정 보 보 호 학 회 지
제25권 제1호, 2015. 2

SW 개발보안을 위한 보안약점 표준목록 연구

안 준 선*, 이 은 영**, 창 병 모***

요 약

정보시스템의 안전을 위한 시큐어 코딩의 중요성이 강조되고 있으며, 이를 지원하기 위한 보안약점 및 보안취약점 관련 연구로서 보안약점목록의 구축, 주요 보안약점의 발표, 보안취약점목록의 구축, 보안약점과 보안취약점 중요도 정량평가 방법의 개발 등이 수행되고 있다. 특히 대표적인 국내 사례로 행정자치부와 한국인터넷진흥원에서는 SW 개발단계에서 보안약점 제거활동을 의무화하는 SW 개발보안을 법제화하여 시행하고 있다. 본 논문에서는 시큐어 코딩을 지원하기 위한 국내외 연구 동향을 소개하고, 행정자치부 SW 개발보안을 위한 보안약점 표준목록 연구결과를 소개한다.

Ⅰ. 서 론

정보시스템의 보안침해를 예방하기 위해서 안전하고 강건한 프로그램을 개발하고자 하는 시큐어 코딩(Secure Coding)의 중요성이 강조되고 있다. 가트너(Gartner)에 의하면 보안 침해의 75% 이상이 응용 소프트웨어와 관련한 것으로 발표되었으며[1], 미국의 경우 2007년도 당시 보안침해 사고 중 소프트웨어의 결함으로 인한 손실이 연간 1800억달러에 달하는 것으로 보고되었다[2]. 기업체의 입장에서도 성공적으로 소프트웨어 개발을 완료하고 운영단계의 소프트웨어 취약점 제거 비용을 절검하기 위하여 시큐어 코딩이 필수적인 요소로 간주되고 있다[3,4].

소스코드의 문제로 인한 침해로부터 정보시스템을 보호하기 위해서는 소프트웨어의 개발 단계에서부터 취약한 형태의 프로그램 작성이 방지되어야 하며, 기존의 소프트웨어에 문제가 있을 경우에는 이에 대한 대응이 신속하게 이루어져야 한다. 이러한 일련의 활동을 지원하기 위해서는 보안약점목록, 중요보안약점 정보 및 보안취약점목록과 같은 지원 정보의 체계적인 구축 및 갱신이 필요하며, 아울러 이를 효과적으로 활용하도록 운영하여야 한다.

미국을 중심으로 표준화 및 정보 구축을 위한 활동이 활발히 이루어지고 있으며, 국내에서도 전자정부 및 공공 정보시스템, 국방 등의 분야에서 시큐어 코딩을 위한 지원활동이 수행되고 있다. 특히 행정자치부에서는 2012년부터 공공시스템을 위한 소프트웨어 발주 사업에서 보안약점 제거작업 및 이에 대한 점검을 의무화하는 SW(Software) 개발보안을 법제화 하여 실시하고 있으며, 그 대상 범위를 점차 확대하고 있다[5].

본 논문에서는 시큐어 코딩을 위한 이러한 국내외 활동을 보안약점과 보안취약점의 관점에서 정리하고, 특히 행정자치부 SW 개발보안과 관련하여 이루어진 보안약점 표준목록 구축 연구를 소개한다. 본 논문의 구성은 다음과 같다. 2장에서는 보안약점 및 보안취약점과 관련한 국내외 연구사례를 소개하며 3장에서는 행정자치부 SW 개발보안 정책과 관련하여 추진된 보안약점 표준목록의 구축을 설명한다. 4장에서는 보안약점 표준목록에 대한 한글 정보 DB의 구축에 대하여 설명하며 5장에서 결론으로 맺는다.

Ⅱ. 시큐어 코딩 지원을 위한 국내외 연구 소개

2.1. 보안약점과 보안취약점

본 절에서는 관련 연구를 소개하기에 앞서 보안약점(Weakness)과 보안취약점(Vulnerability)의 개념에 대하여 설명하고자 한다. [표 1]은 보안약점과 보안취약점

본 연구는 한국인터넷진흥원 ‘최신 소프트웨어 보안약점 분석 및 기준목록 개발’ 과제의 지원으로 수행되었습니다.
* 한국항공대학교 항공전자정보공학부 (jsahn@kau.ac.kr)
** 동덕여자대학교 컴퓨터과학과 (elee@dongduk.ac.kr)
*** 숙명여자대학교 컴퓨터과학부 (chang@sookmyung.ac.kr)

〔표 1〕 보안약점과 보안취약점

	보안약점 (Weakness)	보안취약점 (Vulnerability)
정의	보안취약점의 될 수 있는 소프트웨어의 결함, 실수, 버그 등	공격자가 이용하였을 경우에 시스템의 보안정책을 침해하게 되는 시스템의 허점
특성	일반적 형태 / 근원적	개별적 / 상황 의존적
목록 DB 사례	CWE(Common Weakness Enumeration) CWE/SANS Top 25 OWASP Top 10 행정자치부 보안약점기준	CVE(Common Vulnerabilities and Exposures) NVD(National Vulnerability Database), OSVDB(Open Sourced Vulnerability DB)
중요도 평가 방법론 사례	CWSS(Common Weakness Scoring System)	CVSS(Common Vulnerability Scoring System)

의 정의 및 관련된 연구 내용들을 정리하여 보여주고 있다. 보안취약점은 정보시스템에서 공격자가 이용하였을 경우에 실제 침해로 이어지는 소프트웨어의 허점이다. 보안 취약점은 특정 소프트웨어의 특정 부분과 같은 구체적인 사례로 제시되며, 사용중인 소프트웨어의 문제점으로 발표되는 것이 일반적이다. 보안약점은 보안취약점이 될 수 있는 일반적인 형태를 말하며, 따라서 하나의 보안약점의 형태가 다양한 소프트웨어에서 보안취약점으로 나타날 수 있다. 일반적으로 보안약점의 형태가 프로그램에 존재한다고 해도 항상 보안취약점이 연계되지 않을 수도 있다. 보안약점을 공격자가 접근할 수 있고 공격을 통한 실제적인 피해를 발생시킬 수 있을 때 보안취약점으로 연계되며 이는 다음과 같이 표현할 수 있다.

