2017년 정보보호 R&D 연구기관(KISA, ETRI, NSR)의 기술 이전 대상 정보보호기술 목록

번호	기술명	기관	기술 소개
1	악성코드 자동 분석 및 탐지 기술	KISA	- 입력파일 대상 실행중의 행위정보 자동 분석 및 악성여부 탐지 ※ 신·변종 악성코드의 악성여부 분석 및 탐지 가능 - 시스템/네트워크 보안제품, 악성코드 탐지용 백신제품
2	악성코드 변종 자동탐지 및 그룹분류 기술	KISA	- 대량의 악성코드 환경에서 악성코드 변종의 자동 탐지기술 ※ 악성코드 대부분은 기존 악성코드의 변형된 형태가 활용됨 - 1:1 악성코드 비교 뿐 아니라, 악성코드 그룹의 자동분류 가능
3	좀비PC 자동수집 기술(이메일 기반)	KISA	- 악성코드에 감염된 좀비PC를 자동으로 수집하는 기술 ※ 스팸메일을 분석하여 좀비PC를 수집 - 또한, 동일 악성코드에 감염된 좀비PC그룹(봇넷)을 자동으로 탐지 가능
4	모바일 악성앱 자동수집 기술	KISA	- 모바일 악성앱의 능동적 수집을 위한 유포지 URL 수집 및 악성앱 수집 기술 ※ 패턴없는 블랙마켓 URL 추적, 수집 등 다채널 기반 모바일 악성앱 능동 수집 - 모바일 보안, 모바일 악성앱 수집 도구
5	모바일 악성앱 자동분석 및 변종탐지 기술	KISA	- 모바일 악성앱의 탐지를 위하여 코드 및 행위 분석 기반의 악성 요소 분석 기술 ※ 변종 악성앱 분석, 정적/동적 악성행위 분석 및 탐지 - 모바일 보안, 모바일 악성앱 분석 도구
6	Machine Learning 기반 분석지원 도구	KISA	- 머신러닝 기반 모바일 이상결제 탐지기술(머신러닝 기반 FDS) 이상결제 탐지 이외의 응용분야에 활용할 수 있는 머신러닝 분석을 지원할 수 있는 도구
7	에뮬레이터 기반 지능형 악성앱 행위 무력화 및 분석 기술	KISA	- 가상환경 탐지를 통해 분석을 우회하는 지능형 악성앱 자동분석 기술 ※ 악성앱의 에뮬레이터 탐지 무력화 및 행위 분석 - 모바일 보안, 모바일 악성앱 분석 도구
8	사이버 침해사고 공격정보 및 연관정보 자동수집 기술	KISA	- 사이버 침해사고 공격정보 자동수집 기술 ※ 10개의 Intelligence Feed 채널에서 수집된 침해정보 자동수집/이력관리 - 침해사고 공격 간 연관정보 및 연관관계 자동수집 기술
9	사이버 침해공격에 대한 Intelligence 분석 기술	KISA	- 수집된 침해정보로부터 연관분석 가능한 다수의 Intelligence 분석정보 제공 - 침해공격 간 연관분석 정보 제공을 통한 동일 공격자 추정 가능
10	스크립트 기반 네트워트 공격 탐지·차단 기술	KISA	- 네트워크로 유입되는 악성 스크립트 탐지를 위한 보안 게이트웨이 - 네트워크 단에서 HTML5/스크립트 정보 수집 및 수집 정보 분석 - 가상 환경을 통한 스크립트 행위 정보 정밀 분석
11	악성 스크립트 공격 모바일 보안 기술	KISA	- 안드로이드 기반의 악성 스크립트 탐지 및 실행 차단 기술 - 모바일 환경에서 실시간 웹 트래픽 수집 및 스크립트 분석 - 난독화 스크립트 해제 처리
12	시그니처 기반 악성 스크립트 점검 기술	KISA	- 웹 사이트 스크립트 정보 고속 수집 및 악성 스크립트 내포 여부 점검 - 서버 기반 웹 컨텐츠 고속 수집 및 취약점 점검 기술 - PC기반 웹 사이트 취약점 점검 및 상용 웹 취약점 점검 기술
13	모바일 디바이스의 Agentless 방식 상황정보 수집 기술	KISA	- 웹 기반 서비스에 접근하는 모바일 디바이스 식별정보 수집 ※ 사용자 기기에 별도 앱 설치없이(Agentless) 웹 서비스에 접근하는 사용자/기기 정보 수집 - 기업 모바일 오피스 접속 및 이용에 따른 상황정보 수집/관리 솔루션
14	모바일 기기의 웹 서비스 접속 및	KISA	- 웹 기반 서비스 사용자의 접속·이용행위 분석 및 비정상 행위 판별 ※ 웹 서비스 이용시 발생하는 모든 행위 관리 및 사용자의 과거

번호	기술명		기관	기술 소개
	이용 행위 분석 기술			서비스 이용 패턴 분석 - 기업 내부 웹 사이트 정보 보안을 위한 이상 행위 탐지 솔루션
15	사용자/기기 내부 네트워크 경량 접근제어 기술		KISA	- 사전에 설정한 보안 정책을 통해 개별 사용자 네트워크 접속 제어 ※ 웹 기반 서비스 접속 세션 관리를 통한 외부 사용자 제어 ※ 별도의 앱 설치 없이 네트워크 트래픽 접근 제어 - 기업 내부 네트워크에 접근하는 사용자/기기의 제어 기술
16	악성앱 점검 도구 폰키퍼(Phone Keeper)		KISA	- 스마트폰의 악성 앱 설치 여부 등을 점검해주는 자가 점검 도구 ※ 보안설정 점검, 악성앱 검증, 앱 권한 검증, 앱 분석 요청 등 지원 - 업무용 스마트폰의 보안 상태 점검 도구
17	FIDO 1.0 인증 기술	FIDO 1.0 서버 기술	ETRI	- FIDO UAF (Fast Identity Online) 1.0 규격을 준용하는 서버 및 클라이언트 기술을 제공
18		FIDO 1.0 SW 인증 장치 기술	ETRI	- FIDO (Fast Identity Online) 1.0 규격을 만족하는 SW 인증장치 기술을 제공
19	스마트 채널3 기술		ETRI	- PC/스마트TV 등 스마트 단말기기의 웹브라우저에서 별도 플러그인 설치 없이 스마트폰을 이용해서 피싱/파밍 공격에 안전한 인증을 하는 기술
20	MTM기반 스마트 단말 보안시스템 구현기술	보안기능 추상화 및 미들웨어 관리 기술	ETRI	- 스마트 디바이스(단말)에서 인증/지불/스마트 뱅킹 등과 같은 고수준의 보안성이 요구되는 응용 서비스가 안전하게 운용될 수 있도록 이들 서비스에 미들웨어 관리 및 보안기능 추상화 API를 제공 - 보안 정책 및 미들웨어 설정/관리 기능, 보안 응용 서비스 지원 기능, 보안 기능 추상화 API 제공 기능으로 구성
21		암호 및 컨택스트 관리 기술	ETRI	- 고수준의 보안성이 요구되는 단말의 보안 응용서비스 및 보안정책, 보안 기능 추상화를 효과적으로 지원하는 MTM 기반 암/복호화, MTM 접근을 제어하는 컨텍스트 관리 및 미들웨어 서비스 제공 - MTM Internal Key 기반 데이터 암/복호화 지원기능, MTM 보안기능 사용을 위한 컨텍스트(세션 연결) 관리 기능, MTM 동시 접근 제어용 미들웨어 기능으로 구성
22		단말 무결성 측정 및 검증 기술	ETRI	- 단말 시스템에 전원이 인가되는 시점에 단말의 부트로더, 커널, 안드로이드 시스템, 주요 네이티브 시스템 서버 등의 무결성 측정 및 검증 기능을 단계적으로 수행하여 점검하고, 단말 시스템이 해킹 및 악성코드에 의해서 불법적으로 변경되었을 경우 무결성 검증을 통해 탐지하는 기능을 제공 - 단말 무결성 측정 및 검증 기능, 무결성 검증 정보 통신 및 제어 기능, 무결성 측정 및 검증 구조 관리 기능으로 구성
23		MTM 및 보안서비스 실행엔진 기술	ETRI	- 단말 시스템과 MTM 사이의 세션 연결 설정 및 관리를 통해 명령어를 전송하고, 전송된 명령어 따라 MTM 명령과 보안 서비스 명령을 실행 - 메시지 관리 기능, MTM실행엔진 기능, 보안 서비스 실행엔진 기능으로 구성
24		MTM 암호 및 저장관리 기술	ETRI	- MTM에서 필요로하는 RSA 공개키 암호, 대칭키 암호, 해쉬함수등의 다양한 암호알고리즘을 제공 - MTM용 암호 알고리즘 기능 및 MTM용 저장관리 기능으로 구성
25	데이터 보호 및 안전한 처리를 지원하는 스마트 단말용 은닉형 보안플랫폼 기술	경량 보안 OS 기반 은닉형 보안 플랫폼 기술	ETRI	- 일반영역에서 호출된 보안 API 메시지를 해석 및 관리하는 기능을 포함 - 보안영역 접근에 대한 2-Factor 인증(Admission) 기능, 보안영역 접근제어(Access Control) 및 메시지 관리 기능, KCMVP 대응 암호 알고리즘 및 키관리 기능, 안전한 저장관리(Secure Storage) 기능으로 구성
26		보안플랫폼용 보안 API 및 추상화 기술	ETRI	- 안드로이드OS의 보안서비스가 은닉형 보안플랫폼의 보안기능을 사용할 수 있도록 개발자에게 제공된 API와 일반영역 보안API의 구현을 제공하는 보안영역에서의 추상화 라이브러리로 구성 - 일반영역에서의 보안플랫폼 활용을 위한 보안API 주요 기능, 보안영역의 보안서비스 추상화 기능, 일반영역 메시지 관리 기능으로 구성
27	스마트단말 보안플랫폼용 TYPE-2 가상머신 모니터 기술		ETRI	- 분실 및 도난의 가능성과 악성코드 위협이 높은 스마트단말 환경에서 모바일 OS(안드로이드OS)가 동작하는 일반영역과 보안기능을

