情 報 保 護 學 會 誌
第 12 券 第 5 號, 2002. 10

정보보호제품 성능시험 동향 분석

정 태 인*, 김 진 호*, 신 용 녀*, 박 희 운*

요 약

인터넷의 활성화와 더불어 정보보호제품의 사용이 일반화되고 있으며, 제품의 성능을 객관적으로 측정할 수 있는 성능 시험을 요구하고 있다. 본 논문에서는 정보보호제품의 성능시험동향을 다루고 있다. 먼저, 정보보호제품을 대상으로한 성능시험의 소개와 필요성에 대해서 설명한 후, 국내외 성능시험 현황을 소개한다. 현황에서는 미국과 유럽 등의 해외 시험 기관과 국내의 시험 기관에서 시행하고 있는 성능시험에 대해서 알아본다. 또한 시험 기관의 성능시험방법을 비교하고 정보보호제품의 성능시험에 고려해야 할 사항에 대해 살펴본다.

Ⅰ. 서 론

최근 정보보호에 대한 인식이 제고되고 있는 상황에서, 정보보호제품이 널리 보급되어 사용되어지고 있다. 이러한 정보보호제품은 특성상 보안성(security)이 필수적으로 제공되어야 한다. 이러한 보안성은 외국의 경우 TCSEC(Trusted Computer System Evaluation Criteria), ITSEC(Information Technology Security Evaluation Criteria), 국제공통평가기준(Common Criteria) 등으로 평가 및 인증을 실시하고 있으며, 국내에서는 침입차단시스템, 침입탐지 시스템 각각에 해당하는 평가기준을 통해 평가 및 인증이 이루어지고 있다.[1] 정보보호제품은 일반적으로 네트워크에서 추가되어 사용되기 때문에 보안 관리자는 이러한 제품들이 네트워크에 미치는 영향에 대해서 알고 분석할 수 있어야 한다.[2] 성능과 보안은 서로 트레이드오프(trade-off)의 관계를 가지기 때문에 기존에는 정보보호제품의 보안성에 중점을 두고, 성능 부분은 상대적으로 덜 중시되었다. 그러나 실제 정보보호제품의 사용자들에게는 이러한 성능 부분이 제품 선택에 중요한 역할을 하기 때문에 보다 정확한 정보를 제공하기 위해서 보안성과 함께 성능시험의 중요성이 커지고 있다. 따라서 본 논문에서는 보안성 평가와는 별도로 정보보호제품의 국내외 성능시험 현황을 소개 및 고찰하고 추후 나아갈 방향을 모색하고자 한다.

본 논문의 구성은 2장에서는 성능시험의 개요로 성능시험의 정의, 종류와 중요성에 대해서 설명하고, 3장에서는 미국과 유럽을 중심으로 한 해외 성능시험 기관과 국내 한국정보통신기술협회(Telecommunications Technology Association) 네트워크 시험센터(Network Test Center)의 시험 현황을 살펴보고, 사용한 각각의 방법론에 대해서 기술한다. 4장에서는 시험기관의 성능시험 방법을 비교하고 정보보호제품의 성능시험에 고려해야 할 사항을 살펴보며, 5장에서는 결론을 기술한다.

Ⅱ. 성능시험 개요

1. 성능시험의 정의

먼저 성능의 사전적 의미를 찾아보면 다음과 같다.

- 기계 따위가 지닌 성질이나 기능(표준국어대사전)
- 작업을 처리할 수 있는 능력. 시스템의 생산성을 결정하는 것으로, 처리속도, 처리량, 기억용량, 가용성, 응답시간 등의 복합적인 요소로 평가된다.(컴퓨터용어 대사전)

또한, 정보기술 분야에서 사용될 때에는 다음과 같은 의미를 가진다.

- 컴퓨터가 동작하는 속도, 즉 이론적인 속도 또

* 한국정보보호진흥원(KISA) ({tijung,jhk026,ynshin,hupark}@kisa.or.kr)

는 벤치마크 테스트에서 실제로 수행된 명령어나 연산의 개수를 측정한 결과 중 하나를 의미한다. 벤치마크 테스트는 대개 컴퓨터가 실제로 사용될 분야의 일을 모방해서 시도하는 등, 몇몇 작업을 조합해서 실시한다. 성능은 때로, 몇 가지 종류의 벤치마크 중 어떤 하나로 표시되는 경우도 있다.

