효율적인 시큐어코딩 프로그램 운영을 위한 시큐어코딩 관리 시스템 설계 기법

송석화*, 김민진*, 양승민**, 전문석*
*숭실대학교 컴퓨터학과
**(주)이븐스타
e-mail:shsong@ssu.ac.kr
minjini57@ssu.ac.kr
yan0381@evenstar.co.kr
mjun@ssu.ac.kr

A Design of Secure Coding Management System for Efficient Secure Coding Program Operation

Seokhwa Song*, Minjin Kim*, SeungMin Yang**, Moon-Seog Jun*
*Dept of Computer Science & Engineering, Soongsil University
**Evenstar Inc.

요 약

최근 사물인터넷(IoT)이 도래함에 따라 IT 산업을 중심으로 소프트웨어의 활용 용도가 컴퓨터 뿐 아니라, 의료, 교육, 금융, 자동차, 에너지 등 다양한 분야에서 활용되고 있다. 이처럼 소프트웨어 활용 분야가 본격적으로 확산됨에 따라 소프트웨어 보안 취약점을 이용한 공격위험 또한 증가하고 있으며. 이에 따라 시큐어코딩의 중요성이 부각되고 있다. 본 논문에서는 기존 시큐어코딩 관리 시스템 환경에서 효율적인 시큐어코딩 관리를 위해 운영서버와 Program Server를 이용한 시큐어코딩 관리 시스템 향상 방안을 제안한다. 제안하는 시스템을 시큐어코딩 프로그램에 적용한다면, 시큐어코딩 프로그램 성능향상과 효율적인 시큐어코딩 시스템 관리에 도움이 될 것으로 기대된다.

1. 서론

최근 사물인터넷(IoT)이 도래함에 따라 IT 산업을 중심으로 소프트웨어의 활용 용도가 컴퓨터 뿐 아니라, 의료, 교육, 금융, 자동차, 에너지 등 다양한 분야에서 활용되고 있다. 소프트웨어 활용 분야가 본격적으로 확산되는 이러한 상황에서 소프트웨어 보안 취약점을 이용한 공격위험 또한 증가하고 있다. 실제로 SW 자체의 보안취약점을 악용하는 공격인 UPnP 프로토콜 취약점 공격, 오라클 자바(JAVA)의 제로데이 취약점 공격, 한글 소프트웨어에 존재하는 취약점을 악용한 타깃 공격 등의 공격이 지속적으로 발생하고 있으며, 최근엔 정상적인 애플리케이션에 난독화된 스크립트를 삽입해 정상적인 웹 서비스에 악성코드를 숨겨 이용자들을 감염시키는 지능형 공격이 증가하고 있다. 이에 따라 소프트웨어의 취약점을 개발단계에서부터 사전에 제거해 안전한 소프트웨어를 개발할 수 있는 시큐어코딩의 필요성이 제기 되었고, 이러한 흐름에 따라 행정안전부에서는 2011년부터 시큐어코딩 의무화를 단계적으로 시행하고 있으며, 2015년부터 공공기관과 정보화 산업 전 분야에 걸쳐 시큐어코딩을 의무화적으로 적용한다는 정책을 발표했다.

국외에서는 CWE/SANS에서 가장 위험한 25가지의 소프트웨어의 오류를 정리해 산업에 문제가 되어 왔던 다양한 취약성을 프로그래머들이 예방할 수 있도록 작성된 'CWE/SANS Top 25 Most Dangerous Software Errors', 나 OWASP의 'The Open Web Application Security Project Top 10' 등 취약점을 공개함으로서 개발자가 안전한 프로그램 개발할 수 있는 다양한 정보를 제시하고 있다. 이렇듯 소프트웨어 보안 약점에 대한 이슈가 지속적으로 발생하고 있으며, 이로 인해 시큐어코딩 프로그램의 퍼포먼스의 중요성 또한 증가하고 있다.

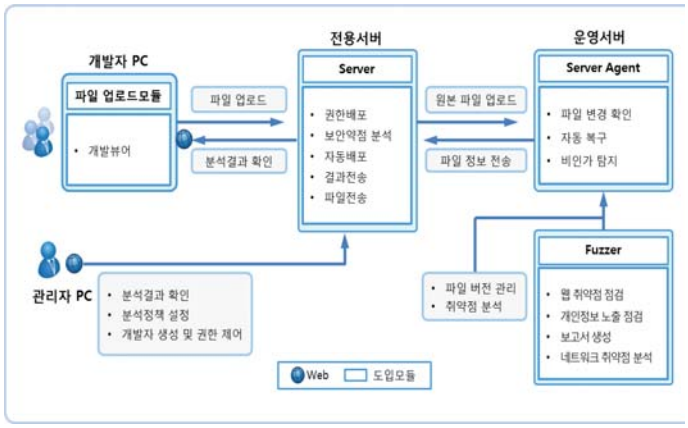
따라서, 본 논문에서는 기존 시큐어코딩 관리 시스템 환경에서 효율적인 시큐어코딩 관리를 위해 운영서버와 Program Server를 이용한 시큐어코딩 관리 시스템 향상 방안을 제안한다.

