Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.5, Oct. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.5.969

ISO/IEC 15408, 18045 기반 소프트웨어 취약성 분석 방법론

임 재 우[†‡]
현대오토에버

Refining software vulnerbility Analysis under ISO/IEC 15408 and 18045

Jae-Woo Im[†‡]
HYUNDAI AutoEver

요 약

국제표준인 공통평가기준에서는 취약성 정보를 수집하고 침투시험을 수행하는 과정을 요구하고 있다. 하지만 촉박한 개발 및 평가 기간에 따라 임시방편의 취약성 점검 및 분석이 이뤄지며 취약성 분석에 대한 체계의 부재로 개발자의 역량에 따라 취약성 분석 및 적용이 제각각 이루어지고 있다. 이에 동일한 평가등급을 획득한 제품임에도 불구하고 보안성 품질이 상이하다. 본 논문에서는 방대한 취약성 정보를 직관적으로 이해하고 적용할 수 있는 취약성 분류체계 및 적용 방안을 제시한다. 뿐만 아니라, 보안성 평가 대상 여부와 무관하게 정보보호제품 개발 시 정보보호제품 개발 및 평가에 실용적으로 적용할 수 있는 정보보호제품의 보안성 품질 관리 방안을 제안하고자 한다.

ABSTRACT

CC (Common Criteria) requires collecting vulnerability information and analyzing them by using penetration testing for evaluating IT security products. Under the time limited circumstance, developers cannot help but apply vulnerability analysis at random to the products. Without the systematic vulnerability analysis, it is inevitable to get the diverse vulnerability analysis results depending on competence in vulnerability analysis of developers. It causes that the security quality of the products are different despite of the same level of security assurance. It is even worse for the other IT products that are not obliged to get the CC evaluation to be applied the vulnerability analysis. This study describes not only how to apply vulnerability taxonomy to IT security vulnerability but also how to manage security quality of IT security products practically.

Keywords: Common Criteria, Security Vulnerability, Security Quality, Penetration Test

I. 서 론

정보보호시스템은 정보보호시스템 공통평가기준(ISO/IEC 15408)과 정보보호시스템 평가 방법론(ISO/IEC 18045)에 근거하여 보안성을 평가받을 수 있다[1][2]. 평가 등급에 따라 보안목표 명세서, 설계서, 설명서, 생명주기 지원, 시험서, 취약성 분석서 등 다양한 증거요구사항을 바탕으로 보안성 평가가 이루어진다.

보안성 평가를 위한 취약성 분석 증거요구사항의 경우 무엇을 해야 하는지는 제시되고 있지만 어떻게 해야 하는지에 대한 부분은 다소 모호하다.

또한, 정보보호시스템의 개발 주기가 짧아짐에 따라 보안성 평가를 위한 다양한 증거요구사항을 준비할

접수일(2014년 9월 4일), 수정일(2014년 9월 22일), 게재확정일(2014년 10월 6일)
† 주저자, mahnduck@hyundai-autoever.com, mahnduck@gmail.com
‡ 교신저자, mahnduck@hyundai-autoever.com, mahnduck@gmail.com(Corresponding author)

수 있는 시간 확보가 어려워지고 있어 제품에서 발견된 취약성의 원인, 재현방법 등의 관리 및 분석이 체계적으로 이루어지기 어려운 것이 현실이다.

본 연구에서는 SAC (Structured Assurance Case)기반의 표준인 ISO/IEC 15408, 18045와 CWE-CVE-CAPEC을 활용한 정보보호제품의 체계적인 취약성 분석 방법을 수립하며, 정보보호시스템의 취약성 분석이 특정 보증등급 획득을 위한 형식적인 절차가 아닌 정보보호시스템의 보안성 품질 측정 및 관리를 위한 효용성 있는 절차로 활용될 수 있는 방법론을 제안한다.

