MOS(Mean Opinion Score)를 이용한 네트워크 보안 QoS(Quality of Service) 평가체계

김점구* · 노시춘**

요 약

네트워크보안 성능평가는 복잡하고 다양한 시스템 환경에서 특정한 단일성능 측정 만으로는 성능평가 측정자체의 의미와 평가결과의 신뢰성이 한계일 수 밖에 없다. 본 논문에서는 보안 QoS의 MOS 측정기법을 사용한 보안기능 만족도 측정방법을 제시한다. 그 내용은 네트워크보안 QoS 만족도에 대한 MOS(Mean Opinion Score) 평가사양 및 운용방법을 개발하여 향후 정보시스템에 대한 고객의 만족도 평가에 활용될 수 있는 QoS 측정/분석 모델을 운용현장에서 활용토록한다. 시스템공급자(개발업체)와 시스템소비자(사용자) 모두가 성능측정 결과를 이용할 수 있도록 가능한 수준의 객관화된 형태의 기준과 방법체계를 개발한다. 개발내용은 보안기능, 네트워킹 기능과 이 두 기능을 종합적으로 평가하는 3개영역의 성능이 상호 연계되는 성능측정 방법론이다. 본연구의 제안 방법론을 사용하여 체계적인 측정환경을 설계 할 경우 운용시스템상에서 보안 QoS의 만족도 산출이 가능하다. 앞으로 다양한 성능측정 기준과 성능측정 방법을 추가적으로 확장하여 네트워크 보안시스템 만족도 평가방법을 업그레이드 시켜나가야 할 것 이다.

A Study of Security QoS(Quality of Service) Measurement Methodology for Network Security Efficiency

Jeom goo Kim* · SiChoon Noh**

ABSTRACT

Network security performance evaluation is a complex and diverse system environments, a single, specific performance measurements alone performance evaluation measure itself and the meaning of the reliability of the evaluation results do not limit the number of days only. In this paper, we propose a method to measure the security features of security, QoS measurement techniques using MOS satisfaction. MOS(Mean Opinion Score) Rating specifications for network security, QoS satisfaction and how to operate the development and operational model for future customer's satisfaction for information systems that can be used to evaluate the QoS measurement/analysis be utilized in the field. Objectified in the form of standards and performance measurement system provider (supplier development) and consumers(users) all the results available so that how to develop a system. Development is the development of information security features, the performance of these two features networking capabilities and a comprehensive evaluation of a three-gaeyoungyeok Correlating performance measurement methodology. Systematic measurement environment designed using the proposed methodology of this study, when the operating system is on the satisfaction of the security, QoS can be calculated. Forward In addition, a variety of performance metrics and performance measurement methods by extending the network security system satisfaction rating upgrade by the way will be.

Key words : QoS(Quality of Service), Measurement, Methodology, Network Security, Efficiency

접수일(2012년 11월 30일), 수정일(1차: 2012년 12월 13일), 게재확정일(2012년 12월 26일)

* 남서울대학교 컴퓨터학과

** 남서울대학교 컴퓨터학과 (교신저자)

1. 서 론

Parasuraman, Zeithaml & Berry (1985, 1988, 1991)는 “서비스품질은 고객의 주관평가에 의해 이루어지며, 지각되고 있는 서비스 품질이란 소비자의 기대와 지각된 서비스의 불일치 방향의 정도”라고 표현했다. QoS 평가는 일반적으로 통신서비스 품질을 대상으로 개발되어 사용되고 있으며 QoS 평가를 보안에 적용하는 방안은 기술적 제약과 QoS 수준 측정상의 문제로 용이하지 않다. 본 연구는 인트라넷 단위 시스템별로 고객만족 측면에서 하나의 네트워크보안 QoS 평가방법론을 연구하기 위한 것 이다. 특히 네트워크 보안 QoS 만족도에 대한 MOS (Mean Opinion Score) 평가사양 및 운용방법을 개발하므로서 정보시스템 고객만족도 평가에 활용될 수 있는 새로운 모델로 제안한다. 네트워크보안 QoS 관리체계는 통신 관련 인프라 시스템 운용에서의 QoS 보증을 위한 업무운용 제반 절차와 기준을 프레임워크화 하여 제도화하는 일련의 규격이다. 연구순서는 네트워크 성능평가 기준, 정보보안 성능평가 기준, 기존평가 방법의 현안사항, QoS평가 체계 설계, 결론의 순서이다.