보안약점+공격자의 접근+정보의 획득,
변조 또는 가용성의 저하 → 보안취약점

이러한 보안약점 및 보안취약점과 관련한 지원 연구로 목록 DB가 구축되어 공개되고 있으며, 보안약점의 경우 중요 보안약점에 대한 정보를 제공하는 활동이 수행되고 있다. 또한 다양한 보안약점 및 보안취약점들의 중요성을 정량적으로 평가하고자 하는 활동이 이루어지고 있다. 이어지는 절들에서 이러한 보안취약점 및 보안약점 관련 연구 사례를 소개한다.

2.2. 보안약점 관련 해외 연구사례

2.2.1. 보안약점 목록 연구

보안약점 목록으로 대표적인 사례로는 CWE (Common Weakness Enumeration)를 들 수 있을 것이다[6]. CWE는 미국 DHS(Department of Homeland Security)의 지원 하에 MITRE에서 관리하고 있으며, 다음과 같은 보안약점 항목들로 이루어져 있다.

- 관점(View): CWE 내의 보안약점을 특정 관점에 의하여 분류한 부분목록이며, 단순나열 또는 비순환 그래프의 형태를 가진다. 현재 32개 관점이 제공되고 있다.
- 카테고리(Category): 공통점을 가진 보안약점들의 집합으로, 244개의 카테고리가 제시되어 있다.
- 보안약점(Weankess): 실제적인 개별 보안약점 항목들로서 현재 719개 항목이 포함되어 있다. 항목의 일반성 정도에 따라 Class, Base, Variant로 구분된다.
- 복합원소(Compound Element): 여러개의 약점이 모여서 하나의 취약한 보안약점을 이루는 경우로서 8개 항목이 포함되어 잇으며, 대표적인 예로 CSRF(Cross Site Request Forgery)를 들 수 있다.

CWE의 모든 약점들은 비순환 그래프의 형태로 상위-하위의 계층구조로 연계되어 있으며, 이러한 계층구조는 관점에 따라 달라진다. 일반적으로 하위의 약점은 상위약점의 좀 더 특수한(specific) 형태에 해당한다. CWE에서는 각 약점항목에 대하여 다음과 같은 정보를 제공한다.

- 보안약점 식별자(CWE ID)와 이름
- 보안약점에 대한 설명
- 관련 언어 및 환경(운영체제, 시스템 형태 등)
- 침해 결과
- 보안약점이 존재할 경우 침해의 성공 가능성

- 관련 취약점 사례(CVE ID)
- 보안약점에 대한 대책
- 관련 상위 및 하위 보안약점
- 해당 약점에 대한 공격방법 (CAPEC)
- 참고문헌

2.2.2. 주요 보안약점 목록

CWE의 경우 실제적인 보안약점으로 727개의 항목을 제공하고 있으나, 프로그램 개발자가 이러한 모든 항목에 대하여 주의하면서 프로그램을 개발하는 것은 실질적으로 어렵다. 또한 개발 중이거나 개발된 프로그램 내의 약점에 대응하는데 있어서도 발생 가능성이 높으며 침해와 연계 가능성이 크고 침해 시 피해가 심각한 보안약점에 대하여 우선적으로 대책을 강구하는 것이 필요하다. 이를 위하여 중요한 보안약점들의 목록을 제시하기 위한 활동이 이루어지고 있으며, 대표적인 주요 보안약점 목록으로 OWASP Top 10[7]과 CWE /SANS Top 25[8]가 있다.

OWASP Top 10은 웹과 관련한 주요 보안 위험에 대한 목록을 제공하는 프로젝트로서 The Open Web Application Security Project에서 관리하고 있다. 2003년도에 처음으로 10개 항목으로 이루어진 목록이 발표되었으며, 소규모로 수정된 2004년판 이후 3년마다 개정되어 2007, 2010, 2013년에 개정 목록이 발표되었다. OWASP Top 10은 2010년부터 보안약점의 개념보다는 위험(Risk)의 개념으로 더 넓은 범위의 웹 관련 위험요소를 다루고 있다.[표 2]는 2013 OWASP Top 10의 목록으로서 각각의 항목은 개별 약점 항목이거나(A3, A8, A9, A10), 포괄적인 약점의 범주를 위험이라는 개념으로 제시하고 있다. 또한 OWASP는 이러한 위험에 대하여 이를 예방할 수 있는 OWASP's ESAPI (OWASP Enterprise Security API), OWASP XSS Prevention Cheat Sheet 등의 다양한 방법론을 위험별로 제시하고 있다.

〔표 2〕 2013 OWASP TOP 10

OWASP Top 10 2013	
A1	인젝션
A2	인증 및 세션 관리 취약점
A3	크로스 사이트 스크립팅 (XSS)
A4	취약한 직접 객체 참조
A5	보안 설정 오류
A6	민감 데이터 노출
A7	기능 수준의 접근 통제 누락
A8	크로스 사이트 요청 변조 (CSRF)
A9	알려진 취약점이 있는 컴포넌트 사용
A10	검증되지 않은 리다이렉트 및 포워드

CWE/SANS Top 25는 일반적인 수행 환경을 위한 주요보안약점 목록으로서 2009년부터 25개의 주요 보안약점을 선발하여 발표하고 있으며, 2011년에 가장 최근 버전이 발표되었다. 2011년에는 중요 보안약점의 선별을 위하여 중요도 정량평가 방법인 CWSS (Common Weakness Scoring System)[9]가 사용되었다. [표 3]은 산출된 25개 항목의 순위와 중요도 점수를 보여준다.

