http://dx.doi.org/10.14400/JDC.2014.12.6.289

보안성과 성능에 따른 침입탐지시스템의 품질평가 모델

이하용*, 양해술**
서울벤처대학원대학교 융합산업학과*, 호서대학교 벤처전문대학원 정보경영학과**

Quality Evaluation Model for Intrusion Detection System based on Security and Performance

Ha-Young Lee*, Hae-Sool Yang**
Dept. of Fusion Industry, Seoul Venture University*
Dept. of Information Management, Graduate School of Venture, Hoseo University**

요 약 침입탐지시스템은 컴퓨터 시스템 내 · 외부의 비정상적인 사용을 실시간으로 탐지하는 시스템으로 기업의 보안을 강화하고 불법적 의도를 사전에 감지하는 적극적인 보안 방안이다. 침입탐지시스템의 성능은 침입탐지시스템의 영역에 해당하는 정보수집, 침입분석, 침입대응, 침입탐지 결과 검토 및 보호, 대응행동, 손실방지 등에 관해 제 역할을 수행하고 있는가를 판단해야 한다. 본 연구에서는 이러한 침입탐지시스템의 요구사항과 소프트웨어 제품평가에 관한 ISO 국제표준을 근간으로 평가모델을 구성하였다.

주제어 : 보안성, 성능, 침입탐지시스템, 품질평가 모델

Abstract Intrusion detection system is a means of security that detects abnormal use and illegal intension in advance in real time and reenforce the security of enterprises. Performance of intrusion detection system is judged by information collection, intrusion analysis, intrusion response, review and protection of intrusion detection result, reaction, loss protection that belong to the area of intrusion detection. In this paper, we developed a evaluation model based on the requirements of intrusion detection system and ISO international standard about software product evaluation.

Key Words : Securiry, Performance, Intrusion detection system, Quality evaluation model

1. 서론

오늘날 IT(Information Technology) 분야가 급속히 발전하고 인터넷 보급 확대 및 사회 각 분야에서 통신망의 활용이 일반화됨에 따라 이를 위협하는 애드웨어, 스파이웨어, 웜과 같은 다양한 보안위협들이 증가하여 정보화에 따르는 다양한 역기능 현상을 유발함으로써 컴퓨팅 환경에 위협을 주고 있다[1].

침입탐지시스템은 컴퓨터 시스템 내 · 외부의 비정상적인 사용을 실시간으로 탐지하는 시스템으로 기업의 보안을 강화하고 불법적 의도를 사전에 감지하는 적극적인 보안 방안이다.

최근에 네트워크를 통한 시스템 침입이 증가하고 있으며 이러한 위협에 대처하기 위한 침입탐지시스템은 네

Received 15 March 2014, Revised 16 April 2014
Accepted 20 June 2014
Corresponding Author: Ha-Yong-Lee(Seoul Venture University)
Email: lhyazby@suv.ac.kr

ISSN: 1738-1916

트워크 트래픽을 검사하여 침입 시도를 미리 알려진 규칙에 근거하여 탐지한다[2].

침입탐지시스템의 성능은 침입탐지시스템의 영역에 해당하는 정보수집, 침입분석, 침입대응, 침입탐지 결과 검토 및 보호, 대응행동, 손실방지 등에 관해 제 역할을 수행하고 있는가를 검토함으로써 평가할 수 있다.

침입탐지시스템은 정보보호시스템의 일종으로 정보보호시스템 사용 환경에서 보안 문제를 해결하기 위한 보안 요구 사항을 국제 공통 평가기준(Common Criteria)[3][4][5] 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 침입탐지시스템에 관한 보호프로파일이 작성된 바 있다[6].

본 논문에서는 침입탐지시스템 보호프로파일과 소프트웨어 제품평가 관련 국제표준인 ISO/IEC 9126과 ISO/IEC 12119의 품질특성 체계를 근간으로 한 침입탐지시스템의 보안성과 효율성 특성 체계의 구축을 중심으로 하여 침입탐지시스템의 품질 수준을 평가할 수 있는 모델을 구축하고자 한다.

본 논문의 2장에서는 침입탐지시스템의 관련 동향에 대해 살펴보고 3장에서는 침입탐지시스템의 보안성과 효율성에 관한 평가 모델을 구축하며 4장에서 결론과 향후 연구과제를 제시하였다.

2. 침입탐지시스템의 주요 기술과 요구사항

침입탐지시스템의 주요 기술 및 도입 시 고려사항에 따른 요구사항을 정리하면 다음과 같다[7].

2.1 침입탐지시스템의 주요 기술

2.1.1 통합보안 기능 지원

오늘날 침입탐지시스템은 다양한 시스템, 네트워크 장비 및 보안시스템과 연동을 통한 통합보안관리 기능을 지원해야 하며, 보안 감사 데이터 통합 관리 뿐 아니라, 그룹별 보안정책 적용 및 관리 편의성을 제공하여야 한다.

