단계별 프로젝트 보안 방안에 대한 연구

신성윤* · 장대현** · 김형진***

A Study on Security Measure of Step-Wise Project

Seong-Yoon Shin* · Dai-Hyun Jang** · Hyeong-Jin Kim***

요 약

유수의 기업체가 사이버공격을 받아 개인정보를 유출당하는 피해 사례가 속출하고 있다. 또한 금전이득의 획득이나 사회적 혼란 유발 등을 목적으로 계획된 해킹사례가 지속적으로 증가하고 있다. 웹사이트 공격의 약 75%가 응용 프로그램의 취약점을 악용하고 있다. 주요 보안 이슈로는 법적 근거에 따른 SW 개발 보안성이 강화되는 추세이다. 프로젝트 팀원의 Application 개발 보안 인식 부족한 것을 사실이다. 또한 수동적 대응과 개발 전단계(SDLC) 전체 영역에 걸친 보안성 검증/테스트 등이 미흡하다. 따라서 뒤늦은 결함발견으로 인한 Rework가 발생되고 있다. 이에 본 논문에서는 IT서비스 기업들이 수행하는 프로젝트 단계별 주요 보안 활동 사례를 살펴본다. 그리고 이를 통하여 실제 프로젝트 단계별로 적용할 수 있는 보안 방안을 제시하고자 한다.

ABSTRACT

Many companies has led to the damage case being leaked to personal information by taking cyber attack. Also, planned hacking cases continues to increase for the purpose of acquiring monetary gain or causing social disruption induction, etc. Approximately 75% of the Web site attacks exploit the vulnerability of the application. Major security issue is to strengthen the S/W development security according to the legal basis. The members of the project team is the fact that the lack of recognition of application development security. In addition, passive response and security validation/testing, etc. throughout the SDLC to the entire area is insufficient. Therefore, rework due to the belated discovery of a defect has occurs. In this paper, we examine the case of the project step-by-step security activities by performing IT services companies. And, through this, we present security measures that can be applied to the step-wise real-world projects.

키워드

사이버 공격, 해킹, 보안 방안, 프로젝트 단계, 보안성 검증/테스트

Key word

Cyber Attack, Hacking, Security Measure, Step-Wise Project, Security Validation/Testing

* 종신회원 : 군산대학교 (주저자, s3397220@kunsan.ac.kr)
** 정회원 : 군산대학교 박사과정, SK C&C,
*** 정회원 : 전북대학교 (교신저자)

접수일자 : 2012. 10. 05
심사완료일자 : 2012. 10. 25

Open Access http://dx.doi.org/10.6109/jkiice.2012.16.11.2459

Ⅰ. 서 론

무수히 많은 기업들의 회사의 운명과 전체적인 사업 기능을 완료하는데 컴퓨터의 이용과 정보 처리는 필수 불가결한 요소이다. 이러한 컴퓨터의 보안 관리 문제로 우리는 종종 고위 관리 및 컴퓨터 자원의 보호를 모색하고 기타 기관들의 무엇보다 소중한 자산을 보호하는데 광범위 하고 포괄적인 보안 관리 대책의 필요성에 효과적으로 보호하고 있다.

국제통화기금(IMF) 전산망 해킹('11.6) 세계군수업체인 록히드 마틴('11.4), 현대 캐피탈 해킹 사건('11.4), 농협 전산망 장애사건('11.4) 등 국내외 유수의 기업체가 사이버 공격, 전문 해커집단에 의한 해킹 등 정보시스템의 해킹으로 인한 피해 사례가 속출하고 있다. 이러한 환경에도 불구하고 국내 민간기업의 81.4%가 IT예산의 1%도 정보보호에 투자를 하지 않고 있는 실정이다. 정부는 현행 정보보호 관련 법령으로 정보통신망 이용촉진 및 정보보호 등에 관한 법률을 기본법으로 하여 분야 및 적용대상에 따라 산발적인 개별법규를 두어 각 분야별, 적용대상별로 정보보호를 위한 규율을 실시하고 있다[1].

