2018 한국차세대컴퓨팅학회
춘계학술대회

장　소 : 제주 제주한라대학교 컨벤션센터

일　시 : 2018. 5. 25(금) 12:40 ~ 5.26(토) 12:00

주최-주관　한국차세대컴퓨팅학회

후　　원　제주한라대학교 LINC+사업단

2018 한국차세대컴퓨팅학회 춘계학술대회

- **대 회 장** : 백성욱 교수(세종대학교)
- **조직 위원장** : 문석환 교수(제주한라대학교)
- **학술 위원장** : 김덕환 교수(인하대학교)
- **학술부위원장** : 노영태 교수(인하대학교)
- **조직 위원**

  노병희 교수 (아주대학교)
  노상욱 교수 (가톨릭대학교)
  신병석 교수 (인하대학교)
  이상웅 교수 (가천대학교)
  염성관 교수 (제주한라대학교)
  최린 교수 (고려대학교)

- **학술 위원**

  권구락 교수 (조선대학교)
  권준호 교수 (부산대학교)
  김동호 교수 (숭실대학교)
  김황남 교수 (고려대학교)
  나중채 교수 (세종대학교)
  박기웅 교수 (세종대학교)
  박남제 교수 (제주대학교)
  박운상 교수 (서강대학교)
  박준석 교수 (인하대학교)
  석준희 교수 (고려대학교)
  신석주 교수 (조선대학교)
  이문규 교수 (인하대학교)
  이미영 박사 (세종대학교)
  유성준 교수 (세종대학교)
  임완수 교수 (금오공과대학교)
  문인규 교수 (DGIST)
  조성제 교수 (단국대학교)
  최동완 교수 (인하대학교)
  한경식 교수 (아주대학교)
  김시우교수 (숭의여자대학교)

2018 한국차세대컴퓨팅학회 세부 프로그램

2018. 5. 25(금)		
12:40~13:10	등록	
13:10~14:00	Keynote Speech 국방 ICT융합 현황과 활성화방안 / 국방기술품질원 권경용 수석연구원	
14:00~14:30	개회식, 시상식(공로상, 우수논문)	
논문 발표	Oral Session 1	Oral Session 2
14:30~15:30	인터넷 뉴스 댓글 기반의 다중 감정 모델 개발 아주대학교 / 김우정, 한재호, 한경식	그룹 랜덤화를 통한 CCTV 객체 추적 데이터 보안 기법 설계 제주대학교 / 이동혁, 박남제
	컨테이너 이미지의 보안 취약성 데이터 수집 및 분석 경북대학교 / 탁병철	군집화 기반의 불균형 마케팅 데이터 분류 기법 고려대학교 / 손민재, 승원, 황인준
	XGBoost를 활용한 노인인지능력 변화 요인 해석 한국과학기술연구원 / 황혜진, 김수현, 송규원	고객의 소비 패턴 변화를 고려한 영화 추천 단국대학교 / 나연묵, 김민제
	Energy Efficient Adaptive Weighted Sum Function for Routing in WSN 조선대학교 / Madiha Razzaq, Seokjoo Shin	임베디드 환경에서 하드웨어 독립성 기반의 센서 플러그 앤 플레이 인하대학교 / 윤다빈, 박무동, 김덕환
15:30~15:45	Coffee break	
논문 발표	Oral Session 3	Oral Session 4
15:45~17:00	A Survey on Residual Network Evolution 조선대학교 / Abol Basher, Abu Naser Rashid Reza, Samsuddin Ahmed, Ho Yub Jung	무선 공유기 환경설정 트랜잭션 분석을 통한 안전한 무선 공유기 환경설정 자동화 시스템 연구 세종대학교, 공주대학교 / 이세한, 서창호, 박기웅
	블록체인 오픈 소스 SW 조사를 통한 블록체인 아키텍처 분석 아주대학교 / 정윤환, 길우근, 노병희	컨테이너 모니터링 툴 프로파일링을 통한 커버리지 영역 분석 세종대학교 / 김민석, 박기웅
	Efficient CNN based artistic style classifier 세종대학교 / Tanveer Hussain, Khan Muhammad, Ijaz Ul Haq, Irfan Mehmood, Sung Wook Baik	소프트맥스 함수를 이용한 통제되지 않은 환경에서의 강인한 실시간 얼굴 인식 가천대학교 / 원옥광, 사하데브 파우델, 서조드 누를라이브, 이상웅
	Ultrasonic Image Classification Based on Convolutional Neural Network 가천대학교 / Dong Yue Wang, Jun Jie Tian,Taeg Keun Whangbo	디지털 변전소를 위한 지능형 자율 네트워크 관리 기술 동향 인하대학교, 한국전기연구원 / 이왕우, 고화랑, 오휘명, 손상우, 김영선, 최성수, 노영태

