단방향 프로토콜 소프트웨어 퍼징을 제공하기 위한 퍼징 상태 판단 기능 설계

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

Design of Fuzzing Status Judgment Function for One-way Protocol Software Fuzzing

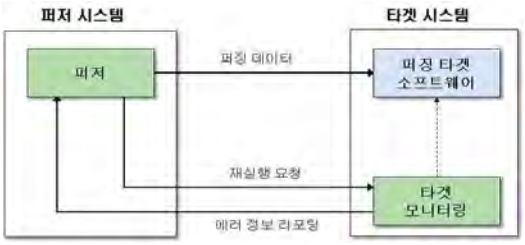
Gae-Il An, Yang-Seo Choi
Cyber Security Research Division, ETRI

요 약

소프트웨어 보안 취약점을 찾는 기술로서 퍼징(Fuzzing)이 있다. 기존 퍼징 기술은 요구-응답형 프로토콜을 사용하는 소프트웨어를 대상으로 하기 때문에 응답 메시지가 없는 단방향 프로토콜에서는 퍼징을 수행할 수 없는 문제가 있다. 본 논문에서는 단방향 프로토콜 소프트웨어에서 퍼징을 수행하는데 필요한 퍼징 상태 판단 기능을 정의하고 설계한다.

1. 서론

퍼징(Fuzzing) 기술은 컴퓨터 소프트웨어에 임의의 값을 무작위로 입력하여 만약 그 소프트웨어에 에러나 시스템 다운과 같은 충돌(crash)이 발생하면 그 원인을 분석하여 그 소프트웨어의 보안취약점을 찾아내는 기술이다[1-2].



(그림1) 퍼징(Fuzzing) 시스템

퍼징 시스템은 (그림 1)에 도시된 바와 같이 퍼저(Fuzzer)와 타겟(target) 모니터링, 그리고 퍼징 타겟 소프트웨어로 구성된다. 퍼저는 퍼징 타겟 소프트웨어에 충돌을 발생시키기 위해 임의의 값을 무작위로 입력하는 모듈이다. 타겟 모니터링은 퍼징 타겟 소프트웨어에 충돌이 발생했는지를 모니터링하고, 퍼저의 요청에 따라 타겟 시스템을 재부팅(rebooting)하거나 퍼징 타겟 소프트웨어를 재실행시키는 기능을 수행한다.

퍼저가 퍼징 타겟 소프트웨어에 퍼징 데이터 송신 기능을 정상적으로 수행하기 위해서는 퍼징 데이터 전송 시점과 퍼징 타겟 충돌 여부, 그리고 퍼징 데이터의 유효성 여부 등 현재의 퍼징 상태를 알고 있어야 한다. 기존 퍼징 기술은 요구(Request) 메시지를 보내면 응답(Response) 메시지를 회신하는 형태인 요구-응답형 프로토콜을 사용하는 소프트웨어를 대상으로 한다. 기존 퍼징 기술은 퍼징 타겟 소프트웨어가 회신하는 응답 메시지를 활용하여 퍼징 데이터 전송 시점과 퍼징 타겟 충돌 여부, 그리고 퍼징 데이터의 유효성 여부를 판단하고 있다.

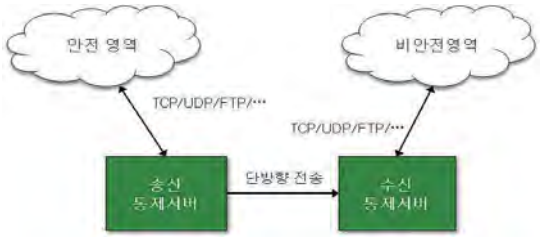
그러나 단방향 프로토콜을 사용하는 소프트웨어를 퍼징 대상으로 하는 경우에는 퍼징 타겟 소프트웨어가 응답 메시지를 회신하지 않기 때문에 기존의 방법으로 퍼징을 수행할 수 없는 문제가 있다. 단방향 프로토콜은 산업제어시스템 환경과 IoT(Internet of Things) 통신 환경 등에서 많이 사용되고 있다. 단방향 통신의 가장 큰 특징은 응답 메시지가 없다는 것이다. 단방향 프로토콜은 흐름 제어가 없어서 퍼징 데이터 전송으로 인한 네트워크 폭주가 발생할 수 있으며, 퍼징 타겟 소프트웨어에 충돌이 발생했는지도 알 수 없고, 또한 현재 전송하고 있는 퍼징 데이터가 유효한지도 알 수 없는 문제가 있다.

