Journal of Digital Convergence
Vol. 17. No. 8, pp. 221-228, 2019
ISSN 1738-1916
https://doi.org/10.14400/JDC.2019.17.8.221

해외 사례 비교를 통한 가상화 제품의 보안기능 요구사항 분석에 관한 연구

이지연
동남보건대학교 경영학과 교수

A Study on Analysis of Security Functional Requirements for Virtualization Products through Comparison with Foreign Countries' Cases

Ji-Yeon Lee
Professor, Department of Business Administration, Dongnam Health University

요 약 클라우드 컴퓨팅 활성화 정책에 따라 가상화 제품에 대한 보안 중요성이 증가하였으며, 보다 안전한 클라우드 환경을 운영하기 위해서는 가상화 제품에 대한 사이버 보안위협 분석 및 보안요구사항 개발이 필요하다. 본 논문은 가상화 제품에 대한 보안특징 및 사이버 보안위협 분석을 통해 보안기능 요구사항 개발을 위한 사전 연구 목적으로 수행되었다. 이를 위해, 미국 및 영국에서 가상화 제품의 보안성 평가를 위해 사용하고 있는 평가제도와 가상화 제품에 대한 보안위협, 보안목적 및 보안요구사항들을 비교했다. 또한, 가상화 제품의 보안특징과 관련된 핵심적인 보안기능 요구사항 개발을 위한 항목 및 절차를 제안하여 보다 안전한 가상화 제품 개발 및 보안 평가기준 마련에 기여하고자 한다.

주제어 : 클라우드 컴퓨팅, 가상화 제품, 보안위협, 보안기능 요구사항, 공통평가기준, 보호프로파일

Abstract The importance of security for virtualization products has been increased with the activation policy of cloud computing and it is necessary to analyze cyber security threats and develop security requirements for virtualization products to provide with more secure cloud environments. This paper is a preliminary study with the purpose of developing security functional requirements through analyzing security features and cyber security threats as well as comparison of foreign countries' cases for virtualization products. To do this, the paper compares evaluation schemes for virtualization products in US and UK foreign countries, and analyzes the cyber security threats, security objectives and security requirements in both countries. Furthermore, it proposes the essential checking items and processes for developing security functional requirements about security features of virtualization products to contribute to its more secure development and the establishment of related security evaluation standards.

Key Words : Cloud Computing, Virtualization Product, Cyber Threat, Security Requirement, Common Criteria, Protection Profile

*Corresponding Author : Ji-Yeon Lee(jylee@dongnam.ac.kr)
Received May 28, 2019 Revised July 1, 2019
Accepted August 20, 2019 Published August 28, 2019

1. 서론

가상화 기술의 발전, 정부의 국내 클라우드 컴퓨팅 활성화 정책, 관련 법률 제정과 더불어 물리적 인프라 사용의 비용절감, 산업 경쟁력 향상을 유도하기 위한 목적으로 클라우드 컴퓨팅 기술 및 보안에 대한 관심이 지속적으로 증대되고 있다[1-3].

그러나, 클라우드 컴퓨팅의 지속적이고 안정적인 발전을 위해서는 클라우드 컴퓨팅의 특징을 고려한 보안위협 분석, 환경 구축, 서비스 운영 및 보안 관리 등 기술적, 관리적, 물리적 측면에 대한 종합적 보안대책 마련 및 시행이 중요시 요구된다. 이에 따라, 클라우드 컴퓨팅 환경 구축, 보안 아키텍쳐, 보안 서비스 측면에서 관련 연구가 진행되었다[4-6]. 관련 연구는 가상화 제품의 보안 요구사항 분석 측면 보다는 클라우드 컴퓨팅 환경을 구성하는 가상화 기술 식별, 안전한 서비스 제공을 위한 신규 보안위협 요소 분석 및 보안 아키텍쳐 제안에 중점을 두고 있다.

보안 측면에서 보다 안전한 클라우드 컴퓨팅 환경을 구축하고 서비스를 제공하기 위해서는 가상화 제품의 보안성이 우선적으로 보장되어야 한다. 특히, 가상화 제품은 클라우드 컴퓨팅 환경 구축 및 서비스를 제공하기 위한 핵심기술을 포함하고 있다[7]. 예를 들어, 하이퍼바이저와 같은 가상화 기술은 PC 또는 서버에 하드웨어 및 가상머신 사이에 위치하여, 다수의 가상머신이 구동할 수 있는 가상화 계층을 제공한다. 해외 뿐만 아니라 국내에서도 서버에 하이퍼바이저 기반의 가상화 기술을 적용하여 소비자에게 클라우드 컴퓨팅 서비스를 제공하는 방식이 널리 사용되고 있다. 우선적으로 보다 안전한 클라우드 컴퓨팅 환경 구축 뿐만 아니라 클라우드 서비스를 활성화하기 위해서는 보안위협에 대응할 수 있는 보안요구사항을 도출하고 이를 준수한 안전한 가상화 제품 개발이 중요하다.