본 논문에서는 IT서비스 기업들이 수행하는 프로젝트 단계별 주요 보안 활동 사례를 통하여 실제 프로젝트 단계별로 적용할 수 있는 보안 방안을 제시하고자 한다.

Ⅱ. 단계별 주요 보안 활동

S/W를 하나의 생명체처럼 만들어질 때부터 사라질 때까지의 변환과정으로 보아 소프트웨어 생명주기(Software Life Cycle)라고 한다. 이러한 소프트웨어를 개발하는 절차(Process)나 개발 단계(Phase)의 반복되는 현상을 소프트웨어 개발주기(Software Development Life Cycle)라고 한다.

현 시대의 소프트웨어 개발이란 프로그램을 짜는 개념에서 보다 확대되어 시스템 개발이라는 용어로 사용되기도 한다. 소프트웨어의 제작 공정 다시 말해서, 소프트웨어 탄생 과정에서 폐기 절차까지의 여러 단계에서 나타나는 소프트웨어의 형상을 가시화(Visualize)한 것을 SDLC 모델이라고 한다.

소프트웨어를 개발 할 때 SDLC 모델의 적용은 아래와 같은 효과를 발휘한다.

1) 개발 프로젝트 비용 산정과 개발 계획수립의 기본이 되는 골격-일정 계획, 예산, 인원, 기타 자원의 배분 역할을 수행하는 도구
2) 용어의 표준화: S/W 개발자 사이와 개발자와 관리자 사이의 합의를 함께 구성
3) S/W 개발 진행 상황 파악: 개발의 지연, 비용의 초과 등의 사태에 대하여 예방하거나 대처하는 기능