번호	기술명		기관	기술 소개
				제공하는 보안영역으로 운영환경을 분리하는 TYPE-2 기반의 가상머신 모니터 기술
28	화이트박스 암호를 이용한 무인항공기 보안 기술		ETRI	- 무인항공기와 같이 공격자에 의해 탈취 가능성이 존재하는 응용에서 기기의 암호키와 암호 데이터를 보호하기 위한 기술
29	스마트디바이스 키누출 HEB 검증보드 (KLA-SCARF)		ETRI	- 스마트카드, OTP 기기, 보안 토큰과 같은 소형 디바이스에서 암호 알고리즘이 구동되는 동안 발생하는 다양한 부가적인 정보(전력소모량, 발생 전자기파 등)를 통해 비밀키를 추출해 내는 키누출 공격에 대한 안전성 검증 시스템
30	스마트 디바이스 키누출 검증 시스템 (KLA_SCARF)	KLA-SCARF 시스템 기술	ETRI	- 개발된 보안 솔루션에 대한 키누출 공격 취약성을 사전에 미리 검증하는 시스템 - 파형 수집 기능, 파형 전처리 기능, 파형 부채널 분석 기능, 프로젝트 관리 및 프로그램 설치 기능으로 구성
31		CEB 보드 기술	ETRI	- 접촉식 카드타입 검증보드에 탑재된 분석 대상(AES, DES, SEED, RSA 등의 보안 알고리즘) 등을 SPA, DPA, CPA 등의 분석 방법으로 안전성을 검증 - 접촉식 카드타입 보안 디바이스 부채널 검증을 위한 카드리더 겸용 보드
32		C2EB 보드 기술	ETRI	- 비접촉식 카드타입 검증보드에 탑재된 분석 대상(AES, DES, SEED, RSA 등의 보안 알고리즘) 등을 SPA, DPA, CPA 등의 분석 방법으로 안전성을 검증 - 비접촉식 카드타입 보안 디바이스 부채널 검증을 위한 카드리더 겸용 보드
33	Human Identity를 위한 원거리 얼굴인식	Human Identity를 위한 원거리 얼굴 검출 기술	ETRI	- 실내, 원거리 환경에서 사람의 얼굴 영역을 검출하는 기능 및 PTZ 카메라를 이용해서 얼굴 영역을 확대하고 영역 재검출하는 기능으로 구성
34		Human Identity를 위한 얼굴 인식 기술	ETRI	- 실내, 원거리 환경에서 얼굴 인식
35	악성코드 비정상 행위 동적 분석 및 시각화 기술	호스트 프로세스 행위정보 수집 기술	ETRI	- 호스트에서 실행되는 모든 프로세스의 행위정보를 API 후킹에 의해 실시간 수집 - 40종 이상의 특성인자 수집
36		호스트 행위 기반 악성코드 분석 기술	ETRI	- 데이터 마이닝 기반 악성코드 탐지 - 프로세스의 행위패턴을 표현할 수 있는 특징벡터로 재구성
37		사이버게놈 기반 악성코드 행위 분석 및 시각화 기술	ETRI	- 악성코드 그룹별 고유 행위 패턴(사이버게놈) 생성 및 분류 - 사이버게놈 기반의 시퀀스 유사도를 통한 악성코드 탐지 - 프로세스 행위 특성인자 및 비정상 행위 분석 결과 시각화
38	호스트 행위기반 악성코드 탐지 기술	호스트 프로세스 행위정보 수집 기술	ETRI	- 호스트에서 실행되는 모든 프로세스의 행위정보를 API 후킹에 의해 실시간 수집 - 40종 이상의 특성인자 수집
39		호스트 행위 기반 악성코드 분석 기술	ETRI	- 데이터 마이닝 기반 악성코드 탐지 - 프로세스의 행위패턴을 표현할 수 있는 특징벡터로 재구성
40	인터넷레이더 3D 시각화 기술	보안상황 3D 시각화 기술	ETRI	- 보안이벤트 수집분석에 의한 공격상황정보 분류 축약 - 공격상황 3D 시각화 - 공격 내역을 표현하는 돔 구조와 공격 대상 지역을 지리정보와 연계하여 표현

번호	기술명		기관	기술 소개
41		네트워크 위협 인지 기술	ETRI	- 다양한 사이버위협 발생 전 봇넷 형성 및 행위 탐지 - C&C 서버와 봇 간의 통신 모니터링에 의한 액티브 봇 행위 탐지 - DNS 트래픽 감시에 의한 비정상 호스트 탐지 및 비정상도 정량화 - 공격 징후 정량화에 의한 위험등급 및 발생가능 공격 규모 산정
42		공격 근원지 추적 기술	ETRI	- 웹 기반 파일 공유 사이트 기반의 추적로그 생성을 위한 업로드/다운로드 이벤트 수집 - 추적로그 전달 프로토콜
43	IALA 공통포멧 기반 관제정보교환 모듈 기술		ETRI	- IALA 공통포멧(IVEF)기반 관제정보교환 모듈 기술은 IALA 표준에 기반하여 관제 시스템의 관제 대상에 대한 정보를 네트워크를 통하여 타 관제시스템 또는 이해관계자의 시스템과 상호 교환하기 위한 기술
44	차세대 무선랜 침해방지 시스템 V1.0	무선침해방지 센서 엔진 기술 – 스마트채널 스케줄링 및 모니터링과 실시간공격 단말차단모듈	ETRI	- 다중 채널 공격 감시를 위한 스마트 채널 스케줄링 기능 - 관리/제어/인증 패킷 파싱 및 무선 침해공격 분석 기능 - 채널 스케줄링 연동 실시간 무선 침해공격 차단 기능
45		무선침해방지 센서 엔진 기술 – 무선지문기반 디바이스 식별 핵심 모듈	ETRI	- 무선지문 정보 수집 및 분석 기능 - 기계 학습 기반 위장 무선 디바이스의 실시간 탐지 기능 - 위장디바이스 식별 분석을 위한 서버 인터페이스
46		무선지문 추출 지원 센서 HW 플랫폼 및 디바이스 드라이버 기술	ETRI	- 센서 HW 플랫폼 기능 - 무선지문 추출 디바이스 드라이버 기능
47		무선위협관리 서버 기술	ETRI	- 서버 보안 관리 기능 - 서버 보안 정책 및 센서 관리 기능 - 서버 보안 이벤트 관리 기능
48	DNP3 방화벽 : IndusCAP- DNP3		ETRI	- 주요기반시설을 겨냥한 멀웨어 서비스거부 공격, 비정상적 공정제어 등으로부터 제어시스템의 가용성 보장을 목표로 하는 산업용 네트워크 보안기술
49	Modbus 기반 제어 어플리케이션 방화벽 어플라이언스기술	산업용 모드버스 방화벽 시스템 기술	ETRI	- Function code 기반의 비인가 명령어 접근제어 설계 및 구현 기능 - 제어 프로토콜 이상탐지 (Sanity Check) 설계 및 구현 기능 - 서비스거부공격 대응을 위한 비정상 제어 명령어 탐지 설계 및 구현 기능 - 사용자 인터페이스 기반 부정접근방지 정책 관리 설계 및 구현 기능
50		산업용 네트워크 모니터링 시스템 기술	ETRI	- 네트워크 구성관리 모니터링 설계 및 구현 기능 - 통신 프로토콜 모니터링 설계 및 구현 기능 - 네트워크 트래픽 모니터링 설계 및 구현 기능
51	LEA 암호 알고리즘		NSR	- IoT 환경 등에 적합한 세계 최고 성능의 고속・경량 블록암호. 각종 암호학적 공격에 대하여 안전하며, 다양한 SW 환경에서 국제 표준 AES 대비 1.5배~2배 속도 제공
52	고속 해시함수 LSH		NSR	- 디지털 데이터의 고유값을 생성하는 암호 알고리즘. - 각종 암호학적 공격에 대하여 안전하며, SW 환경에서 국제 표준 SHA-2/3 대비 2배 이상 속도 제공
53	Windows 보안기능 설정 점검 기술		NSR	- 윈도우 운영체제가 설치된 정보시스템의 보안수준을 강화하기 위해서 필요한 설정의 현재 상태를 확인하고 안전하지 않은 설정값을 안전한 상태로 변경하는 기술
54	보안관제종합관리시스템		NSR	- 이기종 보안관제장비에서 탐지되는 대용량 보안관제 데이터 중 보안