2. 관련연구

2.1 네트워크 성능평가 기준

ITU-T는 권고 E.800 (1994.8)에서 “통신 서비스 이용자 만족도를 결정하는 서비스 성능들의 총체적 효과”로 표현 했으며 ITU-T 권고 I.350에서는 QoS는 “사용자가 느끼는 서비스품질로서 서비스 접근점에서 측정가능한 사건 및 상태로부터 측정할 수 있어야 한다”로 표현했다. QoS 평가 국제기준으로 품질평가 항목이 제시되고 있는데 주관적 방법으로 MOS(Mean Opinion Score)가 있고 객관적 방법으로 E-mode, PSQM Perceptual Speech Quality Measurement, PESQ(Perceptual Evalutionof Speech Quality), PAMS(Perceptual Analysis Measurement System)가 있다. MOS는 ITU-T의 P.800으로 제시된 기준이며 평가자가 느끼는 품질을 5단로 평가한 평균값이다. 품질평가에 사용되는 파리미터별 품질 산출방법 및 평가산식 종류는 e-model, r-value, rating factor, r-factor에 의한 MOS 값 산출, 고객관점 가중치 산출방식 등으로 구분된다[2][5].

2.2 정보보안 성능평가 기준

NSS그룹과 Tolly그룹에서 특히, NSS그룹에서의 성능측정 내역은 상세한 측정기준 및 측정방법에 기초하고 있고, 기가비트 방화벽 또는 멀티기가비트 방화벽 등 시스템군에 대하여 동시에 많은 개발업체들이 참여하여 결과를 발표하고 있다. Tolly그룹의 평가내역은 상대적으로 작은 수의 필수 평가기준에 대해서 수행되고 있다.Tolly Group의 성능평가는 방화벽, IPS의 네트 워크성능과 보안성능으로 구분한다. 네트워크 성능은 처리량과 지연율을 중심으로 수행하며 보안성능은 악의적 트래픽 탐지와 차단의 정확성을 평가한다. VPN장비는 IPSec 및 SSL(Secure Sockets Layer) 알고리즘 지원 여부와 터널링 설정시 처리율 및 지연율, 동시 접속에 대한 평가를 수행한다[6][7][8][9][10].

<표1> 보안성능평가 단체별 사례

단 체	평가항목	특 징
Tolly Group	방화벽,IPS성능평가	네트워크 성능은 처리량과 지연율을 중심, 보안 성능은 악의적인 트래픽 탐지 및 차단의 정확성평가
	VPN 장비	IPSec 및 SSL(Secure Sockets Layer) 알고리즘 지원 여부와 터널링 설정시 처리율 및 지연율, 그리고 동시 접속률 평가
ICSA	안티 바이러스, 방화벽, IPS, VPN 등 정보보호 시스템에 대하여 인증	시스템 개별적인 평가 기준. 매년 기준을 갱신, 신규 평가 기준에 따라 성능 시험을 수행. 평가 시스템에 대해 객관성, 공정성, 신뢰성을 갖추어 평가를 수행한 결과를 통과 또는 실패로 분류하여 통과의 경우 인증 마크를 부여
Veritest	안티 바이러스/스팸 및 웹 보안 장비	안티 바이러스/스팸은 기능성, 성능, 사용자 수용 시험, 웹 보안 장비는 기능성, 성능, 가용성 시험 등평가.Veritest 성능 평가는 유사한 기능의 시스템을 선별하여 기능, 성능, 가용성, 사용성 등의 성능 시험항목을 도출기능, 성능, 가용성, 사용성 등의 성능 시험항목을 도출
N S S Lab	방화벽, IPS, VPN, UTM	보안 시스템을 약 800개 항목으로 객관적 평가엔진의 공격 탐색, 기능성, 성능, 안정성, 가용성 등의 시험항목에 따라 성능을 평가하고 있으며, UTM은 보안 기능의 설정에 따른 네트워크 성능을 기준으로 평가를 수행한다. NSS는 각 정보보호 시스템에 대한 자체 성능 평가 기준을 마련

3. 기존 성능평가 방법의 현안사항

사용자들은 공급자가 제공하는 사양과 기준에 의하여 벤치마크 테스트를 통해 성능평가를 수행한다. 평가항목과 성능기준은 공급자 기준의 전문적 측정기준 및 측정방법에 기초한다. 본 연구자가 자체 조사한 성능평가 시 현장의 어려움은 다음과 같은 현안사항이다.