2.1.2 세션 기반 네트워크 트래픽 분석기능 제공

과거의 일부 네트워크 침입탐지시스템(NIDS)의 경우 세션 기반이 아닌 네트워크 패킷 기반 분석 기능만을 제공하였는데, 이 방식의 경우 패킷 단위 검사만을 수행하므로 정교한 네트워크 공격에는 취약한 특성이 있다. 따라서 NIDS 보안 분석의 정확도 및 낮은 오탐(False Positive)율을 위해서는 패킷 기반 뿐 아니라 반드시 세션 기반 분석 기능을 제공하여야 한다.

2.1.3 자체 보안성 제공 및 로그 재현기능

NIDS 또한 다른 보안솔루션과 마찬가지로 자체적으로 일정 수준 이상의 보안 견고성을 보유 하여야 하며 일반적으로 은닉(Stealth) 기능과 같은 하여 외부에서 NIDS의 IP Address를 인식할 수 없게 만드는 기능이 많이 사용된다. 또한 몇몇 제품에서는 보안사고가 발생한 뒤 사후 Forensic 및 정확한 보안 분석을 위해 세션 재현 기능들도 제공되고 있다.

2.1.4 기타

네트워크 상에서 패킷이 전송될 때 사이즈가 큰 패킷의 경우 IP 레이어 단에서 작은 조각(Fragment)으로 나눠 전송되고 수신측에서는 이를 다시 재조합해서 사용하는데, 인위적으로 조각화(Fragmentation) 현상을 발생시켜 침입차단시스템이나 침입탐지시스템과 같은 보안장비를 우회하기 위한 방법은 예전부터 많이 사용된 공격기법이다. 따라서 오늘날 NIDS는 탐지정확성 및 오탐율 최소화를 위해 IP Fragmentation Reassembly나 TCP Segment Reassemble 등과 같은 기능지원을 통해 정교한 어플리케이션 프로토콜 분석기능을 제공해야 한다.

2.2 침입탐지시스템의 요구사항

침입탐지시스템의 요구사항은 보안기능 요구사항과 보증 요구사항으로 구분된다[6].

2.2.1 보안기능 요구사항

보안기능 요구사항과 관련된 보안기능 클래스에는 보안감사, 식별 및 인증, 보안관리, TSF 보호, TOE 접근,

침입탐지가 있다. 각 보안기능 클래스는 다시 보안기능 컴포넌트로 세분화된다.

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.

3. 침입탐지시스템 관련 품질특성

이 절에서는 침입탐지시스템의 요구사항을 바탕으로 침입탐지시스템의 보안성과 효율성에 관한 특성을 분류하고 분석하고자 한다.

3.1 침입탐지시스템의 보안성 품질특성

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

3.1.1 보안감사성

보안감사성이란 보안과 관련된 행동에 대한 책임을 추적하기 위해 지식정보보안 제품에서 발생하는 관련 사건들의 감사 레코드를 생성, 기록, 검토하고 감사된 사건에 대한 잠재적 보안 위반을 탐지하고 대응행동을 수행하는 능력을 의미한다.

① 보안위반 탐지시 대응행동의 목록을 취하고 규정된 감사데이터를 생성해야 한다.
② 사건을 검사시, 규칙집합을 적용하고 규칙에 기반하여 잠재적 위반을 지적할 수 있어야 한다.
③ 인가된 관리자가 감사 레코드로부터 모든 감사데이터를 읽을 수 있어야 한다.
④ 인가되지 않은 삭제로부터 감사 레코드를 보호해야 한다.
⑤ 감사 데이터가 한도를 초과할 경우, 관리자에게 통보하고 대응행동을 취해야 한다.
⑥ 감사 증적이 포화인 경우, 감사 저장 실패시 취해야 할 행동을 수행해야 한다.

3.1.2 식별 및 인증

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

① 인증 실패를 탐지하고 대응행동을 수행해야 한다.
② 각 사용자에 대해 규정된 보안속성 목록을 유지해야 한다.
③ 사용자에게 행동을 허용하기 전에 사용자를 성공적으로 인증해야 한다.
④ 사용자에게 행동을 허용하기 전에 사용자를 성공적으로 인증해야 한다.
⑤ 인증 데이터의 재사용을 방지해야 한다.
⑥ 사용자에게 행동을 허용하기 전에 각 사용자를 성공적으로 식별해야 한다.