	특이 문구 검출을 고려한 LSTM 기반한국어 웹 게시판 조회수 예측 고려대학교 / 김규형, 황인준	인터넷 커뮤니티 분석을 통한 이슈 판별 기법 세종대학교 / 이재유, 박나리
2018. 5. 26(토)		
논문 발표	**Poster Session 1**	**Poster Session 2**
10:00~12:00	조이스틱으로 방향 조정이 가능한 소총 움직임 제어 임베디드 시스템 구현 금오공과대학교 / Angsanto Stephen Ryan, 김명식, 전일수, 임완수	영상의 부분적 영역 추출을 이용한 영상정보 증가 기법 세종대학교 / 우현준, 김미선, 한동일
	온라인 빅데이터를 통한 소비자 선호도의 딥러닝 기반 분석기법 연구 세종대학교 / Dang Lien Minh, 민경복, 임수현, 문현준	LSTM을 이용한 자기장 기반 실내위치인식시스템 고려대학교 / 배한준, 최린
	딥 러닝 기반 사용자 편의 중심의 유실물 통합 관리 시스템의 설계 및 구현 세종대학교 / 유태우, 정하민, 유현수, 김윤욱, 안용학	TPC-H를 활용한 Goldilocks와 MySQL 성능 비교 단국대학교 / 장시형, 최원석, 전성환, 박성원, 신희성, 나연묵
	일반 데스크탑 PC 기반 풀링 기법을 활용한 딥 러닝 네트워크의 성능 향상 세종대학교 / 조주연, 김미선, 우현준, 한동일	영상 인식을 이용한 길고양이 자동급식기 세종대학교 / 이준형, 배연진, 진승언, 정순혁, 권기학, 문현준
	사진 데이터를 이용한 인공지능 사상체질 판별 시스템 가천대학교 / 최규남, 윤경목, 황보택근	A feature-level data fusion method for predicting stock price: a hybrid model based on stacked denoising autoencoders and deep neural network 세종대학교 / Sang Il Lee, Seong Joon Yoo
	oneM2M 표준기반 IoT 플랫폼을 활용한 커넥티비티 환경 및 위치정보 데이터 관리 인하대학교 / 윤준혁, 윤다빈, 박무동, 김덕환	위성 네트워크의 전송지연 최소화를 위한 물리계층 네트워크 코딩 기술 조선대학교, Iowa State University / 최우열, 김태운
	시뮬레이션을 통한 중도 절단된 두 사건의 선행성 분석 고려대학교 / 김유중, 석준희	구글 검색 엔진을 활용한 기술 키워드 관련 기업 검색 시스템 설계 세종대학교 / 이여진, 유성준, 구영현, 정원희, 장다운, 민아영
	열화상 카메라 기반의 영상 분석 및 동체 인지를 통한 가상펜스 설계 세종대학교 / 임수현, 민경복, 남준영, 문현준	VoiceLock:화자인식을 이용한 스마트 자물쇠 세종대학교 / 김도현, 이하영, 정수진, 권기학, 문현준
	랜섬웨어 탐지원리 분석을 통한 탐지 기법 분류 및 한계점 제시 세종대학교, 공주대학교 / 박건호, 최대선, 박기웅	산학협력을 위한 빅데이터 인프라 실증연구 세종대학교, 한국컴퓨팅산업협회 / 신병주, 유성준, 전석봉, 노재춘, 백성욱, 장윤, 우종필, 최준연, 이미영, 강유진, 공영지