번호	기술명		기관	기술 소개
				이벤트에 대한 검색 및 연관성 분석 업무와 침해사고 대응·관리 업무 수행 시 대응 시간 및 처리 절차를 단축할 수 있는 보안관제용 통합관리시스템
55	스마트폰 앱 행위 모니터링 기술		NSR	- 루팅되지 않은 일반 스마트폰에 앱을 실행시켜 해당 앱의 행위를 실시간 추적 및 GUI를 통해 모니터링하는 기술
56	악성도메인접근 식별 및 차단기술		NSR	- 인터넷 환경에서 악성행위에 이용될 수 있는 악성도메인에 접근하는 호스트를 실시간으로 식별·차단하는 기술
57	안드로이드 앱 역공학 관점 디버깅 기술		NSR	- 안드로이드 앱을 소스코드 없이 안드로이드 앱 파일(.apk)만을 가지고 분석하는 **안드로이드 전용 분석 도구** 기술
58	탐지규칙 유사도 검사 기술		NSR	- 수많은 침입탐지 규칙을 자동으로 검사하여 유사한 탐지규칙을 판별할 수 있는 기술
59	FEA 암호알고리즘을 이용한 형태보존 암호화 기술	형태보존암호화를 위한 형 변환 기술	NSR	- 128 이하의 비트로 표현 가능한 n 자리 radix 진수열을 두 개의 64비트 변수로 변환하거나 그 역변환을 수행하는 함수의 고속화 기술
60		형태보존암호 알고리즘 FEA 고속구현 기술	NSR	- FEA 알고리즘을 64비트 환경에서 고속으로 동작하도록 구현하는 기술
61		암호화 기능 구동 기술 및 인코딩 유지 암·복호화 기능 개발 기술	NSR	- FEA를 이용하여 ASCII 및 유니코드로 정의된 한글 인코딩을 유지하는 암, 복호화 기술
62	GPS 간섭완화 안테나 및 필터링 기술	안테나 부가형 차폐 기술	NSR	- 기존에 설치된 GPS 안테나에 부착하여 간섭 완화를 수행하는 기술
63		단일 안테나 기반 간섭완화 기술	NSR	- 기존 안테나를 대체하는 고성능 간섭완화 기술
64		신호처리 기반 주파수필터링 기술	NSR	- 협대역 신호를 선택적으로 제거하여 GPS 위성 신호 수신을 가능케 하는 기술 - 시각/위치정보를 활용하는 고정/이동국에 활용 예상
65	고전력 전자파 차폐 랙 설계 기술		NSR	- 광대역 주파수 범위의 고전력 전자파로부터 전자기기를 안전하게 보호할 수 있는 저비용 전자파 차폐 랙 설계 기술
66	안테나선로용 EMP 차단 기술		NSR	- 통신대역 EMP 공격으로부터 무선설비 또는 시스템의 안테나선로 보호를 위한 플라즈마-반도체 연동방식의 고전력 펄스 리미터 기술 ※ 통신주파수(In-band) 공격신호는 필터링으로 제거 불가
67	휴대용 고속 불법신호탐지 설계 기술		NSR	- 소형・저전력 휴대용이면서 고속으로 불법신호를 탐지할 수 있는 기술
68	외부침투를 물리적으로 차단하는 신뢰성 있는 자료전송 기술		NSR	- **네트워크를 통한 외부침투를 물리적으로 차단**하면서 **자료전송의 신뢰성을 확보**하는 기술과 저비용 경량을 제작하는 기술

1 악성코드 자동 분석 및 탐지 기술

□ 기술소개

o **(배경 및 필요성)** 최근 알려지지 않은 **신·변종 악성코드가 급증**하고 있으나, **기존의 수동 분석으로는 신속한 대응에 한계**가 있음

※ '15년 4.6억개 악성코드 발생, 그 중 1.4억개(30%)가 신종임(AV-TEST, 2016)

o **(주요기술)** 본 기술은 입력되는 파일을 대상으로 실행과정에서 나타나는 행위 정보를 분석하고 **악성여부를 자동으로 탐지하는 기술**임

- 입력되는 파일을 대상으로 시스템 전반에서 호출되는 API 정보 자동 추출

[기술 개요]

□ 기존 기술과의 차별성

o **(As-is) 백신의 신·변종 탐지한계** 및 **동적 분석의 기술성숙도 부족**

※ 대부분의 제품은 동일 파일에 대한 다른 사용자의 판단 정보를 수집하여 평판 정보로서 제시하고, 실제 판단은 사용자에게 일임하는 경우가 많음

o **(To-be) 신·변종 악성코드의 악성 여부 분석 및 탐지** 가능

- 알려지지 않은 신규 악성코드에 대한 악성 여부 진단 가능

※ 파일이 실행되는 과정에서 호출하는 API의 내역을 분석하여 파일의 악성 여부를 판단

※ API(Application Programming Interface) : 실행파일이 호출하는 운영체제 서브루틴/함수 집합

□ 기술의 활용 분야

o 시스템/네트워크 분야의 보안제품으로써 **신·변종 악성코드 탐지 솔루션**

o 웹 및 이메일 보안 솔루션/장비에 대한 **연동형 보안 솔루션**으로 활용

o Virus백신 분야의 보안제품으로써 **악성코드 탐지용 백신 솔루션**

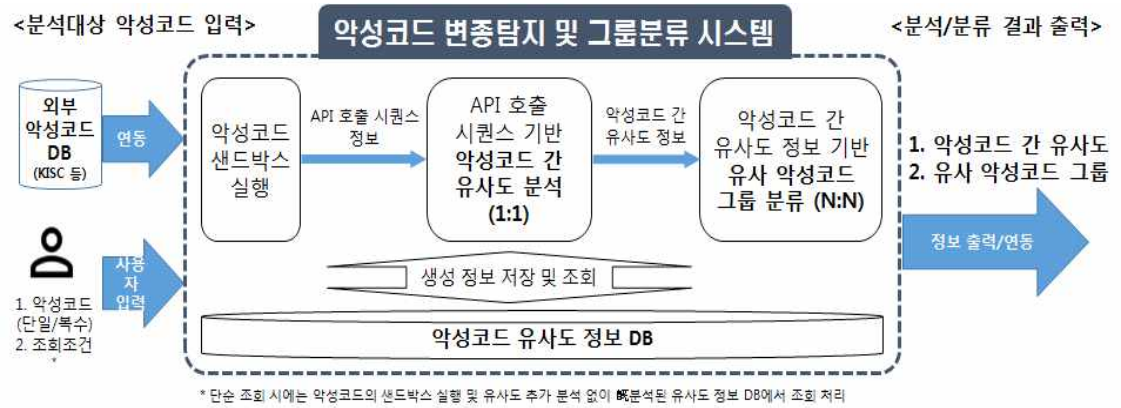
2 악성코드 변종 자동탐지 및 그룹분류 기술

□ 기술소개

o **(배경 및 필요성)** 기존 3.20, 6.25 사이버테러 등에 사용된 **변종들이 지속 출현**함에 따라, 대량으로 출현하는 악성코드들에서 **유사 유형의 그룹을 분류**하고 **우선 분석해야 하는 대상을 자동으로 선별**할 수 있는 기술 필요

o **(주요기술)** 본 기술은 대량의 악성코드가 축적된 상황에서, 행위정보를 기반으로 새로 입력된 특정파일에 대한 **변종 악성코드를 탐지/제시**하고, **이와 유사한 악성코드 그룹을 자동으로 분류**하는 기술

- 대량의 축적된 악성코드를 대상으로 악성코드 그룹 자동분류
- 주어진 특정 악성코드와 유사/변종 관계인 악성코드 탐지/조회



[기술 개요]

□ 기존 기술과의 차별성

o **(As-Is)** 학계를 중심으로 **비시그니처 방식 및 동적/정적의 Hybrid방식의 기법들을 제시**하고 있으나, **학술적 연구단계**에 머물러 있음

※ 대부분의 보안 솔루션들은 악성코드 탐지에만 초점을 맞추어, 본 기술과 같이 유사·변종 그룹분류의 자동화된 제품은 부재한 현황이며 백신진단 결과에 의해 수동으로 그룹분류를 수행함

o **(To-Be) 수치적 유사도 정보 기반의 실용적 자동 그룹분류 및 북한발 악성코드 등 집중 분석이 필요한 대상을 자동 식별** 가능

※ 2,639개 악성코드를 대상으로 시험한 결과, 절반에 가까운 1,121개를 10개 그룹으로 분류 가능 검증

□ 기술의 활용 분야

o APT 대응 분야에서 보안제품으로써 **대량의 악성코드 대응 솔루션/서비스**

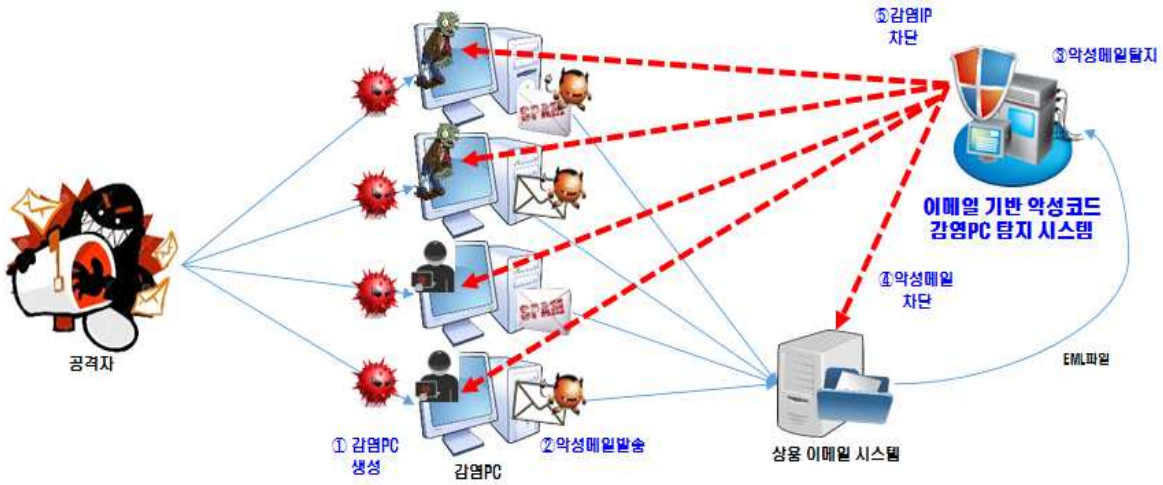
o 보안 담당자·분석가를 위한 **악성코드 분석·대응 도구**

3 좀비PC 자동수집 기술(이메일 기반)

□ 기술소개

o **(배경 및 필요성) 스팸메일의 80%가 악성코드에 감염된 PC에 의해 발송**되며, 이러한 감염 PC는 스팸메일 발송 뿐만 아니라 DDoS 등의 사이버 침해공격에 활용되므로 **적극적 차단이 필요**함

o **(주요기술)** 본 기술은 **이메일을 분석하여 악성코드에 감염된 PC를 자동으로 수집하는 기술**임



[기술 개요]

□ 기존 기술과의 차별성

기존 기술			개발 기술
RBL 차단	금칙어 필터링	첨부파일 백신검사	
알려진 악성 IP/도메인 차단	금칙어를 포함하는 이메일 필터링	첨부파일에 대한 악성코드 백신검사	발송경로 분석을 통한 비정상 이메일 및 좀비PC 탐지
알려진 **패턴에 기반한** 악성 이메일 탐지			**패턴에 기반하지 않는 감염IP 탐지**