〔표 3〕 CWE/SANS Top 25 2011

순위	점수	CWE -ID	보안약점 이름
1	93.8	89	SQL 삽입
2	83.3	78	운영체제 명령어 삽입
3	79.0	120	입력값 크기를 고려하지 않은 버퍼 복사
4	77.7	79	크로스사이트 스크립트
5	76.9	306	적절한 인증 없는 중요 기능 허용
6	76.8	862	권한 미인가
7	75.0	798	코드에 직접 삽입된 신용정보 사용
8	75.0	311	보안에 민감한 데이터에 대한 암호화 부재
9	74.0	434	위험한 파일 업로드
10	73.8	807	신뢰할 수 없는 입력값에 의존한 보안 결정
11	73.1	250	부적절한 권한을 이용한 실행
12	70.1	352	크로스사이트 요청 위조(CSRF)
13	69.3	22	경로 순회
14	68.5	494	무결성 검사 없는 코드 다운로드
15	67.8	863	부정확한 권한인가
16	66.0	829	신뢰할 수 없는 영역에서 제공되는 기능 포함
17	65.5	732	주요 자원에 대한 잘못된 권한 설정
18	64.6	676	잠재적인 위험성이 있는 함수의 사용
19	64.1	327	취약하거나 위험한 암호화 알고리즘의 사용
20	62.4	131	버퍼 크기의 부정확한 계산
21	61.5	307	과도한 인증 시도에 대한 부적절한 제한
22	61.1	601	신뢰되지 않는 URL 주소로 자동 연결
23	61.0	134	제어되지 않은 형식 문자열
24	60.3	190	정수 오버플로우
25	59.9	759	솔트를 사용하지 않는 단방향 해쉬 사용

2.2.3. 보안약점 중요도 정량평가

중요한 보안약점에 대한 우선적인 대응을 위하여 보안약점의 중요도를 정량적으로 평가하기 위한 노력으로 CWSS가 CWE 프로젝트의 일부로 제시되었다. CWSS는 현재 버전 1.0.1이 2014년 9월에 발표되었고, 평가척도 중 일부가 CWE/SANS Top 25의 선정에 사용되었다.

CWSS에서는 보안 약점의 심각성을 평가하기 위한 정량적인 기준으로서 18가지의 평가척도(metric)를 약점 자체의 심각성(Base Finding Metric Group), 공격측면의 심각성(Attack Surface Matric Group), 환경적 측면의 심각성(Environmental Matric Group)의 3개 그룹으로 분류하여 제시하고 있으며, 각 평가척도별 1점 만점의 점수에 기반을 둔 100점 만점의 중요도 점수 산출식을 제공하고 있다.

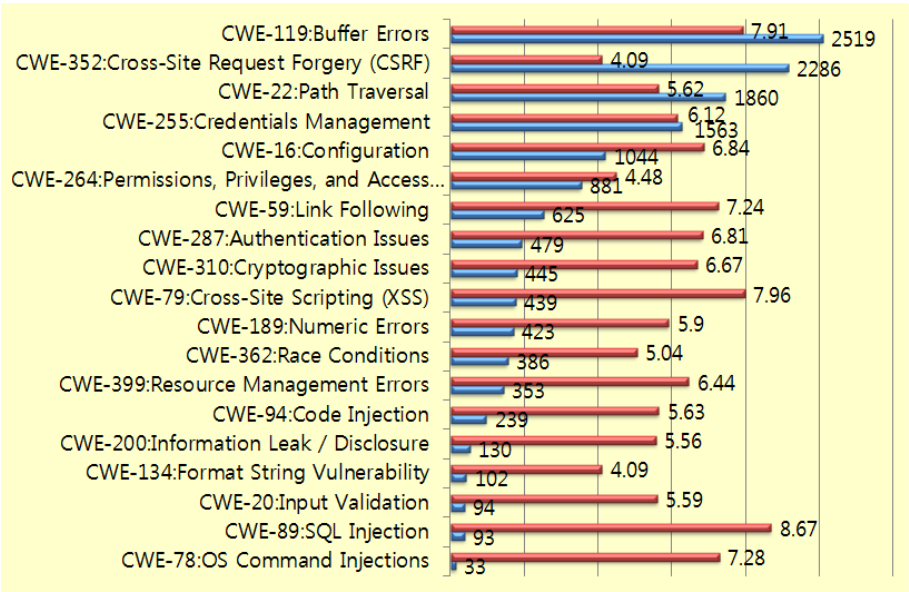
2.3. 보안취약점 관련 해외 연구사례

2.3.1. 보안취약점 목록 연구

보안취약점의 경우에도 보안약점과 마찬가지로 발생한 보안취약점 전반에 대한 목록을 제공하고자 하는 활동이 이루어지고 있다. 보안취약점 목록은 소프트웨어의 사용자에게 운영하고 있는 시스템의 취약점을 파악하여 대응할 수 있도록 하며, 프로그램 개발자에게 있어서도 다양한 사례를 제공함으로써 안전한 프로그램 개발에 도움을 준다. 또한 보안약점 관련 활동과 연계되어, 보안취약점 사례의 원인을 분석하여 보안약점 항목을 도출하거나 보안약점의 중요도를 평가하는 등 상호 보완적인 관계를 가지게 된다.

보안취약점 목록과 관련한 활동으로는 CVE, NVD, OSVDB, CNVD 등이 알려져 있다[10,11,12,13]. CVE (Common Vulnerabilities and Exposures)는 발견된 보안취약점에 대한 일관된 식별을 제공하는 것을 기본 목적으로 하고 있으며 "CVE-년도-순번" 형태의 식별자를 취약점에게 부여하고 있다.