또한, 제품의 보안성을 평가하는 제도 측면에서는 가상화 제품의 보안 특징을 고려한 보안기능의 정확성 및 완전성을 시험하고 보증하기 위한 보안기능 요구사항 개발이 필요하다. 즉, 보안기능 요구사항은 제품의 보안 품질 보증을 위한 평가기준 역할을 수행하기 때문에 보안위협 분석을 통한 보안기능 요구사항 개발은 안전한 제품 개발 뿐만 아니라 제품의 품질 보증을 위한 기준으로서 매우 중요한 역할을 수행한다.

특히, 국제공통평가기준(CC: Common Criteria)은 정보보호제품의 보안성을 평가하기 위한 국제기준이다[8,9].또한, 보호프로파일(PP : Protection Profile)은 제품유형 대상으로 보안기능 및 보증 요구사항을 명시한 문서로서, 보안요구사항 준수 여부를 평가하는데 활용된다[10-12]. 한국을 포함한 30개국은 국제공통평가기준 및 보호프로파일을 기반으로 정보보호제품의 보안성을 보증하기 위한 평가·인증 제도를 활용하고 있다.

가상화 제품의 등장에 따라, 국 및 미국과 같은 사이버 보안 선진국들은 가상화 제품을 대상으로 보안위협을 분석하고 보안요구사항을 개발하여 제품 개발 및 평가기준에 활용하고 있다. 영국은 NCSC 인증기관에서 CPA 평가·인증제도를 운영하고 있으며[13], 서버 및 클라이언트 관점에서 가상화 보안요구사항을 개발하여 적용하고 있다[14,15]. 미국은 NIAP 인증기관에서 국제공통평가기준에 기반한 평가·인증제도를 운영하고 있으며[16], 서버 및 클라이언트 가상화 제품에서 공통으로 사용될 수 있는 보호프로파일을 사용하고 있다[17]. 또한, 해당 보호프로파일을 기반으로 서버 및 클라이언트 가상화 제품에서 사용가능한 추가적인 보안기능 요구사항을 포함하고 있는 PP(Extended Packages for Server Virtualization[18], Extended Packages for Client Virtualization and for Client Virtualization)[19]를 개발하였다.

그러나, 국내의 경우 가상화 제품 측면의 보안위협 분석 및 보안기능 요구사항 개발은 그 중요성에 비하여 상대적으로 연구가 활성화 되지 않은 상태이다. 서버 가상화 시스템에 대한 보안요구사항을 제안하는 관련연구가 진행되었지만, 가상화 계층의 특징을 고려한 보안요구사항 보다는 클라우드 컴퓨팅 환경에서 기존 컴퓨터 보안에 필요한 기밀성, 인증, 접근제어 등과 같은 보안요구사항에 중점을 두고 있다[20]. 또한, 국내에서 클라우드 컴퓨팅 시스템 또는 가상화 제품의 보안성을 평가하기 위해서는 국내 클라우드 환경을 구성하는 가상화 제품의 보안 특징 및 보안위협 요소를 분석을 통한 핵심적인 보안기능 요구사항 개발이 필요한 실정이다.

이에 따라, 본 논문에서는 영국 및 미국의 해외국가들에서 각각 개발한 CPA-SC Server Virtualisation[14] 및 Protection Profile for Virtualization[17] 문서를 대상으로 가상화 제품에 대한 보안특징, 보안위협 및 보안기능 요구사항 등을 우선적으로 비교 및 분석하고자 한다. 또한, 해외국가에서 개발한 가상화 제품 보안요구사항들에 대한 종합적인 비교 및 분석을 통해 가상화 제품 보안기능 요구사항 개발을 위한 필수 항목 및 절차를 제안하고자 한다. 이를 통해, 향후 국내 환경에 적합한 가상화 제품의 보안기능 요구사항 및 시험방법 개발에 활용하고자 한다.

본 논문의 구성은 다음과 같다. 제2장에서는 영국 및 미국에서 개발한 보안요구사항의 개요, 특징, 보안위협 측면에서 비교 및 분석 결과를 설명한다. 3장에서는 보안기능 요구사항을 비교 및 분석한다. 4장에서는 해외사례의 종합적 비교 및 분석 결과를 기반으로 가상화 제품 보안기능 요구사항 개발을 위한 방안을 제시하고자 한다. 마지막으로 5장에서는 결론 및 향후 연구방향을 제시한다.

2. 보안요구사항 및 보안위협

2.1 영국의 보안요구사항 특징

가상화 제품은 하이퍼바이저 가상화 기술을 제공하는 제품과 가상화 기술을 제공하는 운영환경을 이용하는 제품으로 구분할 수 있다. 본 논문에서는 가상화 기술을 제공하는 MS Hyper-V, VMware 등과 같은 가상화 제품을 대상으로 보안요구사항을 분석하고자 한다.

