Journal of The Korea Society of Computer and Information
Vol. 19, No. 10, October 2014
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2014.19.10.117

S/W 개발 보안의 필요성에 따른 법 제도 및 규정 사례 분석

신 성 윤*, 정 길 현**

Case Analysis of Legal System and Regulations according to the Needs of S/W Development Security

Seong-Yoon Shin*, Kil-Hyun Jeong**

요 약

S/W 개발 보안이란 안전한 SW 개발을 위해 잠재적인 보안취약점을 제거하고, 보안을 고려하여 기능을 설계·구현하는 등 SW 개발 과정에서 일련의 보안활동을 말한다. 본 논문에서는 우리에게 정신적, 금전적으로 상당한 피해를 주는 국내외 해킹 사례를 살펴보도록 한다. 웹 사이트 공격의 약 75%가 응용프로그램 즉, S/W의 취약점을 악용한 것임을 상기시킨다. 그리고 이러한 취약점들을 많이 가지고 있는 S/W 개발 보안의 주요 이슈들을 알아보도록 한다. 그리고 보안관련 법 제도 및 규정을 공공부분과 민간부분으로 나누어 제시하도록 한다. 그리고 보안관련 법 제도 및 규정의 세부 내역들을 예를 들어 나타내 보도록 한다.

▸ Keywords : S/W 개발 보안, 보안 취약점, 해킹 사례, 웹 사이트 공격

Abstract

Software Development Security is defined as a sequential procedure such as deleting potential security vulnerability for secure software development, designing or implementing various functions with considering security, and so on. In this paper, we research on domestic or international hacking cases that could damage us mentally or financially. Seventy five percent of Web-site attacks abuses weak points of application programs, or software. We also research on major issues related to software development security with these demerits. And then, we propose public and private laws, regulations, or systems and give some examples with detailed descriptions.

▸ Keywords : S/W Development Security, Security Vulnerability, Hacking Cases, Web-Site Attack

•제1저자 : 신성윤 •교신저자 : 정길현
•투고일 : 2014. 7. 4, 심사일 : 2014. 8. 16, 게재확정일 : 2014. 9. 12.
* 군산대학교 컴퓨터정보공학과(Dept. of Computer Information Engineering, Kunsan National University)
** 장안대학교 인터넷정보통신과(Dept. of Internet Communication, Jangan University)

I. 서 론

우리나라에서는 행정기관 등이 안전한 소프트웨어를 개발하여 각종 사이버위협으로부터 예방·대응코자하기 위하여 SW 개발단계부터 보안약점을 제거하는 'SW 개발 보안' 의무제가 2012년 12월부터 시행되었다.

미국의 정보기술 연구, 자문회사인 가트너에서는 보안 취약점이 포함된 SW는 해커의 공격 목표가 되어 중요한 보안 위협을 초래하며 사이버 침해 사고의 약 75%가 응용 프로그램(SW)의 취약점을 악용한다고 한다. 또한 IBM 사 보고서에서는 정보시스템 운영 이전의 개발 단계부터 보안성의 고려 및 없어지지 아니하고 남아 있는 취약점 제거가 필요하며, 운영 단계에서의 취약점 제거 비용은 개발단계보다 60~100배의 비용이 필요하다고 하고 있다. 따라서 사전 예방 체계 강화를 위한 SW 개발 보안(시큐어코딩) 강화 체계의 도입을 실시하였다. 시큐어코딩(Secure Coding)이란 SW 구현할 때 개발자나 언어의 약점 등으로 발생할 수 있는 취약점을 제거하기 위하여 설계 단계부터 보안을 고려하는 안전한 코딩 방법을 말한다.

