소프트웨어 취약점의 보안성 강화를 위한 연구

김슬기* · 박대우*

*호서대학교 벤처대학원

The Research for Cyber Security Experts

Seul-gi Kim* · Dea-woo Park*

*Hoseo Graduate School of Venture

E-mail : sgkim_18@naver.com, prof_pdw@naver.com

요 약

소프트웨어의 취약점분석에 대한 위험이 발생하고 있다. 소프트웨어의 취약점을 통해 물질적, 금전적인 피해가 발생함에 따라 보안강화의 중요성이 대두되고 있다. 위험잠재요소가 있는 소프트웨어를 사용하는 경우 제조한 기업뿐만이 아닌 해당 소프트웨어를 사용하는 기업 및 개인까지 손실의 위험이 크기 때문에 본 논문에서는 소프트웨어의 취약점을 진단하고, 진단원을 양성하는 교육과정과 진단가이드를 제시하며, 소프트웨어의 취약점 보안성 강화방식을 제안하고자 한다.

ABSTRACT

Analysis of vulnerability of the software for risk. The weakness of the software material, the importance of strengthening security in accordance with financial damage occurred is emerging. There is a potential risk factor not only from the case, the manufacturing to use the software company that appropriate to use a software business and personal risk of loss to size.In this paper due to diagnose and vulnerabilities in software, diagnosis, the curriculum and to cultivate a diagnostic guide, and security vulnerabilities in software.Proposal system for increased.

키워드

취약점(Vulnerability), SW보안(Software Security), 진단원(Consultant), 보안성강화(Security Enhance)

Ⅰ. 서 론

2016년 1월부터 마이크로소프트사에서는 자사 웹 브라우저인 인터넷 익스프로러의 최신 버전을 제외한 이전 버전에 대한 지원을 종료하겠다고 밝혔다. 이러한 것은 최신 버전이 아닌 구버전의 IE에서 새로운 취약점이 발견되더라도 지원을 종료한 이후에는 해당 취약점에 대한 패치가 제공되지 않기 때문에 이를 노린 공격이 증가할 것을 예상된다[1]. 또한 2016년 6월에는 북한이 국내 대기업 그룹사 전산망을 뚫고 들어가 대량의 자료가 유출하고 국가적 규모의 사이버테러를 준비했던 사실이 경찰 수사로 드러났다. 해킹수법으로는 관리자가 아니어도 인증없이 접근해 명령을 내릴 수 잇는 취약점을 통해 해킹 공격을 준비했다. 해당 소프트웨어를 만든 기업도, 사용한 기업도 이러한 취약점을 모르고있었으며 자칫하면 해당 소프트웨어를 사용하는 160여 개 기관과 기업이 한꺼번에 피해를 볼 수 있는 상황이 있었다[2]. 또 다른 사례로는 20개월이 넘게 소프트웨어 취약점에 의한 침해사고로 다양한취약점이 이용되었다. 소셜커머스사이트는 XSS와 Flash취약점을 통해 악성코드 배포 피해를 입었으며 일일 70만여명이 감염되는 침해사고가 발생하였다. 또한 증권가 홈페이지에서는 SQL Injection을 통해 개인정보가 유출되어 개인정보 2만 6천건이 손실되었다. 이러한 사례들은 소프트웨어 취약점에 의한 각종 피해를 발생시킨다[3].

Ⅱ. 관련연구

2.1 사이버해킹 동향

사이버해킹은 보안 패치발표 이전의 제로데이 공격, 웹사이트 해킹 등 지능화된 기법을 이용해 지속적으로 공격하는 APT(Advance Persitent Threat)공격, 모바일 공격 등 사회에 국가 인프라에 대해 확산되는 추세이다. 사이버해킹은 약 75%가 소프트웨어 자체의 보안취약점

을 악용하는 것으로 웹사이트 공격이 대표적이며, 불특정 다수가 쉽게 접근할 수 있고 프로그램의 특성 상 외부 공격에 항상 노출되어 있어 사이버 침해사고가 발생될 가능성이 높아지고 있다. 최근 국내외에서 발생한 고객정보 유출사고는 XSS 및 SQL 인젝션공격 등 웹응요프로그램에 내재된 보안취약점을 주로 악용했는데, 이렇듯 소프트웨어에 내재된 보안취약점은 사이버 침해사고의 주요 원인이 되며, 응용 소프트웨어에 내재된 보안취약점을 악용, 계정탈취·정보유출 등 침해사고를 유발시키지만 관련 보안투자는 미흡한 상황이다.