3.1 시험기간 낭비 및 중복투자 비용 발생

산업체에서 시스템 구매 시 산업체 환경에 맞는 성능시험 항목을 제시하고 시스템 판매자가 공인기관에 산업체 환경에 맞는 시험항목에 대한 평가를 의뢰한다. 이는 구매자에 따라서 요구하는 평가항목이 다르기 때문이지만 시험 기간 낭비 및 중복투자 비용이 발생한다. 발전 하는 네트워크 공격기법에 따라 짧은 생명주기를 갖는 정보보호시스템의 특성에 비추어 치명적 약점이 될 수 있다.

3.2 업체의 성격에 따라 평가 요구 상이

국제적 평가방법은 객관적인 성능평가 모델을 가지고 네트워크 보안장비 성능평가를 하지만 업체 성격에 따라 네트워크성능 보다 정보보호 성능을 중시하는 업체나 정보보호 성능과 네트워크 성능을 동시에 요구하는 경우로 보안성능 평가방법 선택이 쉽지 않다.

3.3 보안,네트워킹 단일성능 측정의 비 효용성

성능평가는 복잡하고 다양한 시스템 환경에서 특정한 보안, 네트워킹 단일성능 측정만으로는 성능평가 측정자체의 의미와 평가결과에 대한 활용도 가치 또한 한계일 수 밖에 없다. 다양한 시스템 환경을 고려한 보안, 네트워킹 분야별 침입차단 단계별, 차단 유형별 보안성능과 네트워킹 성능측정 을 통해서 시스템 효율을 종합적으로 분석 할 수 있어야 한다.

4. QoS 평가체계설계

4.1 평가체계 설계목표

시스템공급자(개발업체)와 시스템소비자(사용자) 모두가 성능측정 결과를 이용할 수 있는 객관 화 형태의 기준과 측정결과에 기반한 성능측정 기준과 방법을 개발한다. 종합적으로 보안성능을 평가할 수 있는 보안기능, 네트워킹기능과 이 두기능을 지원하는 시스템 자체의 성능요소로 상호 연계되는 성능측정 방법론을 개발한다. 설계된 기능은 계량적으로 측정과 검증이 가능해야 한다 [6][7].

4.2 품질관리 모델 구조(IEEE 1061)

품질구조는 Quality, Quality Factor, Quality Subfactor, Metric로 단계화한다. Quality는 목표 시스템이 충족해야 할 품질이며 Quality Factor, 항목, 사용자나 관리자 중심 시스템이 외부에 보이는 품질로서 Characteristic Factors라 한다. Quality Subfactor는 내부항목이며 시스템의 구현자가 다루는 품질이다. Quality Factor를 측정 할 수 있는 소프트웨어 속성으로 바꾼 것으로 Sub-characteristics, Criteria라 한다. Metric인 측정기준은 평가자 중심으로 품질을 측정하는 방법과 척도이다.

<표2> 품질관리 모델 구조

구 분	내 용
Quality	목표 시스템이 충족해야 할 품질
Quality Factor	Characteristics, Factors. 사용자나 관리자 중심. 외부에 보이는 품질
Quality Subfactor	시스템 내부의 구현자 다루는 품질. Quality Factor를 측정할 수 있는 시스템 속성으로 바꾼 것. Sub-characteristics, Criteria라고도 함
Metric	측정기준. 평가자 중심. 품질을 측정하는 방법과 척도

4.3 성능평가의 범위

4.3.1 네트워크보안 성능

정보보안기능은 인프라구조상에서의 ●악성코드 진단 ●악성코드 삭제 ●해킹차단 효율 ●보안 취약점 검출 ●보안패치 이행율이 포함된다. 침입차단 기능은 OSI 계층별 차단, 트래픽 소통 경로별 차단, 방

역 Zone별 차단으로 분류 될 수 있다. OSI 계층별 차단은 Layer2에서 Layer7 까지 계층별로 수행되는 차단기능이다. 경로별 차단은 외부 라우터에서부터 최종 클라이언트 까지의 트래픽 경로별로 수행되는 차단이다. 방역 Zone별 차단기능은 각종 자원별로 차단기능이 수행되는 것이다[7].