SW 보안에 관한 연구로는 기 발생한 메모리 해킹 악성코드에 의한 인터넷뱅킹 사고로부터 파생될 수 있는 공격유형을 도출하고 사용자 인증수단이 해당 공격유형에 어떤 취약점을 노출하는지 살펴봄으로써 사용자 PC에 메모리 해킹 악성코드가 감염되어 있다고 하더라도 안전하게 전자금융 서비스를 완료할 수 있는 사용자 인증수단을 고찰하였고, 무기체계 내장형 SW 적용 수준을 중심으로 사이버전 대응을 위한 국방 SW 개발보안 적용 방안에 대하여 대안을 제시하였다.[1-2]

그 외에도 국내환경에 적합한 진단도구 기능 요구사항과 진단도구의 신뢰성을 보증할 수 있는 평가방법론을 제안하였고 제안된 평가체계의 효과를 분석하기 위한 시범 적용한 결과 및 절차를 제시하였다.[3]

보안취약점은 악의적인 목적을 가진 사용자 등에 의해 악용되어 중요정보 유출, 권한 상승, 보안기능 우회 등의 보안사고가 발생하는 SW 보안요구사항, 설계, 기능 관련 속성이다.[4]

보안약점은 SW의 결함, 오류 등으로 해킹 등 사이버공격을 유발할 가능성이 있는 잠재적인 보안취약점으로 보안취약점의 원인이라고 할 수 있으나 모든 보안약점이 보안취약점이 되지는 않는다.[4-5]

보안 방안에 대한 연구로는 IT서비스 기업들이 수행하는 프로젝트 단계별 주요 보안 활동 사례를 살펴보고 이를 통하여 실제 프로젝트 단계별로 적용할 수 있는 보안 방안이 제시되었다.[6]

또한 해킹에 관하여 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.[7]

그리고 사이버 공격으로 인한 경제적 및 사회적 손해와 주변의 관심이 집중됨에 따라, SW가 오류 및 보안취약점을 가지지 않고 안전하게 정상적으로 작동함을 보장하는 SW 보증에 관한 연구도 활발히 전개되고 있다.[8-11]

본 논문의 구성은 다음과 같다. 2장에서는 국내외 해킹 사례를 살펴보고 3장에서는 S/W 개발 보안의 필요성, 4장에서는 보안관련 법 제도 및 규정과 실례에 대하여 기술하고 5장에서 결론을 맺도록 한다.

보안 관련 법 제도 및 규정은 날로 변하고 있다. 하나의 보안 관련 허점이 나오면 또한 관련 법률은 여러 부서에서 줄줄이 개정되고 발효된다. 본 논문에서는 이러한 법률의 현 주소를 알아보고 법 제도가 어떤 것들이 있는지를 살펴보고자 한다.

II. 국내외 해킹 사례

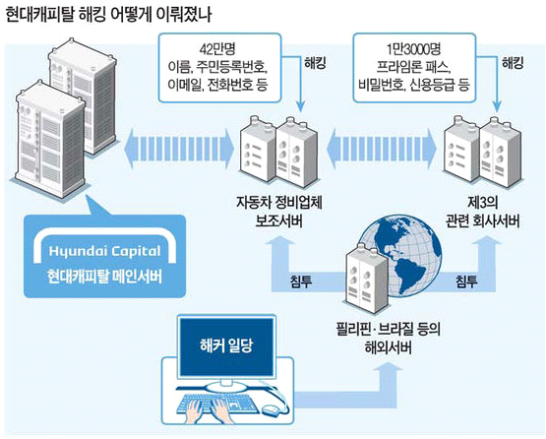
1. 국내해킹[12]

1) DDOS(Distribute Denial of Service attack) 공격('09~'12)

- 해커는 미리 좀비들을 제어하기 위한 C&C 서버들을 수천대 이상 확보, 악성코드를 유포해 좀비 PC들로부터 각종 정보를 수집. 이후 웹하드 홈페이지 두 곳을 해킹하여 업데이트 프로그램을 DDoS 악성코드로 바꿔치는 방법으로 국내의 많은 좀비 PC를 확보하여 DDoS 사이버 테러 공격을 감행

2) 현대 캐피탈 해킹사건('11.4.8)(그림 1)

- 전문 해커집단에 의한 해킹
- 암호화하지 않고 보관 중이던 중요 금융정보 유출 (피해규모: 40여만명 개인정보 유출)



그림출처 : 한국경제
그림 1. 현대캐피탈 해킹 사건
Fig. 1. Hacking of Hyundai Capital

3) 농협 전망 장애사건('11.4.12)
- 농협 외주업체 직원 노트북을 통해 프로그램 삭제 명령이 실행되어 금융서비스 중단사태 발생
(피해규모: 587대 서버 중 273대 피해)