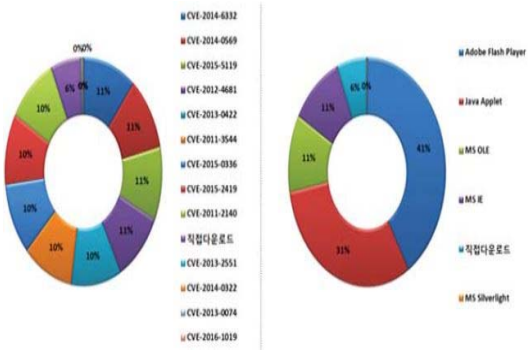

그림 1. 악성코드 취약점 악용현황(좌), 취약한 S/W악용 현황(우) (출처:2016년 2분기 사이버 위협 동향 KISA)

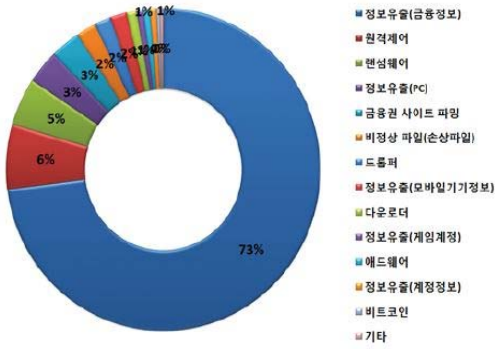

그림 2. 악성코드 유형별 비율 (출처:2016년 2분기 사이버 위협 동향 KISA)

2.2 소프트웨어보안 취약점

소프트웨어보안은 소프트웨어 개발과정에서 소스코드를 작성하는 구현단계에서 보안취약점을 배제하기 위한 '시큐어코딩'을 포함하고 있다. 웹사이트의 경우 불특정 다수가 쉽게 접근할 수 있고, 사용자가 입력한 정보를 처리하는 프로그램의 특성상 외부 공격에 항상 노출되어 있어 사이버 침해사고가 발생할 가능성이 높다. 특히, 소스코드 보안취약점을 이용한 사이버공격은 침입차단 및 침입방지 시스템 등 일반적인 보안장비로는 대응이 어려운 특징을 갖는다.

표1. 소프트웨어보안 취약점 종류 (출처:KISA)

유형	주요내용
입력 데이터 검증 및 표현	프로그램 입력 값에 대한 부적절한 검증 등으로 인해 발생할 수 있는 보안약점
보안기능	인증, 접근제어, 권한 관리 등을 적절하지 않게 구현시 발생할 수 있는 보안약점
시간 및 상태	멀티프로세스 동작환경에서 부적절한 시간 및 상태 관리로 발생할 수 있는 보안약점
에러처리	불충분한 에러 처리로 중요정보가 에러정보에 포함되어 발생할 수 있는 보안약점
코드오류	개발자가 범할 수 잇는 코딩오류로 인해 유발되는 보안약점
캡슐화	불충분한 캡슐화로 인가되지 않은 사용자에게 데이터가 노출될 수 있는 보안약점
API 오용	부적절하거나 보안에 취약한 API 사용으로 발생할 수 있는 보안약점

Ⅲ. 소프트웨어 개발보안 진단가이드 분석

3.1 소프트웨어 개발보안 제도 분석

행정안전부는 사이버공격의 주요 원인인 소프트웨어 보안약점을 전자정부 서비스 개발단계에서 제거하기 위해 정보시스템 구축 시 '소프트웨어 개발보안(시큐어코딩)'을 의무화하기로 했다. 시큐어코딩이란 소프트웨어 개발과정에서 개발자 실수, 논리적 오류 등으로 인해 소프트웨어에 내재된 보안취약점을 최소화하는 한편, 해킹 등 보안위협에 대응할 수 있는 안전한 소프트웨어를 개발하기 위한 일련의 과정을 의미한다. 그 동안은 악성코드를 개별적으로 분석해 대응할 수 있는 패턴을 개발하고 적용하는 방식으로 보안위협에 대응해 왔으나, 하루에 분석할 수 있는 악성코드 수가 한계가 있고 투자에도 제한이 있어 보다 근본적인 해결책이 필요하다.

