http://dx.doi.org/10.14400/JDC.2015.13.5.251

CC와 ISO 표준에 따른 침입방지시스템의 융합 성능평가 모델

이하용*, 양효식**
서울벤처대학원대학교 융합산업학과*, 이글루시큐리티(주)**

Convergence Performance Evaluation Model for Intrusion Protection System based on CC and ISO Standard

Ha-Yong Lee*, Hyo-Sik Yang**
Dept. of Fusion Industry, Seoul Venture University*
Iglu Security Co., Ltd.**

요 약 침입방지시스템은 네트워크에서 공격 서명을 찾아내어 자동으로 조치를 취하여 비정상적인 트래픽을 중단시키는 보안시스템이다. 수동적인 방어를 하는 침입차단시스템이나 침입탐지시스템과 달리 침입경고 이전에 침입을 중단시키는 개념의 솔루션이다. 침입방지시스템의 보안성 성능은 보안감사, 사용자 데이터 보호, 보안 인증 등에 좌우되며 성능은 탐지시간, 처리량, 공격차단 성능 등에 좌우된다. 본 연구에서는 이러한 침입방지시스템의 보안성 성능평가를 위한 모델을 구축하기 위해 CC(Common Criteria : ISO/IEC 15408)와 소프트웨어 제품평가에 관한 ISO 국제표준을 근간으로 하여 융합 성능평가 모델을 구성하였다.

주제어 : 융합, 보안성, 성능, 침입방지시스템, 품질평가 모델

Abstract Intrusion protection system is a security system that stop abnormal traffics through automatic activity by finding out attack signatures in network. Unlike firewall or intrusion detection system that defends passively, it is a solution that stop the intrusion before intrusion warning. The security performance of intrusion protection system is influenced by security auditability, user data protection, security athentication, etc., and performance is influenced by detection time, throughput, attack prevention performance, etc. In this paper, we constructed a convergence performance evaluation model about software product evaluation to construct the model for security performance evaluation of intrusion protection system based on CC(Common Criteria : ISO/IEC 15408) and ISO international standard about software product evaluation.

Key Words : Convergence, Security, Performance, Intrusion protection system, Quality evaluation model

1. 서론

기업의 보안에 있어서 3대 요소라 할 수 있는 인증(Authentication), 권한부여(Authorization), 계정관리

Received 14 March 2015, Revised 22 April 2015
Accepted 20 May 2015
Corresponding Author: Hyo-Sik Yang(Iglu Security Co., Ltd.)
Email: tonnie_yang@naver.com

ISSN: 1738-1916

(Accounting)를 네트워크에 적용한 침입방지시스템(Intrusion Prevention System)은 필수적인 보안 솔루션 중의 하나이다[1]. 침입방지시스템은 공격 서명(attack signature), 프로토콜 비정상 행위 탐지 같은 방식을 통해 악의적인 세션을 차단하고 자동으로 조치를 취함으로써 비정상적인 트래픽을 중단시키는 보안솔루션이다[2, 3].

수동적인 방어 개념의 침입 차단 시스템이나 침입 탐지 시스템(Intrusion Detection System)과 달리 침입 경고 이전에 공격을 중단시키는 데 초점을 둔, 침입 유도 기능과 자동 대처 기능이 합쳐진 개념의 솔루션이다. 또한 해당 서버의 비정상적인 행동에 따른 정보 유출을 자동으로 탐지하여 차단 조치를 취함으로써 인가자의 비정상 행위를 통제할 수 있다.

침입방지시스템의 보안성능은 보안감사, 사용자 데이터 보호, 보안 인증 등에 대한 수준을 검토하고 성능은 탐지시간, 처리량, 공격차단 성능 등을 검토함으로써 평가할 수 있다.

