보안 하드웨어 모니터링 기법에 관한 연구

김현준*, 조명현*, 장지원*, 오현영*, 백윤흥*
*서울대학교 전기·정보공학부, 반도체공동연구소
hjkim@sor.snu.ac.kr, mhcho@sor.snu.ac.kr, jwchang@sor.snu.ac.kr, hyoh@sor.snu.ac.kr, ypaek@sor.snu.ac.kr

A Survey on Hardware Monitoring Technique for Security

Hyun-Jun Kim*, Myung-Hyun Cho*, Ji-Won-Chang*, Hyun-young Oh*, Yun-Heung Paek*
*Dept. of Electrical and Computer Engineering and Inter-University Semiconductor Research Center (ISRC), Seoul National University

요 약

본 논문에서는 시스템이 비정상적인 상태에 진입하였는지를 판단하여 공격에 대한 탐지를 효율적으로 수행할 수 있는 하드웨어 기반 보안 모니터링 기술에 대해 소개한다. 먼저 이벤트 기반으로 커널을 보호하는 모니터링 기법들에 대해 알아볼 것이다. 최종적으로 다양한 이벤트를 유연하게 모니터링할 수 있는 기법을 살펴보고, 이를 바탕으로 보안 하드웨어 모니터링 기법의 향후 연구방향을 모색하고자 한다.

1. 서론

4차 산업시대를 맞이하게 되면서 빅데이터, 인공지능, 클라우드와 같은 첨단 디지털 기술들이 다발적으로 개발되고 이들을 활용한 서비스들이 널리 제공되고 있다. 이 기술들이 발전함에 따라 충분한 컴퓨팅 파워를 제공할 수 있는 디바이스에 대한 수요가 증가하고 있다. 또한 이러한 디바이스들에 대한 공격 위협 또한 점점 커지고 있다.

모니터링 기법은 이러한 디바이스들에 대해 보안을 제공해줄 수 있는 효과적인 솔루션이다. 모니터링 기법은 감시의 대상이 되는 디바이스로부터 얻어낸 정적/동적 정보를 활용해서 시스템이 비정상적인 상태에 진입하였는지를 확인하고, 시스템 관리자 혹은 보안 정책에 의해 시스템의 정지 또는 정상적인 상태로의 복구를 시도할 수 있다.

소프트웨어 기반 모니터링 기법 중 대표적인 방식으로는 가상화 머신 모니터(VMM)를 활용하여 시스템을 감시하는 기술이 있다. 가장 상위층에 있는 모니터링 엔진이 하위 계층의 게스트 운영체제의 동작을 감시하며 시스템의 상태를 체크한다. 하지만 이 방식은 여러 가지 단점을 가지고 있다. 첫 번째는 VMM도 소프트웨어이기 때문에 취약점을 가지고 있다는 문제가 있다. 가상머신의 취약점에 의해 정상적으로 동적 정보를 추출하지 못하거나 모니터링 엔진이 공격당할 수 있다. 두 번째로 악성 행위를 일으키는 프로그램이 가상 환경을 인식하여 모니터링을 회피할 가능성이 있다. 마지막으로 소프트웨어 기반 방식이기 때문에 오버헤드가 크다는 단점이 있다.

하지만 하드웨어 방식 모니터링 엔진은 운영체제와 격리되어 있어 물리적인 공격이 아닌 한 공격당하기 힘들며, 모니터링 엔진이 존재하는지 알 수 없다. 그리고 별개의 하드웨어를 사용하므로 오버헤드가 거의 없다. 따라서 하드웨어 기반 모니터링 솔루션은 효율적으로 타겟 디바이스에 보안을 제공해 줄 수 있다.

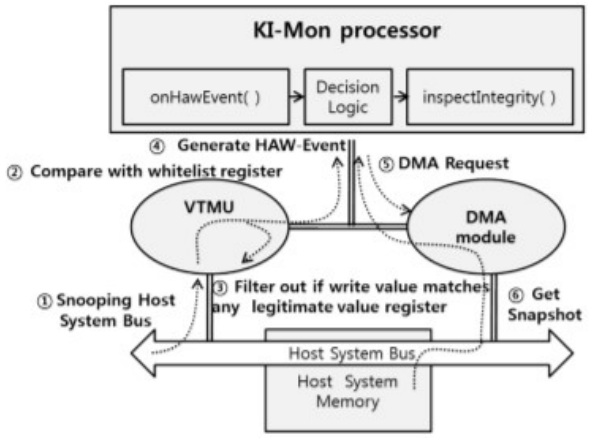
본 연구에서는 이러한 보안 하드웨어 모니터링 기법들에 대해 살펴보고, 이를 기반으로 향후 보안 하드웨어 모니터링 기법의 방향을 모색하고자 한다.