4.3.2 네트워킹 성능

네트워킹 기능은 OSI 7 layer별로 차별화된 네트워킹 기능구조를 형성하고 이 구조상에서 라우팅, 스위칭, 브로드캐스팅 등 인터네트워킹 기능, 데이터 전송기능, 패킷처리 기능을 수행한다. 다이어그램상 네트워킹기능 영역내에 지원기능과 침입차단 기능이 존재한다. 대역폭은 연결된 네트워크에서 사용가능한 트래픽의 양이다. 인터넷 네트워크는 PSTN 망과 달리 일정 전송속도로 음성패킷을 보내도록 설계된 것이 아니기 때문에 전송패킷의 속도가 인터넷 대역폭에 따라 일정치 않을 수 있다[9][10].

4.4 단위기능별 QoS 측정기준

보안 프레임워크를 구현하는 방법으로서 보안기능 부분과 지원기능 부분의 성능이 발휘되며 이 성능을 측정하고 분석하기 위해 성능정보를 구성하고 정의해야한다. 성능정보 항목은 논문의 프레임워크에서 보안기능이 수행되는 과정에서 연동되어 수행되는 시스템 성능 영역, 보안기능 영역, 네트워킹기능 영역이다[11].

4.4.1 네트워크보안 성능 부분

차단구조에서의 차단이 이루어진 실적을 계량화한 수치이며, 악성코드 차단, 해킹차단, 보안취약점 검출, 보안패치율, 보안효율로 구성된다. 침입차단시스템 또는 클라이언트 방역솔루션의 경우는 처리단위 가 Packet Per Second(PPS) 또는 Byte Per Second(BPS)로 표현된다. 보안효율은 악성코드를 차단한 실적과 차단원인으로 Performance에 부작용이 발생한 상호비율이다.

◉ 악성코드 처리수준

- 차단건수 : 차단이 이루어진 악성코드 건수
- 차단율 : 차단건수/ 총발생 또는 침입건수
- 미차단율 : 미차단건수/총발생 침입건수

<표3> 침입차단 QoS 구조

항 목	내 용
필터링 처리량	4 계층 필터와 application payload signature에 기반한 7계층 필터 성능
TCP 연결 비율	4 계층 부하 분배기로 설정한 경우의 TCP 세션에 따른 연결 비율
HTTP 트랜잭션 비율	7 계층 부하 분배기로 설정한 경우 HTTP Get/Reply와 TCP로 구성된 HTTP 트랜잭션 비율
처리 성능	공격 트래픽을 막으면서 올바른 HTTP와 UDP 트래픽 처리 성능

◉ 침입차단 성능

침입차단 성능평가는 방화벽의 기본적 모듈, 로그정보, 방화벽 설치위치(가정, 중소기업, 대기업)에 따른 보안기능을 평가한다.

◉ 보안위험도 : 네트워크보안사고 발생빈도*위협강도

- 위협영향 : 위협이주는 피해의 수준
- 위협발생빈도: 일정기간 동안 위협 발생횟수
- 위협수준 : 위협영향*위협발생빈도

◉ 인증과 암호화 성능

성능평가는 기본기능 및 장비기능 평가로 구분 되며, 기본기능 평가는 관리기능, 악의적인 데이터 탐색 및 인증, 트래픽 탐지, 로그정보 저장 및 보고서 기능을 평가한다.

4.4.2 네트워킹 성능 부분

◉ 지연(Latency)

송신한 하나의 패킷이 측정목적지까지 왕복하는데 소요되는 시간이다. 통신과정에서 음성과 데이타간 신호변환은 당연히 데이터의 감쇄, 지연, 노이즈 가능성을 높이고 그로인한 latency와 jitter를 초래할 수 있다. 측정작업에서는 32bytes의 ICMP ping 패킷을 전송하여 왕복시간을 측정한다.

- 측정단위 : micro second

◉ 네트워크 자원이용 현황(utilization)

네트워크를 구성하는 링크나 노드의 자원 이용 현황을 파악하기 위한 평가 항목. 특히 링크의 utilization과 잠재적인 트래픽 병목지점을 발견하고 예방 대책을 수립하는데 활용하기 위한 목적으로 개발이 필요하다.