	Container Registry를 활용한 CVE 컨테이너 기반 CTF 플랫폼 디자인 세종대학교 / 박준규, 최상훈, 박기웅	PLC 보안성을 강화하기 위한 Sanitizer 구현 단국대학교, 건국대학교 / 최광준, 박준상, 이명건, 조성제, 박민규
	사람 관련 정보를 배제한 이미지 기반 연령 및 성별 예측 모델링 아주대학교 / 조용걸, 전영승, 김보관, 한경식	환경과 활동센싱의 멀티센서를 융합한 인공지능 기반 개인화된 디지털 테라피 케어시스템 설계 아주대학교 / 이주영, 성지훈, 최선탁, 양기훈, 조위덕
	시각 주의 모델을 이용한 비디오 키 프레임 추출에 관한 연구 세종대학교 / Anvarjon Tursunov, Uyen Tran, Nam Pham, Alexandre Larzat, Soonil Kwon, Oh-Jin Kwon, Sung Wook Baik	딥러닝 기반 주식 가격 경향 예측 프레임워크 세종대학교 / 등연명, Syed Ibrahim Hassan, Duong Minh Duc, 문현준
	로그 분석을 위한 로그 템플릿 추출 기법 경북대학교 / 탁병철	블록체인을 활용한 역경매 봉사활동 크레딧 관리시스템 숭의여자대학교 / 김시우, 장명훈
	무선충전 시스템 사용 권한 검증을 위한 보안 요구사항 도출 세종대학교, 전북대학교 / 이양재, 양동민, 박기웅	스마트 미러 스토어 개발 연구 세종대학교 / 양경석, 심효빈, 임다영, 이영걸, 양효식, 주철휘
	Comparison of enhancement techniques for brain Magnetic Resonance Imaging (MRI) Chosun University / Waqas Ellahi, Bumshik Lee	멀티플랫폼을 위한 GIS 애플리케이션 기획 및 구현 세종대학교 / 서성준, 천슬별, 고정민, 남기범, 조상욱
	LSTM을 이용한 주택시장의 순환국면 예측 한국과학기술연구원 / 이관훈, 김수현, 송규원	Python-MATLAB 인터페이스를 이용한 센서데이터의 수치 연산 조선대학교 / 황용운, 이충규
	움직이는 차량에 드론 착륙 방법에 관한 연구 세종대학교 / 박준렬, 우현준, 전영민, 박성호, 김영배, 권기학	무선 센서 네트워크를 위한 반딧불이 생태모방 기반의 동기화 시뮬레이터 설계 및 이의 성능 분석 아주대학교 / 이인태, 노병희
	IoT 빅데이터 딥러닝 시스템 설계 이화여자대학교 / 김경주, 송지현, 이민수	영상에서 슬라이딩 윈도우와 딥러닝 분류 기법을 결합한 드론 인식 기법 세종대학교 / 우현준, 전영민, 박준렬, 권기학
	CNN과 학습전이를 이용한 알츠하이머병의 분류 조선대학교 / 유브라즈 굽타, 권구락	확률론적 허프 변환을 이용한 광전지 모듈 검출 가천대학교 / 크리스 헨리, 박현철, 김세원, 이상웅
	A Brief Overview of Deep Metric Learning Methods 조선대학교 / Samsuddin Ahmed, Abol Basher, Abu Naser Rashid Reza, Ho Yub Jung	A video hash method using SHA-2 for verifying video integrity Chosun University / Sarala Ghimire, Bumshik Lee
	IoT 빅데이터 처리를 위한 규칙 모델 설계 이화여자대학교 / 송지현, 김경주, 이민수	영상처리를 이용한 부표 검출 시스템 동명대학교 / 김경성, 박성은, 전수진, 유종명, 김민철, 신신재, 유선진

