情報保護學會論文誌
第 22 卷 第 6 號, 2012. 12

소프트웨어 보안약점의 중요도에 대한 정량 평가 기준 연구*

안 준 선,[1†] 방 지 호,[2] 이 은 영[3‡]
[1]한국항공대학교, [2]한국인터넷진흥원, [3]동덕여자대학교

Quantitative Scoring Criteria on the Importance of Software Weaknesses*

Joonseon Ahn,[1†] Ji-ho Bang,[2] Eunyoung Lee[3‡]
[1]Korea Aerospace University, [2]Korea Internet Security Agency,
[3]Dongduk Women's University

요 약

소프트웨어 시스템을 보안 침해로부터 보호하기 위해서는 소프트웨어의 개발 단계에서부터 생명주기 전체에 걸쳐 보안약점을 제거하는 작업이 요구된다. 이러한 작업을 수행함에 있어서 계속하여 보고되고 있는 다양한 보안약점들에 대하여 시스템 보안과 실제 활용 목적에 미치는 영향이 큰 보안약점을 선별하여 적절히 대처하는 것이 효과적이다. 본 논문에서는 소프트웨어 보안약점 및 보안취약점의 중요성에 대한 기존의 정량 평가 방법론들을 소개하고, 이를 기반으로 신뢰도가 중요시되는 소프트웨어 시스템에 대하여 보안약점의 일반적인 심각성을 객관적으로 평가할 수 있는 정량 평가 기준을 제안한다. 또한 제안된 기준을 사용하여 2011 CWE/SANS Top 25 보안약점 명세에 대한 중요도 평가를 수행하고 그 결과를 기존 점수와 비교함으로써 제안된 평가기준의 유용성을 보이고자 한다.

ABSTRACT

In order to protect a software system from security attacks, it is important to remove the software security weaknesses through the entire life cycle of software development. To remove the software weaknesses more effectively, software weaknesses are prioritized and sorted continuously. In this paper, we introduce the existing scoring systems for software weakness and software vulnerability, and propose a new quantitative standard for the scoring system, which helps evaluate the importance of software weakness objectively. We also demonstrate the practicability of the proposed standard by scoring 2011 CWE/SANS Top 25 list with the proposed standard and comparing it to the original score of MITRE.

Keywords: software security, software weakness, software vulnerability, scoring system

I. 서 론

소프트웨어 소스코드에 존재하는 보안상의 허점을 제거함으로써 소프트웨어 시스템의 보안을 강화하고자 하는 연구가 활발히 진행되고 있다. 보안에 취약한 소스코드가 보안사고의 주요 원인인 것으로 보고되고 있으며[1], 방화벽이나 사용자 인증 등의 경계를 넘어서 웹을 통하여 자유롭게 접근되고 이동하는 프로그램이 일반화되고 있는 상황에서 시스템 보안 측면에서의 소스코드의 안전성은 그 중요성이 더욱 증가하고 있다.

소프트웨어에서 보안상의 공격을 받을 수 있는 취약한 소스코드 부분 또는 소스코드 형태를 소프트웨어

접수일(2012년 9월 10일), 수정일(2012년 10월 22일), 게재확정일(2012년 10월 27일)
* 본 논문은 2012년 한국인터넷진흥원 '시큐어코딩 기반 SW 개발보안 기반기술 연구' 위탁과제의 연구결과로 수행되었음(KISA-2012-024)
† 주저자, jsahn@kau.ac.kr
‡ 교신저자, elee@dongduk.ac.kr

보안약점(weakness)이라고 한다. 또한 소프트웨어에 존재하는 어떤 보안약점이 실제적으로 공격자의 공격에 취약하여 침해를 당할 수 있을 경우 이러한 허점을 보안취약점(vulnerability)라고 한다. 이러한 보안약점과 보안취약점은 개발단계에서부터 운용단계에 이르는 동안 제거되어야 하며, 관련 연구가 활발히 진행되어 소프트웨어 보안약점 목록인 CWE(Common Weakness Enumeration)와 실제 소프트웨어에 존재하는 보안 취약성의 목록인 CVE(Common Vulnerabilities and Exposures)가 발표되어 널리 참조되고 있다[2,3].

소프트웨어 개발 과정에서 개발된 혹은 개발 중인 소프트웨어에 대하여 보안 분석을 실행하였을 때, 개발자는 일반적으로 다양한 종류의 소프트웨어 보안약점에 대한 보고를 받게 되며, 개발자는 이러한 보안약점들 중에서 무엇이 심각한 약점인지에 대한 우선순위를 정할 수 있을 때 효과적으로 소프트웨어의 보안성을 강화할 수 있다. 또한 개발자뿐만이 아니라 소프트웨어 사용자도 우선적으로 고려하여야 하는 중요 보안약점 목록을 통하여 운용중인 소프트웨어의 보안성을 강화할 수 있고, 아울러 새로 개발되는 소프트웨어 시스템에 대하여 개발자에게 반드시 제거해야 할 보안약점들의 목록을 제시할 수도 있다. 이와 관련하여 CWE/SANS Top 25와 OWASP Top 10과 같은 주요 보안약점 목록이 매년 발표되어 다양한 방면에서 활용되고 있으며[4,5] 또한 이와 병행하여 보안 약점 및 취약점의 중요도에 대한 정량적인 평가방법을 제공하고자 하는 연구가 진행되어 대표적인 평가 방법론으로 CWSS (Common Weakness Scoring System)와 CVSS (Common Vulnerability Scoring System)가 사용되고 있다[6,7]. CVSS는 특정 소프트웨어의 특정 취약성을 평가하기 위한 방법으로서 다양한 분야에서 널리 활용되고 있으며, 관련하여 NVD(National Vulnerability Database)에서 알려진 소프트웨어 취약성들에 대한 기본적인 중요도 점수를 제공하고 있다[8]. CWSS는 소프트웨어 보안약점에 대한 평가 방법으로서 2011 CWE/ SANS Top 25의 선정에 사용되었다.