영국의 'CPA-SC Server Virtualisation'[14] 문서는 단일 하드웨어에서 다수의 운영체제를 구성 및 운영할 수 있는 가상화 제품을 대상으로 보안요구사항을 정의하고 있다. 가상화 제품에서는 서로 다른 가상머신의 보안영역(security domain)에 대한 격리성(isolation)을 보장하는 것이 가장 중요한 보안목적이다.

또한, 보안요구사항을 도출하기 위해 가상화 제품의 주요 구성요소를 다음과 같이 식별하고 있다.

- 가상머신: 호스트 소프트웨어 상에서 동작하며, 서로 다른 가상머신과 상호 통신하거나 자체 네트워크 인터페이스를 통해 다른 네트워크와 통신 가능
- 호스트 소프트웨어: 운영체제, 하이퍼바이저 및 VMM(Virtual Machine Monitor) 포함
- 저장장치: 로컬 하드디스크 또는 SAN 스토리지 장치
- 관리 소프트웨어: 호스트 소프트웨어, 네트워크 등 관리하는 소프트웨어
- 하드웨어: 가상화 기술을 지원하는 CPU(예, 인텔 VT-x, AMD-V) 등 하드웨어 장치

보안요구사항은 크게 개발(DEV), 검증(VER) 및 배치(DEP)의 3가지 관점으로 분류하여 서술하고 있다.

- DEV(Development): 제품을 설계 또는 구현하는 개발자 측면의 보안요구사항
- VER(Verification): 제품에 대한 시험활동 수행하는 검증 측면의 보안요구사항
- DEP(Deployment): 제품을 운영 및 사용하는 사용자 또는 관리자 측면의 보안요구사항

본 논문에서는 제품 보안기능 개발과 관련된 DEV 보안요구사항에 대해 분석했다. DEV 보안요구사항의 경우에는, 비밀채널(covert channel), 소프트웨어 구현결과물(software implementation) 및 저장장치(storage)의 3가지 관점에서 공격대상, 위협요소를 식별 후 관련 보안요구사항을 정의했다. 2.3절에서는 서버 가상화 제품에 대한 DEV 보안요구사항에 대한 요약 내용을 설명하고 있다. 대부분의 보안요구사항은 하드웨어 및 응용 소프트웨어 계층 사이에서 가상화를 제공하는 구성요소 또는 기술(예, SMM, 메모리, 드라이버, Hypercall)에 대한 소프트웨어 구현결과물에 대한 위협에 대응하기 위한 내용에 집중되어 있음을 알 수 있다.

2.2 미국의 보안요구사항 특징

미국에서 개발한 보호프로파일(Protection Profile for Virtualization Version 1.0)[17]은 서버 또는 클라이언트 기반 가상화 제품에서 공통적으로 사용하는 보안기능 요구사항 및 보증 요구사항을 서술하고 있다. 보다 정확히 말해서, 동일 하드웨어 플랫폼에서 다수의 독립적인 컴퓨팅 시스템을 가능하게 하는 소프트웨어 제품을 대상으로 하고 있으며, 가상화 제품의 주요 구성요소를 다음과 같이 식별하고 있다.

- VMM: 하이퍼바이저, Service VM, Guest VM, Helper VM(Virtual Machine)을 포함하는 가상머신 매니저
- Management Subsystem: VMM에 대한 설정 및 관리 수행할 수 있는 관리시스템
- Platform: 가상화제 제품이 설치 및 운영되는 플랫폼으로 하드웨어, 호스트 운영체제, 펌웨어를 포함

가상화 제품은 일반적으로 VMM과 Management Subsystem으로 구성된다. Service VM은 가상머신 동작에 필요한 자원 또는 서비스를 제공하며, 하이퍼바이저를 지원하는 역할을 수행한다. 예를 들어, 물리적 디바이스 접근을 위한 디바이스 드라이버 가상머신 또는 가상머신 상호간 통신 지원 위한 네임서비스 가상머신이 Service VM에 해당된다. Guest VM은 사용자의 독립적인 실행환경을 제공하는 가상머신이며, Helper VM은 Guest VM 동작에 필요한 기능 또는 서비스를 제공하는

가상머신이다. 예를 들어, Guest VM을 위한 바이러스 스캐닝 기능을 제공하는 가상머신은 Helper VM에 해당된다. 다만, 가상화 제품 평가범위의 경우에는 일반적으로 하이퍼바이저, Service VM, Management Subsystem으로 구성된다. 또한, 하이퍼바이저에 특화된 보안기능 요구사항을 포함하고 있지 않다.

2.3 영국의 보안위협 사례

영국의 CPA-SC Server Virtualisation[14] 문서는 보안위협을 명시적이고 구체적으로 식별하고 있지 않다. 보안위협은 가상화 제품 개발(DEV), 검증(VER) 및 배치(DEP)의 3가지 관점으로 구분하여 분류하고 있다. 다음은 영국의 CPA-SC Server Virtualisation[14] 문서의 보안요구사항을 분석한 후 가상화 제품의 보안위협을 도출한 항목이다.