4) 개인정보유출사건('12)
- SK 텔레콤, KT, EBS의 가입자 개인정보의 유출 사건
(피해규모: SK 텔레콤은 20만 건의 고객 개인정보가 유출, KT 전산망을 해킹당해 가입자 외 873만 명의 개인정보가 유출, EBS는 400만명의 아이디와 비밀번호 주소 등이 유출)

5) MBC/KBS/신한은행/농협 전산망 마비('13)
- XecureWeb[제큐어웹] 모듈의 업데이트 기능을 악용한 전산망 마비 사건
(피해규모: 주요방송사의 컴퓨터 마비, 은행의 모든 거래 멈춤)

6) KT 개인정보유출사건('14.1.25)
- Paros 프로그램을 사용하여 홈페이지에서 개인정보 탈취
(피해규모: KT 홈페이지 1200여만명 개인정보 유출)

여기에서 우리가 짚고 넘어가야할 중요한 사항은 IT 예산 대비 정보보호 예산 비율이 은행권 3.4%, 증권 3.1%, 카드 3.6% 등으로 금감원 권고안인 5%를 밑돌고 있으며 민간기업의 81.4%가 IT예산의 1%도 정보보호에 투자하지 않는다는 놀라운 사실이다.

2. 국외해킹

1) 국제통화기금(IMF) 전산망해킹 ('11.6)
2) 세계최대 군수업체 록히드마틴 ('11.5)
3) 소니 플레이스테이션 네트워크 ('11.4)
4) 맥도날드 해킹 ('11.12)
5) 혼다 캐나다 ('11.5)등
6) 네트워크 침입 당한 RSA('11.4)
7) 프랑스의 웹 호스팅 업체 OVH의 내부 네트워크 침입 ('13)
8) 애플은 자사의 개발자 웹사이트에 침입이 발생('13)
9) 일본 웹포털 사이트 2곳 해킹('13)

이와 같은 유수의 기업체가 사이버 공격을 받아 개인정보를 유출당하는 피해가 발생하여 사회적으로 커다란 혼란을 가져왔다. 특히, 이런 해킹들은 금전 이득 획득, 사회적 혼란 유발 등을 목적으로 한 계획된 해킹이라는 점에서 우리가 관심을 가지고 그 방어책을 연구해야 되는 이유이다.

III. S/W 개발 보안의 필요성

S/W 개발 보안의 필요성은 웹 사이트 공격의 약75%가 응용프로그램(SW)의 취약점을 악용하여 해킹을 수행했다는 것이다.

그림 2는 가트너의 웹 해킹 침해 보고서이다. 그림에서 알 수 있는 것처럼 Desktop에서는 침해 발생빈도가 없는 것으로 나타났다. 그리고 Transport에서는 0.5% 미만으로 아주 낮게 나타났고, 웹 바이러스와 스팸이 있는 Network 에서는 3%로 아주 낮게 발생했다. 하지만 점점 더 침해 빈도가 높아져서 웹 서버에서는 10%가 되었고, Application에서는 거의 75%대의 침해 비율을 보였다. 이는 다시 한 번 S/W 개발 보안의 필요성은 웹사이트 공격의 약75%가 응용프로그램(SW)의 취약점을 악용하여 해킹을 수행했다는 것을 증명하는 것이 되었다.

그렇다면 여기서 S/W 개발 보안의 주요 이슈는 무엇인지 살펴보도록 하자.

1) 법적 근거에 따른 SW 개발 보안성 강화 추세
- 개인정보의 안정성 확보 조치 기준 등 개인 정보보호법 준수 요구(제24조, 제29조등)
- 전자 금융거래법 및 전자 금융 감독 규정 준수 요구