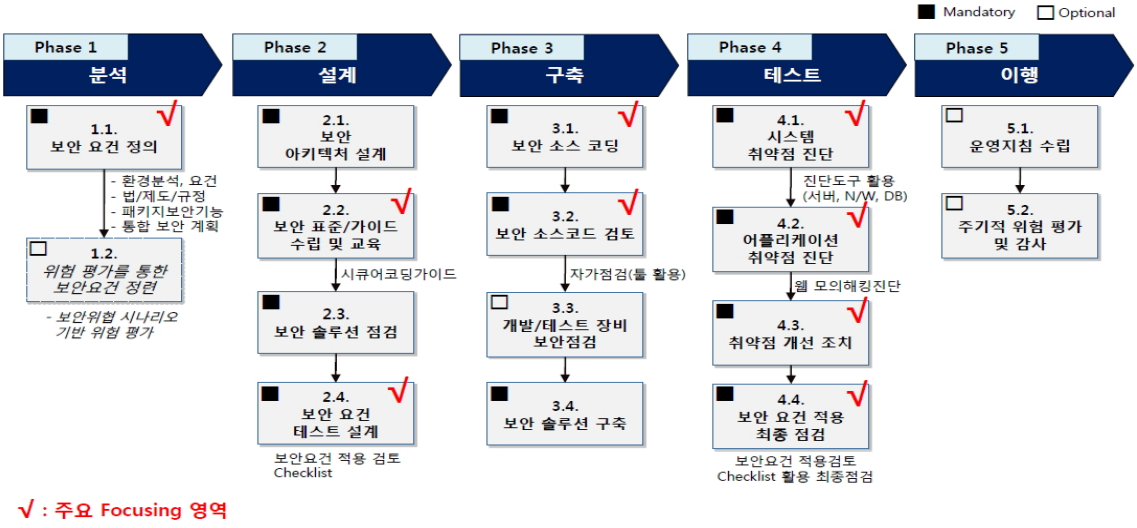

그림1. 프로젝트 단계별 주요 보안 Activity
Fig. 1 Step-Wise Major Security Activity of Project

4) 개발 프로젝트의 충실한 진행: 다양한 문서(산출물)를 작성하는 시기와 검토하는 시기를 제시함

프로세스란 조직이 한 개 이상의 입력을 통해서 가치 있는 산출물을 제공하는 모든 관련 활동들의 집합을 말한다. 전사란 공동의 목표를 추구하기 위해 고객과 상품 또는 서비스가 존재하고, 이를 지원하기 위한 조직, 자원, 기술을 보유하며 필요한 업무 프로세스를 수행하는 조직의 집합체를 말한다. 전사 프로세스란 이 둘을 합한 것이다.

현재 IT서비스 기업의 주요 보안 SDLC 활동은 보안 SDLC(분석/설계/구축/테스트)와 전사 프로세스를 통한 활동으로 크게 두 가지로 구분할 수 있다. 보안 SDLC 활동으로는 크게 네 가지로 분류할 수 있다.

첫째, 보안 법제도에 근거한 보안요건 정의 및 설계/구현 추적은 잘 되고 있는가?

둘째, 보안 설계/코딩 표준 가이드가 적시 활용이 어렵고, 개발자의 기존 코딩 습관을 답습하고 있지 않은가?

셋째, 보안 소스코드 검토(자가 점검, 툴 활용 등)활동은 수행하고 있는가?

넷째, 단계별 보안성 적용 점검 부족으로 뒤늦은 결함이 발견되지 않는가? 이다.

전사적인 프로세스 활동으로 크게 두 가지로 분류할 수 있다.

첫째, 보안성 관련 세부 Task 정의 및 관련 투입공수는 적절한가?

둘째, 단계별 보안 Activity에 대한 Best Practice는 공유/활용되고 있는가? 이다.

프로젝트 단계별로 주요 보안 Activity를 보면 그림1과 같다. 프로젝트는 분석, 설계, 구축, 테스트, 이행의 다섯 단계(SDLC)의 Activity로 각 단계별로 보안 Activity 활동을 전개한다.

첫 번째, 분석단계에서는 고객사의 환경 분석과 보안 요건을 분석하고 정의를 한다. 법, 제도, 규정 등을 검토하고 패키지 보안기능 및 통합 보안계획을 수립하여 보안 위협 시나리오 기반의 위험 평가를 통한 보안 요건을 정의 한다. 어플리케이션 보안 요건 영역으로 익명에게 공개를 목적으로 하는 프로그램을 제외한 모든 어플리케이션은 사용 전 반드시 인증과정을 거쳐야 하며 사용자 권한에 따른 통합인증관리를 지원하도록 설계해야 한다. 어플리케이션 보안 요건 영역은 표 1과 같다.

표 1. 어플리케이션 보안 요건 영역
Table. 1 Area of Application Security Requirement

영역	설명
식별 및 인증	- 개별 ID를 유일하게 식별해야 함. - 패스워드는 길이 제한 및 조합 표준을 적용해야 하며, 주기적으로 변경해야 함. - ID/PW 이외의 강화된 인증 방식을 제공해야 함. - 인증 프로세스는 정의된 보안 요건을 만족해야 함.
접근 통제	- 업무수행자(사용자)의 역할(Role)과 데이터 사용행위에 기반한 접근 및 권한 통제가 이루어져야 함. - 중요 정보의 대량 조회 및 변경 작업은 사전 결재를 득함. - 일정 시간 무 행위 세션에 대해통제 함.
암호화	- 중요 정보(데이터) 전송 또는 저장 시 정보의 기밀성, 무결성을 보장하여야 함. - 암호화는 단방향 및 양방향 암호화를 적용 함. - 암호화 키는 안전성이 보장되어야 함.
개발 보안	- 개발 시 보안 요건을 적용한 설계/코딩, 보안 적용 점검 - 어플리케이션 인터페이스 보안성 확보 및 공용 모듈 관리 - 중요 데이터 관리(보안 등급, 사용 현황 관리)
로깅 및 감사	- 부인 방지를 위해 모든 전자금융 거래 관련 내역은 로깅 및 보관 되어야 함. - 어플리케이션 접속 로그 및 중요 정보에 대한 조회 및 사용 내역은 로깅 및 검토 되어야 함.
취약점 관리	- 사용자에 의한 입력값 검증을 서버단에서 수행함. - 이관 전 어플리케이션 취약점 분석 및 조치가 되어야 함. - 보안성 검토 프로세스 수립(소스 코드 검토, 형상관리)

