시큐어코딩 프로그램 형상관리 시스템 연동 프로세스 설계 방법

이재승*, 정하규*, 박세영**, 전문석*
*숭실대학교 컴퓨터학과
email : ljs0322@ssu.ac.kr

Design Method of Linking Process for Secure Coding Program Configuration Management System

Jaeseung Lee*, Hague Chung*, Seyoung Park Moon-Seog Jun*
*Dept of Computer Science, Soongsil University
**Graduate School of Information Sciences, Soongsil University

요 약

최근 유비쿼터스 컴퓨팅 시대가 도래함에 따라 소프트웨어는 스마트기기, 홈 네트워크 등 다양한 분야에 활용되고 있으며, 이러한 환경 변화에 맞춰 해커들은 소프트웨어의 자체 취약점을 이용한 다양한 악의적 공격을 진행하고 있다. 실제 소프트웨어 보안 취약점으로 인해 발생하는 피해액이 연간 1800억불에 달하고 있으며, 이러한 문제를 방지하기 위해 다양한 시큐어코딩 제품들이 등장하고 있다. 본 논문에서는 기존 시큐어코딩 프로그램의 효율성 향상을 위한 형상관리 시스템 연동 프로세스 방법을 제안한다.

1. 서론

유비쿼터스 컴퓨팅(Ubiquitous Computing)시대가 도래함에 따라 소프트웨어는 스마트기기, 홈 네트워크 등 다양한 환경에서 활용되고 있으며, 이러한 환경에 맞춰 해커들은 소프트웨어의 보안 취약점을 이용한 다양한 공격 시도로 다양한 피해를 야기 시키고 있다.

실제 소프트웨어의 보안 취약점을 이용한 공격으로 전 세계적으로 연간 1800억불에 이르는 피해가 발생하고 있으며, 보안 취약점이 발견된 후 이를 수정하는 과정에서도 많은 비용이 발생하고 있다.

따라서 국내에서는 안전한 소프트웨어 개발을 위해 제도적으로 시큐어코딩 의무화를 진행하고 있으며, '소프트웨어 개발보안 가이드'와 같은 가이드라인을 배포하여 소프트웨어 취약점 보안위협에 대응하기 위해 노력하고 있으며, 국외에서는 CWE/SANS의 'CWE/SANS Top 25 Most Dangerous Software Errors' 나 OWASP의 'The Open Web Application Security Project Top 10' 등 취약점을 공개함으로서 개발자가 안전하게 소프트웨어를 개발하도록 제공하고 있다.

소프트웨어의 보안 취약점의 경우 초기 개발 과정에서 입력 값의 검증 누락, 잘못된 형식 수락으로 인한 버그, 사용자 인증 절차 누락, 시스템 제어 및 권한 설정 오류 등으로 발생할 수 있으며, 이러한 문제점을 초기에 방지하기 위해 개발 단계부터 보안 취약점을 발견하고 분석할 수 있는 시큐어코딩 시스템이 부각되고 있다.

시큐어코딩의 경우 소프트웨어의 설계 단계부터 코딩단계, 통합단계, 베타 과정, 제품 출시 과정 전 과정에서 활용가능하며, 전 단계에 걸쳐 소프트웨어의 오류 및 취약점을 확인하고 분석하여 올바른 방향으로 소프트웨어를 개발 하도록 유도한다. 이렇듯 시큐어코딩의 필요성이 부각됨에 따라 다양한 시큐어코딩 제품들이 출시되고 있으며, 시장규모 또한 증가하고 있다.

본 논문에서는 시중에 활용되고 있는 시큐어코딩 프로그램의 성능 향상을 위해 시큐어코딩 프로그램에 맞는 효율적인 형상관리 프로세스와 형상관리 도구와 취약점 분석 도구의 연동 방법을 제안한다.

2. 제안 내용

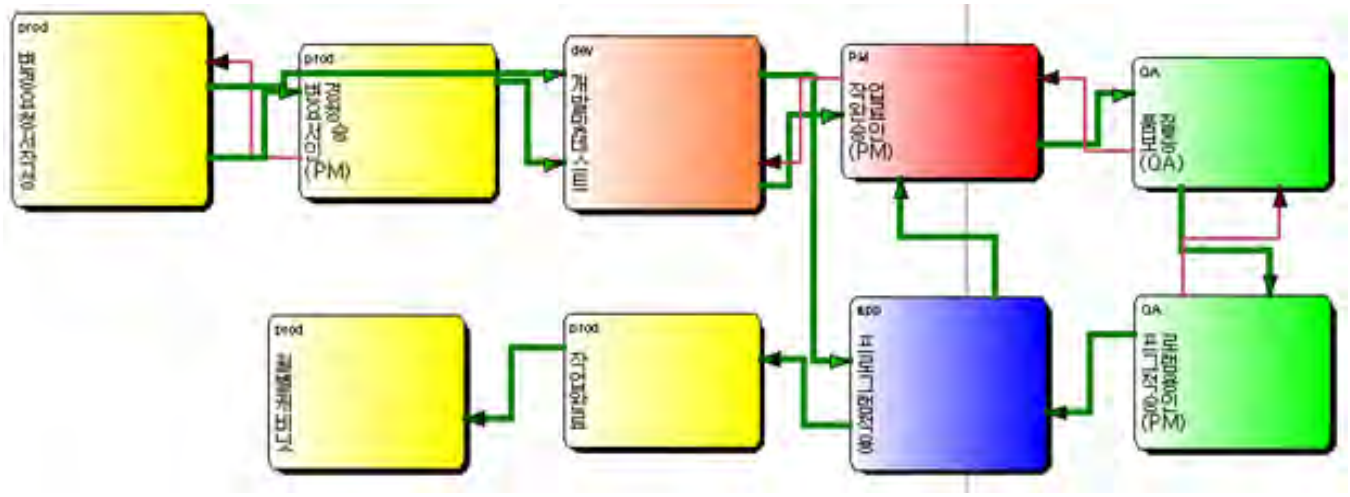
2.1 형상관리 시스템 연동 프로세스

본 논문에서는 소스코드 점검 시스템을 적용하기 위한 형상관리 프로세스를 제안한다. 제안하는 형상관리 프로세스는 다음과 같다.