	웹 기반 졸업 관리 시스템의 설계 및 구현 세종대학교 / 김효준, 이승용, 고용국, 심재훈, 안용학	Analysis on the effect of patch selection for prediction of Alzheimer's disease Chosun University / Muhammad Ammar Malik, Bumshik Lee
	기계학습을 이용한 전자전 위협체의 역추정 모델링 가톨릭대학교 / 장지원, 박헌우, 노상욱	블록체인 오픈소스SW의 임베디드시스템 구현 및 응용 아주대학교 / 고광표, 노병희
	IoT 서버의 자동차 산업 분야 활용 조선대학교 / 정동일, 정지성, 이충규	게임을 이용한 창의적 코딩교육 시스템 숭의여자대학교 / 김시우
	영아 돌연사 증후군 예방 솔루션 세종대학교 / 육문수, 김태균, 박효완, 신우성, 권기학, 문현준	빅데이터 포털 사이트 온라인 시각화 방법에 관한 연구 세종대학교 / 박성호, 이미영, 이경수, 황준철, 백성욱
	Multi-Site 환경에서 전력 사용량 예측을 위한 프라이버시 보장형 패턴 시퀀스 기반 예측 인하대학교 / 권희용, 임종혁, 이문규	Review on Generative Adversarial Networks Chosun University / Abu Naser Rashid Reza, Samsuddin Ahmed, Abol Basher, Ho Yub Jung
	유사도 기반 검색 결과 개수 비례 순위 기법을 적용한 병해충 검색 시스템 설계 및 구현 세종대학교, 국립원예특작과학원 / 이건훈, 유성준, 구영현, 박철호, 윤학림, 박종한	

Oral Session 4 - (25일/금 15:45 ~ 17:00)

- 무선 공유기 환경설정 트랜잭션 분석을 통한 안전한 무선 공유기 환경설정 자동화 시스템 연구
  / 세종대학교, 공주대학교 / 이세한, 서창호, 박기웅

- 컨테이너 모니터링 툴 프로파일링을 통한 커버리지 영역 분석
  / 세종대학교 / 김민석, 박기웅

- 소프트맥스 함수를 이용한 통제되지 않은 환경에서의 강인한 실시간 얼굴 인식
  / 가천대학교 / 원옥광, 사하데브 파우델, 서조드 누를라이브, 이상웅

- 디지털 변전소를 위한 지능형 자율 네트워크 관리 기술 동향
  / 인하대학교, 한국전기연구원 / 이왕우, 고화랑, 오휘명, 손상우, 김영선, 최성수, 노영태

- 인터넷 커뮤니티 분석을 통한 이슈 판별 기법
  / 세종대학교 / 이재유, 박나리

컨테이너 모니터링 툴 프로파일링을 통한 커버리지 영역 분석

Analysis of coverage area through profiling container monitoring tool

김민석, 박기웅†
Min-Seok Kim and Ki-Woong Park

세종대학교 시스템보안연구실, 세종대학교 정보보호학과†
vin0325@naver.com, woongbak@sejong.ac.kr

요 약

최근 컨테이너 기술이 재조명 받고 있다. 컨테이너는 기존의 가상 머신보다 리소스를 적게 사용하고, 다양한 컴퓨팅 환경에서도 안정적으로 작동하는 장점이 있다. 하지만 커널을 공유함으로써 생기는 취약점과 컨테이너가 오픈소스이기에 생기는 위험 등 다양한 취약점이 있다. 이러한 취약점들로 인해 보안 모니터링 툴이 필요함에 따라 많은 보안 모니터링 툴들이 개발되었다. 하지만 툴마다 모니터링 목적과 대상이 상이하여 모니터링 불가 영역이 존재할 수 있고, 필요에 따라 여러 개의 툴을 설치하여 사용해야하는 불편함이 생긴다. 본 논문에서는 현재 존재하는 대표적인 컨테이너 보안 모니터링 툴들의 기능을 분석하여 모니터링 불가 영역인 실시간 보안 모니터링 툴의 개발 제안과 사용자의 필요에 따라 여러 기능을 선택하여 사용할 수 있는 통합 컨테이너 보안 모니터링 툴 개발을 제안한다.

1. 서론

컨테이너 기술은 최근 들어 다시 각광 받고 있다 [1, 2]. 컨테이너는 OS 레벨 가상화 기술 또는 어플리케이션 레벨 가상화 기술로 커널 영역의 cgroups[3]와 namespace[4] 기술을 사용하여 서로 다른 서버에서 구동되는 듯한 환경을 제공한다. 컨테이너 기술의 장점으로는 기존에 사용하던 가상 머신보다 CPU, 메모리, 디스크 등의 자원을 적게 사용하고, 노트북이나 테스트 환경, 실제 운영환경의 다양한 컴퓨팅 환경에서도 안정적으로 실행되는 장점이 있다. 이러한 장점들로 인해 컨테이너 기술은 재조명 받고 있다.

