호스트 기반 침입 탐지 데이터 분석 비교

박대경, 신동규, 신동일
세종대학교 컴퓨터공학과
dkpark@sju.ac.kr, shindk@sejong.ac.kr, dshin@sejong.ac.kr

A Host-based Intrusion Detection Data Analysis Comparison

DaeKyeong Park, Dongkyoo Shin, Dongil Shin
Dept. of Computer Engineering, Sejong University

요 약

오늘날 정보통신 기술이 급격하게 발달하면서 IT 인프라에서 보안의 중요성이 높아졌고 동시에 APT(Advanced Persistent threat)처럼 고도화되고 다양한 형태의 공격이 증가하고 있다. 점점 더 고도화되는 공격을 조기에 방어하거나 예측하는 것은 매우 중요한 문제이며, NIDS(Network-based Intrusion Detection System) 관련 데이터 분석만으로는 빠르게 변형하는 공격을 방어하지 못하는 경우가 많이 보고되고 있다. 따라서 HIDS(Host-based Intrusion Detection System) 데이터 분석을 통해서 위와 같은 공격을 방어하는데 현재는 침입탐지 시스템에서 생성된 데이터가 주로 사용된다. 하지만 데이터가 많이 부족하여 과거에 생성된 DARPA(Defense Advanced Research Projects Agency) 침입 탐지 평가 데이터 세트인 KDD(Knowledge Discovery and Data Mining) 같은 데이터로 연구를 하고 있어 현대 컴퓨터 시스템 특징을 반영한 데이터의 비정상행위 탐지에 대한 연구가 많이 부족하다. 본 논문에서는 기존에 사용되었던 데이터 세트에서 결여된 스레드 정보, 메타 데이터 및 버퍼 데이터를 포함하고 있으면서 최근에 생성된 LID-DS(Leipzig Intrusion Detection-Data Set) 데이터를 이용한 분석 비교 연구를 통해 앞으로 호스트 기반 침입 탐지 데이터 시스템의 나아갈 새로운 연구 방향을 제시한다.

1. 서론

오늘날 정보통신 기술이 급격하게 발달하면서 IT 인프라에서 보안의 중요성이 높아졌고 동시에 사이버상의 공격은 지능형 지속 공격(APT)처럼 고도화 되고 지능적으로 다양해지고 있다. 점점 더 고도화되는 공격을 방어하는 것은 매우 중요한 문제인데, IDS(Intrusion Detection System) 발달 속도가 빠르게 변형되는 공격을 완벽하게 막지는 못한다. HIDS 데이터 분석을 통해서 위와 같은 공격을 방어하는데 현재는 침입탐지 시스템에서 생성된 데이터가 주로 사용된다.[1] 침입탐지 시스템은 네트워크 기반인 NIDS, 호스트 기반인 HIDS 두 가지 방식으로 나눌 수 있다. 네트워크기반 침입탐지 시스템과 달리 호스트 기반 침입탐지 시스템은 시스템 내부와 외부를 전체적으로 모니터링 해야 하는 어려움 때문에 연구가 많이 부족하고 침입탐지 시스템은 새로운 공격 및 내부 공격에 의해 방어 대책이 미흡하고 오경보가 증가하는 문제점이 있다. 호스트 기반 침입탐지 시스템 방식은 오용 탐지와 이상 탐지 2가지 방법으로 나눌 수 있다.[2] 오용 탐지 방법은 시그니처 기반으로 공격을 탐지하기 때문에 기존의 공격을 탐지하는 것은 효과적이지만 반면에 새로운 공격에 대한 탐지는 부적합하다. 이상 탐지 방법은 오용 탐지 방법과 반대로 정상적인 동작 및 행위로 정의된 상태가 아닌 것에 대한 모든 상황을 이상 행위로 판단하여 탐지하게 된다. 즉 오용 탐지 기법과 달리 제로 데이 공격에 대한 탐지에는 적합하지만 정상 동작 및 이상 행위를 판단할 수 있는 많은 데이터가 요구되거나 데이터가 너무 부족하여 기계 학습에 적용하기에는 어려움이 있다.[3]

본 연구에서는 LID-DS(Leipzig Intrusion Detection-Data Set) 데이터 세트와 이전에 공개되었던 UNM (University of New Mexico)과 ADFA(Australian Defence Force Academy) 호스트 침입탐지 시스템 데이터 세트들을 비교 분석하고 LID-DS 데이터 세트와 기계 학습을 이용한 호스트 기반 침입탐지 시스템의 새로운 연구를 제시한다.