1. 변경요청서를 작성하고 승인요청한다.
2. 변경요청서는 PM 승인 후 개발 및 테스트 단계로 이동한다.
3. 프로그램 개발 및 테스트를 수행한 후 작업완료 승인 요청한다.

   이때, 변경요청서에 포함된 수정 및 개발된 소스파일

※ 본 논문은 미래창조과학부의 2015년 고용계약형 SW석사과정 지원사업을 지원받아 수행한 결과임
※ 이 논문은 2015년도 중소기업청의 산학연구마을 지원사업의 지원을 받아 수행된 연구임



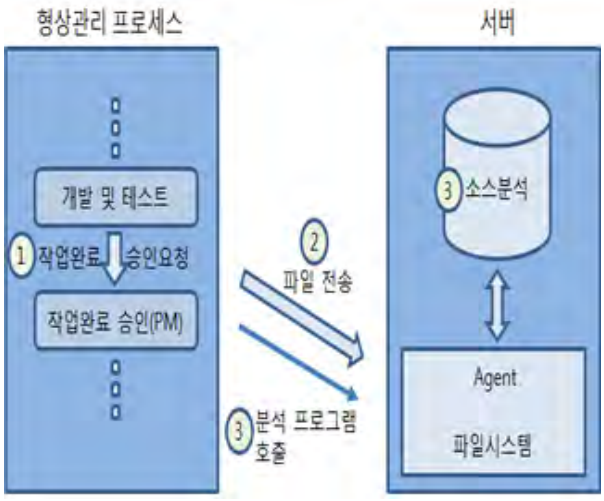
(그림 1) 소스코드 점검 시스템을 적용하기 위한 형상관리 프로세스

들을 분석하기 위해 시큐어코딩 점검시스템 서버로 파일 전송 및 분석 프로그램을 호출한다.

4. 작업완료 승인 요청된 변경요청서는 품질보증 단계로 이동한다.
5. 품질보증 단계에서 품질보증 활동을 거쳐 프로그램 적용 승인(PM)단계로 이동한다.
6. 프로그램 적용 승인 단계의 변경요청서는 PM 승인 후 프로그램 적용 단계로 이동한다.
7. 운영팀에서 운영서버로 프로그램 적용을 수행한다.
8. 변경요청서는 프로그램 적용 완료 후 작업완료 단계로 이동한다.

개발자는 프로그램 개발 및 테스트를 수행한 후, 기존의 저장된 프로그램 개발 서버와는 다른 내용의 프로그램 저장을 시도하며, 저장의 경우, 관리자의 승인을 통해 프로그램에 적용 가능하도록 한다. 또한, 소스코드 점검 시스템과 무관한 품질 보증 등의 운영팀의 추가적인 업무도 수행 가능하도록 설계한다.

2.2 형상관리 도구와 취약성 분석 도구 연동



(그림 2) 취약성 분석 도구 연동

1. 형상관리 프로세스의 개발 및 테스트 단계에서 변경요청서를 작업완료 승인요청 처리(Promote)한다.
   → 형상관리 클라이언트 도구에서 수행한다.
2. 변경요청서에 포함된 수정 및 개발된 소스파일들을 시큐어코딩 프로그램 서버의 파일시스템으로 파일 전송 처리한다.
   → 형상관리 서버의 내부 프로그램에 의해 수정 및 개발된 파일들을 Agent를 통해 파일 전송 처리한다.
3. 파일 전송 이후 시큐어코딩 프로그램 서버의 executer를 호출하여 분석을 실행한다.
   → executer는 형상관리 서버로부터 변경된 목록을 가져오고, 해당 파일만 분석을 처리한다.
4. 분석 완료 후 후속 작업을 실행한다.
   → 시큐어코딩 프로그램 서버에서 분석 완료 후 형상관리 서버의 DB로 결과를 업데이트 처리한다.

3. 결론

최근 IT 산업의 발달로 다양한 분야에서 소프트웨어가 활용되고 있으며, 이에 따라 소프트웨어의 자체 취약점을 이용한 공격이 증가하고 있다. 이에 맞춰 행정안전부에서는 시큐어코딩 의무화를 단계적으로 진행해왔으며, 소프트웨어 보안약점 시범진단 등을 수행하며, 다양한 시큐어코딩 프로그램 등장 및 시장 활성화가 진행되었다. 본 논문에서는 시큐어코딩 프로그램에 적용 가능한 효율적인 형상관리 프로세스를 제안하였다. 제안하는 형상관리 프로세스를 시큐어코딩 프로그램에 적용할 경우 시큐어코딩 프로그램 성능향상에 도움이 될 것으로 기대된다.

참고문헌

[1] 행정안전부, “소프트웨어 개발보안 가이드” 5월 , 2012

[2] 행정안전부, “소프트웨어 보안약점 진단가이드”, 5월 , 2012

[3] Bob Martin, Mason Brown, Alan Paller, Dennis Kirby, “2011 CWE/SANS Top 25 Most Dangerous Software Errors”, 2011.09