침입방지시스템은 정보보호시스템의 일종으로 정보보호시스템 사용 환경에서 보안 문제를 해결하기 위한 보안 요구 사항을 국제 공통 평가기준(Common Criteria)[4, 5, 6] 내에서 선택하여 작성한 제품/시스템군별 보안기능/보안요구사항. 정보보호 제품의 평가를 위해 인정된 보호 프로파일(Protection Profile)에 따라 제품을 개발하고 평가를 받거나, 혹은 개발된 제품의 제원을 보호 프로파일로 등록하고 평가를 받게 된다. 이러한 공통 평가 기준의 V3.1r2를 근간으로 침입방지시스템에 관한 보호프로파일(protection profile)이 있다[7].

본 논문에서는 침입방지시스템 보호프로파일과 소프트웨어 제품평가 관련 국제표준인 ISO/IEC 9126[8]과 ISO/IEC 12119[9], 품질평가 프로세스에 관한 국제표준인 ISO/IEC 14598[10]을 근간으로 한 침입방지시스템의 보안성 성능 특성 체계의 구축을 중심으로 하여 침입방지시스템의 보안 성능을 포함한 효율성 품질 수준을 평가할 수 있는 모델을 구축하고자 한다.

본 논문의 2장에서는 침입방지시스템의 관련 동향에 대해 살펴보고 3장에서는 침입방지시스템의 보안성과 성능 특성에 관한 평가 모델을 구축하며 4장에서 결론과 향후 연구 과제를 제시하였다.

2. 침입방지시스템의 주요 기술과 요구사항

침입방지시스템의 주요 기술 및 침입방지시스템을 도입하고자할 때 고려사항에 따른 요구사항을 정리하면 다음과 같다.

2.1 침입방지시스템의 주요 기술

2.1.1 호스트 기반 침입방지시스템

호스트 기반 IPS의 기술적인 특징은 크게 커널과 함께 동작해 커널 이벤트를 가로채 처리하는 방식과 커널과 독립적으로 작동하는 방식으로 구분되며, 전자는 대부분 접근제어 기능을 가진 트러스트 운영체제(Trust Operating System) 제품들로 분류할 수 있고 후자는 시그니처와 행동 기반 분석 알고리듬을 이용 특정 규칙에 위배되는 이벤트를 필터링하는 제품들로 분류할 수 있다. 시장조사 전문업체인 가트너에 따른 호스트 IPS의 정의는 우선 소프트웨어 제품이어야 하며, 방화벽 룰셋(rule set)과 같은 정책이나 정상/비정상 접근에 대한 학습을 통해 취약한 응용 프로그램을 보호할 수 있어야 한다.

호스트 기반 침입방지시스템의 예로(주)이카디아의 엔터셉트가 있다. 이 제품은 바이러스나 해킹 등 서버를 대상으로 한 외부의 침입을 감지해 차단하고 원격에서 여러 명의 보안관리자가 동시에 수 천대의 서버를 관리할 수 있으며 외부침입 여부를 판단하는 기본 정의 외에 새로운 침입에 대응하는 사용자 정의를 추가할 수 있다.

2.1.2 네트워크 기반 침입방지시스템

네트워크 기반 IPS의 기술적인 특징은 실시간 패킷처리, 오탐지를 최소화하는 기술, 변형 공격과 오용공격의 탐지기술, 그리고 각 상황에 맞는 실시간 반응 기술이라고 말할 수 있다. 역시 가트너의 정의에 따르면 침입방지 능력과 빠른 반응 속도를 위해 네트워크 라인상에 위치한 제품이어야 하며, 세션 기반 탐지(session aware inspection)를 지원할 수 있는 시스템을 말한다. 또한 다양한 종류의 방지 방법 및 방식(시그니처, 프로토콜적인 비정상 행위 탐지)을 통해 악의적인 세션을 차단하는 것도 필수적이다.

네트워크 기반 침입방지시스템의 예로 (주)인프니스 네트웍스의 SOLIGATE RxIPS가 있다. 이 제품은 고객의 네트워크 안정성을 보장하기 위해 정규표현식 전수조

사 기반의 침입방지시스템으로 침입 탐지 및 방어, 침입 차단 기능, 트래픽을 보장 또는 제한하는 품질 보장 서비스(QoS : Quality of Service), 유해 콘텐츠 차단, 다양한 보안 정책 설정을 위한 관리기능 등을 수행한다.