- 처리량(throughput), 개별적인 응답속도 그리고 가용성 등을 모두 포함한 컴퓨터 시스템의 총체적인 효율성을 가리킨다.

따라서, 정보보호제품에서의 성능시험이란 프로토콜 동작의 견고성과 효율성을 확인하는 것으로 볼 수 있다.

성능시험은 시험 의뢰된 장비에 대한 성능을 독립적으로 평가하는 단독시험(Independent Test)과 시험 의뢰된 네트워크 장비와 이미 시장에 출시된 제품 중 시험의뢰자의 요구에 따라 선정된 동일 목적의 네트워크 장비와의 성능을 비교하는 비교시험(Comparative Test)으로 구분될 수 있다. 일반적으로 비교시험은 동급 제품간의 비교자료가 제시되기 때문에 사용자들이 선호하고 개발자 측에서도 자사 제품의 홍보자료로 활용 가능하다. 한편 인증의 관점에서는 단독시험을 하여 일정 기준을 만족하는 제품을 인증하여야 한다.

2. 성능시험의 중요성

제품을 대량 구매하는 사용자의 경우에는 기능 및 성능 요구사항(requirements)을 가장 잘 만족하는 제품을 선택하기 위해서 벤치마킹테스트(BMT)를 실시한다. 그러나 BMT를 수행하는 경우에 표준화된 성능시험 방법론 및 기준의 부재로 인하여, 표준에서 요구하는 요구사항들보다는 다양한 기능들에 치중하는 경우가 많다. 그 결과, 제품 본연의 보안 기능보다 부가 기능에 대한 정보를 얻어서, 원하지 않는 품질의 제품을 구매할 확률이 커진다. 따라서, 표준화된 시험방법론에 근거한 정보보호제품의 성능시험은 사용자들에게 제품 선택 시 고려해야할 유용한 정보를 제공해줄 수 있다.

또한, 독립적인 성격을 가진 기관에 의해서 표준화된 성능시험 방법론 및 기준에 의해 성능시험이 이루어지면, 개발자와 사용자 모두 동일한 종류의 BMT의 반복 실시에 의해 발생하는 중복적인 시간과 금전의 지출을 줄일 수 있다.

성능시험은 객관성 및 공정성이 필수이므로 이를 확보하기 위해서 시험 과정과 결과가 공개되어야 한다. 이렇게 공개된 시험 결과를 활용하여 BMT를 진행하면, 시험항목 및 시험기간을 줄일 수 있어서 개발자 및 사용자들 모두에게 도움이 될 것이다. 또한 최소한의 성능 기준을 만족하는 제품에 인증제도를 실시하게 되면, 개발자들이 이러한 인증에 적합한 제품을 생산하게 되어서 결과적으로 정보보호제품의 신뢰성을 향상시킬 수 있다.

Ⅲ. 성능시험 현황

1. The Tolly group[14]

톨리 그룹(The Tolly group)은 1989년에 설립된 미국의 사설 테스트 전문 기관으로, 커스텀 테스트(Custom Testing), 품질 보증 테스트(Quality Assurance Testing), 알파/베타 테스트(ALPHA/BETA Testing), 비교 벤치마크(Competitive Benchmarks), 톨리 업 투 스펙 인증(Tolly Up To Spec Certification), 톨리 검증 인증(Tolly Verified Certification), 톨리 시험 인증(Tolly Tested Certification)등 7가지 종류에 대한 테스트 및 인증을 수행하고 있으며, 테스트의 공정성을 유지하기 위해서 준수해야할 사항들을 기술한 공정 테스트 헌장(Fair Testing Charter)을 가지고 있다. 이 헌장은 제품 개발자나 공급자를 보증(endorse)하지 않고, 하드웨어나 소프트웨어 판매를 하지 않으며, 직원들의 IT 관련 회사의 주식 보유를 금지한다는 내용들을 포함한다. 또한, 테스트의 공정성을 확보하기 위해서 테스트에 사용한 소프트웨어/하드웨어 및 테스트 방법을 공개하고 있으므로, 향후에 동일한 조건에서 재 테스트가 가능하다. 테스트 결과 보고서는 일반에게 유료로 공개되어 있다.

