소프트웨어 취약점 보안을 위한 시큐어코딩 시스템 설계 기법

이재승*, 구윤회**, 전문석*
*숭실대학교 컴퓨터학과
**(주)이븐스타
e-mail : ljs0322@ssu.ac.kr
kyh@evenstar.co.kr
mjun@ssu.ac.kr

Secure Coding System Design Techniques for the Efficient Operation of the Secure Coding Program

Jae-Seung Lee*, Yun-Hoe Koo**, Moon-Seog Jun*
*Dept of Computer Science, Soongsil University
**Evenstar Inc.

요 약

Internet of Things 시대의 등장과 디바이스의 발달로 소프트웨어가 다양한 분야에서 활용 되면서, 소프트웨어의 자체 취약점을 이용한 공격 시도가 증가하고 있다. 이에 따라, 안전행정부에서는 소프트웨어 개발 사업 분야에 시큐어코딩을 의무화 하였으며, 그 결과로 다양한 시큐어코딩 프로그램이 활용되고 있다. 하지만 기존 시큐어코딩 프로그램의 경우 이력관리나 CMS 연동 과정에서 다양한 문제를 야기 시키고 있으며, 성능적으로도 한계점을 가지고 있다. 따라서, 본 논문에서는 형상관리 시스템과 CMS 연동, 유사도 분석 적용과 실시간 업데이트 등을 적용하는 시큐어코딩 시스템 설계 방법을 제안하였다. 제안하는 설계 기법을 시큐어코딩 시스템에 적용한다면 시큐어코딩 시스템 성능 향상을 물론 다양한 보안위협에 대응 가능할 것으로 기대된다.

1. 서론

Internet of Things(IoT)시대의 등장과 다양한 IT 디바이스들이 지능화, 그린화, 무선화로 인해 소프트웨어는 컴퓨터나 스마트 디바이스 뿐 아니라, 자동차나, 가전기기, 의료기기 등 다양한 분야에서 활용되고 있다. 이렇듯, 소프트웨어 사용이 증가함에 따라, 그에 따른 소프트웨어 취약점을 이용한 공격 시도 또한 다양해지고 있다. 실제 소프트웨어 산업이 2016년 전년대비 4.3% 성장한 12조 5천억 규모에 이를 것으로 전망되고 있으며, 이와 비례 하여 소프트웨어의 자체 취약점을 이용한 공격 시도 또한 지속적으로 증가하고 있다.

이렇듯, 지속적으로 증가하고 있는 소프트웨어 취약점 문제를 근본적으로 해결하기 위해 소스코드 작성 단계(소프트웨어 개발 단계)에서부터 보안 취약점을 점검할 수 있는 시큐어코딩의 필요성이 제기 되었다. 시큐어코딩의 경우 소프트웨어 개발 단계에서부터 이후에 발생할 수 있는 취약점을 도출하여, 개발자가 수정할 수 있도록 유도함으로서 취약점으로부터 원천적 차단이 가능하다. 이에 따라, 안전행정부에서는 2011년부터 시큐어코딩 의무화를 단계적으로 시행하였으며, 2015년 부터는 소프트웨어 전 사업에 거쳐 의무화를 진행하도록 하였다.