□ 기술의 활용 분야

o 이메일 보안 제품으로써 **통합형 이메일 APT 보안 솔루션**

o APT 대응 분야에서 보안제품으로써 **대량의 침해사고 대응 솔루션/서비스**

o 보안관리/관제 분야의 보안솔루션으로써 **스팸메일 차단 및 좀비PC 조치 서비스**

※ 일일 1,000만개 이메일이 유통되는 포털사이트 적용시, 하루 수십만개 수준의 공격IP 탐지가 가능할 것으로 예상됨

4 모바일 악성앱 자동수집 기술

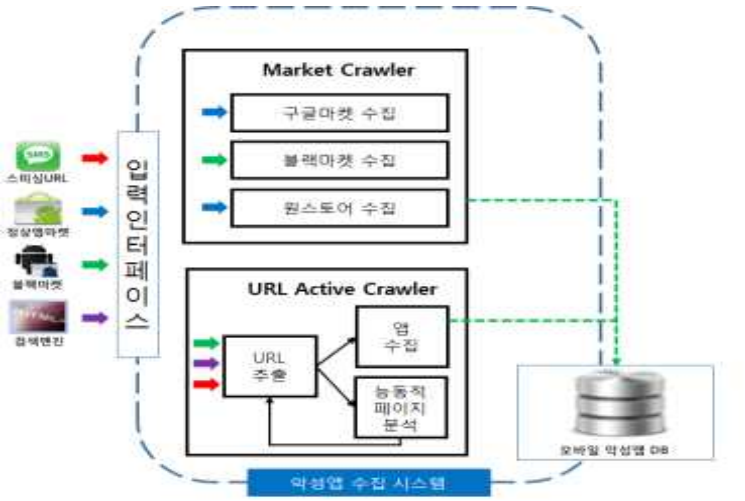
□ 기술 소개

o **(배경 및 필요성) 모바일 악성앱은 다양한 경로를 통해 유포량이 증가**하고 있으며 SMS/MMS, 블랙마켓, 앱마켓 등 다양한 경로를 통해 유포

- '14년 국내 유포된 모바일 악성앱은 143만개로 '12년 26만개 대비 약 550% 증가
- 지속적으로 증가하는 모바일 악성앱에 대한 대응을 위해서는 능동적으로 관련 정보를 수집하는 기술이 필요

o **(주요기술)** 본 기술은 모바일 결제사기의 공격도구인 악성앱을 대상으로 하는 **다채널 기반 광범위 모바일 악성앱 능동 수집** 기술임

- 채널별 특성을 고려한 지속적이고 능동적인 모바일 악성앱 수집 가능



[기술 개요]

□ 기존 기술과의 차별성

o **(As-is)** 악성앱의 주 유포지인 **블랙마켓 추적, 수집 기술**의 부재

- 기존 수집 기술로는 비정기적으로 변경되는 블랙마켓 유포지 추적이 어려움

o **(To-be)** 키워드 기반 **블랙마켓 의심 사이트 수집 및 분석**

- 신규 생성된 블랙마켓 URL 수집 및 기존 블랙마켓 추적 가능

※ 블랙마켓 의심 앱 정적 분석을 통해 의심 사이트 URL 수집

□ 기술의 활용 분야

o 모바일 보안 솔루션의 탐지 성능 향상(악성앱 탐지 패턴 개발)을 위한 기반 기술

o 모바일 악성앱 유포 탐지 서비스(웹/SMS 유포 악성앱 수집) 사업화

5 모바일 악성앱 자동분석 및 변종탐지 기술

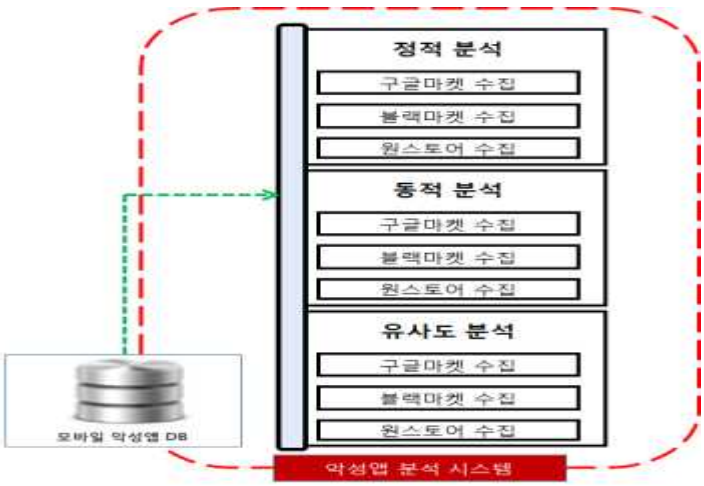
□ 기술 소개

o **(배경 및 필요성)** 악성앱의 국내 유포량 급증에 따라 피해 저감을 위한 신속한 악성앱 탐지 필요성이 높아지면서, 악성행위 탐지요소 도출을 위한 다양한 유형의 분석정보 도출이 필요

- '14년 국내 유포된 모바일 악성앱은 143만개로 '12년 26만개 대비 약 550% 증가

o **(주요기술)** 본 기술은 여러 채널을 통해 수집된 **앱의 정적/동적 분석, 유사도 분석** 등을 통해 **악성행위 유무를 파악하고 악성앱을 탐지**하는 기술임

- 모바일 악성앱의 악성행위를 판단하기 위한 주요 특성 정보 추출·분석
- 추출 및 분석된 악성행위 정보에 따라 유사 악성앱 분석 및 악성여부 탐지



[기술 개요]

□ 기존 기술과의 차별성

o **(As-is)** 기존 시스템의 **신·변종 악성앱 탐지한계** 및 **동적 분석의 기술성숙도 부족**

- 시그니처 기반으로 탐지하는 기존 검사로는 신·변종 대응이 불가

o **(To-be) 알려지지 않은 신·변종 악성앱의 악성 여부 분석 및 탐지** 가능

※ 악성앱 소스코드의 **Method단위 Binary 유사성 비교를 통한 유사 악성앱 탐지**

※ 악성행위와 관련된 **API, 바이러스 점검 결과 등을 통한 악성 의심 앱의 위험도 측정**

□ 기술의 활용 분야

o 모바일 보안 솔루션의 탐지 성능 향상(악성앱 유사도 분석)을 위한 기반 기술

o 모바일 악성앱 유포 탐지 및 대응 서비스(웹/SMS 유포 악성앱 분석/대응) 사업화

6 Machine Learning 기반 분석지원 도구

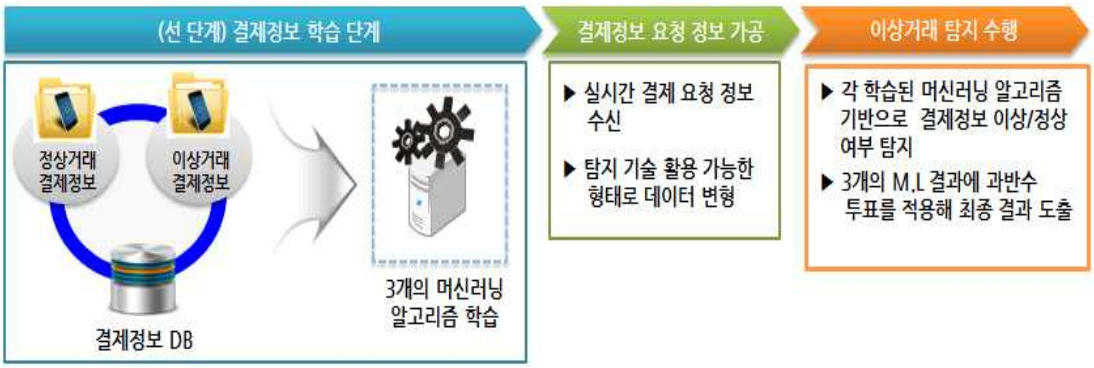
□ 기술 소개

o **(배경 및 필요성)**금융권에서는 이상금융 거래탐지기술(FDS)를 구축·운영하여 금융 사고에 적용하고 있으나, 현 FDS는 기능과 정확도(이상거래 탐지율 0.55%)가 현저히 낮은 수준임

- 지능화되는 금융 사고에 유연하게 대응 가능한 이상거래 탐지 기술이 필요함

o **(주요 기술)** 본 기술은 **머신러닝(Machine learning) 기반으로 데이터 분석 및 패턴 학습을 통해 특정 정보를 탐지(분류)하는 기술임**

- (주 기능) 모바일 결제 분야의 정상/이상거래를 식별하는 기능
- (확장성) 입력 Data 유형(Form) 변경을 통해 다양한 분야에 ML 기반 분석 도구로 활용 가능



<머신러닝 기반 탐지 기술 데이터 처리 개념도>

□ 기술의 차별성

o **(As-is)** 룰(Rule) 기반의 탐지 모델로 정형화된 **룰 이외의 이상거래 탐지 불가**

- 대부분 FDS 기술은 사고분석 및 이상거래 탐지룰 적용 등이 전문가에 의해 이루어짐

o **(To-be)** 학습기반 이상거래 탐지 **로직을 자동 구축하여, 신규 이상거래 자동 탐지 가능**

- 지속적 학습을 통해 변화하는 결제사기 패턴에 유연하게 대응 가능

※ 복수의 러닝머신 알고리즘을 채택하는 앙상블 구조로 이상결제 분류 결과의 신뢰성 제고

□ 기술의 활용 분야

o 금융 분야에서 이상거래 탐지 서비스 및 솔루션에 활용

- 기존에 구축된 FDS 시스템에 미탐지 이상거래를 탐지하기 위한 일환으로 부가 시스템으로 적용하거나, 신규 이상거래 탐지 시스템 구축에 활용 가능