시험 인증에는 3가지 종류가 있는데, 먼저 "톨리 업 투 스펙 인증(Tolly Up to Spec certified)"은 톨리 그룹이 정한 업 투 스펙(Up to Spec) 기준에 따라 시험한 결과가 기준에 적합한 경우에 부여되며, "톨리 검증(Tolly verified)"은 톨리 그룹의 검증(verified) 기준에 따라 시험한 결과가 기준을 만족시키는 경우에 부여된다. "톨리 시험(Tolly tested)"은 시험의뢰자가 요구한 시험항목에 대하여 톨리 그룹이 정한 시험방법과 시험환경에 의해 해당

제품을 시험한 후에 부여되며, 결과가 사실임을 톨리 그룹이 보증한다는 것을 의미한다.

톨리 그룹에서 시행하는 성능시험은 다음과 같은 특징을 갖는다.

- TTA NETC와 상호 제휴를 맺고 있고, 테스트 후 다음과 같은 로고를 부여하고 있다.

- 침입차단 시스템의 성능시험시에 동작은 하되 모든 패킷을 그대로 통과시키는 단일 규칙(single rule)을 적용하여 테스트하였다. 실제 사용환경과 유사하게 적절한 수의 규칙(예를 들어 50여 개)을 적용 후에 테스트하는 것이 필요하다.
- 테스트 의뢰자가 비교시험을 의뢰하는 경우에는 1개 이상의 대상 제품을 선정하여 비교시험을 진행하며, 선정된 대상 제품 개발사에 테스트참여를 요청하여 제품 셋업에 대한 기술지원을 받을 수 있다. 또한 결과 보고서 공개 전에도 대상 제품사에서 의견(comment)을 제시할 수 있도록 하고 있다.
- 테스트 결과는 제품의 개발자나 사용자 모두에게 중대한 영향을 미칠 수가 있기 때문에 테스트의 결과를 정확하고 공정하게 처리하도록 노력하고, 특정 개발자나 제품을 추천하거나 보증하지 않는다. 또한 특정 테스트에서의 좋은 결과가 다른 테스트에서도 동일한 좋은 결과를 의미하지는 않는다는 것과 테스트 결과가 성공이나 실패로 받아들여져서는 안 된다고 권고하고 있다.

2. Miercom[15]

Miercom은 1988년에 설립된 네트워크와 통신 관련 제품에 대한 분석 및 테스트를 수행하는 전문 기관으로, 사설 테스트(Private Testing) 및 네트워크 홍보(NetWORKS As Advertised) 프로그램을 제공하고 있다. 사설 테스트에서는 제품 개발자와 사용자들을 위해서 독립적인 성능 및 유용성(usability)을 테스트하고 있으며, 네트워크 홍보 프로그램은 일종의 베타 테스트 사이트(beta test site)를 제공하는 것으로 1995년부터 운영되고 있다. 이 프로그램은 제품 출시 전에 제품의 유용성, 성능 등에 대한 테스트를 실시하여 요구조건을 만족하는 제품들에게 로고를 부여한다. 2002년 현재까지 62개 사의 제품 테스트 결과 보고서가 공개되어 있고, 무료로 다운로드 가능하다.

Miercom에서 시행하는 성능시험은 다음과 같은 특징을 갖는다.

- 테스트 후 다음과 같은 로고를 부여하고 있다.

- 한 VPN 보고서에는 성능뿐만 아니라 설치, 구성, 운영, 보안등 총 5개의 항목에 대하여 평가를 하고, 각각에 가중치를 부여하여 전체적인 결과를 나타내었다.[9]
  전체 점수 = 15% × (설치/이용 편리성) + 15% × (구성) + 25% × (운영) + 25% × (보안/기능) + 20% × (성능)
- Business Communications Review, NetworkWorld 등과 제휴하여 특정 테스트를 수행한 후 그 결과를 발표하기도 한다. 주로 특정 시기에 이슈가 되는 제품이나 항목에 대한 테스트를 수행한다.

3. NSTL[16]

NSTL은 1983년에 설립된 하드웨어와 소프트웨어 테스트 전문 기관으로, 미국에 본사를 두고 있으며 캐나다, 영국, 대만, 일본, 중국, 인도 등에 테스트 랩을 운영하고 있다. NSTL은 새로운 제품이나 기존의 제품들의 호환성(compatibility), 성능, 비교성능(comparative performance), 유용성(usability), 기능성(functionality)을 테스트하고 있으며, 이러한 테스트 결과는 용량 계획, 구매 지원, 효과 분석 등에 사용되어질 수 있다.