그렇지만 컨테이너 기술에도 보안 위협은 존재한다. 컨테이너 기술은 커널 영역을 공유하기 때문에 커널이 가지는 취약점을 컨테이너도 동일하게 갖게 된다. 또한 컨테이너는 공유되어 재사용되기 때문에 배포될 때에 취약성을 가진 상태의 컨테이너가 유출되거나 혹은 악성코드가 심겨진 컨테이너가 배포될 수 있다. 이외에도 컨테이너 기반의 플랫폼은 다수의 컨테이너가 동시에 실행되기 때문에 병렬적인 모니터링의 어려움과 컨테이너 엔진에 의해 컨테이너가 실행됨에 따라 생기는 가시성 부족 문제 등 다양한 측면에서의 보안 위협이 있다.

이렇듯 컨테이너의 보안 위험성은 계속 거론되고 있다. 이에 따라 컨테이너의 보안 위협을 탐지하고 사고를 예방하기 위한 보안 모니터링 기술이 필요하게 되었고, 많은 컨테이너 보안 모니터링 툴들이 개발되어 사용되고 있다. 하지만 각 툴마다 기능과 성능이 모두 다르기 때문에 모니터링이 불가한 영역이 발생할 수 있고, 사용자들은 필요한 기능과 성능을 가진 툴들을 여러 개 설치해야하는 불편함을 감수해야한다.

따라서 본 논문에서는 기존 컨테이너 보안 모니터링 툴들의 커버리지 영역 이외의 곳을 모니터링하기 위한 툴 개발과 각 툴이 가진 기능과 성능을 사용자의 필요와 상황에 따라 기능과 성능을 선택하여 사용할 수 있는 통합 보안 모니터링 툴의 개발을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 컨테이너 보안 위협 관련 연구에 대해 서술하고, 3장에서는 현재 사용되고 있는 대표적인 오픈소스 및 상용 컨테이너 보안 툴들의 주요 기능을 분석하고 분석 결과를 기반으로 컨테이너 보안 모니터링 툴의 커버리지 영역과 개발 방향을 도출한다. 4장에서는 결론을

† 교신저자: 박기웅 (세종대학교 정보보호학과 교수)

이 논문은 한국연구재단 지원사업(2017R1C1B2003957) 및 2018년도 과학기술정보통신부의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2018-0-00420, API 호출 단위 자원 할당 및 사용량 계량이 가능한 서버리스 클라우드 컴퓨팅 기술 개발)

기술한다.

2. 컨테이너 보안 위협

컨테이너 보안 위협 중 하나는 컨테이너가 운영체제 레벨에서 가상화를 실시하여 운영체제 커널에서 직접 구동되기 때문에 커널을 공유함으로써 커널이 가지고 있는 취약점들을 컨테이너도 갖게 되는 것이다. Dirty Cow[5, 6] 취약점이나 waitid[7] 취약점 등의 커널 취약점을 이용하여 인가되지 않은 사용자가 관리자 권한을 얻어[8] 컨테이너 내의 데이터를 탈취 및 컨테이너 기능 정지와 같은 공격이 가능해진다는 것이다. 또한 호스트 운영체제의 관리자 권한으로 실행되는 것을 이용하여 컨테이너를 탈출하여 관리자 권한을 얻게 될 수도 있다. 이는 구동중인 컨테이너를 공격하거나 정지시킬 수 있고, 다른 컴퓨터도 공격할 수 있음을 의미한다.

추가적으로 레지스트리와 이미지의 배포와 사용이 자유롭다는 것도 보안 위협이 된다[9]. 오픈소스인 컨테이너는 누구나 레지스트리나 이미지를 만들 수 있고, 배포할 수 있다. 이 과정에서 보안에 무지하거나 둔감한 개발자가 취약한 레지스트리 또는 이미지를 배포하게 되거나, 악의를 가진 개발자가 트로이 목마와 같은 악성코드를 심어 배포하는 일이 발생할 가능성이 있음을 의미한다.

3. 컨테이너 보안 모니터링 툴

현재 사용되고 있는 대표적인 오픈소스 및 상용 컨테이너 보안 모니터링 툴들의 주요 기능을 분석하고 컨테이너 구조별 모니터링 부분을 맵핑하였다.