2. 관련 연구

KDD 및 UNM 데이터 세트는 공개적으로 사용이 가능한 데이터이며 침입탐지 시스템의 검증의 기초가 되고 성능 테스트의 기준이 되어 많은 연구들이 진행되고 있다. 하지만 일부 네트워크 정보 중에서 시스템 호출을 통해 프로세스와 커널 간에 전달되는 데이터 형식으로 호스트에서 수집 된 추적을 제공하는데 기존의 데이터들은 더 이상 현대적인 특징을 가지고 있지 않기 때문에 최신 컴퓨터 시스템의 다양한 특징들과 공격 특징들이 반영되지 않아 새로운 데이터가 필요하다.[4,5,6]

프로세스 활동이 여러 프로세스에 분산되어있는 유형의 공격은 프로세스의 활동을 특정 프로그램에 따라 분류되지 않고 여러 프로그램에서 무차별 적으로 수집해야 하는데 ADFA 데이터 세트에서는 정상과 비정상의 분리성이 약하다. 짧은 시퀀스 모델을 기반으로 SVM(Support Vector Machine)알고리즘을 적용하여 중복 된 엔트리는 짧은 시퀀스에 제거되고 정상과 비정상 사이의 기준이 명확해 지기 때문에 기준점이 더 선명해 진다. 또한 시스템 콜 기반으로 구성되어 있는 호스트 기반 침입탐지 시스템 방식을 평가하기 위해 시스템 특징들을 반영하고 있으며 리눅스와 윈도우에 따른 많은 공격 패턴들을 포함하고 있어 많은 연구가 진행되고 있다.[4,5,7,8]

3. 본론

3.1 LID-DS Dataset

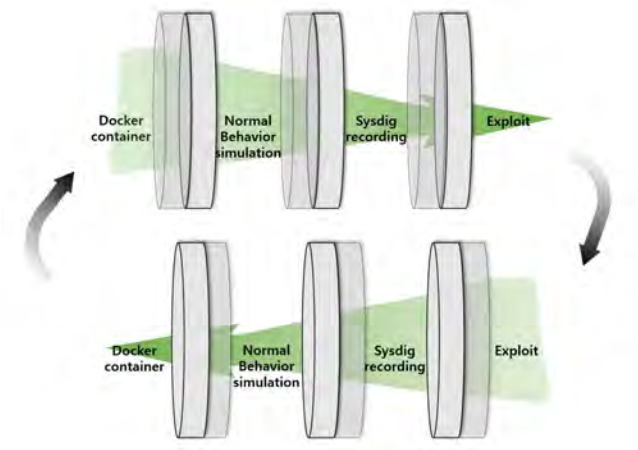
본 논문에서 사용한 LID-DS 데이터 세트는 1990년대 후반, 호스트 기반 침입 탐지 시스템을 연구하기 위해 처음 만들어진 KDD 데이터는 현재까지도 많은 연구자들이 이용하고 있지만 KDD 데이터는 너무 오래된 컴퓨터 시스템의 특징과 공격 패턴으로 이루어져 있어 현재 사용하기에는 적합하지 않다. 2018년 Leipzig University에서 호스트 기반 침입탐지 시스템의 이상 탐지 연구를 위한 LID-DS 데이터 세트를 공개하였다. LID-DS 데이터 세트는 기존 공개되었던 데이터들과 다르게 현재 공개된 데이터 세트들 보다 최신 컴퓨터 시스템의 다양한 특징들과 공격 방법 및 시나리오로 구성되어 있다. LID-DS 데이터를 통해 기존에 데이터 세트들의 데이터가 부족하여 기계학습에 적용하기 어려웠던 부분을 해결하고 기계학습 방법을 이용하여 새로운 이상 행동들을 더 정확하게 탐지하여 차단할 수 있다. 이를 통해 침입탐지 시스템의 문제점인 오경보율을 줄일 수 있다.[4,7,8.9]

LID-DS 데이터 세트는 시스템 호출과 관련된 다양한 데이터가 포함되어 있으며 소프트웨어와 다양한 공격이 기록된다. LID-DS 데이터 세트는 표 1과 같이 공격 방법과 여러 시나리오로 구성되며 시나리오를 통해 정상적인 데이터, 비정상적인 데이터를 생성하고 기록하는 프로세스를 구성할 수 있다.