인텔, 마이크로 소프트, 휴렛 팩커드 등의 제품 테스트 결과 보고서가 공개되어 있고, 무료로 다운

로드 가능하다.

NSTL에서 시행하는 성능시험은 다음과 같은 특징을 갖는다.

- 테스트 후 다음과 같은 로고를 부여하고 있다.

- 보고서에 "NSTL은 이 자료에 있는 어떤 제품에 대해서도 권장이나 지원을 하지 않습니다. NSTL은 이 보고서에서 제공된 자료의 완전함에 대한 적합하고 정확한 정도에 대해 어떠한 보증도 하지 않습니다. NSTL은 개인이나 업체가 이 자료를 사용함으로써 얻는 결과에 대한 어떤 명시적, 암시적 보증도 하지 않습니다."라고 명시하여 시험의 한계와 책임소재를 규정하고 있다.
- 한 VPN 보고서에는 성능뿐만 아니라 보안성과 운영성을 테스트하여 각각에 가중치를 부여하여 전체적인 결과를 나타내기도 하였다. 보안성 테스트는 ISS 인터넷 스캐너를 사용하여 취약성 스캔을 중심으로 하였고, 터널 공격 테스트(compromise test)도 실시하였다. 전체적인 점수는 다음과 같이 계산하였다.[10]
  전체 점수 = 40% × (보안 점수) + 25% × (운영 점수) + 35% × (성능 점수)
- 일반적으로 단독시험이나 비교시험같은 성능시험은 단독으로 수행되는데 반해, 한 VPN 시험보고서는 단독시험과 상호운용성시험을 동시에 실시한 후에 그 결과를 같이 다루고 있다.[11]

4. ICSA[17]

ICSA는 1991년에 설립되었으며, 바이러스백신(antivirus), 침입차단 시스템(firewall), 암호화(cryptography), 침입탐지 시스템(IDS), IPSec, PKI 등 정보보호제품 전 분야에 걸쳐서 인증을 실시하는 미국의 사설 테스트 기관이다. 각 제품별로 개별적인 기준(criteria)을 버전 별로 보유하고 있으며, 변화에 대응하여 기준의 적시성(timeliness)을 유지하기 위해 매년 갱신하고 있다. 이렇게 갱신된 기준에 기반하여 인증을 매년 재 수행하고 있다.

기준은 공개되어 있고, 객관성, 공정성, 신뢰성을 가지며 통과/실패(pass/fail)를 판단할 수 있도록 한다. 인증 기준은 위협이나 위험에 대해 잘 방어하는지에 중점을 두고 있고, 제품의 설계(design), 엔지니어링 원칙, 기술 평가(assessment)에 중점을 두고 있지는 않다. 즉, 특정 기술에 대한 기준이 아닌, 일반성을 가진 기준이다. 테스트는 대부분의 경우 소스 코드를 확인하지 않는 블랙박스(blackbox)방식을 취하고 있다.

인증의 적시성 및 등급 유지(rating maintenance)를 위해서 ICSA는 다음의 세 가지 방식을 이용한다. 그 결과, 한 제품이 인증을 받은 후에 새로운 버전으로 갱신이 되더라도 그 인증이 유효하게 유지된다.

- 제품 개발자가 인증 후에도 지속적으로 ICSA의 최근 기준을 만족하도록 노력을 한다는 계약을 맺는다. 즉, 제품 개발자 자체적으로 품질 보증(quality assurance) 프로그램을 운영하도록 권장하고 있다.
- ICSA에서 무작위 평가(random assessment)를 시행한다. 여기에서 현재의 기준을 만족하지 못하면, 그 사항을 제품 개발자에게 알려주고 2-4주간의 수정기간을 준다. 그 기간 중에 제품 개발자가 기준을 만족시키지 못하면 인증을 취소한다.
- ICSA는 매년 갱신된 기준으로 재인증을 수행한다.

인증 기준의 갱신은 다음과 같은 순서로 진행된다. 제안된 인증 기준을 제품 개발자, 보안 전문가 그룹, 학계, 실제 사용자들에게 보내어 검토를 요청한다. 의견을 수렴한 후에, 보안전문가로 구성된 ICSA의 인증 감독 위원회(certification oversight board)에 의해 최종 승인된다.