3.1 오픈소스 컨테이너 보안 모니터링 툴

오픈소스 컨테이너 보안 모니터링 툴은 별도의 비용 지불 없이 자유롭게 다운 받아서 사용할 수 있는 보안 모니터링 툴이다. 현재 사용되고 있는 오픈소스 컨테이너 보안 모니터링 툴 중 Anchore Navigator, Sysdig, Cilium 등 대표적인 19개의 툴을 분석하였다.

<표 1> 오픈소스 컨테이너 보안 모니터링 툴 목록과 기능

툴	기 능
Anchore Navigator[10]	이미지 검사
AppArmor[11]	실시간 보호
Cilium[12]	실시간 보호, 리소스 모니터링
CoreOS Clair[13]	이미지 검사
Docker capabilities and resource quotas[14, 15]	실시간 보호
Docker-bench security[16]	검사 자동화 스크립트
Dockscan[17]	검사 자동화 스크립트
Falco[18]	행위 모니터링
HashiCorp Vault[19]	보안 저장소(암호, API키 등)
Notary[20]	이미지 위변조 공증
OpenSCAP[21]	이미지 검사
REMnux[22]	통합 분석 도구
SELinux[23]	실시간 보호
Seccomp[24]	실시간 보호
Sysdig[25]	리소스 모니터링
Banyan collector[26]	이미지 검사
Drydock[27]	검사 자동화 스크립트
Batten[28]	검사 자동화 스크립트
Dagda[29]	이미지 검사

오픈소스 보안 모니터링 툴 중에는 Anchore Navigator나 HashiCorp Vault와 같이 추가적으로 금액을 지불하면 더 많은 기능을 수행하는 툴도 있지만, 본 논문에서는 오픈소스 기반에서 기능을 분석하였다. 표 1에서 각 툴들의 기능들을 살펴보면 대부분의 툴이 이미지 검사, 실시간 보호(Run-time protection), 리소스 모니터링, 검사 자동화 스크립트를 수행하고 있으며 이외에도 이미지 위변조 공증(Notary), 행위 모니터링(Falco)과 같은 추가적인 기능을 수행하는 툴이 있다.

3.2 상용 컨테이너 보안 모니터링 툴

상용 컨테이너 보안 모니터링 툴은 매달 혹은 매년 일정 금액을 지불하고 컨테이너에 대한 보안 모니터링 기능을 제공하는 툴을 의미한다. 현재 사용되고 있는 AquaSec, Cavirin, StackRox 등과 같은 대표적인 8개의 툴을 분석하였다.

<표 2> 상용 컨테이너 보안 모니터링 툴 목록과 기능

툴	기 능
AquaSec[30]	이미지 검사, 실시간 보호
BlackDuck Docker Security[31]	이미지 검사
Cavirin[32]	이미지 검사
NeuVector[33]	실시간 보호
StackRox[34]	이미지 검사, 실시간 보호
Sysdig Secure[35]	리소스 분석
Tenable Flawcheck[36]	이미지 검사
Twistlock[37]	이미지 검사, 실시간 보호

<표 2>에 기반 하여 컨테이너 보안 모니터링 상

용 툴의 기능을 보면 컨테이너 이미지 보안 검사, 컨테이너 내부 동작 탐지, 실시간 보호(Run-time protection)를 수행하는 것을 볼 수 있다.

3.3 컨테이너 보안 모니터링 툴 커버리지 영역 분석

현존하고 있는 컨테이너 보안 모니터링 툴들 중 대표적인 오픈소스 컨테이너 보안 모니터링 툴과 상용 컨테이너 보안 모니터링 툴을 분석하였고, 분석 결과를 바탕으로 컨테이너 보안 모니터링 툴들의 커버리지 영역을 알아보기 위해 그림 2와 같이 컨테이너 구조 중 기능이 적용되는 부분에 맵핑하였다. 본 논문에서 분석한 27개의 컨테이너 보안 모니터링 툴들은 컨테이너 구조 중 모니터링이 필요한 모든 부분을 대상으로 보안 모니터링을 수행하는 것으로 분석되었다.

하지만 본 논문에서 분석한 컨테이너 보안 모니터링 툴 중에는 실시간으로 보안 모니터링을 수행하는 툴은 없었다. 또한 컨테이너 보안 모니터링 툴들이 같은 부분을 모니터링 하더라도 툴마다 수행하는 상세한 기능은 조금씩 달랐다. 이는 같은 부분을 모니터링 하여도 툴이 수행하는 상세한 기능이 다르기 때문에 필요한 툴들을 모두 설치해야하는 상황이 생길 것으로 예상된다.

