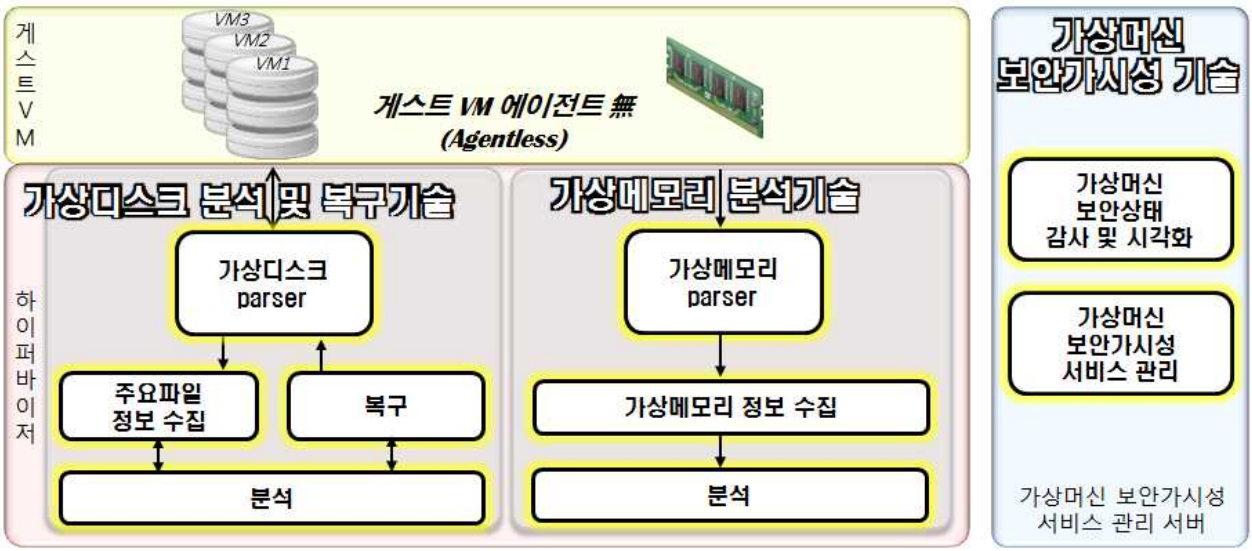
하이퍼바이저 기반
클라우드 가상머신 모니터링 기술

기술키워드	하이퍼바이저, Agentless 보안 모니터링 엔진, 가상 디스크/메모리 분석, 보안 가시성 서비스								
지식재산권	등록 2건(대한민국 1건, 미국 1건)								
기술완성도 (TRL)	기초 실험	개념 정립	기능 및 개념검증	연구실환경 테스트	**시제품 제작**	시제품 성능평가	시제품 신뢰성평가	시제품 인증	상용품

기술개요

- 클라우드 환경 특성에 적합한 하이퍼바이저 기반 보안 모니터링 기술
  - · VM상의 보안기술 우회가 불가능하고 성능저하를 최소화할 수 있는 하이퍼바이저 기반 보안엔진 제공
  - · 가상 디스크 및 메모리 모니터링을 통한 비정상 가상머신 탐지 기능 제공
  - · 가상머신 보안 상태 점검 및 상시 모니터링이 가능한 가상머신 보안 가시성 서비스 제공
- 기술 구성도



기술성

- 기존의 데스크톱 보안 솔루션들은 AV Storm 등 동시다발적 보안 솔루션의 동작으로 인한 성능 저하가 발생하며 개별 솔루션들의 적용으로 보안 솔루션 통합 관리가 어려움
- 기존의 에이전트 기반 중앙집중형 보안 솔루션은 게스트 VM 내에 설치된 에이전트가 정보를 수집하고 별도의 Secure VM에서 보안 태스크를 수행함에 따라 악성코드로 인한 게스트 VM 내 에이전트의 우회 가능성이 존재
- 본 기술은 하이퍼바이저 수준에서 가상 머신 보안 상태를 모니터링하여 비정상 가상머신을 탐지할 수 있는 클라우드 최적화 보안엔진을 제공하여 가상머신 보안 가시성 서비스를 통한 보안 상태 분석 및 복구 기술을 제공함

- 하이퍼바이저 수준 보안엔진을 구동하여 가상 머신 상에 별도의 에이전트를 설치하지 않고 보안 모니터링을 수행하여 에이전트 우회 가능성을 배제함과 동시에 가상머신의 성능 저하를 최소화함으로써 클라우드 인프라 보안성 강화에 기여할 수 있음
- 본 기술은 가상 호스트 보안 상태 점검을 위해 CVE(Common Vulnerability Enumeration), CCE(Common Configuration Enumeration), IOC(Indicator of Compromise) 등의 취약성 데이터베이스를 활용하는 기존 보안 감사 기술과 연동할 수 있으며, 기 개발되어 있는 ETRI의 VDI 서비스 플랫폼인 DaaS(Desktop as a Service)와 연동하여 기술융합을 통한 시너지효과를 창출할 수 있음

시장성

- 클라우드 시장 동향
  - 국내 클라우드 시장 규모는 2016년 약 1조 175억 원으로 추산되었으나, 2020년에는 2조 1800억 원으로 2배 이상 성장할 것으로 전망되며, 세계 클라우드 시장 규모 역시 약 119조에서 232조로 성장할 것으로 전망됨(클라우드 광고 분야 제외)
    ※ 참고자료: 가트너 보고서 "2016-2020년 퍼블릭 클라우드 최종 사용자 지출 전망", '16. 12. 및 '17. 2.
  - 미국, 일본 및 EU 등 여러 국가에서 국가 차원에서의 클라우드 구축을 포함한 정보보안 규정 및 지침 제정, 기술 표준화 시도를 하는 등의 움직임을 보임
- 본 기술은 클라우드 컴퓨팅 환경에 최적화 되어있는 보안 엔진으로 기존 보안 솔루션과 차별화되며 클라우드 컴퓨팅 환경 구축에 사용되는 다양한 가상디스크 포맷을 지원하므로 기존 시스템뿐만 아니라 도입 예정인 클라우드 시스템에서까지 폭넓게 활용할 수 있을 것으로 판단됨

기술 응용 분야

- 클라우드 컴퓨팅을 도입하여 가상머신에 대한 보안 상태를 점검하고 비정상 여부를 복구하는 등 클라우드 보안을 강화하는 기술로서 적용 및 활용이 가능함

관련 특허 등 지식재산권

- (등록) 10-1649909(2016. 8. 16. 대한민국), 9734330(2017. 8. 15. 미국) "가상 머신 취약점 점검과 복구 방법 및 장치"