2.2 침입방지시스템의 요구사항

침입방지시스템의 요구사항은 보안기능 요구사항과 보증 요구사항으로 분류하여 정의할 수 있다.

2.2.1 보안기능 요구사항

보안기능 요구사항과 관련된 보안기능 클래스에는 보안감사, 사용자 데이터 보호, 식별 및 인증, 보안관리, TSF 보호, 자원활용, TOE 접근 등이 있다. 각 보안기능 클래스는 다시 보안기능 컴포넌트로 세분화된다. 예를 들어, 보안기능 컴포넌트로서 보안감사에는 보안경보, 감사데이터 생성, 감사 검토 등이 있고 사용자 데이터 보호에는 정보호름 통제, 단일계층 보안속성 등이 있으며 식별 및 인증에는 인증실패 처리, 사용자 속성 정의, 인증 등이 있다.

2.2.2 보증 요구사항

보증 요구사항과 관련된 보증 클래스에는 보안목표명세서, 개발, 설명서, 생명주기 지원, 시험, 취약성 평가가 있다. 각 보증 클래스는 다시 보증 컴포넌트로 세분화된다. 예를 들어, 보안목표 명세서에는 준수선언, 보안문제 정의, 보안목적 등이 있고 개발에는 보안구조 설명, 구조적인 설계 등이 있으며 설명서에는 사용자 운영설명서, 준비절차 등이 있다.

3. 침입방지시스템 관련 품질특성

이 절에서는 침입방지시스템의 요구사항을 바탕으로 침입방지시스템의 보안성과 성능평가에 관한 특성을 분류하고 분석하고자 한다.

3.1 침입방지시스템의 보안성능 품질특성

보안성이란 소프트웨어가 허가되지 않은 사람이나 시스템의 액세스를 방지하여 정보 및 데이터를 보호하는 능력을 의미하며 보안성능에 관련된 침입방지시스템의 특성으로는 다음과 같은 항목들이 있다.

3.1.1 보안감사

보안감사란 보안과 관련된 행동의 책임추적이 가능하도록 보안관리 사건을 기록 및 유지하고 기록된 데이터를 검토할 수 있는 수단을 제공해야 함을 의미한다.

① 잔재적인 보안위반을 탐지한 경우, 보안목표명세서 작성자에 의해 결정된 혼란을 최소화하는 대응행동의 목록을 취해야 한다.
② 감사대상 사건들의 감사 레코드를 생성할 수 있어야 한다.(사건 일시, 사건 유형, 주체의 신원, 사건 결과)
③ 식별된 사용자의 행동으로 인해 발생한 감사 사건에 대해 사건을 발생시킨 사용자의 신원과 감사대상 사건을 연관시킬 수 있어야 한다.
④ 인가된 관리자에게 감사 레코드로부터 모든 감사 데이터를 읽을 수 있는 기능을 제공해야 한다.
⑤ 모든 감사대상 사건 집합으로부터 감사되어야 할 사건의 집합을 선택할 수 있어야 한다.

3.1.2 사용자 데이터 보호

사용자 데이터 보호란 정보흐름을 거부하더라도 정보흐름의 인가규칙에 기반하여 정보흐름을 명시적으로 인가해야 함을 의미한다.

① 통제된 주체로부터의 정보흐름을 유발하는 오퍼레이션 목록에 대해 거부정책을 강제해야 한다.
② 필요한 사항에 대해 통제된 주체로부터의 정보흐름을 유발하는 오퍼레이션 목록에 대해 허용정책을 적용해야 한다.

3.1.3 식별 및 인증

식별 및 인증이란 해당 정보보호 제품의 관리자를 포함한 사용자의 신원을 식별 및 인증하고 인증 실패시 대응 행동을 제공하는 능력을 의미한다.