인증은 크게 두 단계의 과정으로 이루어지는데, 친숙화(familiarization)와 인증 시험(certification testing)이다. 친숙화 단계에서는 제품에 대한 설명, 시험 기관과 테스트 의뢰자와의 협력 절차 마련, 기술적 문제들의 이해, 제품 셋업 검사 및 셋업 정정 등을 수행하며, 이 과정에서 테스트 의뢰자와의 협력을 필요로 하기도 한다. 인증 시험 단계에서는 테스트 의뢰자가 제출한 제품 테스팅 가이드(testing guide)의 적절성을 평가하고 실제 제품에서의 구현 여부를 확인한다. 시험 결과는 합격과 불합격으로

판정되며, 합격된 제품에 대해서만 그 결과를 언론과 ICSA 관련 웹사이트에 게시한다. 불합격된 제품은 소정 기간 내에 적절하게 수정된 제품을 제출하여 재시험을 요청할 수 있다. 그러나 60일이 경과하면 모든 인증 작업은 종료된다.

ICSA에서 시행하는 성능시험은 다음과 같은 특징을 갖는다.

- 테스트 후 다음과 같은 로고를 부여하고 있다.

- 인증을 희망하는 테스트 의뢰자는 테스팅 가이드에 필요한 정보들을 기술하여 제품과 같이 제출하여야한다. 여기에는 회사정보, 제품특징, 지원 알고리즘, 구현 관련 데이터들이 포함되고 이 문서를 기초로 문서 심사가 수행된다.
- 성능시험보다는 인증 기준에서 요구하는 기능들이 제품에 구현되어 있는지를 주로 테스트한다. 예를 들면 침입차단 시스템의 인증 기준 중에는 다음과 같은 항목이 있다. "요구되는 서비스 보안 정책에 따라서 구성되었을 경우에 후보 침입차단 시스템 제품은 아래에 기술된 이벤트 형태에 해당하는 이벤트에 대해서 로그를 남기는 능력이 있어야 한다." ICSA에서는 이러한 기능이 구현되어 있는지만을 확인한다. 이러한 로그 기능을 사용하게 되면, 사용하지 않는 경우에 비해서 프로세서에 부가적인 부하를 주게 되어서, 시스템의 성능이 하락하게 된다. ICSA에서는 이러한 기능의 사용/비사용시에 발생하는 성능 차이에 대한 테스트는 수행하지 않는다. 그렇지만, 실제 사용자들에게는 이러한 기능들은 동작시켰을 때의 성능 저하에 대한 시험 결과가 더 필요한 정보가 될 것이다.

5. BSI[18]

연방정보기술 보안국(BSI)은 독일의 국가기관으로 1990년 BSI 설립법의 제정에 따라 1991년에 내무부 외청으로 발족되었다. BSI의 영문명은 GISA (German Information Security Agency)이며, 주요 업무는 정보보호시스템 평가기준, 절차 및 도구 개발, 평가 시행 및 평가필증 교부 등에 대한 정책적 규정, 국가 정보보호기관으로서 암호, 정보시스템 보안 및 전자파 보안 등의 보안업무 수행이다. 1998년에 CCMRA(Common Criteria Mutual Recognition Arrangement)에 가입하였고, 2000년에 CCRA-CAP(Common Criteria Recognition Arrangement - Certificate Authorizing Participants)에 가입하였다.[4]

정보보호제품의 보안성 평가 및 인증을 주로 수행하는데, 침입차단 시스템에 대해서 성능, 유용성, 보안성에 대해 연구를 진행하여 2001년에 "Firewall study II"[12]라는 보고서를 작성하였다.

BSI에서 시행하는 성능시험은 다음과 같은 특징을 갖는다.

- 보고서에서 6개의 침입차단 시스템 제품을 대상으로 하여 테스트 실시후 결과를 다루고 있다.
- 3단계로 구성된 침입차단 시스템의 성능 평가 기준을 제시하고 있다.
- 침입차단 시스템의 성능시험시에 모든 IP 패킷을 통과시키도록 설정하는 단일 규칙(single rule)뿐만 아니라 실제 사용환경과 유사하게 60개의 규칙을 적용하여 테스트하였다.