3.1.3 보안관리성

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

① 인가된 관리자만 보안기능을 관리할 수 있도록 제한해야 한다.
② 보안속성의 디폴트값을 제공하도록 강제해야 한다.
③ 식별 및 인증 데이터의 관리를 인가된 관리자로 제한해야 한다.
④ 감사 저장소 용량, 실패한 인증 시도 횟수, 자체 시험이 발생하는 시간 간격 에 대한 한계치의 관리는 인가된 관리자로 제한해야 한다.
⑤ 규정된 관리 기능을 수행해야 한다.
⑥ 인가된 관리자 역할을 유지해야 한다.

3.1.4 보안기능 보호

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

① 전송 중인 모든 보안 관련 데이터의 변경 및 위조를 탐지하는 능력을 제공해야 한다.

② 데이터 및 실행코드의 무결성을 검증하기 위해 자체 시험을 실행할 수 있어야 한다.

3.1.5 접근통제성

접근통제성이란 시스템이 정보흐름을 중재하기 위해 관련 보안 정책에 기반하여 패킷필터링 등을 통하여 외부망으로부터 내부망을 보호하는 능력을 의미한다.

① 사용자 비활동 기간 후 상호작용하는 세션을 잠가 활동을 무력화시켜야 한다.

3.1.6 침입탐지

침입탐지란 시스템이 보안을 위협하는 침입 행위가 발생할 경우 이를 탐지하는 능력을 의미한다.

① 보호대상시스템으로부터 침입탐지를 위해 필요한 정보를 수집해야 한다.
② 수집 데이터에 기반하여 정해진 분석 기능을 수행해야 한다.
③ 보안위반 가능성 및 사실을 탐지하였을 경우 수행해야 할 활동을 수행해야 한다.
④ 인가되지 않은 삭제로부터 저장된 침입탐지 결과를 보호해야 한다.
⑤ 침입탐지 결과에 대한 손실이 예측될 때 필요한 대응행동을 수행해야 한다.
⑥ 침입탐지 결과 기록을 위한 저장소가 포화되거나 기타 문제 발생시 취해야 할 행동을 수행해야 한다.

3.2 침입탐지시스템의 효율성 품질특성

3.2.1 시간반응성

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

① 침입탐지시스템이 침입 발생 후 이를 탐지하기까지 소요된 평균 시간이 적절해야 한다.
② 침입탐지시스템이 주어진 시간 내에 성공적으로 침입을 탐지한 평균 회수가 적절해야 한다.
③ 침입탐지시스템이 침입 사실을 탐지하여 조치할 수 있도록 정보를 제공할 때까지의 평균 시간이 적절해야 한다.

3.2.2 자원효율성

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

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

3.2.3 성능

침입탐지시스템에서 성능이란 침입탐지 기능 측면에서의 성능을 의미한다.

① 최대패킷처리량(throughput)을 측정하여 장비가 패킷 손실 없이 처리할 수 있는 최대 트래픽이 명세된 수준을 준수하여야 한다.
② 제품이 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.

4. 침입탐지시스템의 품질평가 모델

본 연구에서는 침입탐지시스템의 보안성과 효율성 평가모델에 대해, 기반이 되는 품질특성 체계[7][9]를 바탕으로, 평가를 위한 메트릭(metrics, measure), 메트릭의 활용을 위한 품질검사표와 점검표 그리고 이를 종합한 시험모듈을 구성하였다. 침입탐지시스템의 보안성과 효율성에 대한 품질특성은 소프트웨어 제품평가에 관한 국제표준인 ISO/IEC 9126과 ISO/IEC 12119의 품질특성 체계에 근간을 두고 침입탐지시스템 고유의 특성을 반영하여 구성하였다.

두 표준에서는 품질특성으로서 기능성, 신뢰성, 사용

성, 효율성, 유지보수성, 이식성의 6가지 특성을 정의하고 있으며, 보안성은 기능성에 속하는 부특성 중의 하나이나 ISO 25000 시리즈에서는 그 중요성으로 인해 품질특성 중의 하나로 자리잡았다.

시험모듈은 품질평가를 위한 평가 메트릭에 대해 소프트웨어 품질평가 프로세스를 위한 국제표준인 ISO/IEC 14598[8] - 부분 6의 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 품질시험에 관한 전반적인 사항을 정리하여 문서화한 것으로 시험의 개요, 기법, 메트릭에 대한 상세 내용, 적용 절차, 결과에 대한 해석 등을 포함하고 있으며 품질평가 프로세스에 관한 국제표준인 ISO/IEC 14598의 <부분 6>인 평가모듈의 형식에 근거하여 작성하였다. 품질시험 모듈의 체계는 <Table 1>과 같다.

〈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 침입탐지시스템에 대한 보안성에 관한 메트릭과 효율성에 관한 메트릭을 개발하였다. <Table 2>에 보안성에 관한 메트릭의 예를 나타내었으며 <Table 3>에 효율성에 관한 메트릭의 예를 나타내었다.

