VxWorks 환경에서 효과적인 퍼징 테스트를 위한 보안취약점 분석대상 모니터링 기능 설계

안개일, 송원준, 최양서
한국전자통신연구원 정보보호연구본부
e-mail:{fogone, iamwonjunsong, yschoi92}@etri.re.kr

Design of Security Vulnerability Analysis Target Monitoring Function for Effective Fuzzing Test in VxWorks Environment

Gae-Il An, Won-Jun Song, Yang-Seo Choi
Cyber Security Research Division, ETRI

요 약

산업제어시스템에서 사용되는 소프트웨어의 보안취약점을 테스트하기 위한 방법으로 퍼징(Fuzzing)이 사용되고 있다. 퍼징 시스템은 크게 퍼징 대상을 테스트하는 퍼저(fuzzer)와 퍼징 대상을 모니터링하는 모니터링 모듈로 구성된다. 본 논문에서는 VxWorks 환경에서 효과적인 퍼징을 제공하기 위해 요구되는 퍼징 대상 모니터링 기능을 정의하고 모니터링 모듈을 설계한다.

1. 서론

산업제어시스템이란 일반 제조업뿐만 아니라, 공항, 항만, 발전소 등 국가 중요 인프라에 산업공정의 운영을 위해 사용되는 기기와 소프트웨어 그리고 네트워크를 말한다. 산업제어시스템에서는 산업공정이 실시간으로 제어되기 때문에 QNX와 VxWorks 같은 실시간 운영체제를 도입하고 있다.

산업제어시스템으로 개발된 소프트웨어에 버그가 존재한다면 기반시설에 보안취약점이 존재하게 되어 사이버공격을 당할 심각한 위험에 노출될 수 있다. 산업제어시스템에서 사용되는 소프트웨어의 보안취약점을 테스트하기 위한 여러 방법 중에서 퍼징(fuzzing)이 많이 사용되고 있다. 퍼징이란 에러나 충돌(crash)을 일으키기 위해 컴퓨터 프로그램에 무작위 데이터를 입력하면서, 만약 에러 및 충돌이 발생하면 그 원인을 분석하여 보안취약점이나 버그를 찾아내는 방법이다[1]. 퍼징 기법은 테스트 케이스를 어떻게 생성하느냐에 따라서 크게 변이(mutation)기법과 생성(generation)기법으로 구분된다. 변이 기법은 입력 데이터를 임의적으로 변경하여 새로운 입력 데이터를 만드는 방식이고, 생성 기법은 타겟 소프트웨어의 프로토콜에 맞추어 적절한 입력 데이터를 생성하는 방식이다. 어느 기법이 더 우수한지는 퍼징 대상 프로그램 전체를 테스트할 수 있는 양질의 입력 데이터를 얼마나 빨리 생성할 수 있는지를 가리키는 지표인 입력 데이터 유효성과 코드 커버리지(code coverage)에 따라 결정된다.

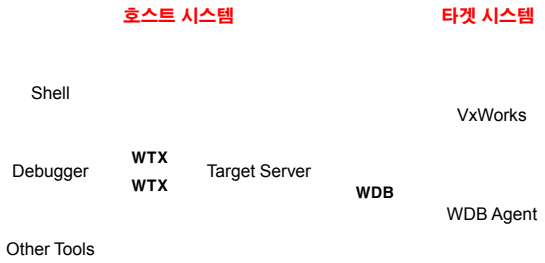
퍼징 시스템은 크게 퍼징 대상을 테스트하는 퍼저(fuzzer)와 퍼징 대상을 모니터링하는 모니터링 모듈로 구성된다. 퍼징 대상 모니터링 모듈은 퍼저를 보조하는 모듈로서 퍼징 대상을 모니터링하고 관리하는 기능을 수행한다. 본 논문에서는 VxWorks 환경에서 효과적인 퍼징을 제공하기 위해 요구되는 퍼징 대상 모니터링 기능을 정의하고 퍼징 대상 모니터링 모듈을 설계한다.

2. 보안취약점 분석대상 모니터링 기능 설계

VxWorks 환경에서 보안취약점 분석대상을 모니터링하는 기존 방법은 크게 재현 방식, VxWorks 도구 방식, WDB 방식, 후킹 방식 등 크게 4가지로 분류될 수 있다 . 재현방식은 충돌이 발생할 때까지 DBI(Dynamic Binary Instrumentation)를 이용하여 데이터 플로우 및 컨트롤 플로우를 저장하고, 향후 저장된 정보를 사용하여 프로그램 및 시스템 충돌을 재현하는 방식이다[2]. VxWorks 도구 방식은 VxWorks에서 제공하는 도구(예, Shell)를 사용하는 방식이며[3], WDB 방식은 VxWorks의 WDB(Wind River Debug) 프로토콜을 사용하여 원격에서 모니터링하는 방식이다[4-6]. 마지막으로 후킹 방식은 VxWorks 운영체제에서 예외 핸들러를 후킹하여 모니터링하는 방식이다. 산업제어시스템 환경에서는 운영체제를 변경하거나 또는 시스템에 별도의 프로그램을 설치하는 것이 제한적일 수 있기 때문에 재현방식과 후킹방식은 범용적이지 못할 수 있다. VxWorks 도구 방식은 수작업으로 진행되기 때문에 사용하기에 불편한 문제가 있다. 따라서 현재 VxWorks 도구 방식이 가장 선호되고 있다.