- 측정단위 : 백분율(%)

◉ 대역폭(Bandwidth)

연결된 네트워크 구간에서 사용 가능한 트래픽의 양이다. 인터넷에서 사용하는 네트워크는 PSTN 망과는 달리 일정 전송속도로 음성패킷을 보내도록 설계된 것이 아니기 때문에 전송패킷 속도가 인터넷 대역폭에 따라 일정하지 않을 수 있다.

- 측정단위 : MB/S(%)

◉ 패킷 전송성능

망 운영 센터에서는 네트워크가 잘 동작하는지를 감시하고, 패킷이나 셀이 설정을 잘못하여 폐기 또는 지연되는지를 분석하여야 한다.

- 측정단위 : 백분율(%)

◉ 신뢰성(Reliability)

각 네트워크 연결 상태에 있어서 얼마만큼의 신뢰(비트에러율 등)를 유지하느냐가 수치로 표현된 것. 망 운영센터에서는 네트워크 장애를 신속히 발견, 장애를 해결하도록 경보를 보내는 기능이 요구된다.

- 측정단위 : 백분율(%)

4.5 QoS 측정체계 설계

보안 QoS 측정 각 단계는 단계별 고유한 성격에 의거 계량화된 정량적 평가를 시행토록 설계한다. 이를위해 보안기능, 네트워킹기능 영역의 세부항목을 체크리스트화 한다. 평가점수는 5단계 만족도수준 등급이며 미흡, 기초, 보통, 정상, 성숙 MOS 수준으로 최종결과가 산출된다. 종합만족도 MOS는 평가자의 주관적 품질이며 본 연구에서 품질목표 기준으로 인용하여 사용한다. QoS분야 파라메터별로 어느정도 품질수준을 목표로 운용해야하는가 수준설정에 대해 국제표준으로 제시된 목표를 참조하되 각 운용시스템 환경을 고려하여 자체 목표수준을 결정한다.

<표4> 보안 QoS 점검방법

측정항목		MOS 수준				
영역	QoS 메트릭스	VL	L	M	H	VH
보안기능	• 악성코드 처리수준 • 보안위험도 • 침입차단 성능 • 인증과 암호화 성능					
	합 계					
네트워킹기능	• 지연(Latency) • 네트워크자원 이용현황(utilization) • 대역폭(Bandwidth) • 신뢰성(Reliability)					
	합 계					

측정 체크리스트는 품질 파라메터별 MOS 측정 기준을 보안 MOS 점검방법에 따라 점검하는 상세내역이다. 작성분야는 보안기능, 네트워킹 기능, 종합만족도 3개영역으로 구성되고 영역별 측정파라메타는 20개 항목, 50개 세부항목 으로 구성된다. 본 논문상에서는 MOS 영역별 상세 체크리스트 작성기준을 제안하고 기술은 생략한다.

4.6 MOS 산출방법

4.6.1 측정 QoS에 대한 만족도 집계

MOS 만족도는 3개 분야별로 만족율(%) = 월 총 만족횟수/월 총 측정횟수×100식으로 산출 하며 월간 달성도(%) = 100 - (94 - 국내구간 만족 율) ×5식으로 신출한다. 평가지표의 동일 분류내 척도를 산출한 후 각 지표의 중요도를 평가하여 가중 값을 부여한다. 가중값은 경우별 중요도 비중이 상이하다.

- 가중치는 전문가 집단의 진단평가와 협의결과 따라 적용여부, 대상, 적용수준을 결정한다
- 가중치 값은 진단평가 평가의 목적, 진단평가의 시기적특성, 업무성격, 업무규모, 업무프로세스 단계, 프로세스중요도 기준으로 부여한다.
- 가중치 값은 동일구룹에 속하는 부여대상 전체를 대상으로 100%의 범위 내 값을 항목에 상대적으로 배분한다.

<표5> MOS 만족도 최종점수

QoS영역	측정 항목	세부 항목	점수 분포	가중 점수	최종 점수
보안 기능	10	50	1-100	0.1 - 0.9.	
네트워킹 기능	10	50	1-100	0.1 - 0.9.	
종합 만족도	10	50	1-100	0.1 - 0.9.	