3.2 소프트웨어 개발보안 진단 가이드

자산정보화사업 수행 시 시큐어코딩을 준수하여 소프트웨어를 개발했는지, 여부를 진단하기 위해 소프트웨어 보안약점 진단기법을 제시한다. 대상은 전자정부 소프트웨어 보안약점 진단원이며 범위는 행정기관 등이 추진하는 정보화사업으로 유지보수로 변경되거나 신규로 개발되는 소스코드 전체로 한다. 발주자 입장에서는 소프트웨어의 보안약점 진단, 제거 요구사항 도출시 활용 할 수 있으며 사업자 입장에서는 자체적으로 소프트

웨어 보안약점을 진단, 제거 시 활용할 수 있다. 진단원 입장에서는 사업자가 수행한 소프트웨어 보안약점 제거 결과 진단 시 활용할 수 있으며, 일반적으로는 소프트웨어 개발보안체계 및 보안약점 진단 및 제거 방법에 대한 이해하는데 활용한다.

Ⅳ. 소프트웨어 취약점의 보안성 강화

4.1 진단원 양성 및 보수교육 교재개발

현재 소프트웨어 진단원 양성을 위한 보수교육과 교재개발은 부족한상황이다. 소프트웨어 보안은 웹서버, 웹응용프로그램 서버 등 웹 관련 자체의 보안취약점을 이용한 공격은 침입차단시스템 등 보안장비로 대응하기 쉽지 않다. 그렇기 때문에 실제 소프트웨어 보안약점 진단을 통해 적절히 대응하고 예방할 수 있는 소프트웨어 보안진단 인력 및 양성에 필요한 교육 보조재 등이 필요한 상황이다. 교재의 구성으로는 기본교육으로 소프트웨어 개발보안 제도·기준, 소프트웨어 보안약점 진단·제거기술, 진단 수행능력의 배양을 위한 교육을 진행하며, 소프트웨어 개발보안 의무화 대상, 범위, 기준과 정보화사업 단계별, 기관별, 주체별 개발보안활동을 교육한다. 또한 소프트웨어 보안약점에 대한 설명 및 보안대책과 JAVA 언어로 작성된 시큐어코딩 예제 기반의 구체적인 진단방법을 소개하며 용어정리와 소프트웨어 보안약점 항목으로 구성한다. 보수교육으로는 지침·기준 등 제도 변경사항, 최신보안약점, 진단·제거기술, 소프트웨어 개발보안 지식의 지속적인 습득 및 기술능력 유지를 위한 교육을 진행한다.

4.2 진단원 시험문제 개발

최근 소프트웨어보안 트렌드를 반영하여, 구현단계 직무분석 내용을 보완하며 설계 및 운영단계에서 보안약점 기준 및 보안진단 방법 등에 관한 문제를 개발한다. 소스코드 보안약점 진단문제로는 파일명과 소스 행번호로 취약지점을 제시하며, 분석결과 레포트 자동 작성 및 시큐어 코딩 예제 등 관련된 문제를 개발한다. 진단원 선발을 위한 1차 필기 기본지식 확인(4지선다형, 단답형)문제와 현장실무 지식을 테스트하는 2차 실기(서술식, 논술식 등)에 활용할 문제유형을 개발한다.