① 허용한 횟수의 실패한 인증시도가 발생한 경우 이를 탐지하고 대응행동을 수행해야 한다.
② IP 주소, 사용자 보안속성 등의 목록을 유지해야 한다.

③ 인가된 관리자에 속한 식별자나 사용자 보안속성 목록을 유지해야 한다.
④ 사용자에게 행동을 허용하기 전에 사용자를 성공적으로 인증해야 한다.
⑤ 사용자에게 행동을 허용하기 전에 각 사용자를 성공적으로 식별해야 한다.

3.1.4 보안관리

보안관리란 해당 지식정보보안 제품의 보안기능, 보안속성, 보안 관련 데이터, 보안 역할 등과 관련된 사항을 관리하는 능력을 의미한다.

① 기능목록의 기능에 대해 행동을 결정/중지/개시/변경하는 능력을 인가된 관리자로 제한해야 한다.
② 보안속성의 디폴트값을 필히 제공해야 한다.
③ 취약성 목록의 갱신은 인가된 관리자만 가능해야 한다.
④ 데이터 목록의 디폴트값 변경/질의/변경/삭제/소거는 인가된 관리자만 가능해야 한다.
⑤ 데이터 목록의 한계치를 인가된 관리자만 명세할 수 있어야 한다.

3.1.5 TSF(TOE Security Function) 보호

TSF 보호란 주기적 또는 관리자의 요구에 따라 무결성을 검증하는 능력을 의미한다.

① TSF 장애가 잘뱅한 경우 안전한 상태를 유지해야 한다.
② TSF의 정확한 운영을 입증하기 위해 필요시(주기적, 요구, 조건) 자체 시험을 실행해야 한다.
③ 인가된 관리자에게 TSF의 무결성(데이터와 코드)을 검증하는 기능을 제공해야 한다.

3.1.6 TOE 접근

TOE 접근이란 관리자가 활동하지 않을 때 관리자의 세션을 잠궈 보안 기능을 보호하는 것을 의미한다.

① 설정된 관리자 비활동 기간 후 관리자 세션을 잠궈야 한다.
② TSF는 TOE를 통과하여 상호작용하는 IT 개체 간의 상호연결이 일정 기간 동안 활동을 중지할 경우 세션을 종료해야 한다.

3.2 침입방지시스템의 성능 품질특성

3.2.1 시간반응성

시간반응성이란 명시된 조건에서 그 기능을 수행할 때 적절한 반응 및 처리 시간과 처리율을 제공하는 소프트웨어의 능력을 의미한다.

① 침입방지시스템이 침입 발생 후 이를 탐지하기까지 소요된 평균 시간이 적절해야 한다.
② 침입방지시스템이 주어진 시간 내에 성공적으로 침입을 탐지하여 조치한 처리량의 규정된 수준에 이르러야 한다.

3.2.2 자원효율성

자원 효율성이란 명시된 조건에서 소프트웨어가 그 기능을 수행할 때 적절한 양과 종류의 자원을 사용하는 소프트웨어의 능력을 의미한다.

① 침입방지시스템의 I/O자원의 사용 정도가 적정 수준이어야 한다.
② 침입방지시스템의 메모리 사용 정도가 적정 수준이어야 한다.
③ 침입방지시스템의 데이터 전송 속도가 적정 수준이어야 한다.
④ 침입방지시스템의 CPU 사용 정도가 적정 수준이어야 한다.

3.2.3 성능

침입방지시스템에서 성능이란 침입방지 기능 측면에서의 성능을 의미한다.

① 최대패킷처리량(throughput)을 측정하여 장비가 패킷 손실 없이 처리할 수 있는 최대 트래픽이 명세된 수준을 준수하여야 한다.
② 처리할 수 있는 최대세션 수가 명세된 수준을 준수하여야 한다.
③ 최대 세션 처리량이 명세된 수준을 준수하여야 한다.
④ 제품이 처리할 수 있는 처리 용량의 규정된 % 수준에서 전송지연이 명세된 수준을 준수하여야 한다.
⑤ 공격에 대한 차단성능에 관한 최대 처리량의 명세된 수준을 준수하여야 한다.