- DEV.M203(비밀 채널 우회): 보안정책을 우회하는 정보전송의 위협 예방 위한 잠재적 비밀채널의 사용을 제한
- DEV.1.M41(소프트웨어 구현결과물 에러): 오류 대응 위한 로그 생성 및 기록
- DEV.1.M42(소프트웨어 구현결과물 에러): 힙 영역 메모리 보호
- DEV.1.M43 (소프트웨어 구현결과물 에러): 스택 영역 메모리 보호
- DEV.1.M44(소프트웨어 구현결과물 에러): 비신뢰 입력 값 대상으로 데이터 유효값(예, 입력 값 크기) 확인
- DEV.1.M159(소프트웨어 로직 에러, 소프트웨어 구현결과물 에러): 소프트웨어 에러 개선을 위한 제품 업데이트
- DEV.1.M179(소프트웨어 가상화 기술 버그에 의한 게스트 OS의 권한상승): 호스트 상에서 하드웨어 기반 CPU 가상화 기술(예, Intel VT-x and AMD-V) 사용
- DEV.1.M180(메모리 핸들링 버그): 가상화 메모리 핸들링 위한 메모리 보안기술(예, Intel Extended Page Tables, AMD Rapid Virtualisation Indexing) 사용
- DEV.1.M184(System Management Mode 에러):가상머신의 호스트 운영체제의 System Management Interrupt를 이용한 SMM 접근에 대한 통제
- DEV.1.M190(Direct Memory Access 에러): 가상머신 호스트 운영체제의 DMA 직접 접근에 대한 통제
- DEV.1.M191(가상머신의 입출력 장치에 대한 인가되지 않은 접근): 가상머신이 다른 가상머신의 입출력 장치에 대한 인가되지 않은 접근을 통제
- DEV.1.M240(컨텍스트 스위치 에러): 가상머신이 다른 가상머신의 이전 단계의 중요 정보에 대한 접근을 방지
- DEV.1.M253(가상머신 디바이스 재할당 에러): 가상머신 디바이스 재할당시 이전 중요 정보는 삭제되어야함
- DEV.1.M267(제품 설정 오류): 자동 보안설정 이행
- DEV.1.M273(비인가된 메모리 데이터 읽기, 비인가된 메모리 데이터 변조, 가상머신 공격): 메모리에 대한 비인가된 접근 통제
- DEV.1.M321(소프트웨어 구현결과물 에러): DEP(Data Execution Protection) 메모리 보호기술 필요
- DEV.1.M340(소프트웨어 구현결과물 에러): ASLR(Address Space Layout Randomisation) 메모리 보호기술 필요
- DEV.1.M350(공유 드라이버 에러): 디바이스 드라이버는 다른 보안영역에 존재하는 데이터를 공유하거나 전송할 수 없음
- DEV.1.M353(제품 설정 오류): 인증된 관리자에 의해서만 제품의 보안 설정이 변경 가능해야함
- DEV.1.M355(호스트에 악성코드 감염, 업데이트 시 취약한 소프트웨어 설치): 안전한 소프트웨어 배포를 위한 소프트웨어 출처의 신뢰성 확인 및 변조 방지 기술 적용
- DEV.1.M356(Hypercall 등 호스트 서비스 에러): 가상머신은 인가된 호스트 서비스에 대한 접근만 가능함
- DEV.2.M177(디스크 이미지 변조, 디스크 이미지의 비인가된 데이터 읽기, 백업 데이터에 대한 비인가된 접근): 디스크 이미지에 대한 접근통제 및 보호
- DEV.2.M213(높은 보안등급 가상머신의 낮은 보안등급 데이터 접근 오류): 높은 보안등급 데이터를 취급하는 가상머신의 낮은 보안등급 데이터에 대한 접근을 통제, 높은 보안등급 데이터 및 낮은 보안등급 데이터 보관하는 저장장치 분리 필요

2.4 미국의 보안위협 사례

영국 사례와 비교해 볼 때, 미국의 보호프로파일에서는 '보안문제정의(Security Problem Definition)' 절에서 보안위협, 가정사항 및 조직의 보안정책으로 구분하

여, 보호프로파일이 준수하는 평가대상 제품이 다루고자 하는 보안문제를 상세히 정의하고 있다.

평가결과의 정확성 및 완전성은 정의된 보안문제에 의존적이기 때문에 가상화 제품 자체 뿐만 아니라 운영환경을 고려하여 보안 위협을 도출하는 과정이 우선적으로 중요하다. 도출된 보안 위협을 통해 조직의 보안정책 및 가정사항을 고려한 후 가상화 제품 또는 운영환경에서 달성할 수 있는 보안목적을 도출할 수 있게 된다. 다음은 미국의 Protection Profile for Virtualization[17] 문서를 분석한 후 보안위협을 도출한 사항이다.