본 논문에서는 보안약점 및 보안취약점의 중요성에 대한 기존의 정량 평가 방법론들을 소개하고, 보안약점에 대한 일반적인 중요성을 평가할 수 있는 객관적인 정량 평가 방법을 제시하고자 한다. 보안약점에 대한 정량 평가 방법으로 CWSS가 제안되고 있지만, 평가 항목들의 등급 기준이 모호하고, 현재까지는 CWSS 연구 결과는 실제 알려진 특정 소프트웨어의 특정 보안약점의 평가를 주된 목적으로 하고 있다는 제약을 가진다. 이에 대하여 본 논문의 연구에서는 기존 CWSS의 연구 결과를 기반으로 하여 높은 보안성을 요구하는 소프트웨어 시스템을 전제로 하여 보안약점 자체에 대한 일반적인 심각성을 평가할 수 있는 객관적인 기준을 제시하고자 한다. 아울러 제안된 보안약점에 대한 평가 방법의 실용성을 기존의 중요 취약점 명세인 2011 CWE/SANT Top 25에 대하여 적용해 봄으로써 그 유용성을 보이고자 한다.

본 논문은 다음과 같이 구성된다. 2장에서는 본 연구의 수행을 위한 관련 기반 연구로서 CWSS와 CVSS를 소개한다. 3장에서는 CWSS를 기반으로 보안약점의 일반적인 평가를 위한 평가 척도를 선정하고 각 평가 척도에 대한 객관적 기준을 제시한다. 4장에서는 개발된 보안약점 평가 방법을 기존의 중요 취약점 명세에 적용한 결과를 제시하여 본 논문에서 제시된 기준의 정당성을 검토하며, 마지막으로 5장에서는 결론을 맺는다.

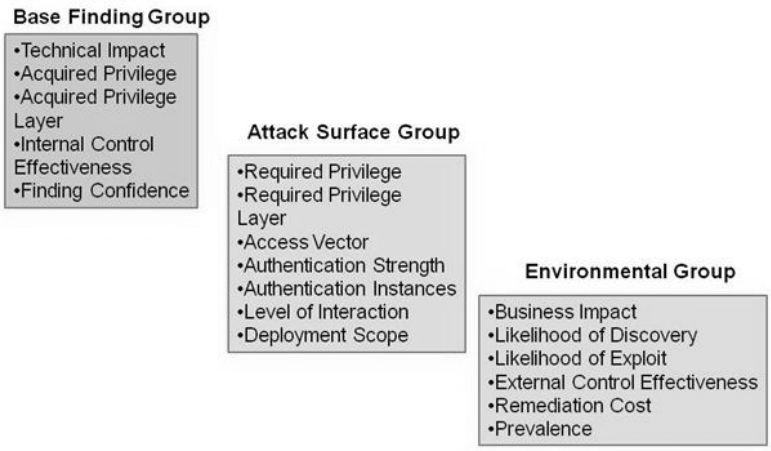
II. 관련연구

본 절에서는 소프트웨어 보안약점의 정량적 평가를 위한 기반 연구로서 CWSS와 CVSS를 소개한다.

2.1. Common Weakness Scoring System

CWSS는 소프트웨어 보안약점의 중요도를 평가하는 평가 체계로 CWE 프로젝트의 일부로 수행되고 있다[6]. CWE와 CWSS의 특징은 안전한 소프트웨어의 개발과 보안 유지에 책임이 있는 당사자들인 정부, 학계, 산업체들이 모여서 만드는 커뮤니티 형태의 협업이라는 점에 있다. 이 프로젝트는 미국 NCSD (National Cyber Security Division)와 미국 DHS (Department of Homeland Security)의 지원을 받아서 진행되고 있으며 현재 CWSS는 버젼 0.8이 2011년 6월에 발표되었고 아직 정식 버젼은 발표되지는 않은 상태이다.

CWSS에서는 보안 약점의 심각성을 평가하기 위한 정량적인 기준으로서 18가지의 평가척도(metric)를 약점 자체의 심각성(Base Finding Metric Group), 공격 측면의 심각성(Attack Surface Matric Group), 환경적 측면의 심각성(Environment Matric Group)의 3개 그룹으로 분류하여 제시하고 있으며, 각 평가



〔그림 1〕 CWSS 평가척도 그룹과 그룹별 하위 요소들

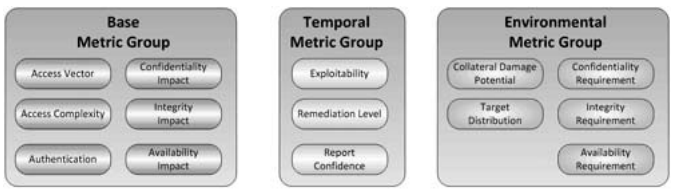
척도별 1점 만점의 점수에 기반을 둔 100점 만점의 중요도 점수 산출식을 제공하고 있다. 〔그림 1〕은 3개의 평가척도 그룹과 그룹별 18개의 하위 요소를 나타낸다.

