다. 또한 LLM을 통한 보강 메커니즘을 결합함으로써, 모델이 단순히 기록된 동작을 재현하는 수준을 넘어, 부족한 전이를 스스로 학습하고 확장하는 동적 모델링으로 진화할 수 있음을 시사한다. 이는 향후 대규모 펌웨어 분석 및 보안 평가에도 적용 가능성을 지닌다는 점에서 중요한 의미를 가진다.

5. 결론

본 논문에서는 임베디드 펌웨어 재호스팅의 어려움을 해결하기 위한 새로운 방향으로, 상태 전이 중심(state-transition-centric) 자동화 접근을 제안하였다. 기존 방식이 단순 기록 재생(replay)이나 제한된 규칙 기반 모델링에 머물러 새로운 입력과 비동기 이벤트 처리에서 한계를 보인 반면, 제안 방식은 펌웨어 - 하드웨어 상호작용을 전이 단위로 해석함으로써 보다 높은 상호작용성과 충실도를 제공할 수 있음을 확인하였다.

UART 및 Timer 예제를 통한 실험 결과, 기존 방식에서 실패하던 새로운 입력과 반복 인터럽트 처리 상황을 제안 방식이 성공적으로 재현하였다. 이는 제안한 접근이 실제 임베디드 보안 분석 환경에서도 의미 있는 개선을 가져올 수 있음을 시사한다.

6. 사사문구

이 연구는 2025년도 산업통상자원부 및 한국산업기술기획평가원(KEIT) 연구비 지원에 의한 연구임 (RS-2024-0404139)

참고문헌

[1] E. Gustafson, M. Muench, C. Spensky, N. Redini, A. Machiry, Y. Fratantonio, A. Francillon, D. Balzarotti, Y. R. Choe, C. Kruegel, and G. Vigna, “Toward the Analysis of Embedded Firmware through Automated Re-hosting,” Proceedings of the 22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID), Beijing, China, 2019, pp. 135 - 150.

[2] C. Spensky, A. Machiry, N. Redini, C. Unger, G. Foster, E. Blasband, H. Okhravi, C. Kruegel, and G. Vigna, “Conware: Automated Modeling of Hardware Peripherals,” Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security (AsiaCCS), Hong Kong, China, 2021, pp. 15 – 30.

[3] C. Lei, Z. Ling, X. Xu, S. Li, G. Liu, K. Dong, and J. Luo, “FlexEmu: Towards Flexible MCU Peripheral Emulation,” arXiv preprint, arXiv:2509.07615, 2025.