- T.DATA_LEAKAGE(데이터 유출 위협): 가상머신의 데이터 유출 공격(예, 가상머신 상호간 데이터 공유)
- T.UNAUTHORIZED_ UPDATE(비인가된 업데이트 위협): 가상화 제품 구성하는 구 소프트웨어 버전 결함 공격 및 업데이트 파일 변조 공격
- T.UNAUTHORIZED_MODIFICATION(비인가된 수정 위협): 가상화 제품 구성요소(예, VMM)에 대한 변조 공격
- T.USER_ERROR(사용자 에러 위협): 가상화 제품이 동일 사용자 대상 서로 다른 가상머신 도메인을 동시에 디스플레이 하는 경우, 서로 다른 가상머신 도메인 상호간 정보 유출 가능한 위협
- T.3P_SOFTWARE(제3자 소프트웨어 위협): 가상화 제품 구성하는 3rd-party 소프트웨어(예, 호스트 OS, 디바이스 드라이버) 취약점에 의해 VMM 악의적 통제 등 악용 가능한 취약점 발생 가능한 위협
- T.VMM_COMPROMISE(VMM 공격 위협): 보안 메커니즘 결함에 의한 VMM 변조 및 우회하는 위협
- T.PLATFORM_COMPROMISE(플랫폼 공격 위협): 가상머신 상호연결 및 네트워크 연결하는 플랫폼에서 비밀성 및 무결성 훼손하는 위협(예, VMM 운영 플랫폼 구성하는 시스템 펌웨어 및 소프트웨어 변조)
- T.UNAUTHORIZED_ACCESS(비인가된 접근 위협):비인가된 관리자에 의해 네트워크 접속을 통해 가상머신 및 가상 네트워크 설정하고 변경하는 위협
- T.WEAK_CRYPTO(암호 위협): 강도가 약한 암호 알고리즘 및 엔트로피 사용에 따른 암호 측면의 위협
- T.UNPATCHED_SOFTWARE(패치되지 않은 소프트웨어 위협): 오래된 또는 패치되지 않은 소프트웨어취약점에 따른 가상화 제품 또는 플랫폼 장악하는 위협
- T.MISCONFIGURATION(설정 위협): 관리자 에러 또는 설정 데이터 오류에 의한 비정상 설정 데이터에 의한 보안기능 비정상 동작하는 위협
- T.DENIAL_OF_SERVICE(서비스 거부 위협): 메모리, 저장 공간 및 처리시간 등 시스템 자원 고갈시키는 서비스 거부 공격

미국의 가상화 제품 보호프로파일은 클라이언트 또는 서버 기반 가상화 제품에서 발생할 수 있는 일반적인 위협을 정의하고 있다. 2.3절에서 보는 바와 같이, 영국 보안요구사항의 경우에는 보안위협에 대응되는 보안요구사항이 메모리 보호, Hypercall 통제 등 하이퍼바이저의 기능에 특화된 보안요구사항을 서술하고 있다. 이점이 미국 보안요구사항과의 큰 차이점이라고 말할 수 있다. 또한, 마이크로소프트의 STRIDE 위협 모델 기법[20][21]과 비교하였을 경우 유사한 보안위협 요소가 식별되고 있음을 알 수 있다. 다만, STRIDE 위협 모델 기법에 포함되어 있는 Elevation of Privilege에 대한 직접적인 보안위협 요소가 포함되어 있지 않으며, T.WEAK_CRYPTO 및 T.UNPATCHED_SOFTWARE 보안위협은 STRIDE 위협 모델 기법에는 포함되지 않은 위협 요소이다. 참고로, STRIDE 위협 모델링 기법에서는 공격유형을 Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service 및 Elevation of Privilege의 6가지로 분류하고 있다.

또한, 미국의 가상화 제품 보호프로파일의 경우에는 보안위협에 대응하기 위한 보안목적을 다음과 같이 식별하고 있다.

- O.VM_ISOLATION(가상머신 격리): 가상머신 상호간 정보 전송 금지 등 가상머신 상호영역 분리
- O.VMM_INTEGRITY(VMM 무결성): VMM 변조 방지 위한 무결성 보장(예, 가상화 제품 설치 및 업데이트 파일 대상 전자서명)
- O.PLATFORM_INTEGRITY(플랫폼무결성): VMM 운영에 필요한 플랫폼(하드웨어 및 소프트웨어) 변조 방지 위한 무결성 보장
- O.DOMAIN_INTEGRITY(도메인 무결성): 게스트 가상머신에서 동작하는 소프트웨어 기능 및 보관되어 있는 데이터는 다른 가상머신의 방해를 받지 않아야 하는 도메인 무결성 보장
- O.MANAGEMENT_ACCESS(관리 접근): 비인가된 관리자 또는 사용자가 VMM 관리 기능에 접속하지 못하도록 접근 통제 보장
- O.PATCHED_SOFTWARE(소프트웨어 패치): 가상화 제품 취약점 방지 위한 최신 소프트웨어 패치
- O.VM_ENTROPY(VM 엔트로피): 보안성이 확보된