II. 관련 연구

2.1 ISO/IEC 18045 취약성 분석

ISO/IEC 18045의 취약성 분석 평가 클래스 (AVA: Vulnerability assessment)에서는 평가자가 수행한 취약성 분석의 엄밀성과 공격자가 잠재적 취약성을 식별하고 악용하는 데 필요한 공격 성공 가능성의 수준에 근거하여 취약성 분석 조사 (AVA_VAN.1), 취약성 분석 (AVA_VAN.2), 집중화된 취약성 분석 (AVA_VAN.3), 체계적인 취약성 분석(AVA_VAN.4), 고도의 체계적인 취약성 분석으로 계층화 되어 있다[2].

취약성 분석은 크게 공개영역 조사를 통한 잠재적 취약성 식별(AVA_VAN.1.2E/2.2E/3.2E/4.2E/5.2E), 설명서, 기능명세, TOE (Target Of Evaluation) 설계 및 보안 구조 설명을 이용한 독립적인 취약성 분석 (AVA_VAN.2.3E/3.3E/4.3E/5.3E), 식별된 잠재적 취약성에 근거한 침투시험 수행 (AVA_VAN.1.3E/2.4E/3.4E/4.4E/5.4E)으로 구분된다.

공개영역 조사를 통한 잠재적 취약성 식별은 TOE 유형과 관련된 보안 이메일 리스트 (AVA_VAN.1/2), 컨퍼런스 프로시딩과 대학과 다른 관련 기관에 의한 연구 활동 (VAN_VAN.3/4/5) 등을 통해 이루어질 수 있다. 독립적인 취약성 분석은 TOE 명세서와 문서를 분석하여 취약성을 악용하는 데 요구되는 공격 성공 가능성과 그 취약성으로 인한 통제 및 손상의 범위에 기반한 잠재적 취약성에 대한 가설 수립을 수립한다. 또한, 보안 구조 설명서를 분석하여 우회, 침해, 직접공격, 감시, 오용 등의 방법으로 TSF (Toe Security Functions)를 무력화시키고 손상시킬 수 있는 방법을 찾아낸다.

식별된 잠재적 취약성에 근거한 침투시험 수행은 TOE의 TSFI (Toe Security Functions Interface)를 통해 TSF (Toe Security Function)(1.3E), 보안 아키텍처의 구조적 속성(2.4E), 특정 메커니즘의 정확한 구현 (3.4E, 4.4E)을 자극하고 반응을 관찰하는 시험을 수행한다. 공격 성공 가능성은 취약성 분석 수준에 따라 기본(1.3E, 2.4E), 강화된-기본(3.4E), 중간(4.4E), 높은(5.4E) 수준으로 구분되어 적용된다.

2.2 CWE & CVE

CWE (Common Weakness Enumeration)는 약점을 설명하는 공통 언어로 코드, 설계, 시스템 아키텍처에서 취약성을 야기할 수 있는 특성 및 속성이 될 수 있다[3]. CWE는 다중 레벨의 계층적으로 구성되어 있어, 구조상 상위 레벨에 위치한 특정 CWE는 여러 타입의 약점을 포괄하는 개념을 제공하며, 하위 레벨의 CWE와 관련될 수 있다.

취약성은 SFR (Security Functional Requirement)을 위반하는 데 사용될 수 있다고 식별한 TOE의 잠재적 약점을 말한다. CVE (Common Vulnerabilities and Exposures)는 취약성 노출을 설명하는 공통 언어로 시스템의 보안 정책을 위반하는 공격을 허용한 취약성과 보안정책 위반 및 공격을 통한 노출을 의미한다[4].