6. NETC (Network test center)[13]

네트워크시험센터(NETC)는 국내외 정보통신 관련 장비의 공정한 시험 및 인증 서비스 제공을 위하여 정보통신부의 지원으로 설립된 국가기관으로 한국전자통신연구원(ETRI)소속으로 출발했으나 한국정보통신기술협회(TTA)로 2001년에 이관되었다. 수행하는 시험 종류로는 네트워크 장비 기능 확인 시험, 네트워크 장비 성능 평가 시험, 네트워크 장비 개발 지원 시험, 네트워크 장비 상호운용성 시험 등이 있다.

시험 인증에는 3가지 종류가 있다. 먼저 "TTA 인증(TTA certified)"은 국제/지역/국내 표준화기구 또는 국제/국내 포럼 및 컨소시엄이 제정한 표준에 따라 해당 제품을 시험/평가한 결과가 인증 기준에 적합한 경우에 부여된다. "TTA 검증(TTA verified)"은 국제/지역/국내 표준화기구 또는 국제/국내 포럼 및 컨소시엄이 제정한 표준에 따라 해당 제품을 시험/평가한 결과가 TTA가 정한 기준을 만족시키는 경

우에 부여된다. "TTA 시험(TTA tested)"은 시험 의뢰자가 요구한 시험항목에 대하여 TTA 또는 TTA와 고객이 공동으로 제정한 시험방법과 시험환경에 의해 해당 제품을 시험/평가한 후에 부여되며, 결과가 사실임을 TTA가 객관적으로 확인했다는 것을 의미한다. 라우터, 스위치, 침입차단 시스템 등에 대한 제품 테스트 결과 보고서가 공개되어 있고, 무료로 다운로드 가능하다.

NETC에서 시행하는 성능시험은 다음과 같은 특징을 갖는다.

- 톨리 그룹과 상호 제휴를 맺고 있고, 테스트 후 다음과 같은 로고를 부여하고 있다.

- 인증을 위주로 하기 때문에 비교시험이 아닌 단독시험을 주로 시행하고 있다.
- 정보보호제품인 침입차단 시스템이나 가상사설망의 경우에는 표준화된 성능 인증 기준이 없기 때문에 "TTA 인증(TTA certified)"이나 "TTA 검증(TTA verified)"은 시험하지 못하며 "TTA 시험(TTA tested)"을 시험하고 있다. 정보보호제품의 경우에는 침입차단 시스템 1개 제품의 시험 결과가 공개되어 있다.
- 침입차단 시스템의 성능시험 시에 동작은 하되 모든 패킷을 그대로 통과시키는 단일 규칙(single rule)을 적용하여 테스트하였다. 그러나 정보보호제품의 경우에는 일반적인 네트워크 성능보다 좀더 특화된 성능시험 기준이 필요할 것이다.

Ⅳ. 정보보호제품 성능시험 고찰

1. 성능시험 기관 비교

톨리 그룹, Miercom, NSTL은 단독시험과 비교시험 등의 성능시험을 주로 시행하고 있다. 사설기관의 특성상 위 기관들은 테스트 의뢰자가 요구하는 항목 위주로 테스트를 수행하고 있으며, 테스트 결과는 주로 홍보용으로 사용된다.

NSTL의 경우 보안성과 상호운용성을 고려한 테스트를 시행하고 있으며, 이외 기관들에서의 시험방법론은 정보보호제품에 특화된 성능시험이라고 보기 힘들며, 인증 실시에도 부적절하다. ICSA의 경우에는 기능시험을 위주로 하는 인증시험을 시행하고 있다. 따라서 비교시험같은 사용자에게 유용한 자료를 제공하지 못하는 단점이 있다. BSI의 침입차단 시스템 보고서는 기능에 대한 요구사항들과 평가 기준을 가지고 있어서 향후 인증 실시에 적절하고 사용자에게도 유용한 정보를 제공하고 있다. NETC의 경우 톨리와 상호제휴를 맺고 성능시험을 실시하고 있으나 인증 기준의 부재로 인증 실시에 어려움이 있고 보안성 시험에 대한 보완이 필요하다.