엔트로피 및 암호알고리즘 사용
· O.AUDIT(보안감사): 보안 이벤트 관련 감사로그 보관 및 보호
· O.CORRECTLY_APPLIED_CONFIGURATION(설정 정확성): 보안정책 및 설정 적용의 정확성 보장
· O.RESOURCE_ALLOCATION(자원 할당): 보안정책에 따라 시스템 자원 할당 제한

3. 보안기능 요구사항

3.1 영국 사례

앞서 살펴본 바와 같이, 영국의 가상화 제품의 DEV 관련 보안요구사항은 비밀채널(DEV.M203), 소프트웨어 구현결과물(DEV.1.M41 ~ DEV.1.M356) 및 저장장치(DEV.2.M177 ~ DEV.2.M213)의 3가지 관점에서 분류하고 있다. DEV 보안요구사항을 분석한 결과, 비밀채널 및 저장장치 보다는 가상화 제공 위한 소프트웨어 구현결과물에 대한 보안요구사항이 대다수를 차지하고 있다. 특히, CPU, 메모리, SMM, DMA, Hypercall, 디바이스 드라이버 등에 대한 보안요구사항이 포함되어 있음을 확인할 수 있다 이는 앞서 언급한 보안영역에 대한 격리성을 보증하기 위해서는 가상머신이 보유하고 있는 정보가 상호침해 될 수 있는 잠재적인 보안약점을 확인하기 위함이다. 즉, 가상머신의 보안영역에 대한 상호침해 방지를 위해서는 CPU를 포함한 하드웨어 계층부터 가상머신이 호출되는 응용 계층의 상호작용을 담당하는 모든 구성요소에 대한 보안요구사항을 고려해야 함을 알 수 있다.

또한, DEV 보안요구사항은 설계 또는 구현 단계에서 발생할 수 있는 보안위협에 대응하기 위한 보안목적을 포함하고 있다. 이에 따라, 가상화 제품의 보안 도메인(security domain)에 대한 격리성 보안속성을 만족하기 위해서는 소프트웨어 구현결과물에 대한 시큐어코딩 뿐만 아니라 보안 설계가 중요함을 알 수 있다. 다만, DEV 보안요구사항은 설계 단계에 대한 보안위협 보다는 소스코드에서 발생할 수 있는 소프트웨어 보안약점을 고려하여 작성되었다. 또한, 일부 보안요구사항의 경우에는 가상화 제품의 보안기능 뿐만 아니라 제품 개발환경에 대한 보안요구사항도 포함하고 있다. 예를 들어, DEV.1M.43은 스택 보호(Stack Protection)에 대한 보안요구사항을 포함하고 있다. 가상화 제품의 소프트웨어 구현결과물을 대상으로 스택 오류와 관련된 공격이 발생할 수 있으며, 이와 같은 공격에 대응하기 위해서는 가상화 제품을 컴파일 할 경우 개발도구에서 모든 라이브러리에 대한 스택 보호 기능이 지원되어야 한다고 명시하고 있다.

3.2 미국 사례

미국의 가상화 제품 보호프로파일에 서술된 보안기능 요구사항을 분석한 결과, 가상화 제품의 주요 보안특징에 해당하는 보안기능 요구사항을 도출할 수 있었다. Table 1은 가상화 제품의 주요 보안특징에 특화된 보안기능 요구사항에 대한 내용을 요약하여 보여주고 있다.영국의 보안요구사항과 비교해 볼 때, 가상화 제품의 보안기능이 제공해야하는 요구사항을 세부적으로 명시하고 있다. 예를 들어, FDP_VMS_EXT.1 컴포넌트는 T.UNAUTHORIZED_ACCESS 위협에 대응하기 위한 보안기능 요구사항들을 다음과 같이 엘리먼트 단위로 보다 세부적으로 서술하고 있다.

· FDP_VMS_EXT.1.1: 가상화 제품은 게스트 가상머신들 상호간 데이터 전송을 위해 다음과 같은 메커니즘을 제공해야 한다: [선택: 메커니즘 없음, 가상네트워킹, [할당: 기타 가상머신 상호간 데이터 전송 메커니즘]]
· FDP_VMS_EXT.1.2: TSF는 관리자가 이러한 메커

Table 1. Major security functional requirements of the Protection Profile

Class	Security Functional Requirements
Crypto Support	FCS_ENT_EXT.1 Entropy for Virtual Machines
User Data Protecton	FDP_HBI_EXT.1 Hardware-Based Isolation Mechanisms
	FDP_PPR_EXT.1 Physical Platform Resource Controls
	FDP_RIP_EXT.1 Residual Information in Memory
	FDP_RIP_EXT.2 Residual Information on Disk
	FDP_VMS_EXT.1 VM Separation
	FDP_VNC_EXT.1 Virtual Networking Components
Management	FMT_MSA_EXT.1 Default Data Sharing Configuration
	FMT_SMO_EXT.1 Separation of Management and Operational Networks
Protection of the TSF	FPT_DVD_EXT.1 Non-Existence of Disconnected Virtual Devices
	FPT_HCL_EXT.1 Hypercall Controls
	FPT_RDM_EXT.1 Removable Devices and Media
	FPT_VDP_EXT.1 Virtual Device Parameters
	FPT_VIV_EXT.1 VMM Isolation from VMs
	FPT_EEM_EXT.1 Execution Environment Mitigations
	FPT_HAS_EXT.1 Hardware Assists