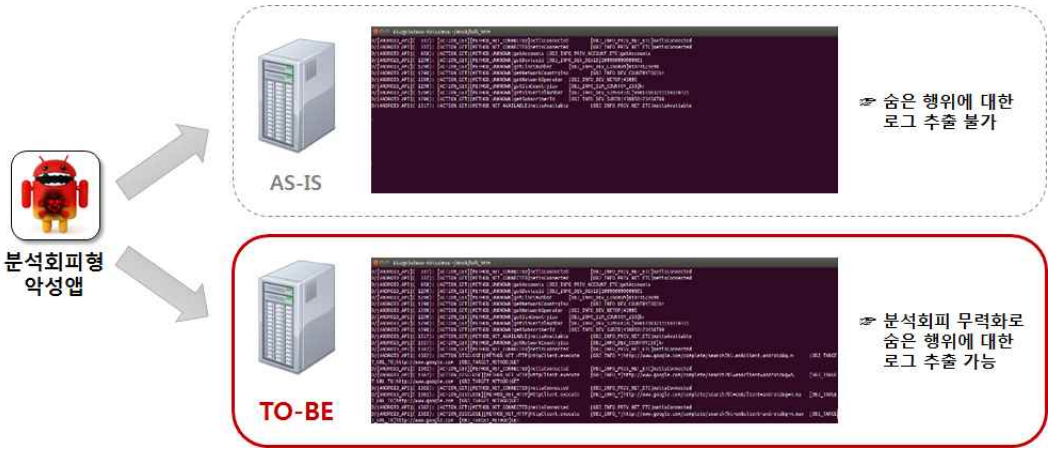
7 에뮬레이터 기반 지능형 악성앱 행위 무력화 및 분석 기술

□ 기술소개

o **(배경 및 필요성)** 악성앱이 생존율을 높이기 위해 자가보호 기술을 탑재하는 등 **지능화·정교화됨에 따라 기존의 분석기술을 우회하는 악성앱이 출현**함

※ '15년 구글의 분석시스템 '바운서'를 우회한 악성앱이 앱스토어를 통해 유포되어 200만대 이상의 기기 및 100만명 이상의 사용자가 감염되는 피해가 발생

o **(주요기술)** 가상환경을 탐지하여 분석을 우회하는 **지능형 악성앱의 분석회피 행위를 무력화**함으로써 **숨겨진 악성행위를 유도**하여 분석로그를 추출함



[기술 개요]

□ 기존 기술과의 차별성

o **(As-is) 분석회피를 시도하는 지능형 악성앱에 대한 자동분석 기술 부족**

※ 대부분의 가상환경 기반 악성앱 동적분석 시스템의 경우 분석회피형 악성앱을 탐지하지 못하고 있으며, 일부 업체의 경우 실제 단말을 사용해 분석을 수행함

o **(To-be) 에뮬레이터 환경에서 분석회피형 악성앱 자동분석 및 탐지 가능**

- 에뮬레이터 환경 탐지 행위 무력화를 통해 숨겨진 악성행위 로그 추출

※ 가상환경 탐지에 사용되는 주요 기술에 대한 분석을 통해 실제 단말로 인식하도록 함

□ 기술의 활용 분야

o 모바일 보안 분야에서 **악성앱 탐지 및 대응을 위한 솔루션/서비스**로 활용

o 모바일 악성앱 탐지 분야에서 **대량의 악성앱 자동분석 시스템/서비스**로 활용

o 모바일 보안 담당자·분석가를 위한 **악성앱 자동분석 도구**로 활용

8 사이버 침해사고 공격정보 및 연관정보 자동수집 기술

□ 기술 소개

o **(배경 및 필요성)** 침해사고와 관련된 악성 IP, Domain 및 악성코드는 재사용되는 경우가 많으며, 이에 대한 이력을 관리할 필요가 있음

o **(주요기술)** 본 기술은 다양한 출처에서 탐지된 침해사고 공격정보(IP, Domain, 악성코드)를 주기적으로 자동수집/공격이력 관리를 통해, 침해사고 분석정보를 제공하는 기술임

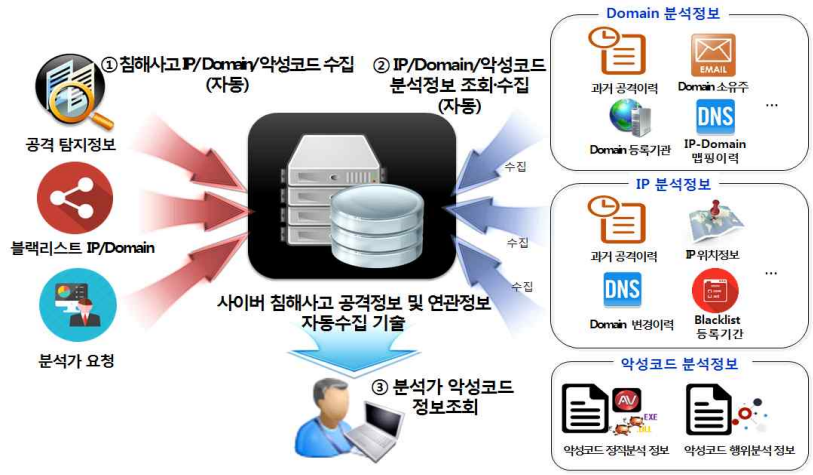
- C&C, 유포지, DDoS 등 침해사고 공격에 활용된 IP, Domain, 악성코드 수집 및 이력관리

※ Cshare, DNSBL서버 등 10개 Intelligence feed에서 침해사고 정보 수집

- 공격 IP, Domain과 관련된 OSINT정보 자동수집

※ OSINT(오픈 소스 인텔리전스) : 공개된 채널로 공유되는 침해사고 관련 분석 정보

※ Intelligence분석을 위한 침해사고 메타데이터(공격자 위치, Email, DNS변경이력 등) 수집



[기술 개요]

□ 기술의 차별성

o **(As-is)** 침해사고 분석 시, 과거의 침해사고와 연관성을 확인하기 위하여 다수의 데이터 분석과 조회가 필요함

o **(To-be) 침해사고 악용IP, Domain, 악성코드에 대한 연관정보를 수집 및 관리**하기 때문에, 침해사고를 분석 할 수 있는 영역이 확대됨

□ 기술의 활용 분야

o 유사 침해사고에 활용되는 **공격IP, Domain, 악성코드의 이력관리** 및 **침해사고 분석정보 제공**

- 침해사고 분석을 위한 공격이력 관리 및 침해사고 Intelligence분석 정보로 활용

9 사이버 침해공격에 대한 Intelligence 분석 기술

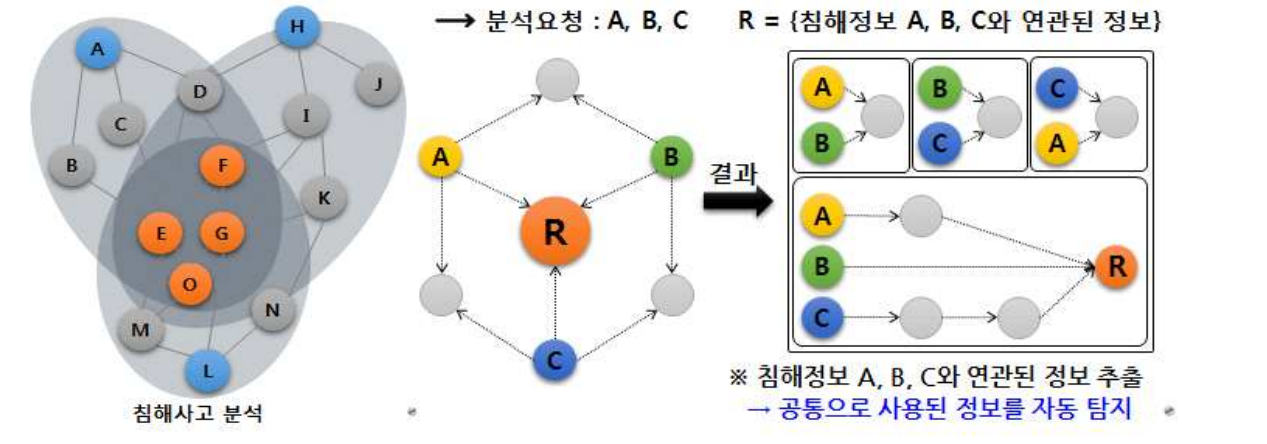
□ 기술 소개

o **(배경 및 필요성)** 침해사고의 확산에 따라 수많은 침해사고 간 연관관계 및 의미분석의 어려움으로 인하여 신속한 대응에 한계가 있음

o **(주요기술)** 본 기술은 침해사고와 연관된 수집정보에서 **주요 연관관계를 추출**하며, 이를 기반으로 침해자원 **연관정보 그룹 간 연관성 수준을 판단**하는 기술임

- 공격자 식별정보(Intelligence 분석근거) 기반 침해정보 간 주요 연관관계 추출
- 연관관계 기반 침해자원 연관정보 그룹 생성 및 그룹 간 연관성 수준 도출

※ 침해정보 메타데이터 기반 연관관계(악성코드 유포/경유/통신, 도메인 등록정보, 동일 네트워크 대역 정보 등)



[침해정보 Intelligence 분석 기술 개요]

□ 기술의 차별성

o **(As-is)** 다각적인 보안 위협의 급증으로 인하여 침해사고 대응을 위한 분석시간 및 대응인력이 부족함

o **(To-be)** 동일/유사 침해사고 분석결과 기반 침해사고 연관관계 자동분석을 통해, **추가적인 사고분석을 위한 정보 도출**이 가능

- 서로 다른 침해사고 간 연관관계 존재여부 및 연관성 수준을 진단하여 침해사고 트렌드 분석 및 공격자원 추적 가능

□ 기술의 활용 분야

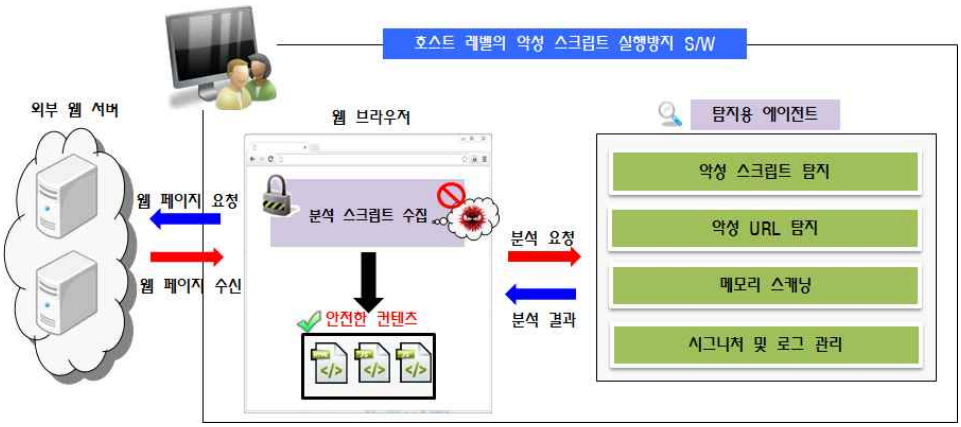
o 신속한 사고분석 및 종합분석을 위한 **침해사고와 연관된 침해정보 제공**

