[별첨 5]

사이버블랙박스 실행파일 수집 및 재구성 기술

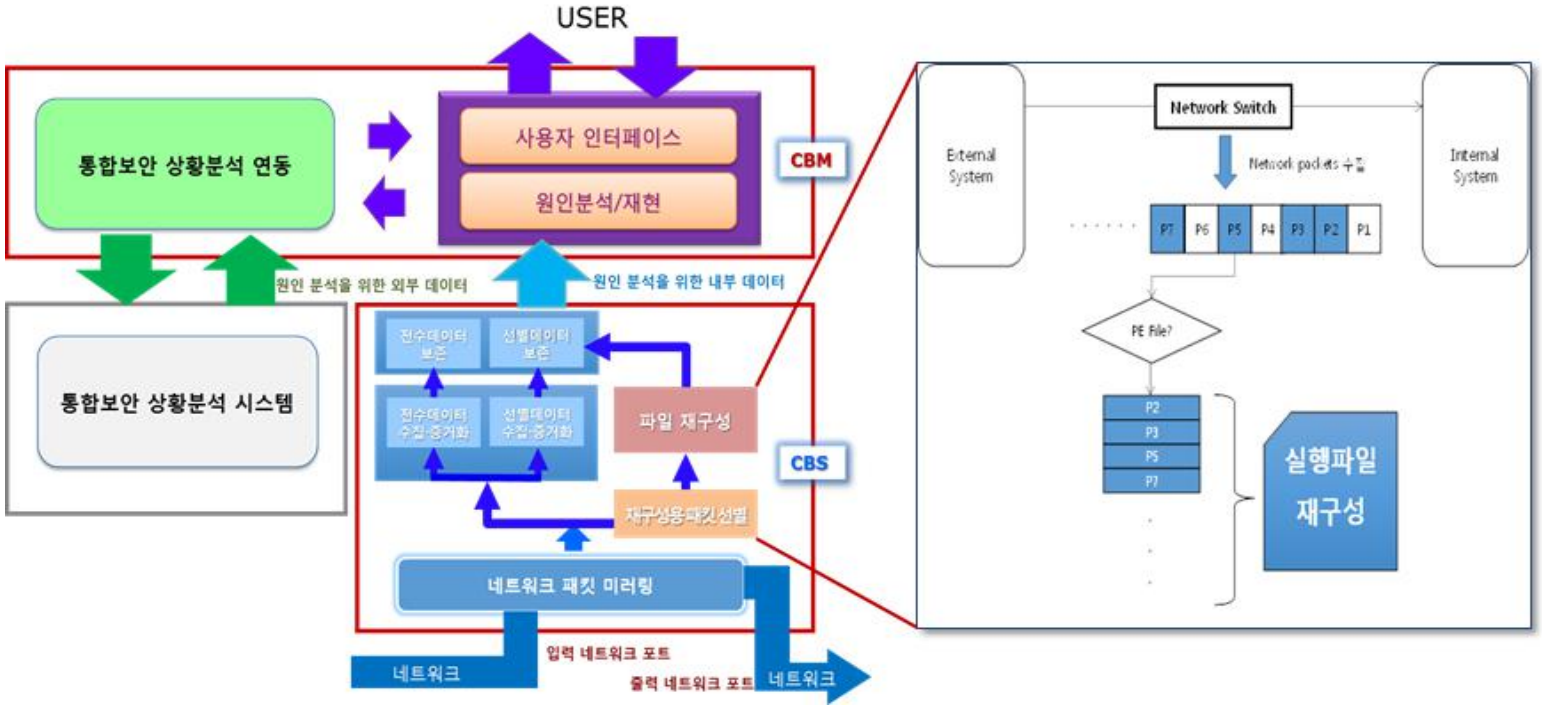
김종현 (jhk@etri.re.kr)
네트워크보안연구실

ETRI 한국전자통신연구원
www.etri.re.kr
SW콘텐츠연구소/사이버보안연구본부

목 차

▣ 사이버블랙박스의 실행파일 수집 및 재구성 기술

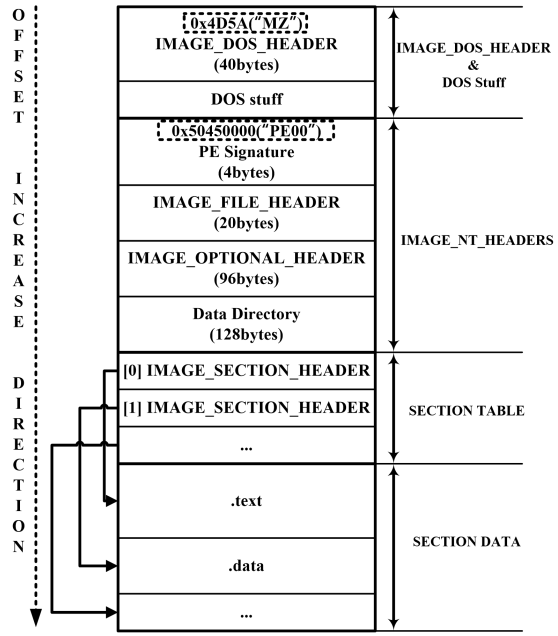
❖ 본 기술은 리눅스 플랫폼 상에서 동장하며 네트워크상에서 전송되는 실행파일인 PE(Portable Executable) 파일을 탐지하고, 이를 재구성하여 원본 실행파일을 도출하는 기술임