4. 결론

본 논문에서는 기존에 있던 대표적인 컨테이너 보안 모니터링 툴의 기능들의 커버리지 영역을 분석하고 모니터링 불가 영역을 파악하여 해당 영역을 모니터링하기 위한 툴 개발과 사용자의 필요와 상황에 따라 기능과 성능을 선택하여 사용할 수 있는 통합 컨테이너 보안 모니터링 툴 개발을 제안하였다. 이를 위하여 현재 존재하고 있는 대표적인 오픈소스, 상용 컨테이너 보안 모니터링 툴 27개의 기능을 분석하고, 각 툴의 기능별로 컨테이너의 모니터링 부분을 맵핑하여 보았다. 그 결과 보안 모니터링이 필요한 부분의 모든 부분을 모니터링 하는 것을 확인하였지만 실시간으로 모니터링 하는 기능이 없음을 확인하였다. 또한 각 툴별로 컨테이너를 모니터링 하는 부분이 다른 경우도 있지만, 같은 부분을 모니터링 함에도 상세한 기능이 다른 경우가 있어 사용자가 필요한 기능을 가진 툴들을 모두 설치하여 사용해야 하는 불편함이 따를 수 있음을 확인했다. 추후 연구에서는 실시간 컨테이너 보안 모니터링 툴과 통합 컨테이너 보안 모니터링 툴을 연구 및 개발을 할 예정이다.

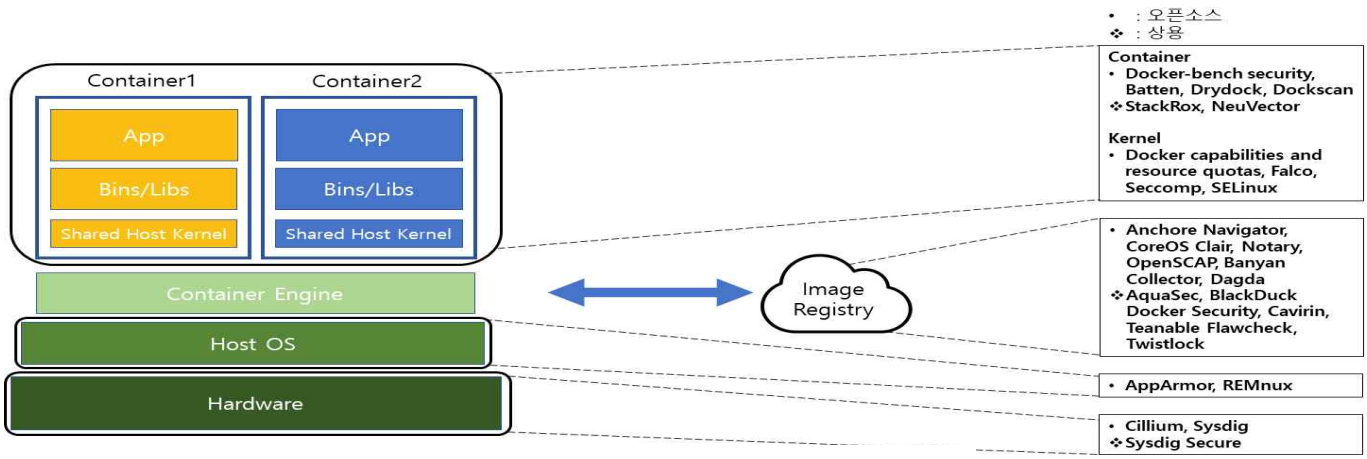
참고문헌

[1] Davide Mulfari, Maria Fazio, Antonio Celesti, “Design of an IoT Cloud System for Container Virtualization on Smart Objects.” Advances in Service-Oriented and Cloud Computing pp 33-47 (2015)

[2] Antonio Celesti, et al. “Exploring Container Virtualization in IoT Clouds.” Smart Computing (SMARTCOMP), 2016 IEEE International Conference on

[3] Paul Menage. “CGROUPS.” Available online at : https://www.kernel.org/doc/Documentation/cgroup-v1/cgroups.txt