본 논문에서는 단방향 프로토콜을 사용하는 소프트웨어에 대해서도 정상적으로 퍼징을 수행할 수 있도록 퍼징 상태 판단 기능을 정의하고 설계한다.

2. 퍼징 타겟 모니터링 기능 설계

기존 퍼징 기술은 요구-응답형 프로토콜을 사용하는 소프트웨어를 대상으로 하기 때문에 퍼징 상태는 퍼징 타겟 소프트웨어가 회신하는 응답 메시지를 분석함으로써 판단할 수 있다. 즉, 퍼저는 송신한 퍼징 데이터에 대한 응답 메시지를 퍼징 타겟 소프트웨어로부터 수신하지 못하면 퍼징 타겟 소프트웨어에 충돌이 발생했다고 판단하며, 퍼징 타겟 소프트웨어의 응답 메시지에 에러나 실패라는 내용이 포함되어 있으면 그 응답 메시지를 유발한 퍼징 데

이터는 유효하지 않다고 판단한다. 또한 전송한 퍼징 데이터에 대한 응답 메시지를 퍼징 타겟 소프트웨어로부터 수신하면 그 퍼징 타겟 소프트웨어는 퍼징 데이터를 수신할 준비가 되어있다고 판단한다.



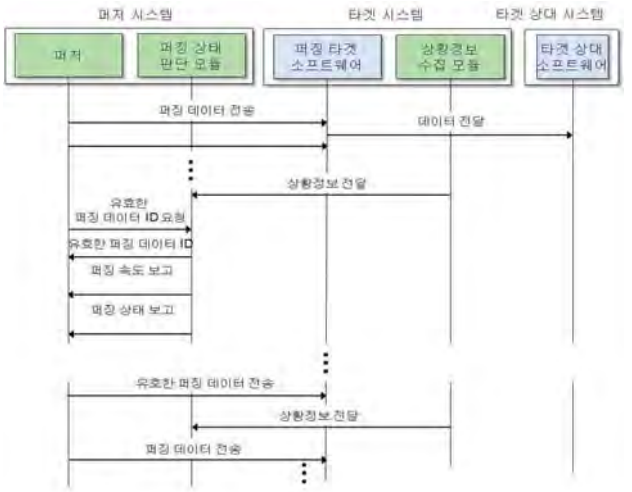
(그림 2) 단방향 데이터 전송 시스템

단방향 프로토콜은 망 분리를 통한 네트워크 보안을 목적으로 단방향 전송 시스템의 형태로 산업제어시스템 환경과 센서/시스템의 상태 정보 및 이벤트 정보 전달을 목적으로 IoT 통신 환경 등에서 많이 사용되고 있다. 단방향 통신의 가장 큰 특징은 응답 메시지가 없다는 것이다. (그림 2)는 산업제어시스템에서 안전영역을 보호하기 위하여 단방향 데이터 전송을 제공하는 송신통제 서버와 수신통제 서버를 도시한 그림이다[3]. 송신통제 서버와 수신통제 서버는 단방향 통신을 수행하기 때문에 송신통제 서버는 수신통제 서버에게 데이터를 보낼 수 있지만, 수신통제 서버는 송신통제 서버에게 데이터를 보낼 수 없다.

