

그레이 박스 테스트를 활용한 스마트 퍼징 시스템 연구

김만식*, 김민진*, 염윤호**, 전문석*

*송실대학교 컴퓨터학과

**송실대학교 정보과학대학원 정보보안학과

e-mail : mansik@ssu.ac.kr

minjini57@ssu.ac.kr

duadbsgh@naver.com

mjun@ssu.ac.kr

A Study on Smart Fuzzing System Based on Grey Box Test

Mansik Kim*, Minjin Kim*, Yun-Ho Yeom**, Moon-Soeg Jun*

*Dept. of Computer Science & Engineering, Soongsil University

**Graduate School of Information Sciences, Soongsil University

요 약

유비쿼터스 시대가 ICT 산업의 발달과 함께 도래함에 따라 이용자들의 요구를 충족시켜주는 다양한 서비스들이 소프트웨어 형태로 등장하고 있다. 이제는 단순 컴퓨터 뿐만이 아니라 모바일, 웨어러블 디바이스, 자동차, 로봇, 의료 산업 등 까지 소프트웨어는 현대 사람들의 삶에 깊이 연계되어 있으며 아직도 그 영역은 팽창하고 있다. 이러한 소프트웨어의 풍부한 발달과 비례로 소프트웨어의 취약점을 공략하여 서비스에 치명적인 위협을 가해 이익을 얻으려는 단체도 증가하게 되었다. 본 논문에서는 소프트웨어를 출시하기 전에 취약점을 미리 탐지·식별 할 수 있는 그레이 박스를 활용한 스마트 퍼징 시스템을 제안한다.

1. 서론

ICT 산업의 발달에 따라 소프트웨어의 분야는 단순 컴퓨터를 넘어 모바일, 웨어러블 디바이스, 자동차, 로봇 의료산업 등 다양한 영역에서 이용되고 있다. 이렇게 소프트웨어가 제공하는 서비스의 규모가 거대해짐에 따라 사용자의 정보나 서비스 품질 저하 등을 노리는 공격이 증가하고 있다. 대표적인 사례로 OpenSSL 하트블리드 제로데이 공격이 2014년 4월 보안 패치 이전의 취약점을 공략하였으며, Paypal은 소프트웨어 자체 취약점을 통해 2010년 사이버 공격을 당했었다[1]. 미국 컴퓨터 보안 전문업체인 Symantec에 따르면 2012년도에만 5,291개의 취약점이 발견되었다고 한다[2].

이제 소프트웨어 취약점은 서비스 제공자의 문제뿐만 아니라 범국가적 사안으로 국내외에서 문제를 해결하기 위해 다양한 노력을 하고 있다. 대표적으로 미국의 MITRE는 미국 국토보안부의 국가 사이버 보안국 지원을 받아 CWE(Common Weakness Enumeration)를 수립하여 소프트웨어 취약점을 분류하고 있으며, CERT(Computer Emergency Response Team)에서는 다양한 개발 언어를 대상으로 시큐어 코딩 가이드를 제공하고 있다[3]. 뿐만 아니라 국내에서는 행정안전부에서 2012년 5월 시큐어 코딩 의무화 법안을 통해 40억 이상의 정보화 사업은 행정안전부가 제공

하는 시큐어 코딩 가이드 라인을 준수하여 43개의 취약점을 반드시 제거해야 한다고 명시하고 있다.

퍼징은 이러한 노력의 일환으로 소프트웨어의 취약점을 검출하기 위한 테스팅 기법으로 Barton Miller 교수 연구실에서 1989년에 개발되었지만 소프트웨어 취약점을 검출하기 위해 많은 시간이 걸린다는 단점을 지니고 있다[4].

본 논문에서는 그레이 박스를 활용하여 스마트 퍼징을 통해 적은 노력으로 소프트웨어의 취약점을 탐지·식별 할 수 있는 시스템을 제안한다. 2장에서는 스마트 퍼징과 그레이박스 테스팅에 대해서 알아본 후 3장에서 이 논문에서 제안하는 시스템에 대하여 자세히 기술한다. 4장에서는 평가를 하고, 5장에서 결론을 제시한다.