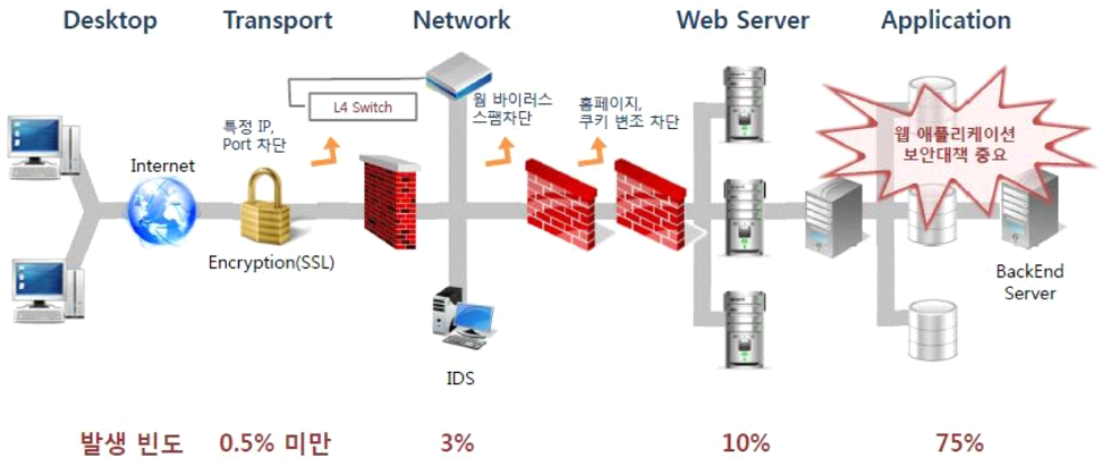


그림 출처 : Gartner

그림 2. Gartner 웹 해킹 침해 보고서
Fig. 2. Web Hacking Invasion Report of Gartner

· 공개용 웹서버 안전한 관리 대책 수립/운용(제17조)
· 보인 취약점 분석/평가 및 이행 계획 수립. 시행 등
- 개발 보안(시큐어코딩) 적용의무화('12.10, 행안부)

2) 프로젝트 팀원의 Application 개발 보안 인식 부족 및 수동적 대응

3) SDLC(Software Development Life Cycle) 전체 영역에 걸친 보안성 검증/테스트 미흡, 뒤늦은 결함 발견으로 인한 Rework 발생

4) 보안 SDLC 관련 활동 Guide 및 Best Practices 공유/활용 미흡

이처럼 S/W 개발 보안의 필요성은 나날이 증가하고 있으며 S/W의 취약점 때문에 발생하는 문제를 해결하기 위하여 다음과 같이 보안관련 법 제도 및 규정을 정비하고 실례를 들어 보았다.

Ⅳ. 보안관련 법 제도 및 규정과 실례

1. 보안관련 법 제도 및 규정

현행 정보보호 관련 법령은 법률인 정보통신망 이용촉진 및 정보 보호 등에 관한 법률을 기본법으로 하여 분야 및 적용 대상에 따라 산발적인 개별 법규를 두어 각 분야별, 적용 대상별로 정보보호를 위한 규율을 실시하고 있다.

또한 보안관련 법 제도 및 규정은 공공부문과 민간부문으로 나누어져 있고 정보보호시책수립에서 국가정보화법과 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 주요정보통신기반보호법에서 정보통신기반보호법, 그리고 각종 평가 · 인증, 점검에서 국가정보화기본법은 공공부문과 민간부분을 망라하여 작성된 법 제도 및 규정이다. 이제부터 우리는 보안관련 법 제도 및 규정을 살펴보도록 하자.

1) 정보보호시책 수립은 공공부분과 민간부분을 망라한 법으로 다음과 같이 분류된다.
· 국가정보화법: 정보보안 전문 위원회
· 정보통신망 이용촉진 및 정보보호 등에 관한 법률: 정보 보호 시책 수립

2) 주요정보통신기반보호는 정보통신기반 보호법으로 공공, 금융, 정보통신 등 분야별 주요 정보통신 기반보호, 정보통신 기반 보호 위원회로 나눈다.