2.3 CAPEC

CAPEC(Common Attack Pattern Enumeration and Classification)은 보안 제품과 서비스의 약점을 악용한 예를 분석하여 생성된 공격 패턴 목록이다[5]. 공격 패턴은 취약한 시스템/네트워크를 대상으로 공격이 어떻게 이루어졌는지 설명하는 추상적인 메커니즘이다. CAPEC은 공격 패턴 설명, 공격 전제조건, 전형적인 노출 가능성, 공격 방법 및 예시로 구성되어 있다. 각 공격패턴은 공격의 설계, 상세한 공격 수행 절차, 공격의 결과 및 완화 대책 등을 제공함으로서 공격자 입장에서 취약성을 재현하고 이를 대응하는데 매우 효과적으로 사용될 수 있다.

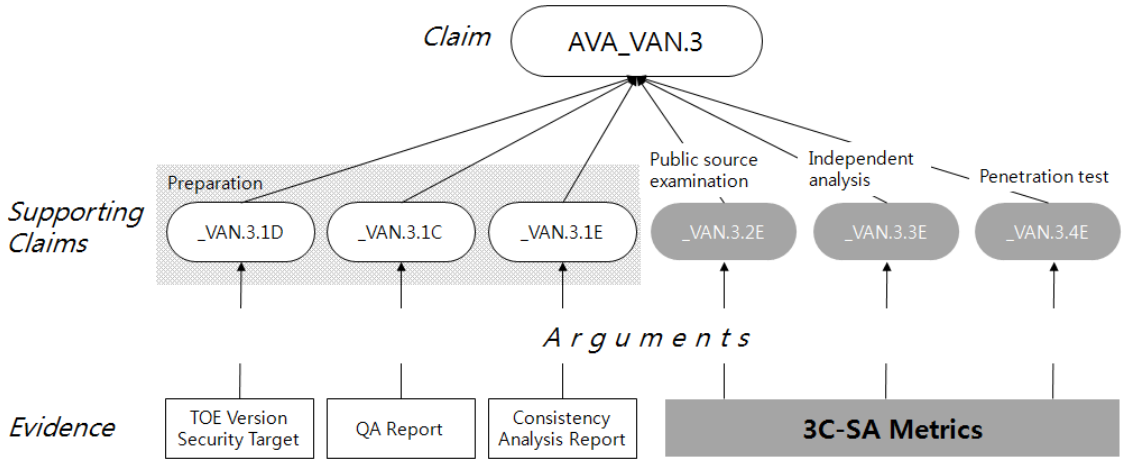

Fig. 1. EAL 4 Vulnerability Analysis SAC

2.4 SAC

Fig.2.의 SAC(Structured Assurance Case)는 보증에 대한 주장(Claim), 이를 뒷받침하는 논거(Argument)와 증거(evidence)로 이루어진 구조화된 논리구조이다[6]. 보증에 대한 주장은 평가 대상의 소프트웨어나 시스템의 특징, 속성, 행동을 주장할 수 있다. 논거는 주장을 지원하는 논리적 명제로 증거와 주장을 연결하는 논리와 추론을 의미한다. 증거는 주장을 증명하기 위한 정보이므로 객관적이고 재현가능하며, 논란의 여지가 없어야 한다. 주로 관찰, 분석, 시험, 측정의 결과를 증거로 사용할 수 있다. SAC의 최상단 주장은 두개의 하위 주장으로 뒷받침되며, 각 하위 주장은 논거에 의해 설명된다. 즉, 하위 주장이 유효하다면, 최상위 주장도 유효하다는 것이 논거이다.