NVD(National Vulnerability Database)는 보안 콘텐츠 자동화 프로토콜(SCAP)을 사용하여 표현된 미국 정부의 표준 기반 취약점 관리 데이터 저장소이다. SCAP를 활용함으로써 취약점 관리, 보안 측정 및 규정 준수의 자동화가 가능하며, NVD는 보고된 보안취약점에 대하여 CVE 식별자, 설명, 중요도 점수 및 관련 척도 평가 결과, 관련 제품 버전 정보, 관련 정보에 대한 링크, 원인 보안약점의 CWE 링크 등을 제공하고 있다. 현재 약 69,000개의 CVE 항목이 저장되어 있으며, 하루 평균 21.7개의 약점항목이 추가되고 있고 그 발생 비율 역시 증가하는 추세이다.



〔그림 1〕 NVD 보안취약점 분석 - 2011년 이후 13,394항목

[그림 1]은 2011년 이후 NVD에 보고된 13,394개의 보안취약점의 원인 보안약점을 분석한 결과이다. 분석한 내용은 해당 약점을 원인으로 한 보안취약점의 심각성 점수와 해당 보안취약점의 발생 건수이다. 발생빈도의 경우 버퍼넘침 약점을 원인으로 한 보안취약점의 사례가 가장 많았으며, 이어서 교차 사이트 요청 위조, 경로 순회 등의 약점을 원인으로 한 취약점이 다수 발견되었다. 취약점의 심각성을 분석해보면, SQL 삽입 약점과 교차 사이트 스크립팅, 버퍼넘침이 원인 보안약점으로 분석된 보안취약점들이 심각성이 높은 것으로 분석되었다.

NVD 외에 대표적인 보안취약점 목록으로는 OSVDB(Open Sourced Vulnerability Database)가 있다. 2002년 8월 Black Hat & Defcon 학술대회에서 설립되어 웹기반 보안취약점 데이터베이스를 제공하고 있으며 현재 약 117,000개의 보안취약점 항목을 제공하고 있다.

CNVD(China National Vulnerability Database)는 중국에서 구축된 취약점 데이터베이스로 보안제품 인증평가기관인 CNITSEC에 의해 운영되고 있으며 2010년 4월부터 약 27,000개의 취약점 정보를 구축하여 서비스를 시작하였다. CNVD는 CNCERT/CC 사무국을 중심으로 중국 ISP, 네트워크 보안 회사들과 소프트웨어 회사 및 인터넷 회사들이 참여하고 있으며, 300명이 넘는 중국내 화이트해커, 소프트웨어 및 디바이스 제품을 판매하는 200개 이상의 회사, 그리고 24명의 멤버들이 기술적인 협력을 통해 운영 중이다.

CNVD는 중국내 사용자들에게 중요한 영향을 미치는 취약점을 일반 소프트웨어, 웹 응용, 운영체제, 데이터베이스, 네트워크 장치, 보안 제품, 산업용 소프트웨어(통신, 모바일 인터넷, 산업용 제어 시스템)의 7개 카테고리로 구분하여 관리하고 있다.

2.3.2. 보안취약점 중요도 정량평가

보안취약점 중요도 정량 평가 방법으로는 FIRST 포럼의 지원으로 개발된 CVSS(Common Vulnerability Scoring System)[14]가 있다. CVSS는 보안 취약점의 심각성 평가를 위한 일반적인 프레임워크를 제공하며, 실제 사용되고 있는 소프트웨어에 존재하여 공격에 침해될 수 있는 실제적인 보안취약점을 대상으로 하기 때문에 CWSS와 차별성을 갖는다. CVSS는 보안취약점을 본질적인 기본 척도(Base Metric), 시간에 따른 척도 (Temporal Metric), 환경적인 척도 (Environmental Metric)의 세 그룹으로 구성된 14개 평가척도에 따라 평가하며, 10점 만점의 정량 평가 결과를 제공한다. 현재 버전 2가 발표되어 NVD에서 전체 보안취약점에 대한 기본 척도 점수가 제공되고 있으며, 버전 3가 개발중에 있다.

2.4. 국내 보안약점 및 보안취약점 관련 연구

2.4.1. 행정자치부 SW 개발보안

행정자치부 SW 개발보안은 전자정부 및 공공소프트웨어에 대하여 소프트웨어 개발단계에서 보안약점을 사전에 제거하고 SW 개발생명주기의 각 단계별로 수행하는 일련의 보안활동을 통하여 안전한 정보시스템을 구축하기 위한 체계로서 추진되었다. 본 정책은 행정기관 및 공공기관 정보시스템 구축·운영 지침에 근거하고 있으며 2012년 40억 이상의 과제를 대상으로 시작하여 2014년 20억 이상 과제로 확대하였고 2015년 전체 감리대상 과제로 확대할 예정이다.

SW 개발보안 정책은 중요 보안약점 목록인 보안약점기준을 중심으로 수행되고 있으며, 이에 기반하여 개발 시의 시큐어 코딩 수행 의무화, 약점 제거 진단 절차를 위한 전문 인력 배출, 관련 정적 분석 도구의 개발 지원 및 인증, 지원정보 구축 및 안내서 출판 등의 사업이 수행되고 있다.

행정자치부 보안약점기준은 47개의 중요한 보안약점 항목으로 구성되어 있으며 전자정부 및 공공 정보시스템의 특성을 반영하여 웹기반의 시스템에 중점을 둔 주요보안약점 목록이다. [표 4]는 47개 보안약점의 구성을 보여주고 있다.