4. 침입방지시스템의 품질평가 모델

본 연구에서는 침입방지시스템의 보안성능 평가모델에 대해, 기반이 되는 품질특성 체계[8, 9, 10]를 바탕으로, 평가를 위한 메트릭(metrics, measure), 메트릭의 활용을 위한 품질검사표와 점검표 그리고 이를 종합한 시험모듈을 구성하였다. 침입방지시스템의 보안성능에 대한 품질특성은 소프트웨어 제품평가에 관한 국제표준인 ISO/IEC 9126과 ISO/IEC 12119의 효율성 품질특성에 근간을 두고 침입방지시스템 고유의 특성을 반영하여 구성하였다.

시험모듈은 품질평가를 위한 평가 메트릭에 대해 소프트웨어 품질평가 프로세스를 위한 국제표준인 ISO/IEC 14598 - 부분 6[11]의 형식에 의거하여 평가를 위한 제반 사항을 문서로서 정의하는 체계이다. 시험을 위한 모듈에 대해 기본적인 사항을 정리하면 다음과 같다.

4.1 시험모듈의 체계와 개발 내역

4.1.1 시험모듈의 체계

시험모듈은 소프트웨어의 품질시험에 관한 제반사항, 즉 시험 기법, 메트릭, 측정 항목 및 개념, 메트릭의 적용 절차, 측정결과의 평점(rating)과 해석 등을 포함하고 있으며 품질평가 프로세스에 관한 국제표준인 ISO/IEC 14598의 <부분 6>에 정의된 평가모듈 구성형식에 따라 만들어졌다. 품질 시험모듈은 <Table 1>과 같은 체계로 구축되었다.

〈Table 1〉 System of Quality Testing Module

Configuration Item	Contents
Outline	**Concept of metric** : The basic concept of evaluation modules
	Measurement purposes : what you want to get through the measurement of the evaluation module
	Metric category : where the metric belongs
	Term Explanation : explanation of related terms
Coverage	**application target** : target such as document or software
	Necessary resources : Tools/resources required to apply the metric
	Techniques : Testing techniques that can be applied
	Considerations : Relevant information to be considered when apply evaluation modules
Reference	Related Documents that metrics are derived
Metric	**Measurement items** : Data items to be measured
	Measurement method : specific measure for the measure item to configure the metric
	Expression : definition of expression using the data items
Application Procedures	Description on specific procedures and method to perform the test
Results interpretation and reporting	**Mapping of the measurements** : The range of metric results
	Interpretation of the measurement results : Provide guidance about how to interpret the measurement results
	Reporting requirements : items to be reported as a document on the measurement results

4.1.2 메트릭 개발 내역

본 연구를 통해 침입방지시스템에 대해 ISO 25000 시리즈[12, 13, 14, 15]의 품질특성 중 효율성 품질특성에 따라 보안성능을 포함한 효율성의 평가 척도(metrics, measure)를 개발하였다. <Table 2>에 보안성능을 포함한 침입방지시스템의 효율성에 관한 메트릭과 개념의 예를 나타내었다.

〈Table 2〉 The example of metrics of security performance

Characteristics	Sub-characteriticcs	Item	Related Items
Efficiency	Time behavior	Mean Time to Detect	How long does it take for intrusion detection system to detect a intrusion on average?
		Mean Throughput	How many times for intrusion detection system to detect a intrusion on average within the time allowed successfully?
		Suitability of Mean Processing Time	How long does it take for intrusion detection system to give information so as to take actions after detection of intrusion?
		…	…
	Resource Utilization	Use rate of I/O resource	Degree of use of I/O resource in IPS(Intrusion Protection System)
		Use rate of memory	Degree of use of memory in IPS
		…	…
	Security Performance	Throughput	Maximum throughput of packet
		Concurrent Session	Processable maximum number of session
		performance of attack protection	Maximum throughput for attack
		…	…

4.2 품질검사표

품질검사표는 시험모듈에 정의된 메트릭을 기준으로 실제 품질 시험을 수행하는 과정에서 편리하게 활용할 수 있도록 필요한 핵심적인 사항들을 추출하여 정리한 표로서 메트릭명과 개념, 측정항목, 메트릭의 계산식, 결과의 영역, 결과값, 문제점 기술 부분 등으로 구성되어 있다. 이러한 품질검사표의 예를 <Table 4>에 나타내었다.