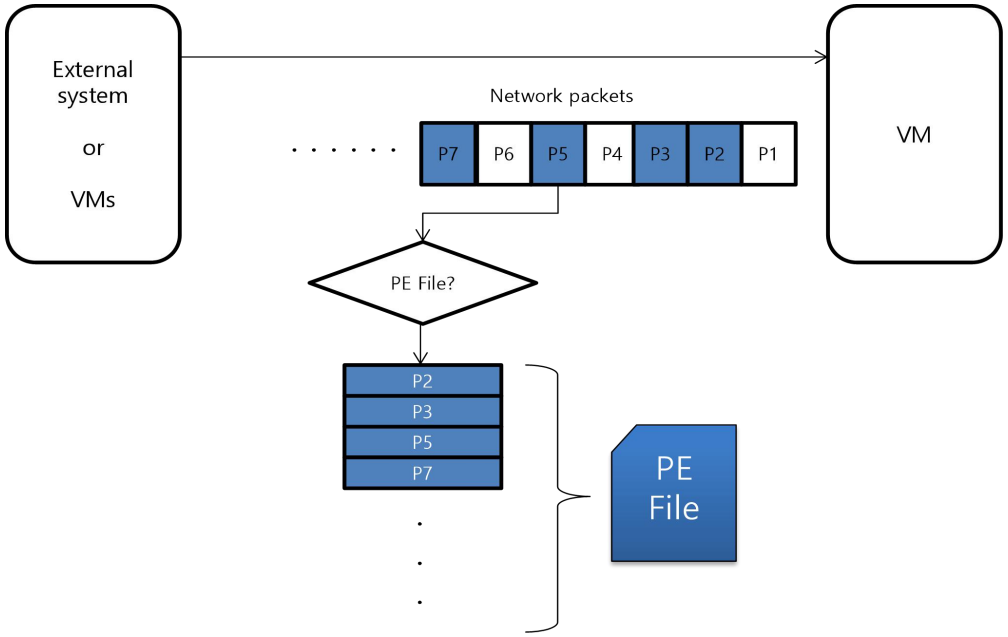
< 개발 기술 운요 개념도 >

▣ 사이버블랙박스의 실행파일 수집 및 재구성 기술

- ❖ 네트워크 상에서 전송되는 패킷을 분석
- ❖ 네트워크 패킷 내에 PE파일의 존재여부를 탐지
  - ❖ PE(Portable Executable)파일: MS 윈도우 OS(Windows XP, Window7 등)의 실행파일 포맷
- ❖ 수집된 패킷으로부터 파일 Contents를 추출하고 이를 재조립하여 실행파일을 구성