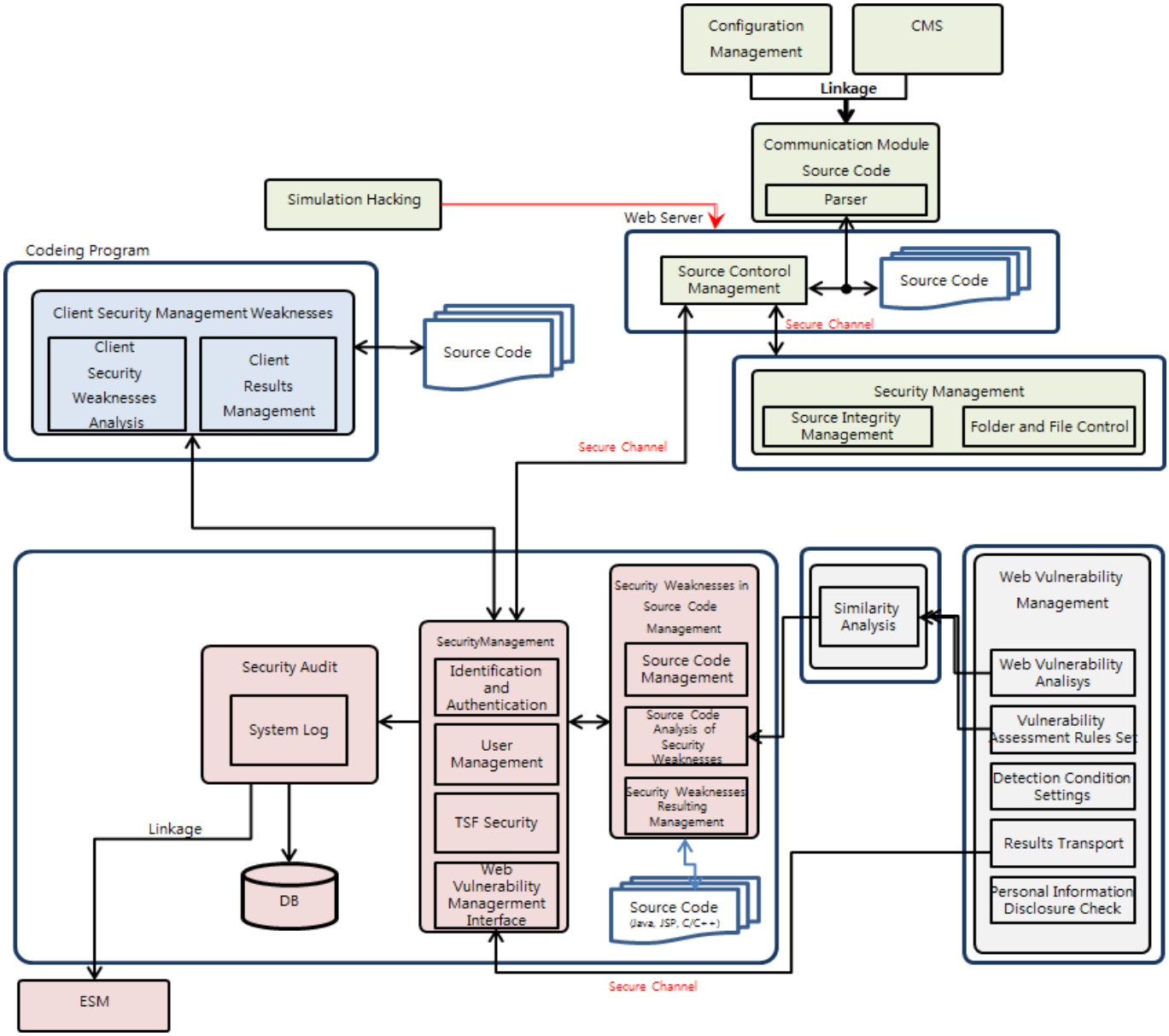
그러나, 현재 기존 시큐어코딩의 프로그램들은 시큐어코딩 시스템 내 자원들의 변경, 수정, 삭제 등 이력관리에 대한 로그관리를 진행하고 있지만, 소프트웨어 취약점의 경우 제로 데이 공격(Zero-Day Attack)과 같이 새로운 취약점이 발생하거나 새로운 보안 이슈가 발생할 경우 실시간으로 소스코드에 적용될 수 없는 환경으로 수정되지 않는 소스코드 발생이 원격지에서 새로운 취약점으로 발생하고 있다. 또한, 다양한 시큐어코딩 프로그램들이 CMS 시스템과의 연동을 통해 다양한 UI를 효율적으로 제공해 주지만, 개인이 제작한 API 모듈에 대해서는 소스코드 취약점을 보완할 수 없기 때문에 악의적인 사용자는 취약한 API 모듈을 통해 공격을 할 수 있는 문제점들을 가지고 있다.

따라서, 본 논문에서는 소스코드 송신 모듈에 형상관리의 연동, CMS연동 과정에서 컨텐츠 단위의 취약점 점검, 유사도분석을 통한 취약점 분석 기능 향상 및 주기적 업데이트, 리포팅 기능 실시간 업데이트 제공 등을 제공하여 효율적인 시큐어코딩 프로그램을 설계하는 시큐어코딩 시스템 설계 방안을 제안한다.

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

2. 시큐어코딩 프로그램 설계도

제안하는 시큐어코딩 프로그램 설계 방안은 (그림 1)과



(그림 1) 시큐어코딩 시스템 프로그램 설계도

같다. 먼저, 소스코드 송신모듈에 형상관리를 연동하여 소스코드 생성, 변경, 삭제를 확인 및 보안점검을 재실행하여 관리하고 안전할 경우 재배포 하는 등의 체계적인 관리가 가능하며, 소스코드 송신모듈에 CMS를 연동하여 컨텐츠 단위로 소스코드의 취약점을 점검하고 관리하며 이를 웹서버에 반영이 가능하다.

시스템로그와 ESM을 연동하여 방화벽, 침입탐지 시스템, 가상사설망 등을 솔루션 화하여 체계적으로 지원 프로그램을 체계적으로 관리 가능하며, 유사도분석을 통해 웹 취약점 분석, 소스코드 보안약점 분석을 중계하고 소스코드에 대하여 패턴 및 유사도 분석 등을 통하여 이를 규칙화하여 소스코드 점검, 주기적 업데이트 내용에도 제공 한다. 또한, 리포트 기능 제공을 통해 보안 취약점 발생 이력과 해결 시기, 해결 방법 등에 대한 현황을 파악하여 체계적인 관리 지원을 할 수 있다.

3. 결론

본 논문은 시큐어코딩 과정을 체계적으로 관리하기 위해 형상관리 시스템, CMS와 연동하는 시스템을 설계 하였으며, 유사도분석을 통한 취약점 분석 기능 향상과 주기적 업데이트, 리포팅 기능 실시간 업데이트 기능 모듈들을 추가하여 효율적인 시큐어코딩 시스템 운영이 가능하도록 설계하였다.

제안하는 시스템을 통해 시큐어코딩 시스템을 구현한다면, 유사도 분석, 실시간 업데이트를 통한 시큐어코딩 프로그램 자체 성능의 향상 뿐 아니라, 형상관리, CMS 연동 등을 통한 체계적 관리를 통해 시스템 자체의 보안적 관리가 가능 할 것으로 기대된다.

참고문헌

[1] 행정안전부, “소프트웨어 개발보안 가이드” 5월 , 2012