니즘들을 게스트 가상머신 상호간 데이터 전송을 [선택: 가능, 불가능]하도록 설정할 수 있도록 허용해야 한다

· FDP_VMS_EXT.1.3: 가상화 제품은 FDP_VMS_EXT.1.1 보안요구사항에 명시되지 않은 메커니즘의 예외 처리 없이 게스트 가상머신이 다른 게스트 가상머신 상호간 데이터를 읽거나 전송할 수 없도록 보장해야 한다

국제공통평가기준에서는 정보보호제품이 보안기능요구사항을 서술하기 위해 반복, 할당, 선택, 정교화의 4가지 오퍼레이션을 허용하고 있다[8]. 즉, 가상화 제품이 상기의 FDP_VMS_EXT.1.1 보안기능요구사항을 서술할 경우에는 선택 및 할당 오퍼레이션을 사용하여 보안기능요구사항을 명세할 수 있다.

4. 시사점

영국 및 미국의 가상화 제품에 대한 보안요구사항들을 종합적으로 비교 및 분석한 결과, 다음과 같은 차이점 및 중요사항들을 발견할 수 있다.

첫째, 평가제도 측면에서 영국의 경우에는 자국의 평가기준에 적용하기 위한 보안요구사항을 작성하고 있으며, 미국의 경우에는 CC 국제공통평가기준에 기반하여 보호프로파일 형태로 보안요구사항을 개발했다는 점이다.

둘째, 보안목적 측면에서 영국의 경우에는 보안 도메인 격리성이라는 보안목적에 중점을 두고 있으며, 미국의 가상화 제품 보호프로파일은 가상머신 상호 격리성 뿐만 아니라 VMM 무결성, 플랫폼 무결성, 가상머신 엔트로피 등 보다 다양한 보안목적을 고려하고 있다

셋째, 가상화 제품의 계층별 보안위협 뿐만 아니라 가상화 제품의 내·외부 네트워크 및 암호 측면의 보안위협을 포함하고 있다. 가상화제품의 초기 개발 단계에서 체계적인 보안위협 분석은 매우 중요하다. 보안위협 분석의 완전성은 보안기능 요구사항 및 보안기능 개발, 보안 취약점과 밀접하게 연관되어 있다. 예를 들어, 가상화 제품 환경설정 파일에 대한 변조와 같은 보안위협을 고려하지 않고 보안기능 요구사항을 개발한 경우, 악성 파일 유입에 따라 한 개의 가상머신 뿐만 아니라 가상화 제품 전체에 대한 침해 또는 중요 정보유출 등의 취약점이 발생할 수 있게 되기 때문이다.

넷째, 보안기능 요구사항 측면에서 영국의 경우에는 하이퍼바이저에 특화된 보안기능 요구사항에 집중하고 있다. 그러나, 미국의 경우에는 Table 1에 표시된 바와 같이, 하이퍼바이저에 대한 특화된 보안기능 보안요구사항 보다는 암호지원, 사용자데이터 보호, 보안관리 및 보안기능성 보호 측면에서 다양한 보안기능 요구사항을 포함하고 있다는 점이다.

영국 및 미국의 가상화 제품의 보안요구사항에 대한 종합적인 비교 및 분석 결과를 바탕으로 다음과 같이 가상화 제품의 보안기능 요구사항 개발에 필요한 핵심적인 항목 및 절차를 제안하고자 한다.

첫째, 가상화 제품이 만족해야하는 보안속성 및 보안목적을 우선적으로 선정해야 한다.

둘째, 소프트웨어 개발, 배포 및 운영단계에서 발생할 수 있는 보안위협을 구분해야 한다.

셋째, 가상화 계층 구조, 물리적 구성요소, 계층적 호출단계, 내부 및 외부의 상호통신 구간에서 발생할 수 있는 보안위협을 고려해야 한다.

넷째, 시험 가능한 수준에서 보안기능 요구사항을 세부적으로 서술해야 한다.

