사이버공격 실시간 추적 가시화 시스템

KiSTi 한국과학기술정보연구원 Korea Institute of Science and Technology Information www.kisti.re.kr

특 허 명 공격자 가시화 방법 및 장치 외 3건

Keyword 보안솔루션, IDS, IPS, 가시화

발 명 자 송중석 외 3명

기 술 성

기술 개요

- 본 특허는 IP 주소에 대한 공격(이상행위)을 실시간 및 통계적으로 가시화함으로써 사이버공격의 근원지와 구조 등을 직관적으로 분석할 수 있는 환경을 제공하는 가시화 시스템에 관한 기술임

기존 기술 문제점

- 개별 IP주소의 이상행위에 대한 상세분석과 실제 공격을 유발하는 IP주소에 관한 장시간 사이버공격과 직접적인 탐지 분석은 불가능
- 추적 정보를 통계값 및 표 등으로 단순하게 표현하기 때문에 보안관제 요원들이 단편적인 텍스트 정보만을 다뤄야 하는 보안 업무의 비효율적 문제 발생
- 기존의 보안이벤트(IP주소, 포트, 프로토콜 등) 기술은 중점적으로 모니터링할 공격자IP를 선정할 수 있는 기술적 부재 존재

기술의 특징 및 우수성

▶ 기술의 특징

- 침해위협관리시스템(TMS)과 침입탐지 방지시스템(IDS·IPS) 등을 탐지한 보안 로그를 실시간으로 처리할 수 있음
- 가시화 시스템 기술로 신·변종 사이버위협을 탐지와 이상행위를 3차원 그래픽 정보를 제공하고 기존 정보와 상관관계를 분석해 제공함으로써 사이버 위협 탐지 업무 수행이 가능
- 공격자 상관정보 가시화 기술은 별도의 알고리즘 없이 악성 IP를 직관적으로 탐지할 수 있음

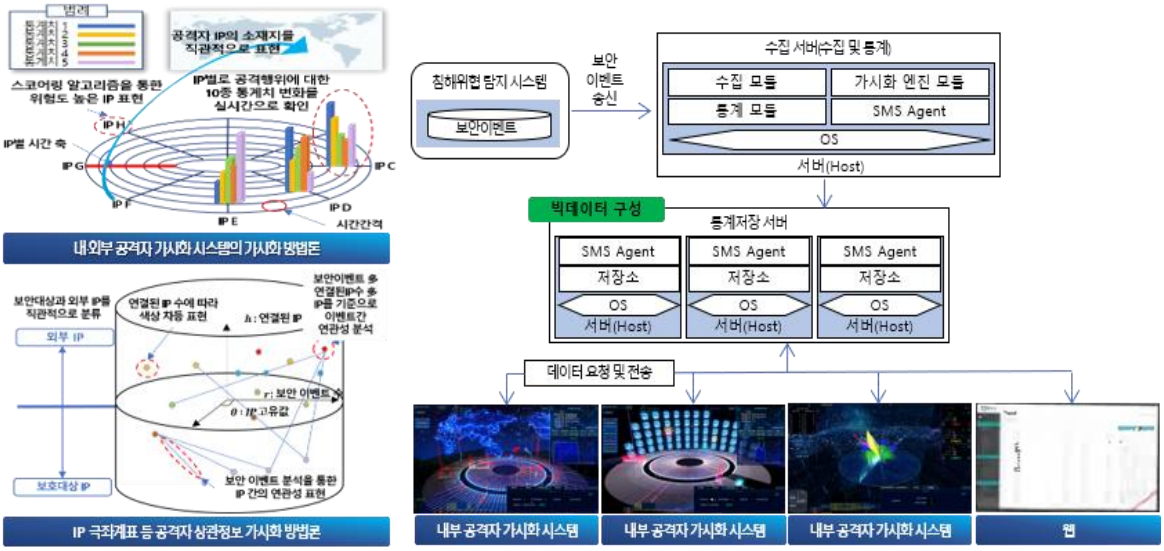
▶ 기술의 우수성

- 실시간 및 통계적 가시화에 기반한 모든 IP의 실제 공격행위 여부를 직관적으로 탐지 및 분석하여 업무 효율성 높일 수 있음
- 공격자 상관정보 가시화 장치는 추가적인 알고리즘이 없이 가시화가 가능하여, 데이터를 일정하게 표현함으로써 왜곡없이 분석결과의 신뢰성을 향상할 수 있음
- 이상행위를 수집하기 위해 대용량 보안정보를 장시간 수집하고 다양한 정보를 조합하여 가시화 가능

사이버공격 실시간 추적 가시화 시스템

상세설명

- 본 기술의 전처리 모듈은 스토리지부터 출발지 정보(출발지 IP주소 등), 목적지 정보(도착지 IP 등), 발생 시간 등이 포함되어 있는 보안이벤트를 수신하여 정보를 추출하고, 통계정보 모듈은 보안이벤트의 대상기관의 내·외부 공격자IP 주소의 구분 등에 관한 통계정보를 생성함
- 가시화 모듈은 보안이벤트의 공격행위를 가시화하는 모듈로 내·외부 공격자 및 공격자 상관정보 가시화 기술로 분류할 수 있음
- 내·외부 공격자 가시화는 24시간 동안 실시간으로 공격행위를 추적 및 분석하여 시각화하는 것으로 매 분마다 이상행위 의심수준이 높은 500개의 IP에 대한 정보를 원반에 배치하고 장기간 및 실시간 행위를 지속해서 관찰할 수 있는 가사화 기술임
- 공격자 상관정보 가시화는 가상의 공간(원통)에 IP정보, 연결된 IP개수, 보안이벤트 수 등의 정보에 기초하여 연관관계에 있는 IP를 연결하여 상관관계를 표현 및 분석 후 100만개의 IP 정보를 3차원으로 가시화 하는 기술임