<표 1> LID-DS 데이터에 저장된 공격방법

데이터 종류	설 명
CVE-2012-2122	동일한 잘못된 암호로 반복적으로 인증하여 공격자가 인증을 우회할 수 있다.
CVE-2014-0160 Heartbleed	서버에 메모리 내용 즉 비밀 키, 데이터에 엑서스 가능
CWE-307 무분별한 인증 시도	무차별 대입 사용자 이름 및 암호 추측 시도
CWE-89 SQL Injection	공격 데이터를 SQL 명령 변수에 삽입
CWE-434 무분별한 파일 업로드 (PHP)	PHP 스크립트와 같은 위험한 유형의 파일을 업로드 할 수 있다.
CVE-2014-3120 임의 코드 실행	공격자가 임의의 Java 코드를 실행할 수 있도록 한다.
CVE-2015-1427 임의 코드 실행	공격자가 임의의 셸 명령을 실행할 수 있도록 한다.
CVE-2017-7529	검사되지 않은 프로그램 코드가 평가 된 후 실행될 수 있도록 한다.
CVE-2018-3760	응용 프로그램의 루트 디렉터리 외부에 있는 파일 시스템에 엑세스할 수 있다.
CVE-2019-5418	조작 된 수락 헤더로 인해 공격 대상 시스템의 파일 시스템에 있는 임의의 파일 내용을 취득할 수 있다.
Zip slip	공격자가 광범위 하게 임의의 파일을 덮어 쓰기를 할 수 있다.
CWE-434 무분별한 파일 업로드 (EPS)	서비스가 다른 이미지 형식의 이미지를 svg 파일 형식으로 변환 후 eps를 사용하여 이미지에 악성 코드를 포함 시킨다.

그림 1은 공격 시나리오를 기록하기 위한 과정이다. LID-DS 데이터 세트의 결과 시스템 호출 추적을 기록하기 위해 공격 대상은 초기 상태를 정의하고 각 공격 후 초기 상태로 되돌리기 위해 Docker10 컨테이너 가상화 소프트웨어 내에서 실행된다. 기록을 위해 LID-DS 프레임 워크를 이용하여 먼저 공격 대상을 호스팅 하는 Docker 컨테이너를 시작하고 그 다음 시나리오에 따라 초기화 작업이 실행되며 정상 동작의 시뮬레이션이 시작된다. 그 후 Sysdig이 활성화되기 전에 짧은 시간동안 기다린다. 이 시간은 Sysdig가 공격 대상 소프트웨어의 시작 효과를 기록하지 못하게 해야 한다. 공격 동작을 기록하는 경우 임의의 시간이 지나면 공격이 시작 되는데 원하는 시간 동안 녹화가 실행 된 후 제어 스크립트에 의해 녹화가 중지 된다. 또한 정상적인 동작 및 사용 된 Docker 컨테이너의 시뮬레이션을 중지하고 제거한다.



(그림 1) LID-DS 데이터 세트의 공격 시뮬레이션 절차

그림 2는 그림 1의 방법으로 생성된 LID-DS의 정상 데이터와 공격 데이터, ADFA의 정상 데이터와 공격 데이터양을 비교하였다.

(그림 2) HIDS 데이터와 공격 데이터 분류

기존에 사용하는 데이터 세트들의 데이터양이 부족하여 기계 학습에 적용하지 못하였다. 반면에 LID-DS 데이터는 시나리오를 통하여 직접 데이터를 생성하기 때문에 방대한 양의 데이터를 수집할 수 있게 된다. 그림 1을 이용하여 생성된 데이터는 표 2의 형식대로 저장된다.

<표 2> LID-DS 데이터의 속성

속 성	설 명
event_number	이벤트 발생 넘버
event_time	고정밀 타임스탬프
cpu	사용된 CPU
user_uid	사용자 UID
process_name	프로세스 이름
thread_id	스레드 ID
event_direction	Enter(>)/Exit(<)
event_type	이벤트 유형
event_arguments	인수 및 반환 값

ADFA 데이터 세트는 일련의 시스템 호출 ID만 포함하고 현대의 공격 패턴을 포함하지 않기 때문에 ADFA 데이터 세트를 이용하여 이상 탐지 테스트를 하기 에는 적절하지 않다.[10]

LID-DS의 데이터 파일 자체의 형식은 표 3과 같다. ADFA와 다르게 LID-DS 데이터에는 시스템 호출의 인수, 반환 값, 고정밀 타임스탬프, 해당 프로세스 이름 및 데이터 버퍼의 내용이 포함되어 있다.[11]

<표 3> LID-DS 저장된 데이터

8 13:16:35.219910910 1 33 apache2 21486 < epoll_wait res=1
9 13:16:35.219919842 1 33 apache2 21486 > accept flags=0

3.2 제안점

LID-DS의 타임스탬프의 값은 기존에 존재하는 데이터들의 타임스탬프 보다 초 단위 까지 측정하는 고정밀 값을 측정하기 때문에 시계열 분석을 통해 기계 학습 하여 이상 탐지를 할 수 있다. 시계열 분석은 과거와 현재의 분석에 대해서는 매우 정확하고 사람의 개입이 필요한 이상 징후 탐지 과정을 거치지 않는다. 결과적으로 데이터 또는 문제에 알맞은 특징을 이상 탐지 하는 효과를 나타내게 되고, 이는 학습에 사용했던 데이터 세트의 범위에 따라 이상 탐지 정확성을 높일 수 있을 것 이다.[12]

LID-DS는 기존의 데이터 세트와 다르게 데이터 버퍼를 저장한다. 저장된 데이터 버퍼를 이용하여 공격자가 특정 공격을 수행하기 전에 나타나는 패턴들을 기계 학습 하여 공격 직전에 미리 탐지하여 이상 탐지 정확성을 높일 수 있을 것 이다.