<Normal PE file format>



<PE file reconstruction>

▣ 기술이전 내용 및 범위

❖ 기술이전 내용

- ✓ 네트워크 트래픽 모니터링 및 PE파일이 포함된 세션 데이터 수집 기술
- ✓ PE파일에 포함되는 데이터만을 추출하여 실행파일 재구성 기술
- ✓ 악성여부 판단 기술과의 연동 기능

❖ 기술이전 범위

- ✓ 소스코드: 사이버블랙박스 실행파일 재구성 프로그램
- ✓ 문서: 시스템 설계서, 개발문서, 기술문서

▣ 기술 개발 현황

❖ 기술성숙도(TRL : Technology Readiness Level) 단계 : (5)단계

구 분	단계	정 의	세 부 설 명
기초 연구 단계	1	기초 이론/실험	◦ 기초이론 정립 단계
	2	실용목적의아이디어, 특허 등 개념정립	◦ 기술개발 개념 정립 및 아이디어에 대한 특허 출원 단계
실험 단계	3	실험실 규모의 기본성능 검증	◦ 실험실 환경에서 실험 또는 전산 시뮬레이션을 통해 기본성능이 검증될 수 있는 단계 ◦ 개발하려는 부품/시스템의 기본 설계도면을 확보하는 단계
	4	실험실 규모의 소재/부품/시스템 핵심성능 평가	◦ 시험샘플을 제작하여 핵심성능에 대한 평가가 완료된 단계 ◦ 3단계에서 도출된 다양한 결과 중에서 최적의 결과를 선택하려는 단계 ◦ 컴퓨터 모사가 가능한 경우 최적화를 완료하는 단계
시작품 단계	5	확정된 소재/부품/ 시스템 시작품 제작 및 성능 평가	◦ 확정된 소재/부품/시스템의 실험실 시작품 제작 및 성능 평가가 완료된 단계 ◦ 개발 대상의 생산을 고려하여 설계하나 실제 제작한 시작품 샘플은 1~수개 미만인 단계 ◦ 경제성을 고려하지 않고 기술의 핵심성능으로만 볼 때, 실제로 판매가 될 수 있는 정도로 목표 성능을 달성한 단계
	6	파일롯 규모 시작품 제작 및 성능 평가	◦ 파일롯 규모(복수 개~양산규모의 1/10정도)의 시작품 제작 및 평가가 완료된 단계 ◦ 파일롯 규모 생산품에 대해 생산량, 생산용량, 불량률 등 제시 ◦ 파일롯 생산을 위한 대규모 투자가 동반되는 단계 ◦ 생산기업이 수요기업 적용환경에 유사하게 자체 현장테스트를 실시하여 목표 성능을 만족시킨 단계 ◦ 성능 평가 결과에 대해 가능하면 공인인증 기관의 성적서 확보
실용화 단계	7	신뢰성평가 및 수요기업 평가	◦ 실제 환경에서 성능 검증이 이루어지는 단계 ◦ 부품 및 소재개발의 경우 수요업체에서 직접 파일롯 시작품을 현장 평가(성능 및 신뢰성 평가) ◦ 가능하면 인증기관의 신뢰성 평가 결과 제출
	8	시제품 인증 및 표준화	◦ 표준화 및 인허가 취득 단계
사업화	9	사업화	◦ 본격적인 양산 및 사업화 단계 ◦ 6-시그마 등 품질관리가 중요한 단계