보안약점 기준은 7개 유형으로 분류되어 있으며, 주로 웹관련 약점이 다수를 차지하고 있고, 네이티브 코드(native code)등을 고려한 버퍼넘침 관련 약점들이 포함되어 있다. 약점 항목의 선정에는 해외 주요 약점목록의 동향과, 국내 공공 정보시스템의 보안취약점 발굴사례, 관련 국내 학계, 산업계의 의견이 반영되었다. 특히, 2013년 두 번째 개정을 수행함에 있어서는, SW 개발보안의 특징을 반영하고 평가의 객관성을 보강한 보안약

〔표 4〕 SW 개발보안을 위한 보안약점기준의 구성

유형	주요내용	개수
입력 데이터 검증 및 표현	프로그램 입력 값에 대한 부적절한 검증 등으로 인해 발생할 수 있는 보안약점 예) SQL 삽입, 버퍼넘침, 자원삽입, 크로스사이트스크립트 등	15
보안 기능	인증, 접근제어, 권한 관리 등을 적절하지 않게 구현시 발생할 수 있는 보안약점 예) 부적절한 인가 허용, 중요정보 평문저장, 하드코드된 패스워드 등	16
시간 및 상태	멀티프로세스 동작환경에서 부적절한 시간 및 상태 관리로 발생할 수 있는 보안약점 예) 경쟁조건(TOCTOU), 제어문을 사용하지 않는 재귀함수 등	2
에러 처리	불충분한 에러 처리로 중요정보가 에러정보에 포함되어 발생할 수 있는 보안약점 예) 오류상황 대응 부재, 오류메시지를 통한 정보노출 등	3
코드 오류	개발자가 범할 수 있는 코딩오류로 인해 유발되는 보안약점 예) 널 포인터 역참조, 부적절한 자원 해제 등	4
캡슐화	불충분한 캡슐화로 인가되지 않은 사용자에게 데이터가 노출될 수 있는 보안약점 예) 제거되지 않고 남은 디버그 코드, 시스템 데이터 정보노출 등	5
API 오용	부적절하거나, 보안에 취약한 API 사용으로 발생할 수 있는 보안약점 예) DNS lookup에 의존한 보안결정 등	2

점 중요도 정량평가 방법론을 개발하여 주요보안약점 목록의 선정에 사용하였다[15].

2.4.2. S/W 신규 보안취약점 신고 포상제

한국인터넷진흥원에서는 2012년 우수 신규 보안취약점 신고에 대해 포상금을 지급하는 ‘S/W 신규 보안취약점 신고 포상제’를 도입하여[16] 해킹사고에 악용될 수 있는 취약점을 사전에 조치하고 관련 전문가의 취약점 발굴을 활성화하고자 하였다.

한국인터넷진흥원의 SW 신규 보안 취약점 신고 포상제는 약점 신고 당시 보안 업데이트가 나오지 않은 제로데이 취약점(Zero-Day Vulnerability)을 대상으로 한다. 신고된 취약점에 대해서는 평가결과에 따라 최고 500만원이 지급되며, 신규 취약점의 중요도를 평가를 위하여 객관적인 평가척도에 기반한 중요도 평가방법을 개발하여 활용하고 있다.

보고된 취약점에 대해서는 한국인터넷진흥원 인터넷침해대응센터 보안공지에서 대응을 권고하고 있으며 아울러 보안 업데이트를 개발하는데 사용되도록 분석 결과를 해당 업체에 전달한다.

Ⅲ. 보안약점 표준목록의 선정

보안약점 목록은 보안취약점 발생 시 원인 분석의 기본 정보가 되며 행정자치부 보안약점기준, CWE /SANS Top 25와 같은 주요 보안약점 도출의 후보군으로서 사용된다. 또한 보안취약점 연구와 보안약점 연구는 중요도 평가, 새로운 보안약점 항목 도출, 원인 보안약점 분석 등에 있어 상호 보완적인 관계에 있다. 본 장에서는 SW 개발보안을 위하여 수행된 보안약점 표준목록 연구를 소개한다.

3.1. 표준 보안약점 선정

본 연구에서는 SW 개발보안 사업을 위한 보안약점 기준 선정 시 후보군으로 사용할 수 있는 보안약점들의 목록으로 보안약점 표준목록을 선정하였다. 대표적인 보안약점 목록으로서 CWE가 있으나 보안약점 항목들의 개수가 700여개로 매우 많고 약점 간의 중복성이 존재하여 주어진 프로그램의 보안취약점에 대한 원인 보안약점을 분석할 시 일관된 원인 보안약점 선정이 어려운 문제가 발생한다. 이에 대하여 본 연구에서는 중복성을 최소화하고 적절한 개수의 항목으로 이루어진 보안약점 표준목록을 선정하여 제공하고자 하였다.

보안약점 표준목록을 선정하는데 있어 고려한 주요 사항은 다음과 같다.

- CWE에 포함된 전체 보안약점을 포괄한다.
- 적절한 약점항목 개수를 유지한다.
- 행정자치부 보안약점기준 등의 주요 보안약점 목록을 최대한 포함한다

보안약점간의 상관관계를 분석함에 있어 CWE에서 제공하는 리서치 관점(Research View)을 주로 활용하였으며, CWE의 전체 보안약점을 분석하여 CWE 전반을 포괄할 수 있는 목록을 도출하였다. 선정 과정에서