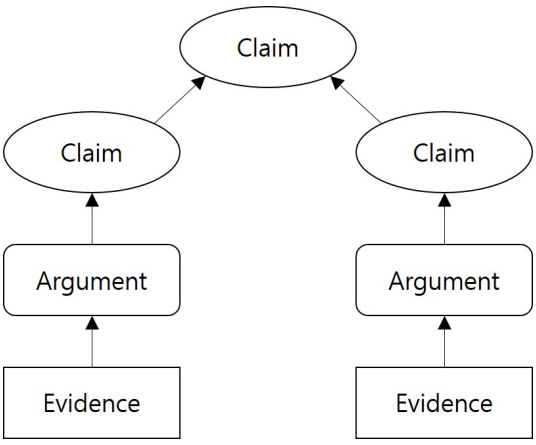

Fig. 2. SAC

ISO 15408/18054는 정보보호 시스템의 수준별 보안성 평가를 위한 기준 및 방법론으로 SAC 기반의 국제표준이다. 각 수준별 보안성 평가를 보증하기 위한 주장(평가보증등급, e.g. EAL 4:체계적인 설계, 시험 및 검토) 이를 보증하기 위한 평가 항목(하위 주장 및 논거), 증거(보증 요구사항 및 평가 요구사항)가 논리적으로 구성된 문서이다.

III. 소프트웨어 취약성 분석 방법론

ISO 15408/18054 평가보증등급 4의 취약성 분석평가 SAC는 Fig.1.과 같다. 최상위 주장(AVA_VAN.3)은 체계적인 설계, 시험 및 검토를 통한 취약성 분석의 완전함을 주장한다. 이를 위한 6개의 하위 주장(Sub-claim)들(Preparation (AVA_VAN 3.1D/3.1C/3.1E: 평가 준비) - Public source examination (AVA_VAN 3.2E: 공개영역 조사) - Independent Analysis(AVA_VAN 3.3E: 독립적 분석) - Penetration test (AVA_VAN 3.4E침투 시험))은 최상위 주장의 완전함을 각각의 논거들로 뒷받침하고 있다. 본 논문에서 제안하는 3C-SA (CWE-CVE-CAPEC based Security Analysis) 모델은 Preparation 하위 주장을 제외한 나머지 하위 주장들의 일관되고 체계적인 증거를 생성하기 위함이다.

3.1 3C-SA 모델

체계적이고 일관된 취약성 분석을 위해 TOE의 구성요소 및 환경에 적합한 CVE-CWE-CAPEC을 식별하여 취약성 분류기준을 적용한 Fig.3. 3C-SA 모델을 개발하였다. CVE의 CVSS(Common Vulnerability Scoring System), CWE의 Likelihood of Exploit, CAPEC의 공격 실행 흐름(Attack execution flow)는 TOE의 취약성 분석 품질을 측정하는 주요 지표로 활용된다. 이와 같은 3C-SA 모델을 기반으로 공격 내성을 측정하기 위해 침투시험을 수행하면, 취약성의 공격 가능성을 증명하게 되고 TOE의 보안성 품질 측정지표인 잔존 취약성 점수를 도출할 수 있다.

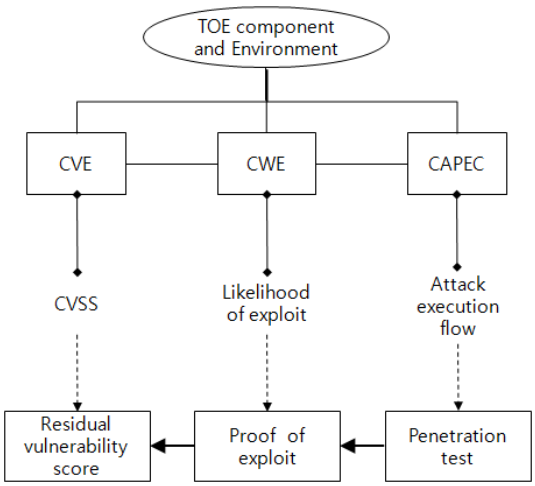

Fig. 3. 3C-SA Model

3.1.1 CVE-CWE-CAPEC 식별 방법

(1) SAC 분석을 통한 잠재적 취약성 식별: 취약성 분석 SAC의 독립적 취약성 분석(AVA_VAN 3.3E)을 통해 수립된 가설을 만족하는 CWE 및 CAPEC을 식별한다. 이러한 식별을 통해 해당 가설에 대한 원인과 이를 실제 공격 패턴으로 가설의 주장을 증명할 수 있다.