현재 CWSS는 이미 발견된 특정 보안약점에 대한 평가인 특정 모드(Targeted Mode)를 중심으로 그 연구가 진행되고 있다. 따라서 보안약점 자체의 일반적인 중요도의 평가를 위해서는 18개 평가척도 중 적용하기에 적합하지 않은 것들이 존재하고 있다. 또한 평가 기준 자체도 아직까지 객관적이지 못한 면이 있어 이에 대한 추가적인 연구가 진행될 것으로 판단된다. 이와 관련하여 중요 보안약점 목록을 제시한 2011 CWE/SANS Top 25에서는 CWSS의 18개 보안척도 중 3개 척도를 설문조사의 방법으로 적용한바 있다.

2.2. Common Vulnerability Scoring System

CVSS는 약점으로부터 실제 발생한 보안취약점의 중요성을 평가하는 연구 결과로 보안취약점 평가를 위한 일반적인 프레임워크를 제공한다〔7〕. CVSS는 실제 발생한 보안취약점에 대한 평가를 목표로 하기 때문에, 개별 소프트웨어 패키지에 대한 보안약점을 진단하는 CWSS와 차별성을 가진다. 그렇지만 CVSS는 물리적인 시스템에 미치는 중요도를 위주로 판단하기 때문에 물리적 시스템이 아닌 사용자 데이터나 기능성에는 영향을 주지만, 물리적 시스템에는 비교적 영향을 적게 주는 보안취약점이 상대적으로 낮게 평가되는 경향을 가지고 있다.

〔그림 2〕는 3개의 평가척도 그룹과 그에 딸린 하위 14개 평가척도를 보여주고 있다. 보안취약점의 침해에 따른 결과와 공격의 용이성을 평가하는 기본 평가척도(Base Metric) 그룹의 평가척도들은 보안취약점의 고유한 성격을 정의하고 교환하는 것을 목적으로 한다. 이를 통하여 사용자가 해당 보안취약점의 심각성을 보다 명확하고 직관적으로 이해할 수 있도록 돕는다. 추가적으로 사용자는 시간에 따라 변할 수 있는 기준들인 시간 평가척도 (Temporal Metric) 그룹과 환경에 따라 변할 수 있는 환경적 평가척도(Environmental Metric) 그룹을 이용하여 자신들의 특정 환경과 발생 시점을 반영한 취약성의 심각성을 정확하게 표현할 수 있다. 이것은 보안취약점으로 야기된 위기를 관리하는데 보다 유용하게 이용될 수 있다.



〔그림 2〕 CVSS 평가척도 그룹과 그룹별 하위 요소

CVSS는 다양한 보안 관련 업체에서 널리 활용되고 있으며 특히 NVD에서는 지금까지 알려진 다양한 보안취약점의 발생 사례에 대하여 기본 평가척도 그룹의 평가 결과를 평가척도별 점수와 함께 제공하고 있다.

III. 보안약점 평가시스템

본 장에서는 CWSS를 기반으로 하여 기존의 보안약점 및 새롭게 추가되는 보안약점의 중요도를 평가할 수 있는 객관적이고 정량적인 기준을 제안하고, 개발된 평가 항목의 근거 및 객관적 기준을 제시한다. CVSS가 이미 발견된 특정 소프트웨어의 취약점 평가를 주된 목적으로 하는데 비하여 CWSS는 소프트웨어 보안약점을 위한 평가 방법론으로서 다양한 상황과 평가 목적에 활용될 수 있는 평가 방법을 제시한다는 특징을 가진다. 또한 CWSS는 소프트웨어 사용 상황의 주요 보안관련 요구를 반영하여 보안약점의 중요도를 평가할 수 있다는 특징을 가진다.

본 연구는 보안상의 높은 안전성을 목적으로 하는 시스템에 대하여 보안약점의 일반적인 심각성에 대한 정량적인 평가기준을 제시하는 것을 목적으로 하고 있으므로, CWSS가 본 연구에 적합한 것으로 판단하였다.

3.1 평가척도의 선택

CWSS는 3개 그룹에 모두 18개의 평가척도를 제시한다. 그러나 현재 이러한 CWSS의 평가 척도는 특정 소프트웨어의 특정 약점을 평가하기 위한 목적형 평가(targeted mode)를 위한 것으로서 본 연구에서와 같이 약점의 일반적인 심각성 평가(general mode)를 위해서는 적합하지 않은 평가 척도가 존재한다. 이와 관련하여 CWSS와 병행하여 수행된 중요 약점 리스트 도출 연구인 2011 CWE/SANS Top 25에서는 전체 18개 척도 중 중요도(importance), 출현도(prevalence), 침해 가능성(likelihood of exploit)의 세 개 척도만을 사용하고 있다. 이에 대하여 본 연구에서는 18개 평가 척도를 검토하여 이 중 보안약점의 일반적인 중요도 평가에 타당한 것으로 판단되는 6개 척도를 반영하였다. 반영된 척도와 선정 이유는 다음과 같다.