3) 침해사고 대응은 공공부문과 민간부분으로 나눌 수 있다.
· 공공부문에서는 국가 사이버 안전 관리 규정으로 공공기관 침해 사고 대응, 국가 사이버 안전 센터, 그리고 정보 통신망 법 등

· 민간부문에서는 정보 통신망 법으로 민간 침해사고 대응과 침해 사고 대응 지원센터

4) 사이버 보안대책 및 조치는 공공부문과 민간부분으로 나누어진다.
· 공공부문에서는 전자정부 법에서는 정보통신망 등 보안대책 수립 및 시행에 관한 법
· 민간부문에서는 정보통신망 법으로 이용자 정보보호와 정보통신망 침해금지법

5) 각종 평가. 인증, 점검에 관한 법으로는 공공부분과 민간부문 그리고 공공부문과 민간부문을 총 망라한 법으로 분류된다.
· 공공부문에는 전자정부 법으로 전자문서의 보안조치와 공공부문 보안 적합성 검증제도
· 민간부문에는 정보통신망 법으로 정보보호 안전진단과 정보보호 관리 체계 인증
· 공공부문과 민간부문을 총 망라한 법으로 국가정보화 기본법이 있으며 이법은 정보 보호 시스템 평가 · 인증 제도를 다루는 법

6) 전자서명은 공공부문과 민간부문으로 나누어진다.
· 공공부문의 전자정부 법으로 행정 전자서명을 다루는 법
· 민간부문의 전자서명법으로 공인 전자서명을 다루는 법

7) 개인 정보 보호에 관한 법으로서 공공부문과 민간부문으로 나누어진다.
· 공공부문에 공공기관 개인 정보 보호법인 주민등록법
· 민간부문에 정보통신망 이용 촉진 및 정보보호 등에 관한 법률로서 신용정보 보호법

이상에서 우리는 법 제도 및 규정에 관해 살펴보았다. 하지만 법 제도는 하루가 다르게 변화하여 보안 관련 법 제도 및 규정이 산업통상자원부의 부정경쟁방지법에도 등장하게 된다는 사실에 입각하게 된다. 다음의 법 제도 및 규정의 실례에서 대략적으로 예를 살펴보도록 하겠다.

2. 법 제도 및 규정의 실례

보안 관련 주요 법 제도 및 규정에 관한 실례를 들어서 법 제도 및 규정의 변화의 세부 내역(예)을 살펴보도록 한다. 우선 정보통신망 법에서 출발한 개인정보보호법에 대하여 살펴보자.

1) 개인정보보호법(관련법령: 정보통신망 법)

제29조(안전조치의무)

개인 정보처리 자는 개인 정보가 분실 · 도난 · 유출 · 변조 또는 훼손되지 아니하도록 내부 관리 계획 수립, 접속 기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적 · 관리적 및 물리적 조치를 하여야한다.

1. 개인 정보의 안전한 처리를 위한 내부 관리계획의 수립 · 시행

2. 개인 정보에 대한 접근통제 및 접근권한의 제한조치

3. 개인 정보를 안전하게 저장 · 전송 할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치

4. 개인 정보 침해사고 발생에 대응하기 위한 접속 기록의 보관 및 위조 · 변조 방지를 위한조치

5. 개인 정보에 대한 보안 프로그램의 설치 및 갱신

6. 개인 정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금 장치의 설치 등 물리적 조치

다음으로는 전자정부 법에서 업무 담당자의 신원 및 접근권한의 확인에 대하여 살펴보자.

2) 전자정부 법

제34조(업무 담당자의 신원 및 접근권한)

업무 담당자 등의 본인 여부 및 접근권한 등을 공인 전자서명 또는 행정 전자 서명으로 신원 확인하여야 한다.

다음으로 전자 금융 거래법에서 나온 전자금융 감독 규정을 살펴보도록 한다. 전자금융 감독 규정에 대한 웹서버 관리 및 분석과 평가, 해킹에 노출되지 않도록 하고 불법적인 사이트에 대한 통제대책 등을 다루고 있다.

3) 전자금융 감독 규정(관련법령: 전자 금융 거래법)

제17조(홈페이지 등 공개용 웹 서버 관리대책)

① 금융기관 또는 전자 금융업자는 공개용 웹서버의 안전한 관리를 위하여 적절한 대책을 수립 · 운용하여야 한다.

② 공개용 웹서버에 게재된 내용에 대하여 다음 각 호의 사항을 준수하여야 한다. (1,2,3,4 …..)