〈Table 4〉 An example of quality inspection table

Measure name		
Attack Prevention Performance		How much is the maximum throughput for attack?
Measurement items	A	The attack throughput specified in intrusion protection system
	B	Real attack maximum throughput in intrusion protection system
expression		- Attack Prevention System = B/A
The range of results		0 ≤ Attack Prevention System ≤ 1 result value
problem		

품질검사표에는 기본적으로 메트릭명과 메트릭이 측정하고자 하는 내용에 대한 문장이 포함되어 있다. 측정항목은 계산식을 통해 메트릭을 구성하는 요소로 1개 이상의 요소로 구성되며 항목 개요와 측정 방법에 대한 기술을 포함한다. 결과 영역은 계산식에 의해 산출되는 값이 나타날 수 있는 영역으로 메트릭들은 전체적으로 0과 1사이의 값으로 사상될 수 있도록 정의하였다.

4.3 점검표

점검표는 품질검사표를 이용하여 측정항목에 대한 측정을 수행하기 위해 작성된 테스트 케이스의 시험 목록으로 구성하였다. <Table 5>는 침입방지시스템의 '공격차단성능'에 관한 점검표로 처리할 수 있다고 명세된 최대 공격 처리량을 준수하는지를 확인하기 위한 점검표의 예를 기술하였다.

〈Table 5〉 Checklist of Throughput

No	Test Case	Maximum Traffic
1	Attach Throughput Test(1st)	Y
2	Attach Throughput Test(2ndt)	Y
3	Attach Throughput Test(3rd)	Y
4	Attach Throughput Test(4th)	Y
5	Attach Throughput Test(5th)	Y
…	…	…
Real attack maximum throughput in intrusion protection system		B
The attack throughput specified in intrusion protection system		A
Attack Prevention Performance = B/A		
Result		

5. 결론

정보화가 진전되고 정보통신망이 발전함에 따라 취약성을 분석하거나 침입차단시스템 등을 구축하기도 하며 네트워크의 보안이 중요한 문제로 대두되면서 보안시스템 중 침입탐지시스템에 대한 관심이 높다.

불법침입과 공격에 대한 노출에 대비해 네트워크 관리자는 시스템 및 응용프로그램에 대한 취약성 정보를 수집하고 대응할 수 있도록 해야 한다. 네트워크 관리자의 역할이 막중한 상황에서 관리자 부재시 시스템 자체적으로 불법침입 등에 대응할 수 있는 보안 솔루션으로서 부각되고 있는 것이 침입탐지시스템이다.

침입방지시스템이 보안 솔루션으로서의 제 역할을 다하고 있는가를 평가하기 위한 방법으로 본 논문에서는 침입방지시스템 보호프로파일과 소프트웨어 제품평가 관련 국제표준인 ISO/IEC 25000 시리즈의 품질특성 체계를 근간으로 한 침입방지시스템의 보안성을 고려한 성능평가 모델의 특성 체계 구축을 중심으로 하여 침입방지시스템의 품질 수준을 평가할 수 있는 모델을 구축하였다.

본 연구를 수행한 성과를 바탕으로 일반적인 소프트웨어 제품평가에 관한 국제표준의 적용만으로는 침입방지시스템 같은 정보보안 관련 시스템의 고유한 보안성 특성에 대한 충분한 반영이 어려울 수 있다는 점을 해소할 수 있을 것이란 점을 의의로 들 수 있다.