본 논문에서는 단방향 프로토콜을 사용하는 소프트웨어에게 정상적인 퍼징을 제공하는데 필요한 기능을 다음과 같이 정의한다.

(1) 상황정보 수집 기능: 퍼징 타겟 소프트웨어와 타겟 시스템을 모니터링하면서 상황정보를 수집하는 기능이다. 여기서 상황정보는 퍼징 타겟 소프트웨어의 CPU 및 메모리 사용량, 타겟 시스템에서 수행하는 네트워크 테스크의 CPU 사용량, 그리고 퍼징 타겟 소프트웨어와 타겟 상대 소프트웨어 간 통신 데이터 등을 포함한다. 여기서 타겟 상대 소프트웨어는 퍼징 타겟 소프트웨어가 통신하는 상대 소프트웨어를 말하며 데이터베이스 시스템, 하드웨어 시스템, 응용 시스템 등이 될 수 있다. (2) 퍼징 속도 결정 기능: 수집된 상황 정보 중에서 네트워크 테스크 및 퍼징 타겟 소프트웨어의 CPU 사용량을 분석하여 퍼저가 퍼징 데이터를 전송할 수 있는 최대 속도를 결정하는 기능이다. (3) 퍼징 유효성 판단 기능: 퍼징 타겟 소프트웨어에 어떠한 충돌도 발생시키지 않는 무의미한 퍼징 데이터는 퍼징 시간만 낭비할 수 있다. 본 기능은 수집된 상황 정보 중에서 퍼징 타겟 소프트웨어와 타겟 상대 소프트웨어 간 통신 데이터와 퍼징 타겟 소프트웨어의 메모리를 분석하여 퍼징 데이터의 유효성 여부를 분석하는 기능이다. (4) 퍼징 타겟 소프트웨어 충돌 탐지 기능: 수집된 상황 정보 중에서 퍼징 타겟 소프트웨어와 타겟 대상 소프트웨어 간 통신 데이터를 분석함으로써 퍼징 타겟 소프트웨어에 충돌이 발생했는지를 탐지하는 기능이다.

본 논문에서는 상기에서 정의된 단방향 프로토콜을 위한 퍼징 상태 판단 기능을 제공할 수 있는 시스템을 설계한다. 퍼징 상태 판단 기능을 제공하는 시스템은 (그림 3에) 도시된 바와 같이 상황정보 수집 모듈과 퍼징 상태 판단 모듈로 구성된다. 상황정보 수집 모듈은 상황정보 수집 기능을 수행하는 모듈이며, 퍼징 상태 판단 모듈은 퍼징 속도 결정 기능, 퍼징 유효성 판단 기능, 그리고 퍼징 타겟 충돌 탐지 기능을 수행한다. 퍼징 상태 판단 모듈의 수행 결과는 단방향 퍼저에서 사용한다.



(그림 3) 퍼징 상태 판단 기능의 동작

3. 결론

본 논문에서는 상황정보를 기반으로 퍼징 상태를 판단할 수 있는 방법을 제시하였다. 제안하는 방법은 단방향 프로토콜을 사용하는 산업제어시스템 및 IoT(Internet of Things) 시스템에 대한 퍼징을 제공할 수 있다는 점에서 기존 방법과 차별된다.

참고문헌

[1] 오상환, 김태은, 김환국, "SW 보안 취약점 자동 탐색 및 대응 기술 분석," 한국산학기술학회논문지 제18권 제11호, 2017

[2] 안개일, 송원준, 최양서, "VxWorks 환경에서 효과적인 퍼징 테스트를 위한 보안취약점 분석대상 모니터링 기능 설계," 한국정보처리학회 추계학술대회논문집, 2019.11

[3] 허영준외 6명, "다중 서비스 단방향 데이터 전송을 제공하는 단방향보안게이트웨이 구현," 한국통신학회 학술대회논문집, 2017.11

Acknowledgement

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