- 기술적인 영향 (Technical Impact) : 본 척도는 주어진 보안약점이 보안취약점으로 연계되어 보안 침해가 발생하였을 경우의 직접적인 피해의 심각성을 평가하게 된다. 2011 CWE/SANS Top 25에서 중요도의 항목으로 포함되었으며, 보안약점과 관련된 취약점들의 일반적인 침해 상황으로부터 유추 가능한 것으로 판단된다.
- 권한 요구도 (Required Privilege) : 본 척도는 보안약점 침해에 필요한 시스템에 대한 접근 권한을 평가하기 위한 항목이다. 주어진 보안약점에 대하여 관련된 사례들의 일반적인 전형을 도출하는 데는 어려움이 있으나, 웹 응용프로그램과 관련된 약점 등에서는 좀 더 적은 권한을 요구하게 되므로 이를 반영하기 위하여 선택되었다.
- 상호작용 정도 (Level of Interaction) : 본 척도는 공격자가 해당 약점으로 인한 취약성을 공격하여 침해에 성공하기 위하여 요구되는 피해자측의 협조적인 동작의 요구 정도를 평가한다. 해당 보안약점으로 인한 보안취약점들의 일반적인 침해 패턴이 CAPEC[9] 등에 의하여 보고되고 있고, 이에 대하여 일반적으로 요구되는 상호작용의 정도를 유추 가능한 것으로 판단된다.
- 발견 가능성 (Likelihood of Discovery) : 본 척도는 해당 보안약점이 발생되는 소프트웨어들의 일반적인 형태와 CAPEC의 관련 침해 방법을 검토하여 제한적인 범위 내에서 평가가 가능한 것으로 판단된다.
- 침해 가능성 (Likelihood of Exploit) : 본 척도는 해당 보안약점으로 인한 보안취약점들의 일반적인 침해 방법이 보고되고 있으므로 이를 바탕으로 일반적인 공격 성공 가능성의 평가가 가능한 것으로 판단된다. 2011 CWE/SANS Top 25에서도 평가에 반영되었으며, CWE에서도 관련 항목을 제시하고 있다.
- 출현도 (Prevalence) : 본 척도는 해당 약점과 연관된 취약점들의 최근 발생상황을 NVD 등의 관련 취약점 데이터베이스를 통해 조사할 수 있다. 2011 CWE/SANS Top 25에서도 평가에 반영되었다.

나머지 12개의 척도는 보안약점 자체의 일반적인 특성으로 평가하는데 적합하지 않거나 높은 신뢰성을 요구하는 소프트웨어에 대해서 보안약점 제거의 용이성과 관련된 항목은 평가항목으로 적합하지 않은 것으로 판단되어 제외되었다. 제외 근거와 관련 척도들은 다음과 같다.

- 소프트웨어가 설치된 특정 환경에 의존적인 척도 : 접근 벡터, 인증 강도, 인증 단계의 횟수, 목적에 대한 영향도
- 특정 소프트웨어의 특성에 의존적인 척도 : 획득된 권한, 획득된 권한의 수준, 발견의 신뢰도, 요구되는 권한 수준, 배포 범위
- 약점의 심각성이 아닌 수정의 비용과 관련된 척도 : 내부 제어의 효과, 외부 제어의 효과, 개선비용

반영되지 않는 평가 척도는 중요도 점수의 산출시 CWSS의 평가 등급 중 제외(Not Applicable)로 평가되며, 이를 통하여 CWSS 방법론에서 제시된 점수 계산식을 그대로 사용할 수 있다.

3.2 평가척도의 객관적 기준

각각의 평가 척도에 대하여 CWSS는 평가 등급과 관련 기준을 제시하고 있지만, 그 기준이 충분히 객관적이지 않은 경우가 많고, 일부 등급에 대한 기준은 제시하고 있지 않은 경우도 존재한다. 때문에 2011 CWE/SANS Top 25에서는 전문가 그룹의 설문조사를 바탕으로 각 평가 척도별 점수를 산정하였다.

본 절에서는 이에 보안약점 평가의 객관성을 확보하기 위하여 기존 CWSS의 평가 척도와 CWE와 NVD의 관련 정보 및 CVSS의 평가 등급별 기준 등을 고려하여 객관적인 기준을 제시하고자 한다.

3.2.1. 기술적인 영향

- 개요 : 해당 SW 보안약점으로 인하여 공격에 침해당했을 경우, 해당 공격 성공으로 인한 기술적인 심각성을 평가한다.
- 평가 방법 : CWE에서 보안약점에 대한 침해 결과(common consequences)로 제시하고 있는 8가지 항목에 대한 관련성을 평가하여 이에 대한 합산 점수를 기준으로 등급을 부여한다. 이때 관련성이란 해당 보안약점으로 인한 직접적인 결과를 의미하며, 간접적인 침해는 제외하는 것을 원칙으로 하나, 간접적인 침해의 사례가 많을 경우에는 이를 포함시킬 수 있다. 또한 데이터와 관련된 항목의 경우 관련 취약점의 CVSS 점수의 기밀성 영향도(confidentiality impact)와 무결성 영향도(integrity impact) 항목을 참고한다. 8가지 항목과 각 항목에 대하여 부여하는 점수는 〔표 1〕과 같으며 허용되지 않은 프로그램 수행의 경우 그 결과의 심각성이 큰 것으로 인식되고 있으므로 더 높은 점수를 부여하였다.

이러한 항목별 점수의 합산으로부터 〔표 2〕와 같이 기술적인 영향 함목의 등급을 부여한다.