(2) 공개영역 조사를 통한 잠재적 취약성 식별: TOE의 운영환경 및 기술적 상황 등의 조건을 만족하는 CWE 및 CAPEC을 식별한다. Table 1.은 잠재적 취약성 집합을 정의할 때, 반드시 포함되어야 하는 최소한의 요건이다.

Table 1.Conditions for Identifying CWE/CAPEC

Item	Conditions
CWE	Weakness_Abstraction = "Base" or "Variant" Applicable_Platforms Detection_Methods Related_Attack_Patterns
CAPEC	Pattern_Completeness = "Complete" Pattern_Abstraction = "Standard" or "Detailed" Attack_Execution_Flow Technical_Context Related_Weaknesses

(3) 잠재적 취약성 필터링: TOE 범위에 포함되지 않는 식별된 잠재적 취약성의 운영환경 및 기술적 요건들을 필터링하여 침투시험의 범위를 최적화한다. 필터링 과정에서 특정 CWE와 CAPEC을 제외할 경우 상세한 이유를 기록한다.

잠재적 취약성은 식별된 CWE와 CAPEC의 참조하는 항목으로 식별할 수 있고, TOE의 운영환경 및 기술적 상황 등을 만족하는 조건으로 필터링한다.

3.1.2 공격 내성 측정 방법

식별된 잠재적 취약성을 기반으로 한 TOE의 공격 내성 측정 및 보고 방법은 다음과 같다.

(1) 침투 시험 설계 및 명세: 각 침투 시험 항목은 식별된 CAPEC의 공격 실행 흐름을 활용하여 설계 및 명세 되어야 한다. 또한, 침투 시험의 완전성을 위해 모든 시험 항목은 식별된 CWE와 CAPEC에 매핑 되어야 한다.

(2) 침투 시험 수행: 침투 시험의 설계 및 명세에 따른 시험 수행으로 TOE의 공격 내성을 측정할 수 있고 잠재적 취약성의 실제 공격 가능성을 증명할 수 있다.

(3) 잔존 취약성 도출: 잔존 취약성은 악용 가능한 취약성과 잔여 취약성을 모두 포함해야 하며, 해당 CVE의 CVSS로 TOE의 잔존 취약성 점수를 도출한다.

Vulnerbility Criteria		CVE	CVSS-Base Score	CWE	Likelihood of Exploit	CAPEC	Resolved	Rational
TOE Environment	Operation System Vulnerabilities	-	0	-	-	-	-	
	Web Vulnerabilities	CVE-2011-0001	7.5	CWE-98	Very High	CAPEC-103	O	Modified TOE and TOE enviornment
	Database Vulnerabilities	CVE-2012-0009	6	CWE-338	High	CAPEC-Custom-01	O	
	Network Vulnerabilities	-	0	-	-	-	-	
Security Architecture	Domain Separation	-	0	-	-	-	-	
	Self Protection	-	0	-	-	-	-	
	Secure Initialization	CVE-2013-0044	9	CWE-45	Low	CAPEC-82		
	Bypassing	CVE 2013-0033	9	CWE-88	Low	CAPEC-25		
Security Functions	Identification & Authentication	CVE-2011-0088	5	CWE-2	Low	CAPEC-98	X	- Likelyhood of Exploit is low and the impact is insignificant, so it is accepted as a residual vulnerability. - Planned to resolve in the next release.
	Security Management	-	0	-	-	-	-	
	Protection of the TSF	-	0	-	-	-	-	
	User Data Protection	-	0	-	-	-	-	
	Cryptographic Support	CVE-2013-0005	6	CWE-45	Medium	-	-	The CAPEC doesn't exist, and failed to implement the test.
	Access Control	-	0	-	-	-	-	
Source Code	C/C++	CVE-2008-0389	8	CWE-23	Medium	CAPEC-45	O	Added the input verification routine for buffer overflow attack
	Java	CVE-2012-0001	5	CWE-256	High	CAPEC-25	O	applied hash (SHA-2) algorithm for the plain password)
	PHP	-	0	-	-	-	-	