기술완성도 (TRL)

기술완성도 : TRL7 (유사 상용품 개발)

TRL1	TRL2	TRL3	TRL4	TRL5	TRL6	TRL7	TRL8	TRL9
기술원리 발표	기술컨셉 설정	기술컨셉 증명	Lab Scale 시제품개발	구현환경 적용실험	Full Scale 시제품개발	**유사 상용품 개발**	상용품 완성	상용품 실시

활 용 분 야

활용분야 및 적용제품

활용분야

- ◆ 네트워크 보안 시스템 분야
- ◆ 시스템보안 솔루션 분야
- ◆ 보안관리 시스템 분야
- ◆ 정보보안 관련 분야

적용제품

- ◆ 이상행위탐지 시스템
  - 방화벽, 웹 방화벽, VPN
  - 웹필터링, 안티스팸 등
- ◆ 침입탐지/방지 시스템(IDS,IPS)
- ◆ 신·변종 사이버 위협 탐지 시스템
- ◆ 통합보안관제 시스템

사이버공격 실시간 추적 가시화 시스템

산업동향(기술 동향 및 트랜드 등)

- 사이버 공격은 미국에서 가장 빠르게 성장하는 범죄로 정교함과 비용이 지속해서 증가하고 있으며, Juniper에 의하면 사이버 범죄자들은 2023년 330억 건의 정보를 탈취할 것으로 예상되며, 전 세계 데이터 유출의 절반 이상이 미국에서 발생할 것으로 추정하고 있음
- 국내에서는 사이버 공격을 받는 시스템이 스스로 형태를 바꿔 해킹을 원천 차단하는 능동형 사이버 자기방어 기술과 네트워크상 주요 서버를 지속해서 변경함으로써 해킹을 막는 네트워크 변이기술 등이 개발되고 있음
- 최근 사이버보안 기술은 기존의 방화벽, 데이터 암호화, 클라우드 보안 등의 기술분야에서 블록체인과 인공지능을 이용한 방식으로 진화하고 있으며, 네트워크 경계에서 발견하지 못한 공격에 대응하기 위해 네트워크 통신 패턴을 기록 및 분석할 수 있는 네트워크 탐지 및 대응(NDR) 솔루션이 제안되고 있음

(출처:kotra_해외시장뉴스)

시장전망(목표시장 규모 및 전망)

- 국내 2019년 정보보안 매출액은 2018년 3,082,926백만원에서 6.3%로 증가한 3,277,687백만원으로 예상됨
- 세계 정보보안 시장은 2018년 약 152,656백만 달러에서 연평균 10.20%로 성장하여 2026년 332,022백만달러로 성장할 예정이며, 국내는 2018년 3,083억에서 연평균 16.41%로 성장하여 2026년 9,495억까지 성장할 것으로 전망됨
- Cybersecurit Ventures에 따르면, 글로벌 사이버 보안 시장은 2004년 35억 달러에서 2017년 1,200억 달러에 달해 무려 35배 급속한 성장을 보이고 있으며, 연간 12~15%의 성장을 통해 2020~2025년 동안 누적 1조 달러의 시장이 될 것으로 전망함
- 또한, IT 보안 관리 서비스 시장 규모는 연평균 12.4%로 꾸준히 성장하여 2023년 169억 달러까지 증가할 것으로 전망됨
- ADS 리서치의 자료에 따르면, 미국의 2019년 사이버 보안 시장 규모는 300억 달러로 전세계 시장의 약 30%의 비중을 차지하고 있을 것으로 예측되며, 미국 연방정부는 미국 전체시장의 50%인 150억 달러의 예산을 집행하고 2022년까지 220억 달러로 확대될 전망

(출처:보안뉴스/IITP_ICT R&D 기술로드맵2025)

지재권현황

권리현황	특허등록번호	발명의 명칭
등록	10-1991737	공격자 가시화 방법 및 장치
등록	10-1991736	공격자 상관정보 가시화 방법 및 장치
등록	10-2038926	공격자 선정장치 및 공격자 선정 장치의 동작방법
등록	10-2038927	공격자 가시화 장치 및 공격자 가시화 장치의 동작방법

문 의 처

기술이전

KiSTi www.kisti.re.kr 한국과학기술정보연구원 Korea Institute of Science and Technology Information

담 당 자 심건욱 선임
연 락 처 042-869-0915
이 메 일 kwsim@kisti.re.kr

기술문의

KiSTi www.kisti.re.kr 한국과학기술정보연구원 Korea Institute of Science and Technology Information

담 당 자 송중석 박사
연 락 처 042-869-0729
이 메 일 song@kisti.re.kr