5. 결론

클라우드 컴퓨팅 기술, 정책 및 관련 산업의 안정적인 발전을 위해서는 가상환경 제공을 위한 핵심 역할을 담당하고 있는 가상화 제품에 대한 보안이 우선적으로 선행되어야 한다. 기존 관련연구는 가상화 제품의 보안 요구사항 분석 측면 보다는 클라우드 컴퓨팅 환경 측면에서 보안위협 분석 및 보안 아키텍쳐 제안에 중점을 두고 있다. 본 논문에서는 가상화 제품에 대한 보안요구사항 관련 영국 및 미국의 해외 사례를 비교 및 분석했다. 이를 위해, 가상화 제품에 대한 보안특징, 보안목적, 보안위협 및 보안기능 요구사항을 종합적으로 비교 및 분석했다. 분석 결과, 가상화 제품은 보안 도메인 격리성이 핵심 보안속성이며 가상화 제품의 아키텍쳐 및 구성요소를 정확히 확인하고, 개발, 검증 및 운영단계에서 발생할 수 있는 종합적인 보안위협을 고려한 보안기능 요구사항 개발이 중요한 사항임을 확인할 수 있었다. 이를 통해, 가상화 제품 보안기능 요구사항 개발에 필요한 핵심적인 항목 및 절차를 제안했다. 본 연구결과를 통해 향후 국내 클라우드 컴퓨팅 환경에 적합한 가상화 제품의 체계적인 보안기능 요구사항 개발 및 보안 품질 측정 기준에 활용할 수 있을 것으로 기대된다.

REFERENCES

[1] J. H. Jung. (2017). An Exploratory Study for Activating Cloud Computing: Focusing on Legislative Alternatives. *Journal of Korean Association for Regional Society, 20(4),* 73-96.

[2] S. W. Ahn. (2019). *Policy and Directions for Revitalizing Domestic Cloud Computing.* Research Report of Software Policy & Research Institute, *2018-009,* 1-103.

[3] E. B. Choi. (2018). A Virtualization Management Convergence Access Control Model for Cloud Computing Environments. *Journal of Convergence for Information Technology, 8(5),* 69-75.

[4] S. H. Lee. (2015). Cloud Computing Issues and Security Measure. *Journal of Convergence for Information Technology, 5(1),* 31-35.

[5] S. Y. Choi & K. M. Jeong. (2018). The Security Architecture for Secure Computing Environment. *Journal of the Korea of Computer and Information, 23(12),* 81-87.

[6] I. S. Lee & D. M. Jang. (2017). A Study on Methods for Providing Security Service in Cloud Computing. *Proceedings of Symposium of the Korean Institute of Communications and Information Sciences,* 1052-1053.

[7] Y. S. Kim. (2014). *Technical Trends on Hypervisor-based Virtualization Security in Cloud Computing*, KISA Internet & Security Focus.

[8] CCMB. (2017). Common Criteria for Information Technology Security Evaluation. Version 3.1, Revision 5.

[9] J. H. Park, S. Y. Kang & S. J. Kim. (2018). Study of Security Requirements of Smart Home Hub through Threat Modelling Analysis and Common Criteria, *Journal of the Korea Institute of Information Security & Cryptology, 28(2),* 513-528.

[10] W. R. Jeon, J. Y. Kim, Y. S. Lee & D. H. Won. (2006). Development of Protection Profile for Smartphone Operating System based on Common Criteria 3.1. *Journal of the Korea Institute of Information Security & Cryptology, 22(1),* 117-130.

[11] D. B. Lee. (2015). A Study on Protection Profile for Multi-Function Devices. *Journal of The Korea Institute of Information Security and Cryptology, 25(5),* 1257-1258.

[12] J. H. Kim. H. M. Jung & H. J. Cho. (2017). Design Plan of Secure IoT System based on Common Criteria. *Journal of the Korea Convergence Society, 8(10),* 61-66.

[13] CPA(Commercial Product Assurance). https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa.

[14] NCSC. (2018). CPA Security Characteristic, CPA-SC Server Virtualisation 1.22.

[15] NCSC. (2018). CPA Security Characteristic, CPA-SC Client Virtualisation 1.22.

[16] NIAP(National Information Assurance Partnership). https://www.niap-ccevs.org.

[17] NIAP. (2016). Protection Profile for Virtualization Version 1.0. https://www..niap-ccevs.org/Profile/PP.cfm.

[18] NIAP. (2016). Extended Package for Server Virtualization Version 1.0. https://www..niap-ccevs.org/Profile/PP.cfm.

[19] NIAP. (2016). Extended Package for Client Virtualization Version 1.0. https://www..niap-ccevs.org/Profile/PP.cfm.

[20] S. Y. Ma, J. H. Ju & J. S. Moon. (2015). The Security Requirements Suggestion based on Cloud Computing Security Threats for Server Virtualization System. *Journal of the Korea Institute of Information Security & Cryptology, 25(1),* 95-105.

[21] F. Swiderski & W. Snyder. (2004). *Threat Modeling. Microsoft Press.*

[22] J. H. Lee, H. Lee & I. H. Kang. (2015). Technical Trends on Threat Modelling for Secure Software Development. *Review of Korea Institute of Information Security and Cryptology, 25(1),* 32-38.

이 지 연(Ji-Yeon Lee) [정회원]

· 1999년 2월 : 동덕여자대학교 전자계산학과 학사
· 2001년 2월 : 고려대학교 컴퓨터학과 석사
· 2013년 2월 : 고려대학교 컴퓨터학과 박사
· 2002년 3월 ~ 현재 : 동남보건대학 경영학과 부교수
· 관심분야 : 소프트웨어공학, 정형기법, 네트워크 보안
· E-Mail : jylee@dongnam.ac.kr