〔표 1〕 기술적인 영향의 평가를 위한 침해 항목 및 평가 점수 기준

Technical Impact 항목	전적인 침해	부분적인 침해	관련 없음
Modify data	2	1	0
Read data	2	1	0
DoS: unreliable execution	2	1	0
DoS: resource consumption	2	1	0
Execute unauthorized code or commands	4	2	0
Gain privileges / assume identity	2	1	0
Bypass protection mechanism	2	1	0
Hide activities	2	1	0

〔표 2〕 기술적인 영향 항목의 점수 부여 기준

등급	점수	평가기준
Critical	1.0	6점 이상
High	0.9	4점~5점
Medium	0.6	2점~3점
Low	0.3	1점
None	0.0	0점
Default	0.6	Default 등급은 일반적으로 사용하지 않음.

〔표 3〕 권한 요구도 항목의 점수 부여 기준

등급	점수	평가기준
None	1.0	약점을 가진 코드에 접근하기 위하여 아무 권한도 필요하지 않을 경우를 말한다. 특히 공개되어 있는 웹 페이지를 위한 웹 응용프로그램에서 발생되는 보안약점은 None으로 평가한다.
Guest	0.9	특정한 관리자의 허락을 요구하지 않고, 불특정 다수에게 허용되는 회원가입 등을 통하여 접근할 수 있는 프로그램 코드의 경우에 해당된다.
Regular User	0.7	특별한 관리자 권한이 없는 정규 사용자 권한을 필요로 하는 경우를 말한다.
Partially-Privileged User	0.6	전체적인 관리자 권한은 필요 없으나, 백업과 같은 부분적인 관리자 권한을 필요로 하는 경우를 말한다.
Administrator	0.1	해당 소프트웨어와 운영체제 전체에 대한 접근 권한을 가진 시스템 관리자 권한이 필요한 경우를 말한다.
Default	0.8	해당 보안약점이 다양한 권한 하에서 수행되는 다양한 소프트웨어에서 발견되는 경우 Default 등급으로 하며, 점수는 Guest와 Regular User의 중간값을 부여한다.

〔표 4〕 상호작용 정도 항목의 점수 부여 기준

등급	점수	평가기준
Automated	1.0	희생자의 협조적인 행동이 필요 없다.
Limited / Typical	0.9	희생자의 일반적인 행동(이메일 열람, 웹페이지 접근)이 동반되어야 침해가 가능하다.
Moderate	0.8	희생자가 경고 메시지를 무시하는 것과 같은 어느 정도 위험할 수 있는 작업을 수행하여야 해당 보안약점에 대한 공격이 이루어진다.
Opportunistic	0.3	공격자가 직접적으로 희생자를 직접적으로 유도할 수 없으며, 희생자의 실수나 다른 사용자의 동작에 대하여 그 피해를 수동적으로 확대시킬 수만 있다.
High	0.1	A large amount of social engineering is required, possibly including ignorance or negligence on the part of the victim.희생자가 잘못된 행동을 하도록 희생자에 대한 직접적인 접근을 포함한 복잡한 사회적 작업을 수행하여야 한다.
No interaction	0.0	희생자의 동작과 관련없이 보안취약점 발생의 가능성이 없으며, 일종의 버그로서만 존재한다.

3.2.2. 권한 요구도

- 개요 : 공격자가 공격을 보안약점을 가지고 있는 코드 또는 기능에 접근하기 위하여 필요한 접근 권한을 평가한다.
- 평가방법 : 해당 보안약점이 주로 발견되는 응용프로그램의 일반적인 형태와, CWE 사이트의 관련 CVE 항목 및 NVD의 관련 취약점 사례를 참고하여, 해당 보안약점을 가진 코드를 수행하기 위한 일반적인 권한을 판단한다. 모든 권한에 골고루 분포되어 있을 경우에는 Default 등급을 부여한다. 각 등급별 기준은 〔표 3〕과 같다.

3.2.3 상호작용 정도

- 개요 : 보안약점을 공격하는데 필요한 피공격자의 협조적인 행동의 요구 수준을 평가한다.
- 평가방법 : 관련된 CAPEC의 공격 패턴과 CVE이 취약점 사례 등을 참고하여 등급에 따라 평가한다. 여러 기준에 모두 해당하는 경우 해당 값들의 중간(median) 값을 부여한다. 등급별 기준은 〔표 4〕와 같다.

3.2.4 발견 가능성

- 개요 : 공격자가 보안약점을 발견할 가능성을 평가한다.
- 평가 방법 : 해당 SW 보안약점에 대하여 CAPEC의 관련 공격 방법과 NVD 등의 취약점 사례들을 참고하여 공격자가 일반적인 시스템에 해당 보안약점을 가진 소프트웨어의 보안약점을 발견할 가능성을 평가한다. 프로그램에 따라 다양하게 분포할 경우에는 Default 값을 부여한다. 등급별 기준은 〔표 5〕와 같다.

〔표 5〕 발견 가능성 항목의 점수 부여 기준

등급	점수	평가기준
High	1.0	공격자가 소스코드의 검토 없이 간단한 시도나 자동화된 도구를 사용하여 보안약점을 발견할 가능성이 높은 경우에 해당한다.
Medium	0.6	보안약점을 공격하기 위하여 소스코드의 검토나 역공학(reverse engineering)을 수행하여야 할 경우에 해당한다.
Low	0.2	공격자가 보안약점을 발견하기 위해서는 전문화된 기술과 상당한 시간을 투입하여 넓은 범위의 소스코드에 대한 자세한 검토를 수행하여야 한다.
Default	0.6	다양한 형태로 보안약점이 발견될 경우에 중간값을 취한다.