- 수집된 침해사고 정보기반 연관관계를 추출·관리하여, 대형 침해사고 분석에 활용

10 호스트레벨 악성 스크립트 탐지/실행방지 기술

□ 기술 소개

o 사용자 PC의 웹 브라우저에서 실행되는 웹 컨텐츠(HTML, 자바스크립트 등)에 대해 악성 여부를 검사하고 차단하는 악성스크립트 탐지 전용 백신



[기술 개념도]

o 웹 브라우저에 삽입된 플러그인 S/W를 통해 웹 페이지 추출
- 사용자 브라우저에서 웹페이지 실행 이전 시점 체크하여 웹 페이지 및 외부 링크 URL의 소스 추출

o 시그니처 검사 및 스크립트 실행 함수분석을 통한 악성 검증
- 웹 지연 시간 최소화를 위한 시그니처 기반 고속 정적 분석 진행
- 악성 행위를 유발하는 자바스크립트 함수 정보를 기반으로 탐지

o 메모리 스캔 및 난독화된 스크립트 탐지
- 프로세스 메모리 덤프 정보를 기반으로 악성 스크립트 추출
- 난독화*된 자바스크립트에 대한 원본 추출 및 악성 검사

*** 난독화 스크립트: 코드자체를 이해할 수 없도록 변형하여, 기존 보안장비의 탐지를 회피**

□ 기술의 차별성

o (**사용자 PC단 악성스크립트 차단**)기존 백신에서는 악성코드를 대상으로 탐지하나, 본 기술은 브라우저의 실행 웹 페이지를 분석→ 악성스크립트 차단
- (적용방식)플러그인 방식으로 웹 브라우저에 보안 프로그램 등록
- (탐지 대상)난독화 스크립트, 자바스크립트 API, 의심 태그 검사

□ 기술의 활용 분야

o 일반 PC 및 모바일용 악성 스크립트 차단 전용 백신으로 활용

11 네트워크 레벨 스크립트 기반 사이버 공격 차단 기술

□ 기술 소개

o **사용자 PC와 웹 사이트 간 모든 웹 트래픽를 수집하여 악성 스크립트에 대해서 탐지하는 웹 보안 기술**

- 네트워크상의 모든 웹 트래픽에 대해서 정적 분석 및 동적 분석 실행
- 별도 자바스크립트 엔진을 통해 스크립트를 직접 실행 하여 난독화된 스크립트의 원본 및 실행 함수 정보 등을 추출 하여 악성 검증

[스크립트 기반 DDoS 공격 시나리오]

□ 기술의 차별성

o **(웹 컨텐츠 정밀 분석)**본 기술은 웹 페이지를 구성 하는 모든 컨텐츠에 대한 정밀 검사를 진행하고, 난독화된 스크립트 탐지가 가능한 기술임.

- 기존 네트워크 침입탐지 솔루션의 경우 패킷 단위의 트래픽 분석을 통해 악성 코드를 탐지하나, 본 기술은 웹 페이지의 외부 링크 소스까지 포함 검사
- 난독화 여부 검사 및 원본추출 스크립트의 악성 여부 검사
- (적용방식)기존 웹 방화벽, IDS/IPS 장비와 동일한 구간 위치
- (탐지 대상)난독화 스크립트, 자바스크립트 API, 의심 태그 검사

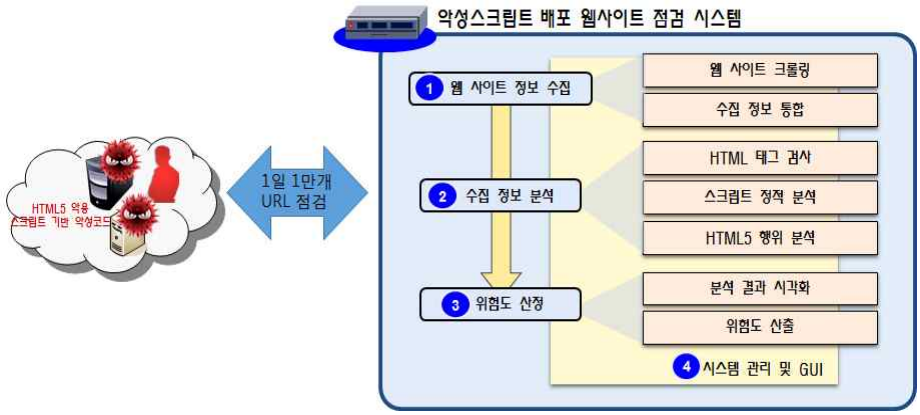
□ 기술의 활용 분야

o 악성 스크립트 차단을 위한 네트워크 보안 장비로 활용

12 악성 스크립트 배포 웹 사이트 점검 기술

□ 기술 소개

o 악성 스크립트가 등록된 웹 사이트의 웹 컨텐츠에 대해서 사전 수집 및 분석을 통해 검증하는 기술



[시스템 구성도]

o 본 기술은 입력된 점검 대상 웹 사이트에 대해서 주기적인 웹 사이트를 스캔하여 게시된 악성 스크립트를 탐지하는 웹 보안 기술 임

- 웹 사이트를 자동 스캔하여 난독화 스크립트* 추출, 스크립트 변조 여부 점검

*** 난독화 스크립트: 코드자체를 이해할 수 없도록 변형하여, 기존 보안장비의 탐지를 회피**

□ 기술의 차별성

o **(HTML5 웹사이트 고속 점검)**웹 사이트 점검을 위한 HTML5 문서 고속 스캔 및 가상 환경에서 HTML/스크립트의 행위 분석 기술 적용

- 대용량 HTML 문서 크롤링 및 고속 처리 기술 구현을 통해 홈페이지 변조, HTML5의 취약 태그 및 API 검사

  *** 1일 50개 HTML5, 1만개 HTML4 사이트 대상 스크립트 검사**

- 상세 행위 분석을 위해 단일 웹 페이지의 사용자 이벤트(마우스, 키보드 등)을 가상 브라우저에서 직접 실행 검사

□ 기술의 활용 분야

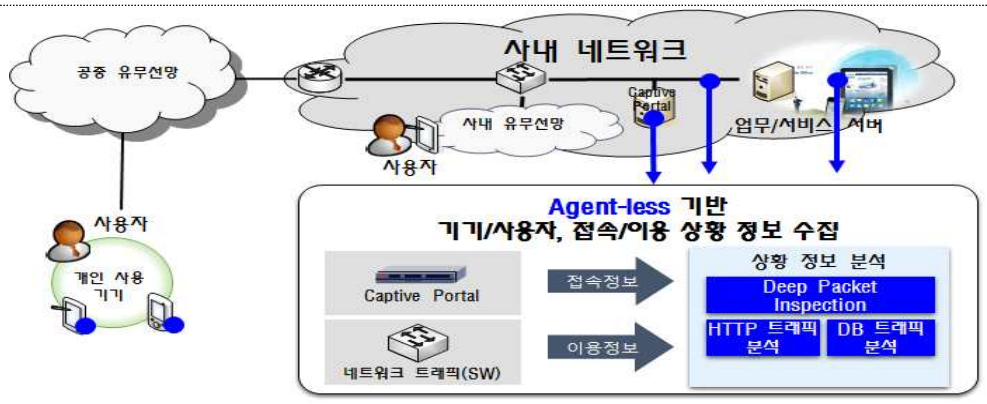
o 웹 사이트 점검 스캐너로 활용

13 모바일 디바이스의 Agentless 방식 상황정보 수집 기술

□ 기술 소개

o Agentless방식으로 회사 업무망에 접근하는 기기 정보를 수집하고, 사용자의 서비스 접속 및 이용 행위에 따른 상황정보를 수집하는 기술임

※ 상황 정보 : 사용자가 기업 내부 서비스에 접속 및 이용하는 모든 행위를 데이터로 규정하여 상황을 인식하기 위한 정보



[기업 내부 네트워크 접근 사용자/기기 상황정보 수집]

- 모바일 기기 정보 수집(Browser Fingerprinting 기술 활용)
  ※ Browser Fingerprinting : 웹 페이지에 Java Script를 적용하여 Web Browser에 접속하는 기기 정보를 수집하는 기술
- 사용자 인증 정보 수집(Captive Portal 인증, 인증 서버 연동)
- 서비스 이용 정보 수집(웹 서비스 이용 정보, DB 자원 이용 정보)

□ 기술의 차별성

o **(As-Is)** 기존 모바일 기기 보안 기술은 단말기 관점에서의 보안 기술임
- MDM/MAM : 모바일 기기 관리를 위해 기기에 Agent 설치 필요

o **(To-Be)** 개발한 기술은 여러 관점에서의 상황정보를 기반으로한 보안 기술임
- '누가', '언제', '어디서', '어떻게', '무엇을' 기준으로 사용자 및 기기, 행위 정보 등을 종합적으로 수집하여 상황을 인식하고 관리할 수 있음
- Agent 설치, 기업 데이터 저장 형태에 관계없이 네트워크 트래픽만으로 상황정보를 수집

□ 기술의 활용 분야

o 기업 모바일 오피스 접속 및 이용에 따른 상황정보 수집 및 관리 기술로 활용

14 모바일 기기의 웹 서비스 접속 및 이용 행위 분석 기술

□ 기술 소개

o 기업 모바일 오피스를 이용하는 사용자의 접속 및 이용 행위를 분석하여 비정상 행위를 판별하는 기술

- 비정상 행위 판별을 위해 사용자의 네트워크 트래픽을 수집하여 분석 및 관리
- 사용자의 과거 행위 정보와 현재 발생한 행위와의 유사도를 분석하여 비정상 행위를 판별하고 관리자에게 정보를 제공