표2. 진단원 시험문제 예제

• 4지선다형 문제
다음 문제 중 탐지유형과 사례가 맞지 않는 항목은? ① 부적절한 입력 탐지≦Session Cookie ② SQL Injection 탐지≦Hibernate ③ XSS≦JSP ④ 취약한 URL Redirection≦SHA-1
• 단답형 문제
1) 취약한 URL Redirection 사례 및 설명을 하시오? 2) SQL Injection 탐지의 사례 및 설명을 하시오?
• 논술식 문제
상당수 침해사고가 응용 소프트웨어에서 발생함에 따라 소스코드 등에 존재할 수 있는 잠재적인 보안 취약점을 제거하기 위해 정부에서는 소프트웨어 보안약점 기준을 마련하였다. 대표적인 보안약점의 7가지 유형과 소프트웨어 개발보안 적용 대상 및 범위, 기준, 소프트웨어 개발단계에서 소프트웨어 보안약점 진단방법에 대하여 설명하시오?

4.3 진단원 파일럿 테스트

시험과목, 신규문제, 선발절차 등 객관적인 검증을 위한 최소 10인 이상으로 1회 파일럿테스트를 실시하고, 보완이 필요하면 추가적으로 선발 파일럿테스트를 제공할 것이다. 또한 소프트웨어보안약점 진단원, 소프트웨어 보안 관련 인력 대상의 최소 10인이상의 파일럿테스트를 실시할 것이다. 테스트 유형으로는 화이트박스 테스트, 블랙박스 테스트, 정적분석, 동적분석, 수동분석, 자동분석으로 테스를 진행한다[4].

4.4 투입인력·비용기준

감리법인 등 보안약점 진단기관의 진단원 투입소요 예측 참고를 위해 정보화사업 규모별 투입인력 기준을 제시해야한다. 감리대가 산정방식으로는 두가지가 있는데 첫 번째는 투입인력의 수와 기간에 의한 산정방식(MD방식)이 있으며, 두 번째는 한국정보사회진흥원의 감리대가 산정기준이 있다. 투입인력의 수와 기간에 의한 산정방식은 매년 한국소프트웨어산업협회에서 공지되는 소프트웨어 노임단가와 감리 투입공수를 이용하여 산정하는 방식이다. 감리 총 투입공수(MD)는 계약하는 감리 전체범위에 대하여 투입인력(M:인력수)과 기간(D:횟수, 일수)을 곱하여 산정되는값이다. 노임단가는 소프트웨어의 노임단가를 적용한다. 한국정보사회진흥원의 감리대가 산정기준은 사업비 규모에 따른 요율을 정하여 산정하는방식이다. 단, 법제화 이전에 활용되던 요율표의 경우에는 투입공수에 의한 산정방법과 유사한 수준의 대가가 산정될 수 있도록 연도에 따른 보정, 물가상승률을 반영 등을 통하여 개정한 후 새롭게 공지될 예정이다. 이를 통해 정보화사업 규모를 예산, 투입자원 등을 등급을 나누어 각 급별(등급) 최소 투입인력 기준을 수립하여 실제 투입인력을 제시한다.

Ⅴ. 결 론

소프트웨어의 취약점을 통해 물질적, 금전적 피해가

많이 발생함에 따라 취약점의 보안성 강화가 필요하다. 소프트웨어의 취약점을 진단하여 패치가 이루어져 보안성을 강화시키는데, 이때 진단하는 진단원의 기준을 제시하여 진단원 양성을 하여 더 많은 취약점을 찾아내는 것이 보안성을 강화시키는 방법이라고 생각된다. 또한 소프트웨어 개발보안 제도 분석을 통해 시큐어코딩의 보안성 문제와 가이드라인을 제시함에따라 소프트웨어의 취약점을 최소화시켜 피해를 줄일 수 있다고 생각한다.

참고문헌

[1] AhnLab Clinic Center, “소프트웨어”, http://acc.giro.or.kr/secu_view.asp?seq=24474, 2016.1.4
[2] “SW 취약점 노리는 사이버공격, 아이뉴스24, 2016.6.16
[3] “소프트웨어 개발보안 제도 및 정책방향”, 2013.4, KISA
[4] “소프트웨어 개발보안 제도 및 정책방향”, 2013.4, KISA