3.2.5 침해 가능성

- 개요 : 필요한 공격에 필요한 권한과 접근 방법 및 인증을 가지고 있는 공격자가 해당 보안약점을 공격하였을 경우 공격이 성공할 가능성을 평가한다.
- 평가방법 : CWE의 관련 보안약점 항목의 해당 항목을 우선적으로 반영한다. 해당 항목이 아직 없을 경우에는 NVD 등의 취약점 사례들을 참고하여 일반적인 가능성을 제시된 기준에 따라 평가한다. 다양하게 분포되어 있을 경우 Default 값을 부여한다. 그 등급별 기준은 〔표 6〕과 같다.

3.2.6 출현도

- 개요 : 해당 보안약점이 실제적으로 출현하는 정도를 평가한다.
- 평가방법 : 해당 보안약점과 관련된 취약점의 최근 3년간의 발견 사례를 NVD(National Vulnerability

〔표 6〕 침해 가능성 항목의 점수 부여 기준

등급	점수	평가기준
High	1.0	공격자가 해당 보안약점을 발견하여 공격함으로써 침해를 성공할 확률이 매우 높은 경우를 말하며, 안정적인 공격방법을 쉽게 개발할 수 있는 경우이다. CWE의 Likelihood of Exploit 평가가 high 이상인 경우에 해당한다.
Medium	0.6	공격자가 해당 보안약점을 공격할 확률이 높으나, 성공 확률이 가변적인 경우를 말한다. 또한, 성공의 경우에도 일반적으로 여러 번의 공격을 시도하게 된다. CWE의 Likelihood of Exploit 평가가 medium인 경우에 해당한다.
Low	0.2	일반적으로 공격 대상이 될 확률이 매우 낮은 보안약점으로서 공격의 성공 가능성도 제한적인 경우이다. CWE의 Likelihood of Exploit 평가가 low인 경우에 해당한다.
None	0	공격당하거나 해당 보안약점으로 인한 보안 침해가 없을 경우로서 단순한 버그인 경우이다.
Default	0.6	해당 보안약점으로 인한 침해 가능성이 다양할 경우에 중간값을 부여한다.
Quantified	0.4/0.8	CWE 평가에 medium to high이거나 low to medium인 경우 해당 등급의 중간값(0.8, 0.4)을 부여한다.

〔표 7〕 출현도 항목의 점수 부여 기준

등급	점수	평가기준
Widespread	1.0	해당 보안약점이 관련 프로그램 형태에 매우 널리 퍼져 있는 경우이다. 최근 3년간 관련 취약점이 300건 이상 발견된 경우에 이 등급을 부여한다.
High	0.9	해당 보안약점이 매우 자주 발견되는 경우이나 일반적으로 퍼져있지는 않은 경우이다. 최근 3년간 관련 취약점이 30건 이상 300건 미만 발견된 경우에 이 등급을 부여한다.
Common	0.8	해당 보안약점이 가끔씩 발견되는 경우이다. 최근 3년간 관련 취약점이 10건 이상 30건 미만 발견된 경우에 이 등급을 부여한다.
Limited	0.7	해당 보안약점이 거의 발견되지 않는 경우이다. 최근 3년간 관련 취약점이 10건 미만 발견된 경우에 이 등급을 부여한다.
Unknown	0.5	새로운 보안약점이기 때문에 아직 발견되지 않은 경우이거나, 관련 자료가 없을 경우에는 unknown으로 평가한다.

Database)에서 조사하여 해당 보안약점으로 인한 보안취약점 발생의 빈번한 정도를 평가한다. 관련 보안취약점의 발생 사례는 NVD(National Vulnrability Database)를 검색하여 조사할 수 있다. 그 등급별 기준은 〔표 7〕과 같다. 각 등급의 건수에 대한 사항은 관련 2011 CWE/SANS Top 25의 평가 사례와 실제 조사된 취약성 사례를 고려하여 설정하였다.

IV. 정량적 평가 시스템의 적용

4.1 정량적 평가 시스템의 적용

CWSS에서는 기술적인 영향 척도나 목적에 대한 영향 척도가 0일 때에는 심각성을 0으로 계산하며, 그 외의 경우에는 다음과 같은 산출식에 의하여 중요도를 산출한다〔2〕. 본 연구에서는 CWSS를 이용하여 산출된 기존의 중요도와의 일관성 유지 및 상대적 비교를 위하여 보안약점의 중요도 평가시 CWSS에서 제시한 다음의 중요도 산출식을 사용하였다.

중요도 점수 = 약점 자체의 심각성 × 공격 측면의 심각성 × 환경적 측면의 심각성

- 약점 자체의 심각성 = 〔(10 × 기술적인 영향 + 5 × (획득된 권한 + 획득된 권한 수준) + 5 × 발견의 신뢰도) * 내부 제어의 효과〕 × 4.0
- 공격 측면의 심각성 = 〔20 × (권한 요구도 + 요구되는 권한 수준 + 접근 벡터) + 20 × 배포 범위 + 10 × 상호작용정도 + 5 × (인증 강도 + 인증 횟수)〕 / 100.0
- 환경적 측면의 심각성 = 〔(10 × 목적에 대한 영향 + 3 × (발견 가능성 + 침해 가능성) + 3 × 출현도 + 개선비용) × 외부 제어의 효과〕 / 20.0

본 연구에서는 18가지 척도 중 6가지 척도를 사용하고 있으므로 나머지 척도에 대해서는 제외(Not Applicable)로 설정하여 최대 점수인 1.0을 부여한다.