Security Anlaysis Result	CVSS(Score/Count	Likelyhood of Expl
	6/1	Low
	5/1	Medium
Security Quality Score	11	

Planned to apply to the next release
Failed implementation

Fig. 4. 3C-SA Metric

3.2 3C-SA 매트릭스

Fig.4. 3C-SA 매트릭스는 3C-SA 모델을 통해 식별 및 필터링 후 도출된 잠재적 취약성을 이용하여 TOE의 공격 내성을 측정하고 TOE의 일관되고 체계적인 보안 품질지표를 관리하기 위해 개발하였다.

논리적인 취약성 분류 기준으로 TOE의 환경 구성요소, 보안구조, 보안기능, 소스코드 등이 존재한다[1][7]. 이를 기반으로 TOE의 구조적 문제 및 취약성 발생 원인을 파악하기 위해 보안성 평가 보증 문서를 분석하여 상세 취약성 분류 기준을 추가 도출하였다. TOE 환경 구성요소 및 보안 기능은 구현된 TOE의 특성에 따라, 보안기능의 세부 분류기준은 ISO 15408-2부 보안요구사항의 기능 클래스별로 추가/삭제할 수 있도록 구성해야 한다. 소스코드 또한, TOE를 구현한 언어로 구성되어야 한다.

CVE, CWE, CAPEC은 3.1.1절의 CVE-CWE-CAPEC 식별 방법을 통해 도출된 각 항목의 식별자를 의미한다. CVSS-Base Score와 Likelihood of Exploit은 식별된 CVE와 CAPEC의 속성이다. Resolved는 해당 CVE의 취약성 해결 여부, Rationale은 비고 정보이다. 이와 같은 식별된 정보는 취약성 분류 기준에 따라 매핑되어야 한다.

3C-SA 매트릭스는 침투 시험 후 해결 취약성과 잔여 취약성의 이력을 관리함으로써 취약성 분석 절차를 통해 보안 품질을 체계적이고 일관적으로 관리할 수 있게 한다. 또한, 분석 결과(잔여 취약성)는 잔여 취약성의 합계를 통해 TOE의 보안 품질을 수치화할 수 있다.

IV. 취약성 분석 예시

본 논문에서 제안한 3C-SA 모델에 기반하여 TOE A의 취약성을 아래와 같이 분석할 수 있다. TOE A는 C++과 JAVA로 구현되었으며, DB를 사용하고 있는 웹 애플리케이션 기반의 정보보호 제품이라고 가정한다.

1. 독립적 취약성 분석(AVA_VAN 3.3E)을 통해 수립된 가설을 만족하는 잠재적 취약성을 식별 (Fig. 5. 1.1)

1. CVE-CWE-CAPEC Determination		
	1.1 Identify Potential Vulnerabilities from existing SAC	- CWE - 98, 338, 45, 88, 2 - CAPEC - 103, 82, 25, 98
	1.2 Identify Potential Vulnerabilites from public sources	- CWE - 342, 120, 45, 23, 256, 31, 9, - CAPEC, 28, 75, 45, 25, 98
	1.3 Filtering Vulnerabilites (TOE Components and Environment)	- CWE - 98, 338, 45, 88, 2, 45, 23, 256 - CAPEC - 103, 82, 25, 98, 45, 25 - CVE-2011-0001, 2012-0009, 2013-0044, 2013-0033, 2011-0088, 2013-0005, 2008-0389, 2012-0001
2. Assessment for TOE susceptibility to attack		
	2.1 Design and specify CAPEC based penetration testing	
	2.2 Execute attack execution flow baed penetration testing	
	2.3 Determine residual vulnerabilites and evaluate security quality	Residual Vulnerabiilites CVE-2011-0088 CVE-2013-0005