③ 금융기관 또는 전자 금융업자는 홈페이지 등 공개용 웹서버에 대해 6개월마다 취약점을 분석 · 평가하고 그 이행계획을 수립 · 시행하여야한다.

④ 금융기관 또는 전자 금융업자는 공개용 웹서버가 해킹 공격에 노출되지 않도록 적절하게 대응 조치하여야 한다.

⑤ 금융기관 또는 전자 금융업자는 단말기에서 음란, 도박 등 업무와 무관한 프로그램 또는 인터넷 사이트에 접근하는 것에 대한 통제대책을 마련하여야 한다.

다음으로 안전행정부의 S/W 개발 보안에 관한 실제적인 법률을 살펴보도록 한다. 시큐어토딩 가이드 준수와 S/W 개발 보안 적용 의무화 등을 다룬다.

4) SW 개발 보안(안전행정부)

① 보안 취약점 유형에 따른 시큐어코딩 가이드 준수 요구 - 입력 데이터 검증/표현 API 악용 등 7가지 보안 취약점 유형에 따른 소스코드 관점의 가이드 준수

② 공공 정보화 사업에 소프트웨어 개발 보안 적용 의무화 ('12년 10월부터)

다음으로 2014년 8월 개정될 안전행정부의 개인정보보호법에서 주민등록번호를 어떻게 수집되고 이용되는지, 유출될 경우 과징금 제도 및 CEO에 대한 징계 권고 등을 살펴보자.

5) 개인정보보호법(안전행정부)

① 주민번호 수집·이용 원칙적 금지 - 주민번호 수집·이용이 원칙적으로 금지되고, 법령에 구체적 처리 근거가 있는 경우, 정보주체나 제3자의 급박한 생명·신체·재산상 이익을 위해 명백히 필요한 경우 등 예외적인 경우에만 수집·이용 가능. 기존에 정보주체의 동의를 받아 주민번호를 수집·이용하는 것이 금지되고, 기 수집한 주민번호는 법 시행 후 2년 이내(2016년 8월까지) 파기해야 하며, 위반시 3천만원 이하의 과태료 부과.

② 과징금 제도 - 주민번호가 유출되고, 이에 대한 안전성 확보조치를 다하지 않은 경우에는 5억원 이하의 과징금 부과.

③ CEO 징계 권고 - 주민번호 유출 등 법 위반시 해당 기관의 대표자나 책임 있는 임원에 대한 징계를 권고할 수 있도록 하여 기업이나 기관 전체의 개인정보보호에 대한 인식과 책임성 강화

다음으로 2014년 2월 개정한 산업통상자원부의 부정경쟁방지법이다. 여기에서는 영업 비밀을 포함하고 있는 문서를 보호하기 위한 전자 지문의 추출 및 활용에 관한 법을 다루고 있다.

6) 부정경쟁방지법(산업통상자원부)

① 부정경쟁행위에 관한 보충적 일반조항 마련 - 타인의 상당한 투자나 노력으로 만들어진 성과 등을 공정한 상거래 관행이나 경쟁질서에 반하는 방법으로 자신의 영업을 위하여 무단으로 사용함으로써 타인의 경제적 이익을 침해하는 행위를 부정경쟁행위에 관한 보충적 일반조항으로 신설함.

② 영업비밀 원본증명제도의 도입 - 영업 비밀을 포함하고 있는 전자문서의 원본 여부를 증명하기 위하여 그 전자문서로부터 고유의 식별값인 전자지문을 추출하여 원본증명기관에 등록하고, 필요한 경우 원본증명기관이 전자지문을 이용하여 그 전자문서가 원본임을 증명하는 영업비밀 원본증명제도 도입.

③ 위조상품 신고포상금제도의 근거 규정 마련

④ 벌칙 규정에서의 영업비밀 보유주체 확대 - 개인이나 비영리기관의 영업 비밀을 유출한 자도 형사 처벌의 대상으로 포함.

이상에서 우리는 보안관련 법 제도 및 규정과 그들의 실례

를 들어 살펴보았다. 보안관련 법과 규정은 하루가 다르게 변하여 새롭게 개정되고 발효되고 있다. 이러한 시점에서 현재의 국내외 해킹 사례와 S/W 개발 보안의 필요성, 그리고 보안관련 법 제도 및 규정과 실례에 대한 본 논문의 중요성은 매우 크다고 볼 수 있다.

