21 전시기술
사이버 표적공격 추적 기술

+ Inventor Information

김익균 박사
한국전자통신연구원 지능보안연구그룹

연구이력

1) 다중소스 데이터의 Long-term History 분석기반 사이버 표적공격 인지 및 추적 기술 개발
2) 자동차 전장시스템의 실시간 오류 감지 및 복구 프로세서 SW 개발
3) 신경모사 인지형 모바일 컴퓨팅 지능형반도체 기술 개발
4) 초저에너지 프로세서를 위한 NZV 마이크로 그레인 아키텍처 기술

+ Applications

- 차세대 보안정보 및 사건관리, 빅데이터 보안 분석, 안티바이러스 엔진 등 사이버 보안 응용서비스분야

+ Contact Point

- 소속 : 한국전자통신연구원 사업화협력실
- 담당자 : 김호민
- 전화 : 02-860-1804
- E-mail : hominkim@etri.re.kr
- Hompage : www.etri.re.kr

+ Background

- 사이버 해킹 공격에 대한 역추적 기술은 호스트 기반의 연결 역추적 방법(Host based TCP Connection Traceback), 네트워크 패킷 기반의 역추적 방법(Network IP Packet based Traceback) 및 IP 주소를 속이고 통신하는 공격(IP Spoofing)에 대하여 패킷의 실제 송신지를 찾아내는 역추적 방법 등이 제안되고 있음
- 기존의 보안 기술은 알려진 악성코드에 대한 감시 및 방어에만 집중했음

+ Key Technology Highlights

- 사이버 표적공격에 대한 선제적 대응 시스템으로 기존의 잘 알려진 해킹, DDoS, 바이러스 외 장기간 호스트, 네트워크 등 다양한 형태의 네트워크 소스들을 수집·분석한 빅데이터를 통해 공격을 빠르게 인지하고 공격자를 역추적하는 기술임
- 장기간 호스트와 네트워크를 모니터링을 통해 저장된 빅 데이터를 바탕으로 의심스러운 포트가 발견되었을 때 비정상적 내부연결을 탐지하여 경고함
- 상세 악성행위 및 호스트를 분석하여 연관성 분석결과 조회를 통한 공격 여부를 판단하고 공격에 대한 징후를 찾아냄
- 분석결과를 바탕으로 3D모델링으로 시각화한 행위패턴 스펙트럼을 작성하여 분석하고 행위에 따른 악성코드를 탐지함
- 넷플로우(Netflow) 정보기반 역추적 알고리즘을 활용하여 경유지와 근원지를 파악하여 공격 시스템의 위치와 실제 해킹을 시도하는 해커의 위치가 서로 다르더라도 경유지 포함 실제 해커의 위치인 공격 근원지 추적이 가능함

FIDO 플랫폼 기술 구성도

+ Discovery and Achievements

- 기존 ISP 인터넷 구성 변경 또는 새로운 통신 프로토콜 추가 없이 라우터로부터 수신되는 Netflow 정보를 이용하여 공격 경유지 및 근원지에 대한 실시간 추적 기능 제공함으로써 빠르고 정확하게 해커의 위치를 파악 할 수 있음
- 위성 GPS기반의 3차원 사용자 인터페이스(3D GPS GUI)기능으로 공격근원지, 경유지, 공격 피해지의 분포를 쉽게 파악하여 연결 상태를 빠르게 분석 할 수 있음

+ Intellectual property rights

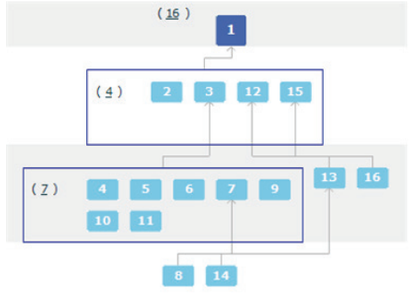
No.	출원번호	특허명	현재상태 (2018년 4월 기준)
1	10-2016-0052154	넷플로우 기반 연결 핑거프린트 생성 및 경유지 역추적 방법	출원
2	10-2015-0017334	새로운 공격 유형의 자동 탐지 및 공격 유형 모델 갱신을 통한 지능형 침입 탐지 시스템 및 방법	출원
3	10-2016-0051673	비정상 프로세스의 연관 데이터 분석을 이용한 A P T 공격 인지 방법 및 장치	출원
4	10-2016-0032041	악성 코드 탐지 장치 및 방법	출원
5	10-2016-0025189	윈도우 API분석을 이용한 어플리케이션의 행위 판단 장치 및 방법	출원
6	10-2017-0059539 (10-1769575)	움직임 탐색시 효율적인 움직임 벡터 추출 방법 및 그 장치	등록유지
7	10-2016-0016959	광대역 네트워크 환경을 위한 실시간 전송 파일 재구성 장치 및 방법	심사중
8	10-2015-0105866	네트워크 데이터 분석에 기반한 비정상 연결 행위 탐지 장치 및 방법	심사중
9	10-2015-0023306	실제 자원들을 이용하여 악성 코드를 실행하는 컴퓨팅 장치, 악성 코드의 정보를 관리하는 서버 시스템, 및 그것들을 포함하는 전자 시스템	심사중
10			

+ Exemplary Claim

Patent number : 10-2016-0052154

- 존속기간(예상)만료일 : 2036년 4월 27일

<청구항 계층 분석>



Claim Structure

- 전체 청구항(16), 독립항(1), 종속항(15)

Exemplary Claim

- 피해지 및 연결체인 상의 마지막 연결인 타겟 연결에 해당되는 공격지의 아이피 패킷 속성 정보를 포함하는 역추적 요청을 수신하는 단계
- 아이피 패킷 속성 정보를 바탕으로 관련 연결에 대한 핑거프린트를 생성하고, 넷플로우 콜렉터로 관련 정보를 요청하는 단계
- 핑거프린트 생성 시에 만들어진 타겟 연결에 대한 경유지 연결을 검출하여, 선별된 대상 연결이 상기 타겟 연결과 동일한 연결체인 상에 존재하는지 여부를 확인하는 단계
- 타겟 연결과 동일한 연결체인 상에 존재하는 것으로 확인된 상기 대상 연결에 대하여 공격자 호스트를 기준으로 한 연결 순서를 결정하는 단계를 포함하는 넷플로우 기반 연결 핑거프린트 생성 및 경유지 역추적 방법식의 무인비행체