〔표 1〕 성능시험 기관 비교

	Tolly group	Miercom	NSTL	ICSA	BSI	NETC
설립 년도	1989	1988	1983	1991	1991	1991
국가	미국	미국	미국	미국	독일	한국
제공테스트	P	P,I	P,I	I,F,C	S,C	P,I,F
비고	사설 기관	사설 기관	사설 기관	사설 기관	국가 기관	국가 기관

P : 성능시험, I : 상호운용성시험
F : 기능시험, S : 보안성 평가, C : 인증

2. 정보보호제품 성능시험 고찰

지금까지 미국, 유럽을 중심으로 해외 정보보호제품의 성능시험 기관 현황을 살펴보았다. 아직까지 정보보호제품의 성능 기준에 대한 표준이 제정되지 않았기 때문에 대부분의 성능시험은 IETF(Internet Engineering Task Force)의 RFC(Request for Comments) 문서를 기준으로 진행이 되고 있다. 하지만, 이러한 RFC 문서들은 정보보호제품에 특화되어 있기보다는 일반적인 네트워크 장비의 성능시험을 위한 것이다. 성능시험에 활용되는 RFC 문서들을 살펴보면 다음과 같다.

- RFC 1242 벤치마크 용어[5]
- RFC 2285 LAN 스위칭 장비를 위한 벤치마크 용어[6]
- RFC 2544 벤치마크 방법론[7]
- RFC 2647 침입차단 시스템 성능을 위한 벤

치마크 용어[8]

현재 시행되는 정보보호제품의 성능시험에서는 RFC 2544에 기반하여 가장 일반적으로 적용 가능한 처리량(throughput)과 지연(latency), 동시 커넥션 수 정도를 시험항목으로 사용한다. 이러한 항목들은 일반적인 네트워크 제품인 라우터, 스위치를 테스트하기에는 적합하나 정보보호 제품을 테스트하기에는 부족하다. 즉, 정보보호제품의 보안요구사항들이 시험항목이나 시험조건에 반영되어야만 한다. 우선적으로 RFC 2647에서 다루고 있는 비트 전달 비율(Bit forwarding rate), 규칙집합(Rule set), NAT (Network Address Translation)등이 고려될 수 있다.

특히 정보보호제품은 네트워크 제품의 특성도 가지고 있지만, 기본적으로 정보보호가 주목적이기 때문에 자체적으로 보안 취약성을 가지고 있으면 안된다. 따라서, 취약성 분석툴을 사용한 분석이 성능시험 전에 필수적으로 선행되어야 한다.

또한 제품에 사용된 기술에 대해 사실표준(de facto standard)이나 공식표준(de jure standard)이 존재하는 경우에는 이 표준을 따르고 있는지에 대한 표준적합성 시험도 이루어져야 한다. 그래야, 이러한 표준에 내재된 취약성이 발견되었을 경우에도 쉽게 보완조치가 이루어질 수 있다. 표준을 따르지 않는 제품에 대해서는 내재된 취약성이 밝혀져서 보완이 이루어지기가 상대적으로 어렵기 때문이다.[3]

인증의 경우에도 단순히 몇 가지 기능의 구현여부를 판단하는 것보다 정보보호제품에 필수적인 기능들에 대해서는 기준을 정하는 것이 필요하다. 기준을 수 단계의 등급으로 나누어서, 모든 필수기능들에 대해서 최하등급을 통과한 경우에만 인증을 한다. 인증을 받은 제품들 중에서는 이러한 등급을 수치화하여서 비교 가능한 수치를 제시하도록 하면 제품의 사용자측에게도 유용한 정보가 될 것으로 예상된다.

〔표 2〕는 침입차단 시스템에 적용 가능한 기준의 예이다.

성능시험에 사용하는 도구(tool)는 상용제품을 이용하는 것이 일반적이며, 이러한 제품은 네트워크 성능시험에 특화되어 있는 하드웨어나 소프트웨어로 시험항목에 대해서 자동화된 시험을 실시한다.

하드웨어의 경우에는 OSI 3계층 이하를 주로 테스트하고 소프트웨어의 경우에는 4계층 이상을 테스트할 수 있다. 그러나 대부분이 고가라는 단점이 있다. 따라서 소프트웨어의 경우에는 오픈 소스(open source)등을 적극 활용하여 벤치마킹용 소프트웨어를 개발하고 공개용 소프트웨어로 배포하는 것이 필요하며, 이러한 공개용 소프트웨어를 통해서 개발자나 사용자 모두 제품의 성능시험을 쉽게 실시 할 수 있을 것이다.