Fig. 5. Example of Security Analysis

2. 공개 영역(CWE, CAPEC 데이터베이스)에서 Table 1.의 조건에 따라 잠재적 취약성을 식별 (Fig. 5. 1.2)
3. TOE의 구성 요소 및 운영환경에 적합하지 않은 잠재적 취약점 필터링 (Fig. 5. 1.3)
4. 식별된 취약점의 CAPEC을 기반으로 침투 시험을 설계하고 수행 (Fig. 5. 2.1~2)
5. 침투 시험결과 취약점 CVE 2011- 0088, 2013-0005 잔존 (Fig. 5. 2.3)

CAPEC-Custom-01의 경우 공개 영역의 CAPEC이 존재하지 않아 CAPEC 형식에 맞게 자체 개발할 수 있음을 보인다. 잔존 취약점의 경우 CVE-2011-0088의 경우 수정이 가능하지만 공격 영향이 TOE에 미치는 영향이 매우 미미하여 다음 릴리스 적용을 선언하고, CVE-2013-0005의 경우 재현이 불가능하여 잔존 취약성으로 분류하였다.

분석결과 TOE A는 2개의 잔존 취약성(6점, 5점)을 통해 보안 품질은 11점을 획득하였다(0점 만점).

이러한 체계적인 취약성 분석결과를 통해 TOE A의 보안 품질을 수치화할 수 있으며 동일 취약성 대응에 대한 중요한 자산을 축적할 수 있다.

V. 결 론

취약성 분석은 정보보호 제품의 보안성 검증에 가장 중요한 부분이다. 기존에는 정보보호제품 시스템 평가 방법과 취약성 수집/분류 방법이 있었으나, 체계적이고 일관성 있는 취약성 분석 절차의 부재로 정보보호 제품의 보안성 품질 검증 시 많은 시간과 노력이 소요되거나 보안 품질 검증 및 향상에 큰 도움이 되지 못하고 있다. 이에 본 논문에서는 SAC 기반의 표준과 CVE, CWE, CAPEC을 활용한 3C-SA 모델을 제안하였다.

3C-SA 모델을 통해 운영환경, 보안 구조, 보안 기능, 소스코드 등 다양한 관점에서 보다 체계적인 취약성 분석체계를 수립하고 정보보호 제품의 보안성 품질을 수치화한다면 정보보호 제품의 보안 품질 검증 및 향상에 기여할 수 있을 것이다.

향후에는 3C-SA 모델을 실제 제품에 적용하여 비교 및 분석 할 것이며, 3C-SA 모델에 CVSS 체계를 적용하여 정보보호제품의 보안 품질 측정 방법을 고도화하는 연구를 수행고자 한다.

References

〔1〕 "Information technology -- Security techniques -- Evaluation criteria for IT security Part 1,2,3," ISO/IEC 15408-1/2/3, 2009.
〔2〕 "Information technology -- Security techniques -- Methodology for IT security evaluation," ISO/IEC 18045, 2005.
〔3〕 CWE, "https://cwe.mitre.org"
〔4〕 CVE, "http://cve.mitre.org"
〔5〕 CAPEC, "http://capec.mitre.org"
〔6〕 Thomas R. Rhodes, Frederick E. Boland Jr, Elizabeth N. Fong, and Michael J. Kass, "Software assurance using structured assurance case models," 7608, NIST Interagency/Internal Report (NISTIR), May 2009.
〔7〕 Ki-Seok Bang, Il-Gon Kim, Ji-Yeon Lee, Jun-Seok Lee, and Jin-Young Choi "Classification criteria and application methodology for evaluating IT security products," Jonornal of Korea Knowledge Information Technology Society, 6(5), pp. 105-112, Nov. 2011.

〈저자소개〉

임 재 우 (Jae-Woo Im) 정회원
2010년 2월~2013년 8월: ㈜안랩 책임
2013년 9월~현재: ㈜현대오토에버 과장
〈관심분야〉 정보보호제품 보안성 평가, 취약성 분석, 자동차 보안