두 번째, 설계단계에서는 보안 표준과 가이드를 수립하여 프로젝트 투입인력을 대상으로 시큐어 코딩 가이드 등의 정의된 보안 교육을 실시하고, 보안 요건 적용을 검토하여 체크리스트를 구축한다. 단위 업무 시스템별 구성요소에 대해서 보호대상을 개별적으로 식별하고, 단위 업무시스템은 표 2의 예시와 같이 업무시스템이 설

치되는 시스템 노드(서버 시스템), 노드의 특정 디렉토리에 설치되어 구동되는 어플리케이션 모듈, 모듈간의 통신을 위한 인터페이스로 구분하여 식별한다.

표 2. 보호대상 정의(예시)
Table. 2 Definition of Protection Subject(Example)

구성요소	설명
시스템 노드	어플리케이션 모듈이 설치될 IP주소를 가진 물리적 시스템을 의미함. 특정 업무시스템 식별할 때 해당업무에 포함되는 시스템 및 상호 통신을 하는 타 시스템을 포함함
어플리케이션 모듈	시스템 내부에 설치되는 어플리케이션 모듈 중 해당 업무시스템의 구성요소에 포함되는 어플리케이션 모듈을 의미함
인터페이스	어플리케이션 모듈 상호간의 정보교환을 위한 모든 통신방식을 포괄하여 의미함 (예:FTP), DB-Link, EAI, SOCKET, HTTP, rhost)

보안속성 설계로는 개별 업무시스템별로 보호대상 정의 테이블에서 식별된 보호대상 노드, 모듈은 분석단계에서 정의 된 보안기준에 따라 보안속성을 설계한다. 보호대상 정의 테이블에 보안속성 설계를 추가하여 보안 속성 설계로 상세화 한다. 보안 속성으로는 보호대상, 엑세스 허용대상, 접근통제 영역, 식별 및 인증 영역, 암호화 영역으로 크게 다섯 가지로 분류할 수 있다. 표 3은 식별 및 인증 영역에 대한 예시이다.

표 3. 보안속성 설계-식별 및 인증 영역(예시)
Table. 3 Design of Security Attribute-Area of Identify and Certification(Example)

속성	설명	예시
ID	보호대상으로 접근하는 모든 엑세스 허용 모듈의 ID 형태 또는 고정된 ID일 경우 ID의 텍스트	Key파일, ID
PW	엑세스시 패스워드 인증의 수행 여부	O,X
기타	ID, PW 인증 이외에 추가적인 인증 방법 적용시 해당 방법을 구체적으로 기술	인증서, 토큰

행정안전부는 정보시스템SW개발운영자를 위한 “소프트웨어 개발보안 가이드” (’11.9월 2판 발행)을 통하여 정보시스템 개발단계에서 고려해야할 주요 보안 취약점에 대한 소스코드 레벨에서의 대응조치에 대한 가이드를 제시하고 있다[2,3]. 표 4는 설계단계의 보안으로서 SW보안 취약점 유형을 나타내고 있다.

설계단계의 검증은 구체적인 시스템의 구현 산출물이 나오기 전이므로 문서검토의 방식으로 진행되며 어플리케이션의 보안설계에 초점이 맞추어져 있다.