〈Table 2〉 The contents of test modules about security of Intrusion Detection system

Subcharacteritics	Item	Related Items
Security	Security Alarm	Does the system take the list of corresponding action when the security violations is detected?
	Audit Data	Does the system create specified audit data?
	Audit Review	Can approved administrator read all audit data from audit record?
	Storage Protection	Does the system protect audit record from unapproved deletion?
	Corresponding Action	Does the system take corresponding action when audit data exceed the limit?
	Loss Prevention	Does the system take an action which should take if the audit trails are full?
	...	...

〈Table 3〉 The contents of test modules about efficiency of Intrusion Detection system

Subcharac teritics	Item	Related Items
Efficiency	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?
	...	...

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		How long does it take for intrusion detection system to give information so as to take actions after detection of intrusion?
Suitability of Mean Processing Time		
Measurement items	A	Limiting value of Mean Processing Time
	B	Mean Processing Time
		make test cases and figure out the sum of time which take to test and devide it by the number of test cases.
expression		- Suitability of Mean Processing Time = 1- min (1, B/A) - $B = \frac{\sum_{i=1}^{n} Ti}{N}$ - Ti = processing time of i th test - N= the number of test cases of processing time
The range of results		0 ≤ Suitability of Mean Processing Time ≤ 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 침입탐지시스템의 Throughput에 관한 점검표로 패킷 손실 없이 처리할 수 있는 최대 트래픽이 규정된 수준에 이르는 가를 확인하기 위한 점검표의 예를 기술하였다.

〈Table 5〉 Checklist of Throughput

No	Test Case	Maximum Traffic
1	Maximum Traffic Test(1st)	Y
2	Maximum Traffic Test(2ndt)	Y
3	Maximum Traffic Test(3rd)	Y
4	Maximum Traffic Test(4th)	Y
5	Maximum Traffic Test(5th)	Y
...	...	...
The average of the maximum traffic processible without packet loss		
The number of N		
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.

침입탐지시스템이 보안 솔루션으로서의 제 역할을 다하고 있는가를 평가하기 위한 방법으로 관련 표준에 입각한 평가 모델을 구축할 필요성이 제기된다.

따라서 본 논문에서는 침입탐지시스템 보호프로파일과 소프트웨어 제품평가 관련 국제표준인 ISO/IEC 9126과 ISO/IEC 12119의 품질특성 체계를 근간으로 한 침입탐지시스템의 보안성과 효율성 특성 체계의 구축을 중심으로 하여 침입탐지시스템의 품질 수준을 평가할 수 있는 모델을 구축하였다.

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

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

REFERENCES

[1] Dong-Jin Shin, Hae-Sool Yang, Design and Implementation of an Intrusion Detection System based on Outflow Traffic Analysis, Journal of Korea Contents Association, Vol 9 No. 4, p.131, 2009. 4.

[2] Taek-Khun Kim, Sang-Kyun Yun, The Design and Implementation of Network Intrusion Detection System Hardware on FPGA, Journal of The Korea Society of Computer and Information, Vol. 17, No. 4, p. 12, 2012. 4.

[3] ISO/IEC 15408-1:2009, Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model.

[4] ISO/IEC 15408-2:2008, Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components.

[5] ISO/IEC 15408-3:2008, Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components.

[6] Kyunggu-Lee, Byungkyu-No et al., Intrusion Detection System Protection Profile V2.0, Korea Information Security Agency & Hannam University, 2008. 4.

[7] http://sinic45.blog.me/50168373818

[8] ISO/IEC 9126, "Information Technology - Software Quality Characteristics and metrics

[9] ISO/IEC 14598, "Information Technology - Software product evaluation - Part 1~6.

[10] ISO/IEC 12119, "Information Technology - Software Package - Quality requirement and testing".

이 하 용(Ha-Yong Lee)

- 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 해 술(Hae-Sool Yang)

- 1975년 2월 : 홍익대학교 전기공학과 졸업(학사)
- 1978년 8월 : 성균관대학교 정보처리학과 졸업(석사)
- 1991년 3월 : 日本 오사카대학 정보공학과 S/W공학 전공(공학박사)
- 1975년 5월~1979년 6월 : 육군중앙경리단 전자계산실 시스템분석장교
- 1980년 3월 ~ 1995년 5월 : 강원대학교 전자계산학과 교수
- 1986년 12월 ~ 1987년 12월 : 日本 오사카대학교 객원연구원
- 1995년 6월 ~ 2002년 12월 : 한국소프트웨어품질연구소 소장
- 2010년 3월 ~ 2011년 2월: 호서대 글로벌창업대학원 원장
- 1999년 11월 ~ 현재 : 호서대학교 벤처전문대학원 교수
- 관심분야 : S/W공학(특히, S/W품질보증과 품질평가, 품질감리 및 컨설팅, SI), S/W프로젝트관리, 품질경영.
- E-Mail : hsyang@office.hoseo.edu