2. 관련연구

2.1 스마트 퍼징

무작위로 값을 산출하여 소프트웨어에 입력하여 충돌이나 예견되지 않은 결과값을 도출함으로써 소프트웨어의 취약점을 탐색 및 식별하는 테스트를 퍼징이라 한다. 그러나 퍼징을 통한 입력값 대비 결과값의 전수조사는 많은 시간을 요구한다는 단점이 있다. 스마트 퍼징은 이러한 단점을 극복한 테스팅 기법으

* 본 논문은 미래창조과학부의 2015년 고용계약형 SW 석사과정 지원사업을 지원받아 수행한 결과임

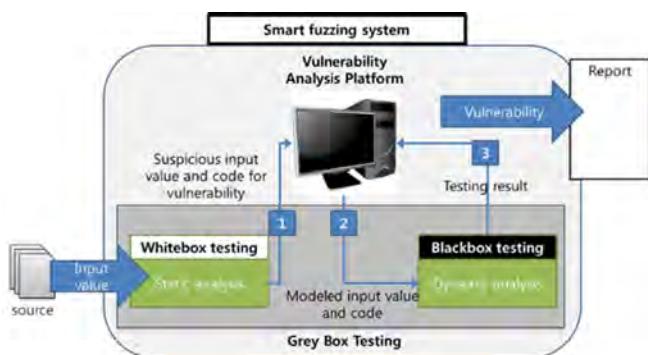
This work was supported by the ICT R&D program of MSIP/IITP. [R0112-14-1061, The analysis technology of a vulnerability on an open-source software, and the development of Platform]

로 무작위로 입력값을 선출하는 것이 아니라, 일정한 규칙을 통하여 모델링화 된 입력값을 통해 결과값을 도출하는 자동화된 퍼징 시스템이다[5]. 소프트웨어의 규모와 수가 증가하는 만큼 스마트 퍼징은 소프트웨어 테스트를 위한 필수적 요소가 되고 있다.

2.2 그레이박스 테스팅

소프트웨어를 테스트를 하기 위해 대표적으로 블랙박스 테스트와 화이트박스 테스트가 있다. 블랙박스 테스트는 소프트웨어의 내부적 사양(소스코드, 기술요소 등)을 모르는 상태에서 값을 입력하여 결과값을 도출하는 테스트로, 수행하기 쉽다는 장점이 있지만 시간이 많이 걸리고 논리적 오류를 탐지 하지 못한다는 단점이 있다. 화이트박스 테스트는 소프트웨어 소스코드에 접근하여 내부적 동작을 검사하여 입력값이 어떻게 결과값을 도출하는지 검사하는 테스트로, 논리적 오류 및 숨어 있는 에러를 식별할 수 있다는 장점이 있지만 수행하기 어렵고 비용이 비싸다는 단점이 있다. 그레이박스 테스트는 이러한 블랙박스 테스트와 화이트박스의 장점을 결합한 테스트 기법이다[6].

3. 제안하는 스마트 퍼징 시스템



(그림 1) 제안하는 스마트 퍼징 시스템

제안하는 스마트 퍼징 시스템 구조는 [그림 1]과 같이 그레이박스 테스트와 취약점분석 플랫폼으로 이루어져 소스코드를 입력값으로 취약점을 탐지·식별한다. 그레이박스 테스트는 화이트박스 테스트와 블랙박스 테스트를 취약점 분석 플랫폼과 연계해서 취약점을 검출하고, 취약점 분석 플랫폼은 취약점 시그내처를 저장하고 비교 분석하며, 그레이박스에서 도출한 결과값을 모델링화하고 취약점을 판별하여 보고한다.