〔표 5〕 보안약점 표준목록

영역	영역별 보안약점 번호	개수
입력데이터 검증 및 표현	22, 41, 59, 66, 78, 79, 89, 90, 91, 94, 99, 112, 113, 114, 117, 119, 134, 138, 157, 170, 172, 178, 185, 190, 352, 427, 434, 436, 439, 601, 624, 643, 652, 781, 799, 807, 829, 917, 918, 925	40
보안기능	203, 213, 214, 216, 221, 226, 228, 250, 252, 259, 266, 267, 271, 282, 285, 287, 295, 306, 307, 312, 319, 321, 323, 327, 330, 346, 347, 349, 351, 353, 357, 358, 359, 377, 402, 424, 494, 521, 524, 526, 532, 539, 540, 547, 548, 552, 553, 592, 598, 603, 613, 636, 637, 642, 654, 656, 732, 757, 758, 759, 921, 926, 927, 939, 940, 941, 2011	67
시간과 상태	362, 367, 384, 497, 662, 834	6
오류 처리	209, 248, 369, 390, 391, 755	6
코드오류	400, 405, 410, 415, 416, 418, 430, 457, 465, 471, 476, 480, 506, 514, 561, 562, 563, 665, 670, 672, 675, 681, 682, 684, 697, 768, 770, 772, 841, 843, 913	31
캡슐화	488, 489, 495, 496, 501, 2013	6
API 오용	350, 573, 628, 676, 695, 749	6
기타 표준 보안약점	2001, 2002, 2003, 2012	4
합계		166

각 약점의 의미를 검토하여, 하나의 표준약점에 포함될 수 있는 세부 약점들은 하위약점으로, 표준약점으로 선정하기에 어려운 추상적인 형태의 약점인 경우에는 상위 약점으로 재분류하고 그 관계를 명시함으로써 주어진 임의의 CWE 항목이 어떤 표준약점 항목과 연관되는지를 명확히 제시하고자 하였다. 또한, 약점을 포괄하는 항목이 새로 필요할 경우 새로운 약점항목을 일부 추가하였다.

보안약점 표준목록은 166개의 약점항목으로 구성된다. 보안약점 표준목록은 CWE의 모든 보안약점을 포괄하도록 선정되었으므로, 하나의 표준보안약점 항목은 0개 이상의 하위 보안약점들을 대표할 수 있다. 예를 들어 CWE-22 경로 순회는 표준 보안약점이면서 20개의 하위 보안약점을 포괄하고 있으며, 행정자치부 보안약점기준과 SANS Top 25에 포함되어 있다.

3.2. 보안약점 표준목록의 구성

본 연구에서는 보안약점 표준목록에 포함된 166개의 보안약점을 보안약점의 성격에 따라 분류하기 위하여 MITRE에서 2005년도에 발표한 7 Pernicious Kingdoms[17]와 행정자치부 소프트웨어 개발보안 가이드에서 제시된 분류에 근거하여, 영역을 선정하였다. 선정된 영역은 입력데이터 검증 및 표현, 보안기능, 시간 및 상태, 오류 처리, 코드오류, 캡슐화, API 오용 영역으로 모두 7개이다.

또한 기타 영역으로 EJB, J2EE, Struts의 나쁜 사용 관행들과 ASP.NET 잘못된 구성(ASP.NET Misconfiguration)을 각각 하나의 표준 보안약점으로 선정하고, 이와 관련된 보안약점들을 하위 보안약점으로 분류하였다. 본 연구에서 선정한 166개의 표준 보안약점을 영역별로 정리하면 [표 5]와 같다.

보안약점 표준목록의 선정 과정에서 CWE에 포함된 보안약점으로는 대표하기 어려운 보안약점들이 존재하는 것이 발견되었다. 대표적인 예가 EJB, J2EE, Struts의 나쁜 사용 관행들이다. 따라서 본 연구에서는 기존의 CWE와는 별도로 6개의 보안약점을 추가하고 이를 표

〔표 6〕 신규 보안약점 항목

약점 번호	보안약점 이름
2001	EJB 나쁜 관행
2002	J2EE 나쁜 관행
2003	Struts 나쁜 관행
2011	패스워드관리
2012	ASP.NET 잘못된 구성
2013	부적절한 캡슐화 조정자

준 보안약점으로 선정하였다. [표 6]은 본 연구에서 추가한 표준 보안약점이다.

CWE 리서치 관점의 723개 보안약점 항목을 분석한 결과 표준약점 166개, 상위약점 55개, 하위약점 500개, 해당사항 없음 2개로 분류되었으며, 그 분포는 [표 7]과 같다. 해당사항 없음으로 분류된 약점은 불충분한 구획화(Insufficient Compartmentaliza ‐tion, CWE-653)와 불충분한 심리적 수용성(Insufficient Psychological Acceptability, CWE-655)으로서 소스코드와 관련된 소프트웨어 보안약점과 직접적인 연관성이 없는 경우이다.

CWE 리서치 관점은 일부 제외된 약점 외에는 CWE의 전체 보안약점을 포함하고 있으므로, 본 연구에서 선택한 표준보안약점 목록은 CWE의 전체 약점 목록을 포괄하고 있다고 간주할 수 있다.

〔표 7〕 약점 계층 분류별 개수

구분	개수	비율
표준	**166**	22.96%
상위	55	7.61%
하위	500	69.16%
해당 없음	2	0.28%
합계	723	

3.3. 행정자치부 보안약점기준과의 비교

본 연구에서 선정한 166개의 보안약점 표준목록은 2013년 발표된 행정자치부 보안약점기준을 모두 포괄하고 있으며, 각 영역별 약점의 분포는 비율은 [표 8]과 같다.

본 연구에서 제안된 보안약점 표준목록과 행정자치부 보안약점기준에서 가장 높은 비율을 차지하는 영역은 ‘보안기능’ 영역이며, 그 다음으로 ‘입력데이터 검증 및 표현’ 영역의 보안약점이 높은 비율을 차지하고 있다. 2개의 목록이 가장 큰 차이를 보이는 영역은 ‘코드오류’ 영역으로 보안약점 표준목록에는 31개의 보안약점이 선정되어 18.7%를 차지한 반면, 행정자치부 보안약점기준에서는 4개만이 선정되어 8.5%를 차지하고 있다. ‘캡슐화’ 영역의 경우는 보안약점 표준목록에는 6개, 행정부 보안약점기준에는 5개가 포함되어 비율에서 3.6%, 10.6%라는 차이를 보이고 있다.