2. 제안 내용

2.1 시스템 구성도

제안하는 시스템 구성은 소스파일을 업로드, 다운로드, 편집하는 개발자 PC, 소스파일 권한 배포, 보안약점 분석을 통한 파일 및 결과를 전송하는 전용서버, 소스파일 취약점 점검을 진행하는 운영서버, 취약점을 점검하고 분석결과를 제공해주는 Fuzzer, 전용서버로부터 받은 분석결과를 토대로 정책 및 권한을 설정하는 관리자 PC 등으로 구성되어있다.

※ 이 논문은 2016년도 중소기업청의 산학연구마을 지원사업의 지원을 받아 수행된 연구임.

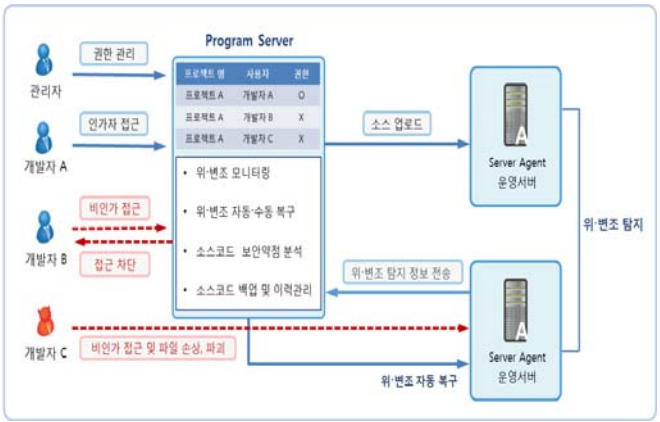


(그림 1) 운영단계에서의 시큐어코딩 관리 시스템

2.2 운영단계에서의 시큐어코딩 관리 시스템

개발자 PC는 개발뷰어를 통해 소스파일을 전용서버에 업로드, 다운로드, 편집을 진행하며, 업로드 된 소스파일은 전용서버를 통해 권한배포 및 보안약점 분석을 진행하여 운영서버로 원본 소스파일을 업로드한다. 운영서버는 파일 변경 확인, 자동 복구, 비인가 탐지 등을 통해 취약점 점검을 진행하며, Fuzzer와 연동하여 웹 취약점 점검, 개인정보 노출 점검, 보고서 생성, 네트워크 취약점 분석 등을 통해 파일 버전을 관리하고 취약점을 분석한다. 운영서버는 소스파일에 대한 취약점 점검 결과 파일 정보를 전용서버로 전송하며, 개발자 PC는 전용 웹을 통해 전용서버로부터 소스파일 취약점 점검 분석결과를 확인한다. 관리자 PC는 웹을 통해 전용서버로부터 업로드 된 취약점 분석 결과 정보를 확인하고 분석정책 설정 및 개발자 생성 및 권한 제어를 설정한다.

2.3 시큐어코딩 관리 시스템 Server Agent 구성도



(그림 2) 시큐어코딩 관리 시스템 Server Agent 구성도

관리자와 개발자는 Program Server에 접근이 가능하며 운영서버는 Program Server를 통해 기존 운영서버의 위·변조 현황을 모니터링 하여, 권한 외의 사용자 및 공격자의 자원 위·변조 시 자동 및 수동 복구 기능을 제공하며, 소스코드 보안약점 분석 및 백업 및 이력관리를 제공한다. Program Server를 통해 소스 업로드 된 운영서버는 위·변조 자동 복구 운영서버와 상호협력 하여 위·변조 탐지가 이루어진다. 비인가 접근 또는 파일 손상, 파괴 접근시에는 위·변조 탐지 정보 전송을 통해 접근차단이 된다.

3. 결 론

최근 IT 산업을 중심으로 소프트웨어의 활용 용도가 다양한 분야에서 적용되고 있다. 소프트웨어 활용 분야가 본격적으로 확산됨에 따라 소프트웨어 보안 취약점을 이용한 공격위험 또한 증가하고 있으며. 이에 따라 시큐어코딩의 중요성이 부각되고 있다. 본 논문에서는 기존 시큐어코딩 관리 시스템 환경에서 효율적인 시큐어코딩 관리를 위해 운영서버와 Program Server를 이용한 시큐어코딩 관리 시스템 향상 방안을 제안하였다. 제안하는 시큐어코딩 관리 시스템은 운영서버를 통해 비 인가자의 자원 위·변조 탐지 및 자동 복구가 가능해 시큐어코딩 프로그램 성능향상과 효율적인 시큐어코딩 시스템 관리에 도움이 될 것으로 기대된다.

참고문헌

[1] 행정자치부, “공개SW를 활용한 소프트웨어 개발보안 점검가이드”, 2016.02
[2] 행정자치부, “소프트웨어 보안약점 진단가이드”, 2014.05
[3] 행정자치부, 한국인터넷진흥원, “JAVA 시큐어코딩 가이드”, 2016.03
[4] 행정자치부, 한국인터넷진흥원, “모바일 전자정부서비스 앱 소스코드 검증 가이드라인 v5.0” 2015.12
[5] Bob Martin, Mason Brown, Alan Paller, Dennis Kirby, “2011 CWE/SANS Top 25 Most Dangerous Software Errors”, 2011.09
[6] OWASP, “The Open Web Application Security Project Top 10”, 2013.10