스마트 퍼징 테스트 대상이 되는 소프트웨어는 처음에 소스코드의 형태의 입력값이 되어 그레이박스 테스트 내의 화이트박스 테스트를 통해 정적 분석을 수행하게 된다. 화이트박스 테스트는 정적 분석을 통해 소스코드내의 논리적 취약점을 검출하고 최종적으로 취약점을 도출할 것이라 의심되는 입력값과 의심 코드를 취약점 분석 플랫폼에게 전달한다. 의심 코드와 입력값을 전달 받은 취약점 분석 플랫폼은 기존에 취약코드로 검출되어 DB에 저장하고 있던 취

약점 시그내처와 비교분석을 하여 취약코드를 판별하고 블랙박스 테스트를 위한 입력값을 모델링한다. 입력값 모델링은 취약점 시그내처를 기반으로 취약코드가 실행되기 위한 실제 SW 입력값과 기대되는 취약점 결과를 선별한다. 최종 테스트를 위하여 블랙박스 테스트에게 모델화된 입력값과 소스코드를 전달한다. 또한 옵션으로 비교분석에서도 취약점이라 결정되지 않은 값도 신규 취약점에 대비하기 위해서 모델화하여 블랙박스 테스트에 보낼 수 있도록 한다. 옵션에서는 해당 SW에 결과값을 예측할 수 없는 정규화되지 않은 입력값으로 선별하여 블랙박스 테스트를 통해 취약점이 노출되는지 정상 결과와 비교분석 한다. 블랙박스 테스트는 취약점 분석 플랫폼으로부터 전달받은 데이터로 동적 테스트를 진행한다. 동적 테스트를 통해서 최종적으로 취약점을 확정하고 취약점 분석 플랫폼에게 보고한다. 옵션으로 취약점의 심 코드로 판별되지 않았지만 취약점이 검출된 코드 또한 추가로 보고한다. 블랙박스 테스트로부터 결과데이터를 전달 받은 취약점 분석 플랫폼은 확정된 취약점에 대하여 보고서를 작성하고, 신규 취약점은 추가로 시그내처를 생성하여 DB에 보관한다. 최종적으로 사용자에게 취약점 검출 결과를 전달한다.

4. 제안 시스템 평가

제안하는 스마트 퍼징 시스템은 기존의 퍼징 시스템에서 무작위로 모든 값을 대입하는 전수조사 테스트 수행으로 많은 시간이 필요로 하는 문제점을, 화이트박스와 블랙박스의 장점을 결합한 그레이박스를 활용하여 취약점 분석 플랫폼과의 연계를 통해 효율적으로 취약점을 검출하도록 하였다. 기존의 시스템을 구성요소를 활용하여 구축하기 쉬운 시스템 구조를 제안 하였을 뿐만이 아니라, 각 구성요소의 역할과 요구사항을 기술하여 시스템을 체계화 하였다.

5. 결론

ICT 산업이 발달함에 따라 증가하고 있는 소프트웨어 취약점은 이제 단순 기업이 아니라 국가적 사안으로 다뤄지고 있다. 이러한 취약점은 소프트웨어가 출시되기 이전에 미리 차단하기 위해서 탐지 및 식별하여 사전에 보안 테스트를 수행 할 수 있는데, 퍼징을 통하여 무작위 입력값에 대한 취약점을 검출할 수 있다. 본 논문에서는 이러한 기존의 퍼징 시스템이 취약점을 검출하는데 많은 시간과 노력을 필요하는 문제를 해결하기 위하여, 그레이박스 테스트와 연계된 취약점 분석 플랫폼을 통하여 자동화된 스마트 퍼징 시스템을 제안함으로써 효율성을 향상시키고 시스템을 체계화 하였다.

참고문헌

- [1] Software security weaknesses diagnostic guide, KISA, 2012
- [2] Symantec, "2013 Internet Security Threat Report, Volume 18," 2013

- [3] Robert C. Seacord, The CERT C Secure Coding Standard, Addison-Wesley, October 2008
- [4] Sutton, Michael, Adam Greene, and Pedram Amini. Fuzzing: brute force vulnerability discovery. Pearson Education, 2007.
- [5] Bekrar, S., Bekrar, C., Groz, R., & Mounier, L. Finding software vulnerabilities by smart fuzzing. In Software Testing, Verification and Validation (ICST), IEEE Fourth International Conference, pp. 427-430. 2011
- [6] KHAN, Mohd Ehmer; KHAN, Farmeena. A Comparative Study of White Box, Black Box and Grey Box Testing Techniques. Editorial Preface, 2012, 3.6