[사용자 계정 정보 및 기기 관리 소홀을 통한 보안 위협]

- 공격자는 유출된 직원 계정 및 빈번한 변경, 임대, 분실 등의 경로로 사용자 인증 정보가 저장된 기기를 도용하여 기업 정보 유출 시도
- 내부 또는 협력업체 직원이 악의적인 목적으로 모바일 오피스에 접속하여 기업 내부 정보를 무분별하게 조회·수집하여 유출 시도

□ 기술의 차별성

o (As-Is) 기존 방화벽·IDS·IPS 등 알려진 공격 패턴을 탐지하는 기술
- [한계점] 정상 사용자의 계정, 기기를 도용한 공격자의 접속 판단 불가

o (As-Is) 사용자 인증 기반 네트워크 접속 제어 시스템(NAC)
- [한계점] 내부 네트워크 접속 이후 발생하는 사용자의 비정상 행위 판단 불가

o (To-Be) 업무 서비스 이용에 대한 모든 사용자의 행위를 분석 및 관리
- [차별성] 정상 사용자의 계정/기기를 도용하거나, 악의적인 의도를 품은 정상 사용자의 비정상적인 서비스 이용 행위 탐지

o (To-Be) 과거 접속 상황과의 유사성, 업무 서비스 이용 행위 패턴 분석
- 패턴화된 행위 비교 기술을 활용한 6가지 이상 행위 패턴 심층 분석

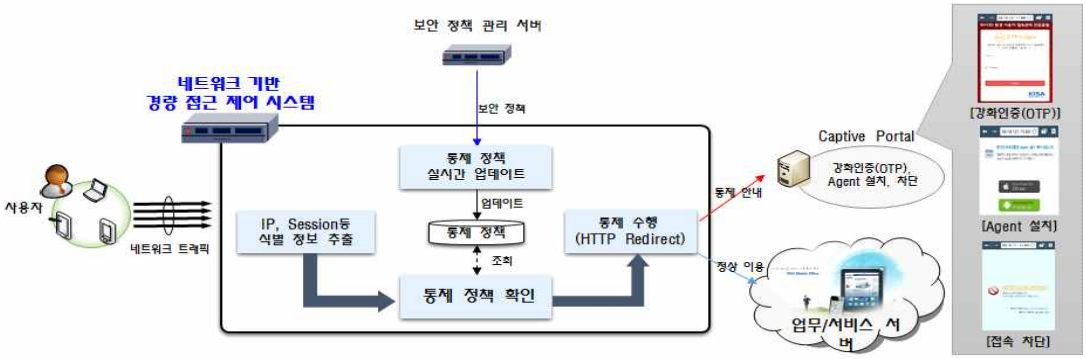
□ 기술의 활용 분야

o 기업 내부 웹 사이트 정보 보안을 위한 비정상 행위 탐지 기술로 활용

15 사용자/기기 내부 네트워크 경량 접근제어 기술

□ 기술 소개

o 기업내부에서 사용자별 보안 정책 연동을 통해 네트워크 제어 기능을 수행하는 기술



[IP/SessionID 기반 사용자 기기 내부 네트워크 접근제어]

- 사용자/기기의 회사 업무망 접근 허용 여부를 동적으로 관리하며, 연동된 통제 정책에 따라 사용자를 실시간으로 제어
- 사용자 접근시 IP와 Session ID를 기준으로 해당 사용자의 통제 정책을 조회하여 통제 수행

□ 기술의 차별성

o **(As-Is)** 기존 네트워크 접근 제어(NAC) 및 기기 제어(MDM) 기술
- [한계점] 기기 제어를 위해 별도의 소프트웨어 설치가 필요하며, 미설치시 외부 네트워크에서의 내부 접속 사용자에 대한 제어 한계 존재

o **(To-Be)** Agent-less 기반 네트워크 트래픽 접근 제어
- 별도의 Agent 설치 없이 트래픽 제어만으로 사용자 제어 수행

o **(To-Be)** Session ID 관리를 통한 외부 사용자 제어
- IP 이외에 Session ID를 추가로 관리함으로써 외부 사용자 및 공용 Wi-Fi를 통한 접근 시에도 정확한 사용자 식별 및 실시간 제어 수행

o **(To-Be)** 상황정보 기반 보안 수준별 동적 제어
- 정적인 규칙 설정이 아닌 상황정보 기반 보안 정책 연동을 통해 동적인 제어 수행
- 사용자의 단순 차단 이외에 보안 수준별로 차등 조치

□ 기술의 활용 분야

o 기업 내부 네트워크 접근 사용자/기기 경량 제어 기술로 활용

16 악성앱 점검 도구 폰키퍼(Phone Keeper)

□ 기술 소개

o 스마트폰의 보안설정 점검, 백신설치 여부, 악성앱 점검 등을 해주는 스마트폰 보안 자가점검 도구

[폰키퍼 개요]

□ 주요기능

o **(보안설정 점검)** 비밀번호, 출처를 알 수 없는 앱 설치 허용 옵션 등을 점검 후, 보안이 취약한 항목에 대하여 조치방법 제시

o **(악성앱 점검)** 스마트폰에 설치된 앱(App) 중 악성행위를 하거나, 개인정보를 저장하는 앱을 탐지하여 삭제

o **(앱권한 점검)** 앱 고유의 특성과 다른 기능을 사용하는 경우 사용자가 이를 인지하고 삭제할 수 있도록 지원

o **(앱 분석요청)** 스마트폰에 설치된 악성 의심 앱(App)을 KISA에 전달하여 여러 백신업체의 온라인 백신 진단 결과를 확인할 수 있도록 지원

o **(보안공지)** 실시간 침해사고 정보 및 대응방안에 대한 정보 전달

□ 기술의 차별성

o **(보안설정 점검)** 모바일 악성 코드에 감염되지 않도록 패스워드 설정, 백신 설치 실행 등을 안내하는 기능 제공

o **(보안공지 알림)** 기존 스마트폰 백신과 달리 스미싱 문자 등 각종 보안 공지에 대한 알림 서비스 제공

□ 기술의 활용 분야

o 스마트폰 보안 상태 점검 도구로 활용

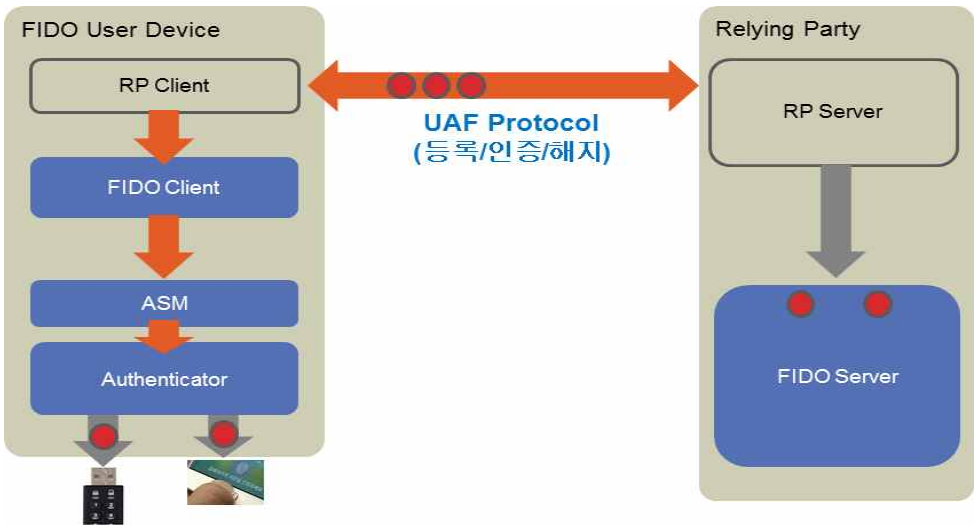
17 ~ 18 FIDO 1.0 인증기술

□ 기술소개

o **(배경 및 필요성)** 기존 패스워드 및 공인인증기술의 이용 불편함과 보안 취약성이 제기됨에 따라 온라인에서 안전한 인증 프로토콜을 사용하면서 보안요구사항에 따라 사용자를 인증하는 방법을 선택할 수 있는 기술 필요

o **(주요기술)** 본 기술은 FIDO 1.0 UAF (Universal Authentication Framework) 표준을 준용하여 사용자의 스마트폰에서 인증장치를 FIDO 서버에 등록/인증/해지와 거래확인 기능을 제공하는 기술

- **(세부기술 1) FIDO 1.0 서버 기술**
  - 다양한 환경의 서비스에서 FIDO 1.0 인증 기술을 이용하여 사용자를 인증할 수 있도록 하는 서버 및 클라이언트 기능을 제공
  - FIDO 1.0 서버 기술, FIDO 1.0 클라이언트 기술, FIDO RP Client 기술로 구성
- **(세부기술 2) FIDO 1.0 S/W 인증장치 기술**
  - 사용자가 소지한 안드로이드 계열 스마트폰에서 간단한 패스코드 입력을 통해 FIDO 1.0 인증 기능을 제공하여 별도의 장치를 추가하지 않고도 사용자에게 친숙한 패스코드 입력을 통해 안전한 FIDO 1.0 인증 기능을 제공
  - FIDO 1.0 ASM 기술 및 FIDO 1.0 인증장치 기술로 구성



[기술개념]

□ 기존 기술과의 차별성

o **(As-Is)** 현재 인증기술은 개별 인증방법만을 지원하여 다양한 보안요구사항을 지원하기 위해서는 다중 인증서버의 설치가 불가피함

※ 공인인증기술로 사용자 인증을 하는데 지문인식 인증기술을 추가하려면 지문인식 인증서버 설치가 필요하여 비용과 관리의 부담이 발생함

o **(To-Be)** FIDO 기술 적용시 사용자 환경에서는 바이오(지문/홍채/얼굴/음성) 인증 및 보안 토큰 인증을 요구사항에 맞게 다양하게 사용할 수 있음