4.6.2 최종 MOS 산출 및 비교분석

종합만족도 MOS는 보안기능, 네트워킹 기능으로 구성되고 측정점수, 가중점수, 평가점수로 집계된다. 평가점수는 5단계의 MOS수준 등급으로 분류된다. 5단계 등급은 미흡, 기초, 보통, 정상, 성숙으로 구분되며 각각 1-100 까지 분포를 가진다. 평가점수를 운용목표와 비교하여 달성도를 분석한다. 달성실적 미진분야를 발췌 하여 원인분석 및 개선작업에 활용한다.

<표6> 4개 영역의 보안 MOS

평가분야	평가점수	목표점수	달성도	MOS 수준				
				미흡	기초	보통	정상	성숙
				1-20	21-40	41-60	61-80	81-100
보안 기능								
네트워킹 기능								
종합평균								

5. 결 론

본 논문에서는 보안 QoS의 MOS 측정기법을 사용한 인프라스템에서 보안기능 만족도 측정 방법을 제안했다. 네트워크보안 QoS 만족도에 대한 MOS(Mean Opinion Score) 평가사양 및 운용방법을 개발하므로서 향후 고객 만족도 평가에 활용될 수 있는 측정/분석기능 새로운 모델이 필요하다. 제안방법론을 통해 체계적 측정환경을 갖출 경우 운용환경에서 보안 QoS 만족도 산출이 가능한 방법이 제시되었고 만족도 측정 메커니즘을 통해서 개선된 네트워킹 기능과 정보시스템 기능을 위한 효율성 제고방법론 개발이 가능함을 보여주고 있다. 앞으로 다양한 성능 측정기준과 성능측정 방법을 추가적으로 연구함으로써 보안시스템 만족도 평가방법을 업그레이드시켜 가야할 것이다.

참고문헌

[1]노시춘,네트워크 보안 효율성 제고를 위한 보안 QoS (Quality of Service) 측정방법론 연구,사단법인 한국사이버테러정보전학회,2011.3

[2]노시춘,의료정보시스템상에서의 네트워크 보안기능 프레임워크와 보안 아키텍처 설계방법,한국사이버테러정보전학회,2011.3

[3]노시춘,네트워크보안 품질모델 구조설계와 축정방안에 관한연구,남서울대학교논문집,2012.8

[4]김점구,노시춘,ISO/IEC9000모델을 참조한 웹 애플리케이션 보안품질 관리체계 설계.한국융합보안학회,2012.6

[5]노시춘,품질기반 웹 애플리케이션 개발을 위한 소프트웨어아키텍처 설계절차 정립,2012.9

[6]ISTF-004, "침입차단시스템 로그형식 표준", 한국정보통신기술협회, 2001

[7]TTAS.KO-12.004, "네트워크 보안 장비에 대한 성능 측정 방법“, 한국정보통신기술협회, 2006

[8]VeriTest, http://lionbridge.com, 2011.s

[9]ICSA Labs, http://www.icsalabs.com, 2011.

[10]Tolly Group, http://tolly.com., 2011.

[11]NSS Labs, http://www.nss.co.uk, 2011.

[12]Sichoon Noh, Kuimam J.Kim, "Improved Structure Management of Gateway Firewall Systems for Effective Networks Security", Springer, 2003.

[13]Sichoon,Noh,"Building of an Integrated Multilevel Virus Protection Infrastructure", IEEE Computer Society,2005.12

[저 자 소 개]

김 점 구 (Jeom goo Kim)

1990년 2월 광운대학교
전자계산학과 이학사
1997년 8월 광운대학교
전자계산학과 석사
2000년 8월 한남대학교
컴퓨터공학 박사
1999년 3월~현재 남서울대학교
컴퓨터학과 정교수
IT융합연구소장

email : jgoo@nsu.ac.kr

노 시 춘 (SiChoon Noh)

1987년 2월 고려대학교
경영정보학 석사
2005년 2월 경기대학교
정보보호기술 박사
2002년 11월 KT 시스템보안부장
2004년 12월 KT 충청전산국장
2005년3월 ~ 현재 :남서울대학교
컴퓨터학과 교수
IT융합연구소연구위원

email : nsc321@nsu.ac.kr