V. 결 론

SW 개발 보안이란 편리하고 안전한 소프트웨어를 개발하기 위하여 겉으로 드러나지 않고 숨은 상태로 존재하는 보안의 취약점을 없애고 이를 고려하여 각각의 기능을 설계 및 개발하고 현하는 일련의 보안활동을 말한다. 본 논문에서는 현재 우리 국민에게 상당한 정신적 및 금전적, 사회적으로 피해를 입힌 주요 국내외 해킹 피해 사례를 살펴보았다. 그리고 이들 웹 사이트 공격의 약 2/3가 어플리케이션 프로그램의 취약점을 나쁘게 악용한 사례. 즉, S/W의 취약점을 악용한 사례임을 알았다. 이 시점에서 취약점들을 많이 가지고 있는 S/W 개발 보안의 주요 이슈들을 알아보았고, 보안관련 법 제도 및 규정을 공공부분과 민간부분으로 나누어서 알아보았으며, 보안관련 법 제도 및 규정의 세부 내역들을 예를 들어서 살펴보았다. 앞으로는 해킹에 대한 방지책을 구체화하여 SW 개발 보안을 체계적으로 구현할 수 있는 방법에 대한 연구가 활성화 되어야 할 것이다.

참고문헌

〔1〕 Lee, Hanwook, Shin, Hyu Keun, "A Study of The Robust User Authentication Methods for Memory Hacking Attacks," KIISC review, VOL. 23, NO. 6, pp. 67-75, 2013

〔2〕 Choi. June Sung, Kim. Woo Je, Park. Won Hyung, Kook. Kwang Ho, "Defense SW Secure Coding Application Method for Cyberwarfare Focused on the Warfare System Embedded SW Application Level," Journal of the Korean Association of Defense Industry Studies, Vol. 19, No. 2, pp.90-103, 2012

〔3〕 Jiho Bang, Rhan Ha, "Evaluation Methodology of Diagnostic Tool for Security Weakness of e-GOV Software," The Journal of Korea Information and Communications Society," Vol. 38C, No. 4, pp. 335-343, 2013. 4

〔4〕 P. E. Black, M. Kass, M. Koo, and E. Fong, "Source code security analysis tool functional specification version 1.1," NIST Special Publication 500-268, Feb. 2011.

〔5〕 MOPAS, "Guidelines on building and operating Information Systems," MOPAS Notification No.2012-25, June 2012

〔6〕 Seong-Yoon Shin, Dai-Hyun Jang, Hyeong-Jin Kim, "A Study on Security Measure of Step-Wise Project," Journal of the Korea Institute of Information and Communication Engineering, Vol. 18, No. 4, pp. 771-778, Apr. 2012

〔7〕 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

〔8〕 G. McGraw, "Software assurance for security," IEEE Computer, vol. 32, pp. 103-105, Apr. 1999.

〔9〕 G. McGraw and B. Potter, "Software Security Testing," IEEE Security and Privacy, Vol.2, pp.81-85, Sep. 2004.

〔10〕 B. Arkin, S. Stender and G. McGraw,"Software penetration testing," IEEE Security & Privacy, vol.3, pp. 84-87, Jan.2005.

〔11〕 D.P. Gilliam , T.L. Wolfe, J.S. Sherif and M. Bishop, "Software Security Checklist for the Software Life Cycle," Proceedings of the Twelfth International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, pp. 243,Jun. 2003.

〔12〕 http://certlys82.tistory.com/57

저 자 소 개

신 성 윤

2003년 2월: 군산대학교
컴퓨터과학과 이학박사
2006년~현재: 군산대학교
컴퓨터정보공학과 교수
관심분야 : 영상처리, 컴퓨터비전,
가상현실, 멀티미디어
Email : s3397220@kunsan.ac.kr

정 길 현

2001년: 한양대학교
컴퓨터공학과 공학박사
현 재: 장안대학교 IT학부
인터넷정보통신과 교수
관심분야 : 정보통신,
모바일 SW 개발,
네트워크 프로토콜
Email : khjeong@jangan.ac.kr