〔표 8〕은 중요도 평가의 예로서 SQL 삽입(SQL Injection) 보안약점에 대한 평가척도별 점수 및 근거와, 이로부터 산출된 중요도 점수를 보여주고 있다. 기술적인 영향 항목은 관련된 침해 종류로부터 얻어진 점수(4점)를 기준으로 High(0.9)로 평가되었으며,

〔표 8〕 SQL 삽입 보안약점에 대한 중요도 평가 결과

<table>
<tr><th>평가항목</th><th colspan="2">평가결과</th><th>평가 근거</th></tr>
<tr><td>기술적인 영향</td><td>H</td><td>0.9</td><td>
<table>
<tr><th>TI 항목</th><th>점수</th></tr>
<tr><td>Modify data (2/1/0)</td><td>1</td></tr>
<tr><td>Read data (2/1/0)</td><td>1</td></tr>
<tr><td>DoS: unreliable execution (2/1/0)</td><td>0</td></tr>
<tr><td>DoS: resource consumption (2/1/0)</td><td>0</td></tr>
<tr><td>Execute unauthorized code or commands (4/2/0)</td><td>0</td></tr>
<tr><td>Gain privileges / assume identity (2/1/0)</td><td>1</td></tr>
<tr><td>Bypass protection mechanism (2/1/0)</td><td>1</td></tr>
<tr><td>Hide activities (2/1/0)</td><td>0</td></tr>
<tr><td>합계 (6~:C, 4~5:H, 2~3:M, ~1:L, 0:N</td><td>4</td></tr>
</table>
</td></tr>
<tr><td>권한 요구도 (RP)</td><td>N</td><td>1.0</td><td>웹을 통한 불특정 사용자의 공격이 가능하므로 None으로 평가한다.</td></tr>
<tr><td>상호작용 정도 (IN)</td><td>Aut</td><td>1.0</td><td>피해자 측의 특정 동작을 요구하지 않으므로 Automated로 평가한다.</td></tr>
<tr><td>발견 가능성 (DI)</td><td>H</td><td>1.0</td><td>해당 약점이 존재할 가능성이 있는 입력값에 대하여 자동화된 도구 등을 이용하여 널리 알려진 공격 패턴을 입력하여 약점 존재 여부를 확인할 수 있으므로 High로 평가한다.</td></tr>
<tr><td>침해 가능성 (EX)</td><td>H</td><td>1.0</td><td>해당 약점이 존재할 경우 쉽게 공격 스트링을 전송하여 공격할 수 있으며, 성공 가능성 또한 높으므로 High로 평가한다.</td></tr>
<tr><td>출현정도 (P)</td><td>W</td><td>1.0</td><td>최근 3년간 발견된 취약점 사례가 NVD의 경우 300건을 넘어 1000여건에 해당하므로 Widespread로 평가한다.</td></tr>
<tr><td>중요도 전체 점수</td><td colspan="3">96</td></tr>
</table>

웹을 통하여 불특정 다수의 공격이 가능하므로 권한 요구도는 None(1.0)으로 평가되었다. 다른 4개의 항목도 평가 기준에 따라 객관적으로 평가되었다.

4.2 2011 CWE/SANS Top 25에 대한 평가

본 연구에서 제시된 평가 척도의 적절성과 객관성을 테스트하기 위하여 본 연구의 정량 평가 시스템을 2011 CWE/SANS Top 25에 적용하였다. 〔표 9〕는 CWE/SANS Top 25 리스트에 포함된 전체 보안 약점들에 대한 평가 결과를 보여준다.

본 논문에서 제안된 방법론을 이용한 결과는 전체적으로 CWE/SANS Top 25의 순위와 부합하였으며 일부 항목에 대해서 상이점이 발생하였다. 이는 다음과 같은 사항이 반영된 것으로 판단된다.

- 본 연구에서는 6개의 척도를 반영하였으나, CWE/SANS Top 25에서는 3개 척도만을 반영하였다.
- 기술적인 영향 항목의 평가에 있어 CWE/SANS Top 25의 조사에서는 객관적인 기준을 제시하지 않았기 때문에 평가의 차이가 발생할 여지가 있으며 또한 다른 항목의 요소가 반영될 가능성도 있는 것으로 판단된다.
- CWE/SANS Top 25에서 버퍼 넘침 오류에 대해서 낮은 점수를 부여한 경향이 발견되며 이러한 점은 CWE/SANS Top 25 선정이 설문조사를 기반으로 하였기 때문에 소스코드 취약성이 강조되는 웹과 관련한 오류에 피조사자들이 좀 더 높은 중요도를 부여한 것으로 예상된다.