2. 보안 하드웨어 모니터링 기법

2-1. KI-Mon [1]

본 기법은 시스템에 영향을 미칠 수 있는 동작에 대해 이벤트를 생성한 다음, 하드웨어 로직으로 분석하여 커널이 비정상상태인지를 확인한다. 그 대상은 커널 내 특정 오브젝트가 메모리 내에서 변경될

경우 그 쓰기 주소와 변형(mutation)된 값을 이벤트로 형성한다. 일차적으로 화이트리스트 기법을 사용하여 커널 내 불변 오브젝트 (invariant)가 변경되었는지 확인한다. 그 외의 변형 가능한 자료 구조에 대해서는 콜백 검증 (callback verification)을 호출하여 문맥적(Semantically)으로 올바른 변형인지를 소프트웨어적으로 체크한다. 이를 위해 변경되는 값들을 전용 메모리에 기록해두고 이를 가속기로 해싱한 값을 제공하여 문맥을 파악할 수 있게 해준다. 모니터링에 사용되는 메모리의 버스 트래픽은 VTMU (Value Table Managment Unit)을 통해 하드웨어적으로 모니터링하고, 필요할 때에만 이벤트를 생성하여 적은 오버헤드로 모니터링이 가능하다. 해당 연구는 하드웨어를 활용하여 고속으로 커널 내 오브젝트를 모니터링하고, 콜백을 통해 유연하게 복잡한 추가 검증을 수행할 수 있다는 점에 의의가 있다.

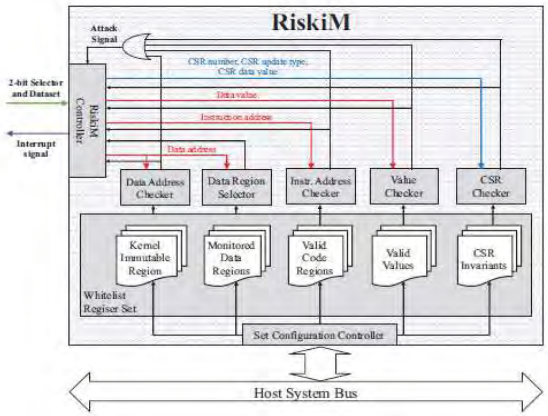


(그림 1) KI-Mon 동작 흐름도

2-2. RiskiM [2]

본 기법은 오픈 소스로 공개된 RISC-V 프로세서를 수정하여 코어 내부 정보를 추출해낼 수 있는 인터페이스를 구축하고, 코어 외부의 모니터링 엔진을 통해 커널이 비정상상태인지를 확인하고, 커널의 무결성을 보장한다.

모니터링에 필요한 정보를 얻으면서도 RISC-V, 소프트웨어 스택과의 호환성을 보장하기 위해 코어의 RTL 코드를 최소한으로 수정하였다. 이를 통해 추가한 인터페이스에서는 메모리 쓰기에 대해 명령어 주소, 데이터 주소, 데이터 값을 추출하고, 코어 내부 정보를 저장하는 CSR 값의 변화할 경우 CSR 숫자, 업데이트 타입, CSR 값을 추출해낸다. 이들이 묶여서 데이터 셋의 형태로 코어 외부로 전달되고, 외부의 모니터링 엔진에서는 주소, 값에 대한 전용 검증 모듈이 있어 이들에 대한 검증을 순서대로 수행한다. 해당 연구는 기존에 존재하던 Intel PT, ARM PTM와 같은 디버그 인터페이스에 의존하지 않고, RISC-V를 조금 수정하여 전용 인터페이스를 추가하여 기존에 사용하지 못하던 코어 내 정보를 추출하여 모니터링을 수행할 수 있는 엔진을 개발했다는 점에서 그 의의가 있다.