향후, 침입방지시스템에 대한 품질평가 모델을 실질적으로 적용하여 평가사례를 구축하고 지속적인 분석을 통해 객관성 있는 평가 체계를 구축할 필요가 있다.

REFERENCES

[1] Moon-Goo Lee, Secured Verification of Intrusion Prevension System Security Model Based on CPNs, Journal of the Institute of Electronics Engineers of Korea, Vol 48, No. 3, p. 76, 2011. 5.

[2] Carl Endorf, Jim Mellander and Eugene Schultz, Intrusion Detection and Prevention, Osborne Computer Book, 2004. 1.

[3] Joshua Heling, Balancing Detection and Prevention in the Deployment of network Intrusion Technology,

SecurePipe white paper, 2005.
[4] ISO/IEC 15408-1:2009, Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model.
[5] ISO/IEC 15408-2:2008, Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components.
[6] ISO/IEC 15408-3:2008, Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components.
[7] Hang-Soo Lee, Young-Soo Kim et al., Network Intrusion Prevention System Protection Profile V2.0, Korea Information Security Agency & Hannam University, 2008. 4.
[8] ISO/IEC 9126, Information Technology - Software Quality Characteristics and metrics
[9] ISO/IEC 12119, Information Technology - Software Package -- Quality requirement and testing".
[10] ISO/IEC 14598, Information Technology -- Software product evaluation -- Part 1~6.
[11] ISI/IEC 14598-6, Software engineering -- Product evaluation -- Part 6: documentation of evaluation modules, 2001.
[12] ISO/IEC 25000, Systems and software engineering -- systems and software Quality Requirements and Evaluation(SQuaRE) -- Guide to SQuaRE, 2014.
[13] ISO/IEC 25010, Systems and software engineering - Systems and software Quality Requirements and Evaluation(SQuaRE) - System and Software quality models, 2011.
[14] ISO/IEC 25020, Software engineering - Softawre product Quality Requirements and Evaluation(SQuaRE) - Measurement reference model and guide, 2007.
[15] ISO/IEC 25051, Software engineering - Systems and software Quality Requirements and Evaluation(SQuaRE) - Requirements for quality of Ready to Use Software Product(RUSP) and instructions for testing, 2014.

이 하 용(Lee, Ha Yong)

- 1993년 2월 : 강원대학교 전자계산학과 졸업(이학사)
- 1995년 2월 : 강원대학교 대학원 전자계산학과 SW공학전공(이학석사)
- 2005년 2월 : 호서대학교 벤처전문대학원 컴퓨터응용기술학과졸업(공학박사)
- 1996년 3월 ~ 2005년 8월 : 경희대, 경원대, 선문대, 호서대 컴퓨터공학부강사
- 1995년 6월 ~ 2002년 12월: 한국SW품질연구소 선임연구원
- 2005년 9월 ~ 현재 : 서울벤처대학원대학교 교수
- 관심분야 : 소프트웨어공학(특히, S/W 품질보증과 품질평가, 품질감리, 객체지향 프로그래밍, 객체지향 분석과 설계, 컴포넌트기반 S/W 개발방법론, 품질평가)
- E-Mail : lhyazby@svu.ac.kr

양 효 식(Yang, Hyo Sik)

- 2008년 2월 : 호서대학교 컴퓨터공학과 졸업(학사)
- 2012년 2월 : 호서대학교 벤처전문대학원 정보경영학과 졸업(석사)
- 2015년 2월 : 호서대학교 벤처대학원 융합공학과 졸업(공학박사)
- 2009년 1월 ~ 2014년 10월 : 한국IT진흥(주), KT네트웍스(주), UL Korea(주) 근무
- 2014년 11월 ~ 현재 : 이글루시큐리티(주) 전임컨설턴트
- 관심분야 : 소프트웨어 프로세스 인증 및 시험, 물리보안 시스템, 소프트웨어 및 네트워크 보안, 정보서버 보안관리
- E-Mail : tonnie_yang@naver.com