# S/W 개발 보안에 따른 법 제도 및 규정 분석

신성윤* · 진동수*** · 신광성* · 이현창** · 이양원*

*군산대학교 컴퓨터정보공학과

**원광대학교 정보전자상거래학부(융복합창의연구소)

***경인여자대학교 경영과

# Legal System and Regulation Analysis by S/W Development Security

Seong-Yoon Shin* · Dong-Soo Jin*** · Kwong-Seong Shin* · Hyun-Chang Lee** · Yang-Won Lee*

*Dept. of Computer Information Engineering, Kunsan National University

**Div. Of Information and Electronic Commerce(Institute of Convergence and Creativity)
Wonkwang University

***Dept. of Business Administration, Kyung-In Woman's University

E-mail : {s397220, waver, ywrhee}@kunsan.ac.kr, hclglory@wku.ac.kr, dsjin777@kiwu.ac.kr

Acknowledgement : "This research is partially supported by Institute of Information and Telecommunication Technology of KNU"

## 요 약

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.

## ABSTRACT

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.

## 키워드

S/W 개발 보안(S/W Development Security), 보안 취약점(Security Vulnerability), 해킹 사례(Hacking Cases)

## Ⅰ. 서 론

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]

## II. 국내외 해킹 사례

국내해킹

1) DDOS(Distribute Denial of Service attack) 공격('09~'12)
2) 현대 캐피탈 해킹사건('11.4.8)
3) 농협 전망 장애사건('11.4.12)
4) 개인정보유출사건('12)
5) MBC/KBS/신한은행/농협 전산망 마비('13)
6) KT 개인정보유출사건('14.1,25)

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)

## III. S/W 개발보안의 주요 이슈

1) 법적 근거에 따른 SW 개발 보안성 강화 추세
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

## IV. 법 제도 및 규정 실례

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 공공 기관 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

## V. 결 론

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.

## 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