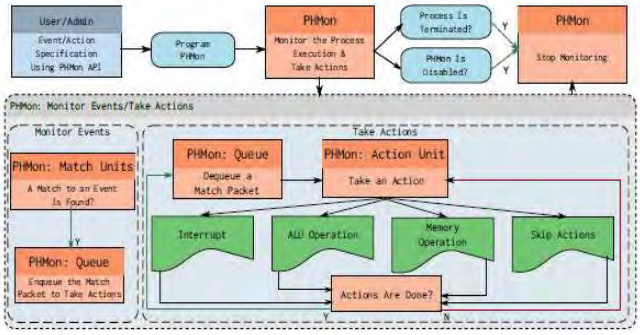


(그림 2) RiskiM 구조

2-3. PHMon [3]

본 기법은 이벤트를 여러 개의 모니터링 룰(rule)과 행동 (action)의 집합으로 나타낸다. 추출한 동적정보에 룰을 적용하여 이벤트를 인식하고, 이에 대응되는 행동을 수행하는 프레임워크를 개발하였다.

본 모니터링 엔진은 RISC-V 코어를 수정하여 명령어 트레이스를 얻을 수 있다. 이에는 명령어, 주소, 데이터 값, 인터럽트, 메모리 리퀘스트 등의 다양한 정보들을 포함하고 있다. 또한 Linux OS를 수정하여 각 프로세스에 대해 다양한 보안 정책을 적용할 수 있다. 해당 프레임워크를 통해 커널과 같은 시스템의 무결성을 보장하는 것도 가능하며, 가속화된 퍼징 (Fuzzing), 디버깅 (Debugging)에도 사용가능하다. 해당 연구는 코어 내 내부 정보를 하드웨어적으로 특정 룰과 매칭시키고 이에 대응되는 행동을 정의하여 다양한 보안 정책을 적은 오버헤드로 구현했다는 점에서 의미가 있다.



(그림 3) PHMon 동작 흐름도

3. 차후 하드웨어 모니터링 연구 방향

모니터링에 필요한 정보를 추출하고 사용하는 부분에 있어서 충분히 많은 연구가 진행되어 왔다. 하지만 이 정보를 통해 시스템의 비정상적인 시스템을 진단하는 방식은 대부분 화이트리스팅 방식에 치중되어 있어 이에 대한 더 많은 연구가 필요하다.

이에 대한 솔루션으로 머신러닝을 들 수 있다. 머신러닝을 사용하면 여러 이벤트들의 패턴을 좀 더 추상화된 벡터 형태로 추출해낼 수 있고, 해당 벡터를 사용해 특정 보안 태스크를 수행하는 모델을 생성할 수 있다. 또한 머신러닝은 하드웨어 기술을 통해 가속을 할 수 있기 때문에 효율적으로 하드웨어 모니터링을 수행할 수 있을 것으로 예상된다.

4. 결론

본 논문에서는 보안 하드웨어 모니터링 기법을 다룬 3개의 연구를 살펴보고, 각각의 논문에서 어떤 방식을 통해 하드웨어 기술을 모니터링에 사용했는지 알아보았다. 차후의 연구에서는 정보를 추출하고 처리하는 것뿐만 아니라 이를 활용해 어떻게 시스템의 비정상적인 상태를 진단하거나 기타 보안 목적의 기능을 수행할 수 있는지가 중요할 것이다.

5. Acknowledgement

본 연구는 2020년도 정부(과학기술정보통신부)의 재원으로 한국연구재단 (NRF-2017R1A2A1A17069478), 2020년도 두뇌한국21플러스사업 , 2020년도 정부 과학기술정보통신부의 재원으로 정보통신기술진흥센터 (No.2017-0-00213, 능동적 사전보안을 위한 사이버 자가변이 기술 개발)의 지원을 받아 수행된 연구임.

참고문헌

[1] Lee, Hojoon, et al., “Ki-mon: A hardware-assisted event-triggered monitoring platform for mutable kernel object”, USENIX Security Symposium, Washington D.C., U.S.A, 2013

[2] Hwang, Dongil, et al., “RiskiM: Toward Complete Kernel Protection with Hardware Support”, DATE, Florence, Italy, 2019

[3] Delshadtehrani, Leila, et al. "PHMon: A Programmable Hardware Monitor and Its Security Use Cases", USENIX Security Symposium, 2020