취약점 자동 검증 플랫폼 제작 계획안

고려대학교 정보보호대학원 정보보호학과

박성하, 김영준, 이휘원, 김현학

1. 개요

본 계획은 기존에 수행중인 1-Day 익스플로잇을 메타스플로잇 모듈로 제작하는 작업의 연장선에 있는 프로젝트를 제안한다. 현재 메타스플로잇 모듈로 제작된 익스플로잇을 검증하기 위해 기존에는 사람이 직접 적합한 환경을 구성하고 취약한 프로그램을 설치한 뒤, 익스플로잇이 동작하기 위한 행위들을 수행해야하는 일련의 작업들이 필요하다. 취약점 PoC 또는 모듈에 대한 검증은 이를 사용하고자 하는 기관/단체들에게 있어 필수적인 요소이다. 따라서, 본 프로젝트에서는 기존의 공개된 취약점들을 수집하고 익스플로잇 형태로 전환하는 프레임워크 구축 및 취약점 모듈을 효율적으로 검증할 수 있도록 다양한 실행 환경을 지원하는 에뮬레이터 기반의 취약점 자동 검증 시스템을 구축하는 것을 목표로 한다.

2. 연구 설계

기본적으로 현재 진행하고 있는 작업에 기반하여 메타스플로잇 모듈과 연동할 수 있도록 개발한다. 즉, 메타스플로잇 모듈 및 취약한 프로그램을 입력으로 받아 검증 결과를 출력하는 형태로 제작한다. 입력을 받은 뒤, 모듈 명세에서 실행 환경 정보를 추출하여 적합한 가상 환경에 입력 받은 프로그램과 모듈을 업로드 후 가상 환경 내의 메타스플로잇을 이용하여 모듈을 동작시킨다. 특정한 이벤트를 발생시키는 페이로드를 자동으로 설정하여 모듈을 실행시킨다. 해당 이벤트가 발생하는지의 여부로 익스플로잇을 검증할 수 있다. 이때, 바로 입력을 받아 실행시킬 수 있는 경우와 프로그램이 Standalone 형태인 경우는 비교적 간단하게 구현할 수 있지만, 취약점을 발생시키기 위해 프로그램에서 일련의 작업(Interaction)이 필요한 경우, 정형화해서 자동화하기는 어렵다는 문제가 있다. 또한, 실행 흐름을 완전히 변경하는 경우는 쉽게 검증이 되지만, 메모리 정보를 유출하거나 특정한 레지스터만 컨트롤이 가능한 취약점 등 많은 경우가 존재하므로, 이를 포괄하기 위해서는 새로운 아이디어와 연구가 필요하다. 일단, 비교적 쉬운 경우부터 시작한 뒤 복잡한 경우들을 포괄할 수 있도록 플랫폼을 발전시켜 나가는 방향이 적합할 것으로 보인다. 기본적인 설계는 아래와 같으며, 추후에 변경되거나 추가될 수 있다.

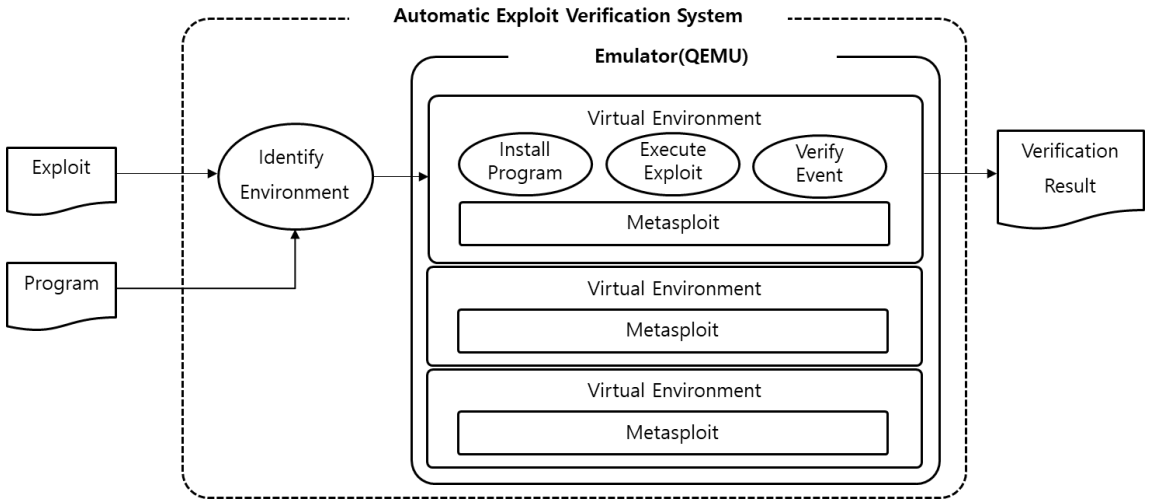

그림 1. 취약점 자동 검증 플랫폼 구조

3. 향후 계획

기간	작업 내용
2019년도 상반기 (2019.04~08)	- PoC가 존재하는 1-Day 익스플로잇에 대한 메타스플로잇 모듈 포팅 작업 진행 - 다양한 환경에서, 다양한 대상에 대한 익스플로잇들을 직접 포팅하면서 필요한 작업 식별 - 식별한 문제를 기반으로 자동화에 필요한 이슈 및 해결방안 모색하여 설계 구체화
2019년도 하반기 (2019.09~2020.02)	- PoC가 존재하는 1-Day 익스플로잇에 대한 메타스플로잇 모듈 포팅 작업 진행 - 가상환경 구축을 위한 기술(하이퍼바이저/에뮬레이터) 연구 - 필요한 환경 구축 - 샘플 모듈 식별하여 각 모듈에 대한 자동화된 검증 모듈 개발 - 보다 단순하게 검증이 가능한 모듈을 대상으로 하며, 구현에 집중 - 기본적으로 작성된 검증 모델로 논문 투고(워크샵/학술대회급)
2020년도 상반기 (2020.03~2020.08)	- PoC가 존재하는 1-Day 익스플로잇에 대한 메타스플로잇 모듈 포팅 작업 진행 - 기존에 공개된 QEMU/KVM 기반의 S^2E 플랫폼 커스터마이징 - 2019년도 하반기 작업에서 식별된 문제점을 기반으로, 보다 복잡하게 검증이 필요한 익스플로잇까지 확장이 가능하도록 추가 연구 진행
2020년도 하반기 (2020.09~2021.02)	- PoC가 존재하는 1-Day 익스플로잇에 대한 메타스플로잇 모듈 포팅 작업 진행 - 2020년도 상반기 작업에서 식별된 문제점을 기반으로, 보다 복잡하게 검증이 필요한 익스플로잇까지 확장이 가능하도록 추가 연구 진행
2021년도 상반기 (2021.03~2021.08)	- 쌓인 데이터들을 기반으로 기존의 다른 연구들 식별하여 비교/검증 및 고도화 - 성능 개선 및 추가적인 이슈 보완하여 논문 투고(SCI급 저널/컨퍼런스)