[4] Pam Baker “Understanding and Securing Linux Namespaces.” Available online at : https://www.linux.com/news/understanding-and-securing-linux-namespaces(2016.10.18)



(그림 1) 툴 기능별 컨테이너 모니터링 부분 맵핑

[5] A.P. Saleel, Mohamed Nazeer, Babak D. Beheshti “Linux kernel OS local root exploit” Systems, Applications and Technology Conference (LISAT), 2017 IEEE Long Island

[6] Delwar Alam et al. “Study of the Dirty Copy on Write, a Linux Kernel memory allocation vulnerability” Consumer Electronics and Devices (ICCED), 2017 International Conference on

[7] Daniel Shapira. “Escaping Docker container using waitid() - CVE-2017-5123.” Available online at : https://www.twistlock.com/2017/12/27/escaping-docker-container-using-waitid-cve-2017-5123/(2017.12.27)

[8] Delwar Alam et al. “Study of the Dirty Copy on Write, a Linux Kernel memory allocation vulnerability” Consumer Electronics and Devices (ICCED), 2017 International Conference on

[9] Theo Combe, Antony Martin, Roberto Di Pietro “To Docker or Not to Docker: A Security Perspective.” IEEE Cloud Computing(Volume: 3, Issue: 5, Sept.-Oct. 2016)

[10] Andrew Cathrow. “Introducing Anchore Navigator” Available online at : https://anchore.com/blog/introducing-anchore-navigator/(2016.10.4)

[11] Steve Beattie. “About” Available online at : https://gitlab.com/apparmor/apparmor/wikis/About (2017.11)

[12] Cilium. “Introduction to Cilium.” Available online at : http://docs.cilium.io/en/latest/intro/#why-cilium

[13] Quentin Machu. “CoreOS Introduces Clair: Open Source Vulnerability Analysis for your Containers.” Available online at : https://coreos.com/blog/vulnerability-analysis-for-containers.html (2015. 11. 13)

[14] Lab: Control Groups (cgroups). Available online at : https://github.com/docker/labs/blob/master/security/cgroups/README.md

[15] Lab: Capabilities. Available online at : https://github.com/docker/labs/blob/master/security/capabilities/README.md

[16] Docker Bench for Security. Available online at : https://github.com/docker/docker-bench-security/blob/master/README.md

[17] dockscan. Available online at : https://github.com/kost/dockscan

[18] Mark Stemm. “About Falco” https://github.com/draios/falco/wiki/About-Falco (2016. 12. 22)

[19] What is Vault. Available online at : https://www.vaultproject.io/intro/index.html

[20] Notary. Avalilable online at : https://github.com/theupdateframework/notary

[21] OpenSCAP User Manual. Available online at : https://static.open-scap.org/openscap-1.2/oscap_user_manual.html

[22] REMnux Docs. Available online at : https://remnux.org/docs/

[23] INTRODUCTION TO SELINUX. Available online at : https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/5/html/deployment_guide/ch-selinux

[24] SECure COMPuting with filters. Available online at : https://www.kernel.org/doc/Documentation/prctl/seccomp_filter.txt

[25] sysdig. Available online at : https://github.com/draios/sysdig

[26] Banyan Collector: A framework to peek inside containers. Available online at : https://github.com/banyanops/collector

[27] What is drydock? Available online at : https://github.com/zuBux/drydock

[28] batten - Docker Audit Toolkit. Available online at : https://github.com/dockersecuritytools/batten

[29] Dagda. Available online at : https://github.com/eliasgranderubio/dagda

[30] AQUA CONTAINER SECURITY PLATFORM. Available online at : https://www.aquasec.com/products/aqua-container-security-platform/

[31] Container Security. Available online at : https://www.blackducksoftware.com/solutions/container-security

[32] Docker. Available online at : https://cavirin.com/solutions/cloud-containers/docker.html

[33] The Industry’s First Multi-Vector Container Firewall. Available online at : https://neuvector.

com/run-time-container-security/
[34] PREVENTION, DETECTION, AND RESPONSE FOR CONTAINERS. Available online at : https://www.stackrox.com/overview/
[35] Tenable Acquires FlawCheck. Available online at : https://www.tenable.com/flawcheck
[36] Why Twistlock? Available online at : https://www.twistlock.com/