〔표 9〕 2011 CWE/SANS Top 25에 대한 정량 평가 비교

순위	CWE-ID	보안약점 이름	Top25 점수	평가결과
1	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	93.8	96
2	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	83.3	94.6
3	CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	79.0	90.2
4	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	77.7	95
5	CWE-306	Missing Authentication for Critical Function	76.9	87.4
6	CWE-862	Missing Authorization	76.8	85.2
7	CWE-798	Use of Hard-coded Credentials	75.0	83.9
8	CWE-311	Missing Encryption of Sensitive Data	75.0	79.4
9	CWE-434	Unrestricted Upload of File with Dangerous Type	74.0	80.2
10	CWE-807	Reliance on Untrusted Inputs in a Security Decision	73.8	80.2
11	CWE-250	Execution with Unnecessary Privileges	73.1	78.3
12	CWE-352	Cross-Site Request Forgery (CSRF)	70.1	74.4
13	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	69.3	78.2
14	CWE-494	Download of Code Without Integrity Check	68.5	78.3
15	CWE-863	Incorrect Authorization	67.8	74.6
16	CWE-829	Inclusion of Functionality from Untrusted Control Sphere	66.0	74.2
17	CWE-732	Incorrect Permission Assignment for Critical Resource	65.5	73.4
18	CWE-676	Use of Potentially Dangerous Function	64.6	73.4
19	CWE-327	Use of a Broken or Risky Cryptographic Algorithm	64.1	69.8
20	CWE-131	Incorrect Calculation of Buffer Size	62.4	85.2
21	CWE-307	Improper Restriction of Excessive Authentication Attempts	61.5	65.5
22	CWE-601	URL Redirection to Untrusted Site ('Open Redirect')	61.1	69.4
23	CWE-134	Uncontrolled Format String	61.0	85.2
24	CWE-190	Integer Overflow or Wraparound	60.3	71
25	CWE-759	Use of a One-Way Hash without a Salt	59.9	63.7

V. 결 론

소프트웨어 시스템을 보안 침해로부터 보호하기 위해서는 소프트웨어의 개발 단계에서부터 생명주기 전체에 걸쳐 보안약점을 제거하는 작업이 요구된다. 이러한 작업을 수행함에 있어서 계속하여 보고되고 있는 다양한 보안약점들에 대하여 시스템 보안과 실제 활용 목적에 미치는 영향이 큰 보안약점을 선별하여 적절히 대처하는 것이 효과적이다.

본 논문에서는 소프트웨어 보안약점 및 보안취약점에 대한 기존의 정량 평가 방법론들을 소개하고, 이를 기반으로 신뢰도가 중요시되는 소프트웨어 시스템에 있어서 보안약점의 일반적인 심각성을 객관적으로 평가할 수 있는 정량 평가 기준을 제안하였다. 또한 제안된 기준을 사용하여 2011 CWE/SANS Top 25 보안약점 명세에 대한 중요도 평가를 수행하고 그 결과를 기존 점수와 비교함으로써 제안된 평가기준이 실제 관련 연구자들의 경험과 부합됨을 보였다.

향후 연구로는 보안약점 기준의 객관성을 높이기 위한 연구가 수행되어야 할 것이며, 아울러 제외된 CWSS의 평가 척도 중 보안약점의 일반적 중요도 항목으로 추출할 수 있는 요소를 추가로 추출해 내어 이를 평가 척도로 추가적으로 반영하고자 하는 연구를 진행할 예정이다. 이러한 연구는 독자적인 정량평가 척도의 개발로 이어질 것이며, 이에 기반 하여 우리나라의 실정에 맞는 주요 소프트웨어 약점목록의 제시도 가능할 것으로 판단된다.

참고문헌

〔1〕 Theresa Lanowitz, "Now is the time for security at application level," Gartner G00127407, http://www.gartner.com/id=487227, Dec. 2005.

〔2〕 Common Weakness Enumeration (CWE), http://cwe.mitre.org.

〔3〕 Common Vulnerabilities and Exposures (CVE), http://cve.mitre.org.

〔4〕 2011 CWE/SANS Top 25 Most Dangerous Software Errors, http://cwe.mitre.org/top25.

〔5〕 Top 10 2010 - OWASP, https://www.owasp.org/index.php/Top_10_2010.

〔6〕 Common Weakness Scoring System (CWSS), http://cwe.mitre.org/cwss.

〔7〕 Common Vulnerability Scoring System (CVSS), http://www.first.org/cvss.

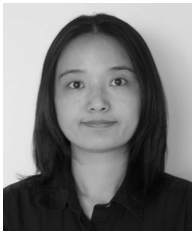
〔8〕 National Vulnerability Database, http://nvd.nist.gov/home.cfm.

〔9〕 CAPEC-Common Attack Pattern Enumeration and Classification (CAPEC), http://capec.mitre.org.

〈著者紹介〉

안 준 선 (Joonseon Ahn) 종신회원
1992년 2월: 서울대학교 계산통계학과 졸업
1994년 2월: KAIST 전산학과 석사
2000년 8월: KAIST 전산학과 박사
2000년 8월~2001년 8월: KAIST 프로그램분석시스템연구단 연구원
2001년 9월~ 현재: 한국항공대학교 항공전자및정보통신공학부 교수
〈관심분야〉 프로그래밍언어, 프로그램 분석, 소프트웨어 보안, 프로그램 병렬화,

방 지 호 (Ji-ho Bang) 정회원
1997년 2월: 홍익대학교 컴퓨터공학과 졸업
2001년 8월: 홍익대학교 컴퓨터공학과 석사
2007년 2월: 홍익대학교 컴퓨터공학과 박사수료
2001년 7월~현재: 한국인터넷진흥원 책임연구원
〈관심분야〉 SW 개발보안, 모바일 보안, 정적분석



이 은 영 (Eunyoung Lee) 종신회원
1996년 2월: 고려대학교 전산과학과 졸업
1998년 8월: 고려대학교 전산과학과 석사
2004년 1월: Princeton University 전산학 박사
2004년 1월~2004년 12월: University of Ottawa 박사후 연구원
2005년 3월~ 현재: 동덕여자대학교 컴퓨터학과 교수
〈관심분야〉 소프트웨어 보안, 프로그래밍언어, 클라우드 컴퓨팅