〔표 8〕 영역별 보안약점 비율 (%)

영역	보안약점 표준목록		행정자치부 보안약점기준	
	개수	비율	개수	비율
입력데이터 검증 및 표현	40	24.1	15	31.9
보안기능	67	40.4	16	34.0
시간과 상태	6	3.6	2	4.3
오류 처리	6	3.6	3	6.4
코드오류	31	18.7	4	8.5
캡슐화	6	3.6	5	10.6
API 오용	6	3.6	2	4.3
기타	4	2.4	0	0.0
합계	166	100	47	100

Ⅳ. 한글화된 SW 보안약점 표준목록 DB 구축

한글화된 SW 보안약점 표준목록을 위한 DB 구축을 위해 먼저 XML 구조를 설계하였다. 각 보안약점의 한글화된 DB의 구조는 CWE의 구조를 기초로 하되 각 항목의 이름과 설명은 모두 한글화하고 불필요한 요소는 최대한 삭제하여 활용도를 높일 수 있도록 구성하도하였다. 또한 각 보안약점에 대해서 중요도 정량평가 방법[15]에 기반한 중요도 점수와 평가 척도별 점수를 제공하였다.

하나의 보안약점을 기술하기 위한 한글화된 약점정보의 구성은 다음과 같다. 한 항목은 필요에 따라 여러 개의 하위 항목들을 가질 수 있다.

- CWE ID/한글명/영문명
- 설명(Description): 보안약점에 대한 설명을 기술한다.
- 관련항목(CWE Relationships): 해당약점과 관련된 상위 및 하위 CWE 약점을 (*상위/하위, CWE_ID*)*의 형태로 기술한다. (*는 0개 이상을 의미)
- 관련 플랫폼(Applicable Platforms): 보안약점의 관련 플랫폼을 관련 언어, 운영체제, 소프트웨어 수행구조 등으로 분류하여 기술한다.
  - 관련 언어(Languages): 관련 언어를 기술하며 명시하지 않으면 전체에 해당한다.
  - 운영체제(Operating Systems): 관련 운영체

제를 기술하고 명시하지 않으면 전체에 해당한다.
  - 소프트웨어 수행구조(Architectural Para-digm): 메인프레임, 클라이언트-서버, n-단계, 웹-기반, 모바일 응용프로그램 등으로 소프트웨어 수행구조를 분리하여 기술한다.
- 약점 도입 시기(Time of Introduction):보안약점이 소프트웨어에 포함되는 개발단계를 기술한다.
- 중요도: 보안약점의 전체 중요도 점수와 다음의 각 평가 척도별 점수를 기술한다.
  - 기술적 영향
  - 권한 요구도
  - 상호작용 정도
  - 발견 가능성
  - 침해 가능성
  - 출현 정도
- 기술적 영향(Common Consequence): 보안약점의 기술적 영향을 다양한 침해의 형태에 따라 *(종류, 설명)**의 형태로 기술한다.
- 취약점 발생 예시(Demonstrative Examples): 보안약점의 예제와 설명을 *(예제, 설명)*$^{+}$의 형태로 하나 이상 기술한다. (+는 1개 이상을 의미한다.)
- CVE 발생 사례(Observed Examples):보안약점 관련한 CVE 발생 사례를 *(CVE 참조, 설명)*$^{+}$의 형태로 기술한다.
- 분류 맵핑(Taxonomy Mappings): 행정자치부 보안약점 기준, 7 Pernicious Kingdom, OWASP Top 10 등과 같은 다른 보안약점 분류 기준에서 해당 약점으로 대응되는 정보를 *(보안약점분류, 〈약점명〉)**의 형태로 기술한다.
- 참고문헌(References): 보안약점 관련 참고문헌들을 기술한다.
- 작성일(Content History): 보안약점의 최초작성일과 수정일을 *(최초작성/수정, 수정일)*$^{+}$의 형태로 기술한다.

이러한 보안약점의 DB 구조를 XML 스키마 형태로 작성하였으며, 스키마는 각 항목이 가질 수 있는 데이터의 구조를 정의하고 필요에 따라 각 항목이 가질 수 있는 가능한 값을 나열할 수 있다. 이 스키마를 기준으로 보안약점 표준목록 XML 데이터베이스를 작성하며, 스키마를 이용하여 작성된 XML 데이터베이스의 무결성을 자동으로 검사할 수 있다.

예를 들어 “관련_플랫폼” 항목의 경우에 가질 수 있는 세부항목 원소의 형태는 다음과 같이 “관련_언어”, “운영체제”, “소프트웨어_수행구조”이며 각 세부항목 역시 가질 수 있는 데이터의 구조나 값이 정의된다.

```
<xs:element name="관련_플랫폼" minOccurs="0">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="관련_언어"
        type="Languages_List_Type"
       minOccurs="0" maxOccurs="1">
      </xs:element>
      <xs:element name="운영체제"
        minOccurs="0" maxOccurs="1">
      <xs:complexType>
        ...
      </xs:complexType>
      </xs:element>
      <xs:element name="소프트웨어_수행구조"
       minOccurs="0" maxOccurs="1">
       ...
      </xs:element>
    </xs:sequence>
  <xs:complexType>
<xs:element>
```

다음은 “소프트웨어_수행구조” 항목의 값에 대한 스키마 정의로서 가능한 문자열 값이 명시된다.

```
<xs:simpleType>
  <xs:restriction base="xs:string">
    <xs:enumeration value="메인프레임"/>
    <xs:enumeration value="클라이언트-서버"/>
    <xs:enumeration value="n-단계"/>
    <xs:enumeration value="웹-기반"/>
    <xs:enumeration value="모바일 응용프로그램"/>
    <xs:enumeration value="SOA"/>
    <xs:enumeration value="자원공유 병행 시스템"/>
  </xs:restriction>
</xs:simpleType>
```

보안약점 표준목록 DB 구조를 위해 작성한 XML 스키마 파일의 크기는 약 1,400 줄 정도이다. 이 XML 스키마를 기준으로 하여 166개 SW 보안약점 표준목록을 위한 XML 데이터베이스를 작성하였다. XML 데이터베

이스 파일의 크기는 약 26,500 줄로서 보안약점 한 항목당 160줄 정도이다.