〔표 2〕 침입차단 시스템용 인증 기준 예

	C	B	A	비고
처리량	40 Mbps 이하	40-70 Mbps	70 Mbps 이상	최대가 100 Mbps의 경우
패킷 처리량	10,000 pps이하	10,000 - 30,000 pps	30,000 pps 이상	
동시 커넥션수	10,000 이하	10,000 - 30,000	30,000 이상	제품에 따라 임의로 제한하는 경우도 있음
지연	1000 us 이상	100 - 1000 us	100 us 이하	

V. 결 론

본 논문에서는 정보보호제품의 성능시험 기관 현황을 소개하고, 시험 기관의 성능시험 방법 비교와 정보보호제품의 성능시험 시 고려해야 할 사항에 대해서 살펴보았다.

성능시험은 크게 2가지로 분류할 있다. 첫 번째는 일반적인 벤치마킹 기법을 사용하여 동일 시험 조건에서의 처리량(throughput)이나 지연(latency)을 측정하는 것이다. 여기에는 단독시험과 동급의 제품을 비교하는 비교시험이 있다. 두 번째는 기능의 구현여부를 판단하여 인증을 하는 시험이다. 전자는 유용한 데이터를 제공하여 주기는 하지만 인증 시행에는 적절하지 않고, 후자는 인증에는 적절하나 유용한 데이터를 제공할 수 없다. 따라서, 이 두 가지 방법을 절충하여 중요한 기능 중 벤치마킹이 가능한 항목들을 선택하여 적절한 최저 기준을 만족하는 경우에 인증을 하는 방법이 적당할 것이다. 물론, 여기에는 정보보호제품의 특성상 보안성의 평가나 인

증을 통과한 제품의 경우에만 이러한 성능시험 방법론이 적용되어야 할 것이다.

참고문헌

[1] 한국정보보호센터, "정보보호시스템 평가방법론 연구", 1996.12
[2] 한국정보보호센터, "정보보호시스템 성능평가 지표연구", 1999.12
[3] 한국정보보호센터, "정보보호제품 표준적합성 연구", 2000.12
[4] 한국정보보호센터, "정보보호시스템 평가인증 가이드", 2000.12
[5] IETF, "RFC 1242 Benchmarking Terminology for Network Interconnection Devices", 1991.7
[6] IETF, "RFC 2285 Benchmarking Terminology for LAN Switching Devices", 1998.2
[7] IETF, "RFC 2544 Benchmarking Methodology for Network Interconnect Devices", 1999.3
[8] IETF, "RFC 2647 Benchmarking Terminology for Firewall Performance", 1999.8
[9] Miercom, "Lab testing summary report : Lucent VPN Firewall Brick 201", 2000.7
[10] NSTL, "VPNs: Performance, Security and Management for All", 2000.1
[11] NSTL, "Test Report for Intel Network Systems", 2001.4
[12] BSI, "Firewall study II", 2001.5
[13] TTA, http://www.tta.or.kr
[14] The Tolly group, http://www.tolly.com
[15] Miercom, http://www.mier.com
[16] NSTL, http://www.nstl.com
[17] ICSA, http://www.icsalabs.com
[18] BSI, http://www.bsi.de

〈著者紹介〉

정 태 인 (Tae-In Jung)
1998년 2월 : 한양대학교 전기공학과 졸업
2000년 2월 : 한국과학기술원 전기및전자공학과 석사
2001년 7월~현재 : 한국정보보호진흥원 기술표준팀 연구원
관심분야 : 모터제어, 네트워크, 정보보호

김 진 호 (Jin-Ho Kim)
2000년 2월 : 포항공과대학교 수학과 및 컴퓨터공학과 졸업
2002년 2월 : 한국정보통신대학원 대학교 정보보호그룹 석사
2002년 2월~현재 : 한국정보보호진흥원 기술표준팀 연구원
관심분야 : 암호이론, 암호프로토콜, 정보보호

신 용 너 (Young-Nyuo Shin)
1999년 2월 : 숭실대학교 컴퓨터학부 졸업
2001년 8월 : 고려대학교 컴퓨터학과 석사
2002년 1월~현재 : 한국정보보호진흥원 기술표준팀 연구원
관심분야 : 정형기법, 컴포넌트, 정보보호

박 희 운 (Hee-Un Park)
정회원
1997년 2월 : 순천향대학교 컴퓨터학부 졸업
1999년 2월 : 순천향대학교 전산과 석사
2002년 2월 : 순천향대학교 전산과 박사
2002년 1월~현재 : 한국정보보호진흥원 기술표준팀 선임연구원
관심분야 : 암호프로토콜, 키 관리, 네트워크보안