4. 결론 및 추후 연구

본 논문에서 소개하는 LID-DS 데이터 세트는 관련 연구에서 언급 한 이전 데이터 세트의 문제점이였던 시스템의 최신 보안 취약점을 최신 상태로 유지했으며 기본 스레드 정보가 사라지지 않고 새로운 유형의 HIDS를 평가하는 데 사용할 수 있는 방식으로 데이터를 기록한다. 표 4는 앞서 언급 한 데이터 세트들의 속성에 대한 비교이다.

<표 4> 데이터 세트 속성 비교

속 성	LID-DS	ADFA-LD	UNM	KDD99
Arguments	o	x	x	o
Returnvalues	o	x	x	o
Timestamps	o	x	x	o
Process ID	o	x	o	o
Not outdated	o	o	x	x
Data buffers	o	x	x	x
Amount of data	o	x	x	o

추후에는 LID-DS 데이터 세트로 기록된 정상적인 데이터와 비정상적인 데이터를 이용하여 초 단위까지 기록하는 타임스탬프 속성을 가지고 시계열 분석을 통하여 기계 학습을 진행한 후 이상 탐지 하는 연구를 진행할 계획이다. 또한 특정 공격이 시작되기 전에 데이터 버퍼에서 반복되는 현상들을 기계학습을 통해 이상 탐지 하는 방법과 앞서 제시한 두 가지 방법으로 새로운 공격이나 내부 공격자에 대한 탐지 정확도를 올리기 위한 연구 계획하고 있다.

Acknowledgement

본 연구는 방위사업청과 국방과학연구소의 지원으로 수행 되었습니다 (UD190016ED).

참고문헌

[1] Su, Yunfei, et al. "A framework of apt detection based on dynamic analysis." 2015 4th National Conference on Electrical, Electronics and Computer Engineering. Atlantis Press, 2015.

[2] 최윤정, and 박승수. "이상탐지 (Anomaly Detection) 및 오용탐지 (Misuse Detection) 분석의 정확도 향상을 위한 개선된 데이터마이닝 방법 연구." 한국정보과학회 학술발표논문집 (2006): 238-240.

[3] 최승오, and 김우년. "제어시스템 침입탐지 시스템 기술 연구 동향." 정보보호학회지 24.5 (2014): 7-14.

[4] Mouttaqi, Tarik, Tajjeeddine Rachidi, and Nasser Assem. "Re-evaluation of combined Markov-Bayes models for host intrusion detection on the ADFA dataset." 2017 Intelligent Systems Conference (IntelliSys). IEEE, 2017.

[5] O. Yavanoglu and M. Aydos, "A review on cyber security datasets for machine learning algorithms," 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, 2017, pp. 2186-2193.

[6] Pendleton, Marcus, and Shouhuai Xu. "A dataset generator for next generation system call host intrusion detection systems." MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM). IEEE, 2017.

[7] Creech, Gideon, and Jiankun Hu. "A semantic approach to host-based intrusion detection systems using contiguousand discontiguous system call patterns." IEEE Transactions on Computers 63.4 (2013): 807-819.

[8] Xie, Miao, and Jiankun Hu. "Evaluating host-based anomaly detection systems: A preliminary analysis of adfa-ld." Image and Signal Processing (CISP), 2013 6th International Congress on. Vol. 3. IEEE, 2013.

[9] Röhling, Martin Max, et al. "Standardized container virtualization approach for collecting host intrusion detection data." 2019 Federated Conference on Computer Science and Information Systems (FedCSIS). IEEE, 2019.

[10] Khraisat, Ansam, et al. "Survey of intrusion detection systems: techniques, datasets and challenges." Cybersecurity 2.1 (2019): 20.

[11] Grimmer, Martin, et al. "A modern and sophisticated host based intrusion detection data set." IT-Sicherheit als Voraussetzung für eine erfolgreiche Digitalisierung (2019): 135-145.

[12] 문성은, et al. "기계학습 및 딥러닝 기술동향." 한국통신학회지 (정보와통신) 33.10 (2016): 49-56.