표 4. 설계단계 보안-SW보안 취약점 유형
Table. 4 Security of Design Step-SW Security Weak Point Type

구분	SW보안 취약점 유형
입력 데이터 검증 및 표현	- 프로그램 입력 값에 대한 검증누락 또는 부적절한 검증이나 사용되는 데이터의 잘못된 형식 지정 - XSS,SQL 삽입, 버퍼 오버플로우, 운영체제 명령어 삽입 공격 등
API 악용	- 의도된 사용에 반하는 방법으로 API를 사용하거나, 보안에 취약한 API를 사용하여 발생 - Get(), J2EE: System.exit()함수 등
보안 특성	- 보안특성(인증, 접근제어, 기밀성, 암호화, 권한관리 등)을 부주의하게 구현 시 발생 - 부적절한 인가, 하드코드 된 패스워드, 취약한 암호화 알고리즘 사용 등
시간 및 사례	- 동시 또는 거의 동시 수행을 지원하는 병렬 시스템, 프로세스 또는 스레드 환경에서 시간 및 상태를 부적절하게 관리하여 발생 - 데드락, 자원에 대한 경쟁조건, 세션 고착 등
에러 처리	- 에러를 불충하게 처리하거나 전혀 처리를 하지 않거나 에러 정보에 과도하게 많은 정보가 포함될 경우 - 에러 처리 루틴의 누락, 에러 처리 시 필요 이상의 정보 노출 등
코드 품질	- 복잡한 소스코드로 인해 관리성, 유지보수성, 가독성이 저하되어 SW 개발 및 유지 보수 시 타입변환 오류, 자원(메모리 등)의 부적절한 반환 등과 같이 개발자가 범할 수 있는 코딩오류로 인해 유발되는 보안취약점 - 자원의 부적절한 반환 등
캡슐화	- 중요한 데이터 또는 기능성을 불충분하게 캡슐화 하였을 때 인가되지 않은 사용자 또는 시스템에게 데이터누출이 가능해지는 보안 취약점 - 제거되지 않고 남은 디버거코드, 시스템데이터 정보 누출 등

세 번째, 구축단계에서는 자가 점검을 통하여 소스코드를 검토하고 전 단계에서 정의된 보안 구축을 검토하고 확인하는 절차가 필요하다. 암호화 솔루션을 적용하지 않을 경우, 프레임워크 단에서 보안적용을 통해 보안성 강화를 고려할 필요가 있다. J2EE프레임워크의 경우, JDK에서 제공하는 보안관련 패키지, 클래스, 라이브러리, 설정파일 등을 식별/활용이 가능하다.

소스코드 보안취약점을 점검하기 위해서는 입력값 검증 등 소스코드 보안 취약점 점검 수행 절차를 정의하여 점검하여야 한다.

보안 요건 정의서에 제시된 각 보안 요건 ID별 상세요건으로 세분화하여 구현 프로그램에 기능이 반영되었는지 점검하여야 한다.

네 번째, 테스트 단계에서는 보안요건이 구현되었는지 검토하고, 취약성 점검 및 프로젝트 수행사의 최종 검토와 고객사의 보안요건 최종 확인이 필요하다. 표 5는 테스트 단계의 진단 항목의 예시이다.

표 5. 테스트 단계-진단 항목(예시)
Table. 5 Test Step-Diagnosis Item(Example)

점검항목	위험도
SQL Injection 취약점	상
XSS(Cross Site Scripting) 취약점	상
디렉토리 목록 노출 취약점	하
관리자 페이지 노출 취약점	중
파일업로드 취약점	상
파일다운로드 취약점	상
파라미터변조 취약점	상
취약한 인증 취약점	상
불필요한파일 취약점	하
CSRF(Cross Site Request Forgery) 취약점	중
검증되지 않은 리다이렉트와 포워드	중

※ "2011년06월 금융회사 공개용 서버 침해 사고 및 취약점점검 기준"으로 한 11대 취약점점검항목

마지막으로 보안의 이행 활동 단계로서 보안 활동을 실행하는 단계이며, 운영지침 수립과 주기적인 위험 평가 및 감시를 수행한다.