▣ 실행파일 수집 및 재구성 기술

- 기존의 악성파일 수집기술은 백신프로그램 등을 통해 사용자에 의해 제공받는 형태로 악성파일이 사용자 시스템에 설치된 이후에만 수집이 가능하였음
- 또는 Honeypot 등을 이용하여 수집하였으나 공격 성공 이후에 수집되는 경우가 대부분이었음
- 최근에는 네트워크 상에 공유된 파일이나, 악성 URL 정보를 이용한 악성파일 수집이 가능하나 파일 수집에 상당한 시간이 소요되는 단점이 있음
- 본 기술은 실시간으로 송신되는 실행파일을 탐지하고 수집하는 기술로서 추가적인 응용프로그램이나 프로토콜 분석이 필요하지 않은 기술임
- 기존 장시간이 소요되었던 PC 기반의 디지털 포렌식 기술의 한계를 보완하여 침해사고 분석시간 단축, 침해사고 증거 선별 및 효율적인 관리가 가능함

▣ 예상 응용제품 및 서비스

예상 제품/서비스	예상 수요자(층)
사이버 블랙박스 침해공격 원인분석 및 실행파일 재구성 시스템	국가 CERT 및 ISP 망 사업자
사이버 블랙박스 침해공격 원인분석 및 실행파일 재구성 시스템	공공기관 및 교육기관
일반 환경의 실행파일 재구성 서비스	기존 네트워크 보안 업체

▣ 기술이전 업체 조건

❖ **해당사항 없음**

▣ 사업화시 제약조건

❖ **해당사항 없음**

▣ 사업성

예상 제품/서비스	예상단가 (천원)	이전기술의 비중(%)	잠재적/현재적 경쟁자와 가격, 시장 등에서 경쟁상 유리한 점	판매 가능 시기
사이버 블랙박스 시스템	100,000	40%	a. 가격경쟁력면: 기존 외산제품에 비해 저렴하며 기능 요구사항에 따라 변동 가능 b. 시장환경면: 침해사고 발생 시 원인분석을 위한 증거데이터 확보에 대한 요구사항 증가 c. 기타: 기능면에서 경쟁력 있음 (실시간 실행파일 재조립 기술)	2015

- ❖가격 경쟁력: 상용제품의 기능 요구사항에 따라 변동가능
- ❖상용화를 위한 생산설비 등 추가비용: S/W 이므로 생산 설비 등 추가비용 없음
- ❖상용화를 위한 추가적인 기술개발 내용: 해당 없음

▣ 국내외 시장 동향

- 국내의 사이버 공격 탐지/대응 관련 보안 시장은 `14년부터 연 평균 3.7%씩 성장하여, `19년 시장규모는 약 5,614억 원까지 증대될 것으로 추산함 (출처 : 2013 국내 정보보호산업 실태조사(KISA, 2013))
- 전 세계 사이버 공격 탐지/대응 관련 시장은 `14년 139,542억원 규모이며, 연 평균 1.4%씩 성장하여, `19년까지 시장규모는 약 149,846억원까지 증대될 것으로 추산함 (출처 : 2012 세계 지식정보보안산업 비교 분석(KISA, 2012))
  - 전 세계 사이버 공격 탐지/대응 관련 시장 자료가 없는 관계로, 국내 시장 점유율을 세계 지식정보보안시장 현황에 반영하여 추정함
- 국내외 시장규모

(단위: 백만불, 억원)

관련 제품 /서비스	시장	1차년도 (2015)	2차년도 (2016)	3차년도 (2017)	4차년도 (2018)	5차년도 (2019)	합계
네트워크 보안 관리 솔루션	해외	1,573.5	2,311.5	3,395.6	4,988.1	7,327.5	19,596.2
	국내	314.7	462.3	679.12	997.62	1,465.5	3,919.24

감사합니다.

www.etri.re.kr

♣ 연락처 : SW콘텐츠연구소/네트워크보안연구실 김익균 책·연 (042-860-5442, ikkyun21@etri.re.kr)