WDB 방식에서 WDB 프로토콜은 VxWorks 시스템사

의 WDB 에이전트를 통해 호스트에게 시스템 수준의 디버깅 서비스를 제공하는 RPC(Remote Procedure Call) 프로토콜이다. (그림 1)에 도시된 바와 같이 WDB 프로토콜 시스템은 VxWorks가 설치된 타겟 시스템에서 WDB 프로토콜 서버기능을 수행하는 WDB 에이전트와 WDB 프로토콜 클라이언트기능을 수행하는 타겟 서버로 구성된다. 타겟 서버는 쉘과 디버거 등 VxWorks 디버깅 도구와 VxWorks 간의 통신을 지원하기 위해 WTX(Wind River tool exchange) 프로토콜도 제공하고 있다. WDB 프로토콜은 세션관리(타겟 에이전트 접속 등), 메모리 연산(메모리 블록 읽기/쓰기 등), 컨텍스트 제어(새로운 컨텍스트 생성/삭제 등), 레지스터 조작(레지스터 설정/읽기), 가상 I/O, 이벤트 등록/삭제, 디버깅, 기타(함수 호출 등) 기능을 제공한다.



(그림 1) WDB 프로토콜 시스템

본 논문에서는 VxWorks 환경에서 효과적인 퍼징을 지원하기 위해 요구되는 보안취약점 분석대상 모니터링 기능을 다음과 같이 정의한다.

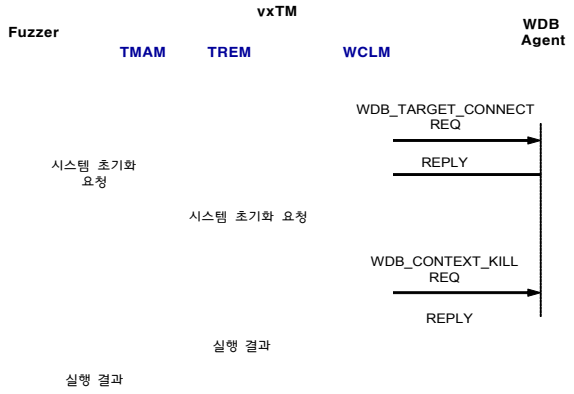
(1) 실행 상태 모니터링 기능: 보안취약점 분석대상이 정상적으로 동작하고 있는지를 모니터링하는 기능

(2) 충돌 탐지 및 관련 정보 획득 기능: 보안취약점 분석대상이 설치된 시스템이 비정상적으로 종료되었을 때, 그 종료를 유발시킨 소스코드의 위치와 관련정보(예, PC, 레지스터 정보 등)를 획득하는 기능

(3) 시스템 초기화 기능: 보안취약점 분석대상이 설치된 시스템이 비정상적으로 동작할 때, 보안취약점 분석대상 프로그램을 재실행하거나 시스템 자체를 재부팅(reboot)하는 기능

(4) 구성정보 수집 기능: 보안취약점 분석대상이 설치된 시스템의 구성정보(예, 테스크 ID, 테스크 이름, 시스템 정보 등)를 수집하는 기능

본 논문에서는 상기에서 정의된 보안취약점 분석대상 모니터링 기능을 제공할 수 있는 모니터링 시스템을 설계한다. 분석대상 모니터링 시스템은 TMAM(Target MAnagement Module), TNOM(Target NOtification Module), WCLM(WDB CLient Module) 등 총 3개의 모듈로 구성된다. TMAM은 시스템 초기화 기능과 구성정보 수집 기능을 제공하며, TNOM은 실행 상태 모니터링 기능 수행과 충돌 탐지 기능을 제공한다. WCLM은 WDB 프로토콜 클라이언트 기능을 제공한다. (그림2)는 시스템 초기화 기능을 제공하는 시퀀스 다이어그램이다.



(그림 2) 시스템 초기화 기능 시퀀스 다이어그램

3. 결론

본 논문에서는 VxWorks 환경에서 효과적인 퍼징을 제공하기 위해 요구되는 퍼징대상 모니터링 기능을 정의하고 퍼징대상 모니터링 모듈을 설계하였다.

참고문헌

[1] Parul Garg "Fuzzing-Mutation vs. Generation" INFOSEC Jan. 2012, https://resources.infosecinstitute.com/fuzzing-mutation-vs-generation/#gref

[2] Chunlei Ma, Xiang Long, Bo Jiang, Zhenyu Zhang "Replay Debugging of Real-Time Vxworks Applications" 2015 IEEE 39th Annual International Computers, Software & Applications Conference, 2015, 568-573

[3] 김우년, 장문수, 서정택, 김상욱 “제어프로토콜 퍼징 기반 열차제어시스템 취약점 검출 기법” 한국통신학회논문지, Vol.39 No.4, 2014

[4] Yannick Formaggio “Attacking VxWorks: from Stone Age to Interstellar,” 44CON LONDON 2015, 2015

[5] Knownsec Security Team "VxWorks Fuzzing: Vulnerability Mining Debugging & Exploitation of Industrial Control Real Time Operating Systems" 2016, http://blog.knownsec.com

[6] Jinlin Liu, Guangyuan Fu, Hailong Li "Research on VxWorks System Vulnerability Mining and Security Assessment" 2nd International Conference on Artificial Intelligence and Engineering Applications, 2017, pp. 634-643

Acknowledgement

본 연구는 2019년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2016M2A8A4952280)