Ⅴ. 결 론

본 논문은 시큐어 코딩을 위한 보안약점 및 보안취약점 국내외 연구 동향을 정리하고, 아울러 행정자치부 SW 개발보안의 기반 데이터로 활용하기 위한 보안약점 표준목록 구축 연구를 소개하였다.

보안약점 표준목록은 CWE 전체 보안약점을 포괄하면서도 최대한 중복성을 배제하도록 선정되었으며, 선정된 각 보안약점에 대하여 중요도 정량평가를 수행하고, 평가 결과를 포함하여 보안약점에 대한 주요 한글 정보로 구성된 보안약점 XML 데이터베이스를 구축하였다.

본 연구의 결과는 다음과 같은 향후 연구에 활용될 수 있을 것이다. 먼저 작성된 XML DB를 효과적으로 활용하고, 이에 대한 정보의 공유 및 피드백을 통한 지속적인 개선이 이루어지도록 모바일 앱, 웹사이트 등 다양한 형태의 활용 시스템의 구축이 필요할 것이다. 그리고 보안약점목록을 보안약점기준의 체계적인 관리에 효과적으로 활용하기 위해서 발생한 보안취약점에 대하여 원인 보안약점을 판정할 수 있는 방법론에 대한 학문적인 연구가 필요할 것이다. 또한 보안취약점 DB의 구축을 추진하고 이를 보안약점 DB 관리 및 보안약점기준 관리와 연계함으로써 관련 정보의 전체적인 환류체계를 구축할 수 있을 것이다. 이러한 일련의 작업을 위해서는 다양한 기관이 보안취약점 사례 등의 기반 데이터를 공유할 수 있는 협력 및 보안 체계가 수립되어야 할 것으로 판단된다.

참 고 문 헌

[1] Gartner, "Now is the time for security at application level", http://www.gartner.com/id=487227, Dec., 2005.

[2] David Rice, *Geekonomics: The Real Cost of Insecure Software,* Addison- Wesley Professional, 2007.

[3] Benefits of the SDL, Microsoft, www.microsoft.com/security/sdl/about/benefits.aspx

[4] Bola Rotibi, The Business Value of Software Static Analysis, Macehiter Ward-Dutton Limited. August, 2008

[5] 행정기관 및 공공기관 정보시스템 구축·운영 지침 개정, 행정자치부고시 제2013-36호, 2013

[6] Common Weakness Enumeration (CWE), http://cwe.mitre.org/

[7] 2010 OWASP (The Open Web Application Security Project) Top 10, https://www.owasp.org/index.php/Top_10_2013-Top_10

[8] 2011 CWE/SANS Top 25 Most Dangerous Software Errors, http://cwe.mitre.org/top25/

[9] Common Weakness Scoring System (CWSS), http://cwe.mitre.org/cwss/

[10] Common Vulnerabilities and Exposures (CVE), http://cve.mitre.org

[11] National Vulnerability Database, http://nvd.nist.gov/home.cfm

[12] OSVDB:Open Sourced Vunerability Database, http://osvdb.org

[13] CNVD: China National Vulnerablity Database, http://www.cnvd.org.cn

[14] Common Vulnerability Scoring System (CVSS-SIG), http://www.first.org/cvss

[15] 안준선, 방지호, 이은영, “소프트웨어 보안약점의 중요도에 대한 정량 평가 기준 연구”, *정보보호학회논문지*, 19권6호, pp.1407-1417, June, 2012년.

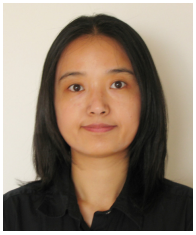
[16] 취약점신고-S/W 신규 보안 취약점 신고 포상제, https://www.krcert.or.kr/kor/consult/consult_04.jsp, 한국인터넷진흥원 인터넷침해대응센터

[17] K. Tsipenyuk , B. Chess and G. McGraw "Seven Pernicious Kingdoms: A Taxonomy of Software Security Errors", *IEEE Sec. & Privacy*, vol. 3, no. 6, pp.81-84 2005

〈저 자 소 개〉

안 준 선 (Joonseon Ahn)
종신회원

1992년 2월 : 서울대학교 계산통계학과 졸업
1994년 2월 : KAIST 전산학과 석사
2000년 8월 : KAIST 전자전산학과 박사
2001년 9월 ~ 현재 : 한국항공대학교 항공전자정보공학부 교수
관심분야 : 프로그래밍언어, 프로그램 분석, 소프트웨어 보안



이 은 영 (Eunyoung Lee)
종신회원

1996년 2월 : 고려대학교 전산과학과 졸업
1998년 8월 : 고려대학교 전산과학과 석사
2004년 1월 : Princeton University 전산학 박사
2005년 3월~현재 : 동덕여자대학교 컴퓨터학과 교수
관심분야 : 소프트웨어 보안, 프로그래밍언어, 클라우드 컴퓨팅

창 병 모(Byeong-Mo Chang)
정회원

1988년 2월 : 서울대학교 컴퓨터공학과 졸업
1990년 2월 : KAIST 전산학과 석사 졸업
1994년 2월 : KAIST 전산학과 박사 졸업
1995년 3월 ~ 현재 : 숙명여자대학교 컴퓨터과학부 교수
관심분야 : 프로그래밍언어, 프로그램 분석, 소프트웨어 보안