보안요건 적용 점검 체크리스트를 정의하여 점검 방법과 반영 여부에 대한 점검으로 사용자 인증과 입력 값 검증을 통해 점검해야 한다. 또한, 해커의 입장으로 가정하여 Target 시스템에 대한 불법 침입을 시도하고, 내부망에서의 모의해킹과 외부 망에서의 모의해킹 방식으로 진단을 한다. 침입자의 목적은 인터넷에 오픈되어 있는 대상 시스템으로의 침입 후 대상 시스템의 관리자 권한 및 데이터를 얻어내는 것과 내부망의 금융정보 또는 고객 관련 데이터를 획득할 수 있는 보안 취약점을 발굴하는데 목적이 있다.

보안 취약점을 진단하기 위한 웹 모의 테스트 진단 도구로 사용하는 도구들은 주로 자체 개발시스템 취약성 점검스크립트로 계정 및 패스워드, 시스템파일 설정, 네트워크 서비스 설정, RootKit, 백도어 점검, 시스템파일 무결성 점검, 프로세서 및 네트워크 점검 등의 종합적인 시스템취약성 점검을 위해 사용된다.

Ⅲ. 결 론

본 논문에서는 프로젝트 단계별 주요 보안 Activity를 이해하고, 보안요건 항목 및 세부 요건 Best 사례를 습득하였으며, 프로젝트 각 단계별 보안 방안 Guide 및 사례를 통하여 SDLC 전 영역에 걸친 Seamless 한 보안성 검증 및 테스트 역량을 확보할 수 있었다.

또한, 본 연구를 통하여 고객사가 민감하게 느낄 수 있는 보안 부분에 대해서는 프로젝트 관리자와의 협의를 통해 프로젝트 각 단계별로 진단/개선/결과 세부 보고서를 취합하여 고객에게 설명하고 고객이 궁금한 사항과 향후 진행 방향 등에 대한 협의를 수행함으로써 프로젝트 전 단계를 통한 고객과의 신뢰를 확보할 수 있었다.

참고문헌

[1] Won-Hee Nam, Dea-Woo Park, "A Study on Cloud Network and Security System Analysis for Enhanced Security of Legislative Authority," *The Journal of the Korean Institute of Information and Communication Engineering,* Vol. 15, No. 6, pp. 1320-1326, 2011. 6

[2] 행정안전부, "정보시스템 SW개발 운영자를 위한소프트웨어 개발 보안 가이드," 2판, 2011.9

[3] 인포섹, “금융권 서버대상 침해사고·취약점 점검 서비스,” 2012. 5.

저자소개

신성윤(Seong-Yoon Shin)

2003년 : 군산대학교 컴퓨터과학과(이학박사)
2003년 ~ 2006년 : (주)네트플러스 연구원
2006년~현재 : 군산대학교 컴퓨터정보공학과 교수
2009년 ~ 2011년 : 한국정보통신학회 멀티미디어 및 응용 분과위원장
2012년 ~ 현재 : 한국정보통신학회 재무상임이사
※관심분야 : Image Processing, Multimedia, Computer Vision

장대현(Dai-Hyun Jang)

1995년 : 세종대 정보처리학과 학사
2011년 : 군산대학교 컴퓨터정보 공학과 공학석사
현재 : SK C&C 공공영업부 부장
군산대학교 컴퓨터정보공학과 박사과정
※관심분야 : Image Processing, Computer Graphics, Multimedia

김형진(Hyeong-Jin Kim)

2000년 ~ 2003년 : 군산대학교 정보통신공학과
현재 : 전북대학교 IT응용시스템 공학과 교수
※관심분야 : Communication Network, Ubiquitous, Multimedia System