□ 기술의 활용 분야

o 기존 공인인증기술이 적용되던 금융, 보험 및 증권거래와 온라인쇼핑에 적용

o 건물 출입통제 및 오프라인 결제 등 O2O (Online-To-Offline 비즈니스에 적용 가능

19 스마트채널3 기술

□ 기술소개

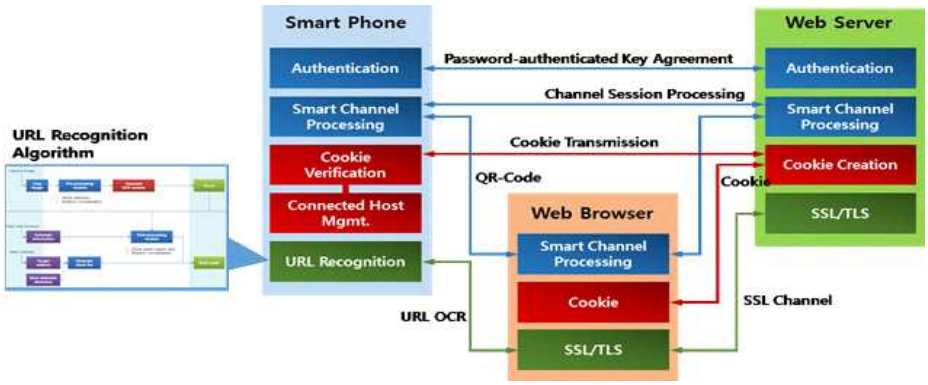
o **(배경 및 필요성)** 피싱(Phishing)/파밍(Pharming) 공격을 통한 사용자의 인증, 금융 정보 유출 심각

o **(주요기술)** 본 기술은 브라우저 독립성을 유지하여 어떠한 플랫폼의 어떠한 브라우저에서도 별도 플러그인 없이 동작하는 인증/결제 기술로, 서버와 클라이언트 간의 상호인증 프로토콜, 보안쿠키 및 스마트폰 카메라로 서버 URL을 검증하여 피싱/파밍을 차단하는 기술

※ 스마트채널 : 스마트폰을 활용한 QR코드 기반의 2 Channel 상호인증 프로토콜

※ 보안쿠키 : 재사용 공격 방지 및 키관리를 해결한 보안쿠키를 이용한 웹브라우저 체크 기술

※ SSL 주소 검증 : 스마트폰 카메라를 이용한 서버의 HTTPS 주소 인식 기술



<스마트채널3 기술개요>

□ 기존 기술과의 차별성

o **(As-Is)** 피싱/파밍 공격을 막기 위해, 매번 PC에 별도의 전용 소프트웨어 설치나 사용자의 적극적인 개입을 요구함

※ 제로데이 악성코드 등을 활용한 고도화된 피싱/파밍 공격에 안티 피싱/파밍 소프트웨어가 공격받는 취약성 존재

※ 사용자가 직접 URL 주소나 SSL 연결 여부를 확인해야 하는 번거로움 존재

o **(To-Be)** 사용자의 스마트폰에서 서버-클라이언트 인증을 수행하고, URL 주소를 스마트폰 카메라로 검증하여 보안성과 편의성 모두 개선함

□ 기술의 활용 분야

o 피싱이나 파밍 공격으로부터 안전한 인증·결제 솔루션/서비스

20 ~ 24 MTM기반 스마트 단말 보안시스템 구현 기술

□ 기술소개

o **(배경 및 필요성)** 개방형 OS 기반의 스마트 단말기 보급 확산과 자유로운 앱 생태계로 인하여 해킹, 피싱(스미싱) 등의 **보안 위협이 증가하고 단말 분실 및 도난으로 인한 정보 유출 가능성이 매우 높음.**

o **(주요기술)** 본 기술은 MTM(Mobile Trusted Module)을 이용하여 **모바일 단말의 무결성 검증을 통해 단말 시스템의 불법적인 변경을 탐지하는 기술**임

- Secure Booting 및 플랫폼 무결성 검증 기능을 통해 안전한 실행환경 보장
- 악성 앱의 탐지 및 실행 차단을 통해 서비스의 신뢰성 보장

- **(세부기술 1) 보안 기능 추상화 및 미들웨어 관리 기술**
  - 스마트 디바이스(단말)에서 인증/지불/스마트 뱅킹 등과 같은 고수준의 보안성이 요구되는 응용 서비스가 안전하게 운용될 수 있도록 이들 서비스에 미들웨어 관리 및 보안기능 추상화 API를 제공
  - 보안 정책 및 미들웨어 설정/관리 기능, 보안 응용 서비스 지원 기능, 보안 기능 추상화 API 제공 기능으로 구성
- **(세부기술 2) 암호 및 컨텍스트 관리 기술**
  - 고수준의 보안성이 요구되는 단말의 보안 응용서비스 및 보안정책, 보안 기능 추상화를 효과적으로 지원하는 MTM 기반 암/복호화, MTM 접근을 제어하는 컨텍스트 관리 및 미들웨어 서비스 제공
  - MTM Internal Key 기반 데이터 암/복호화 지원기능, MTM 보안기능 사용을 위한 컨텍스트(세션 연결) 관리 기능, MTM 동시 접근 제어용 미들웨어 기능으로 구성
- **(세부기술 3) 단말 무결성 측정 및 검증 기술**
  - 단말 시스템에 전원이 인가되는 시점에 단말의 부트로더, 커널, 안드로이드 시스템, 주요 네이티브 시스템 서버 등의 무결성 측정 및 검증 기능을 단계적으로 수행하여 점검하고, 단말 시스템이 해킹 및 악성코드에 의해서 불법적으로 변경되었을 경우 무결성 검증을 통해 탐지하는 기능을 제공
  - 단말 무결성 측정 및 검증 기능, 무결성 검증 정보 통신 및 제어 기능, 무결성 측정 및 검증 구조 관리 기능으로 구성

- **(세부기술 4) MTM 및 보안서비스 실행엔진 기술**
  - 단말 시스템과 MTM 사이의 세션 연결 설정 및 관리를 통해 명령어를 전송하고, 전송된 명령어 따라 MTM 명령과 보안 서비스 명령을 실행
  - 메시지 관리 기능, MTM실행엔진 기능, 보안 서비스 실행엔진 기능으로 구성
- **(세부기술 5) MTM 암호 및 저장관리 기술**
  - MTM에서 필요로하는 RSA 공개키 암호, 대칭키 암호, 해쉬함수등의 다양한 암호알고리즘을 제공
  - MTM용 암호 알고리즘 기능 및 MTM용 저장관리 기능으로 구성

[기술 개요]

□ 기존 기술과의 차별성

o **(As-Is) 모바일 백신, MDM등을 이용하여 모바일 단말의 Application level의 변경 및 훼손 여부를 검증함으로써 검증 범위가 제한 적임**

※ 시스템 라이브러리 검증, 커널 및 부트로더 영역의 신뢰성 검증은 불가능함

o **(To-Be) MTM을 기반으로 모바일 시스템의 전반적인 영역에 대해 변경 및 훼손 여부를 검증할 수 있음**

※ 적용방식 : 모바일 단말의 커널 및 응용 프로그램에 적용

※ 탐지대상 : 모바일 단말의 부트 코드, 커널, 시스템 라이브러리 등 시스템 영역 전반의 코드영역에 대한 변경 및 훼손 탐지

□ 기술의 활용 분야

o 스마트 단말용 **금융 서비스**(MTM기반의 모바일 뱅킹, 지불, 결제) 보안

o MTM 보안 칩을 활용한 **스마트 디바이스용 보안**

25 ~ 26 데이터 보호 및 안전한 처리를 지원하는 스마트 단말용 은닉형 보안플랫폼 기술

□ 기술소개

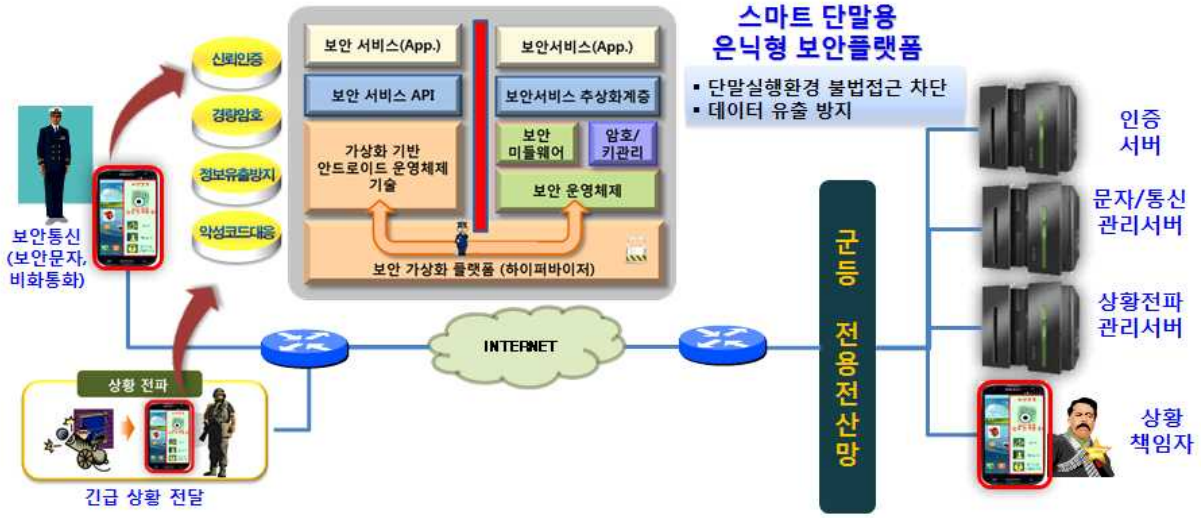
o **(배경 및 필요성)** 악성 코드의 지능화 및 진화로 인해 악성 코드에 의한 스마트단말 내의 정보 유출 피해가 급증하는 환경에서, 정**보 유출 방지 및 보안 연산에 대한 신뢰된 운영환경 제공**이 가능한 보안플랫폼 기술의 요구가 증가하고 있음

o **(주요기술)** 본 기술은 스마트 모바일 단말 환경에서 **비인가된 접근을 차단**하고, 모바일 단말의 **안전한 운영 환경을 보장**하기 위한 모바일 단말 보안 플랫폼 기술

- 가상화를 통한 분리된 운영환경 기반의 보안 기능 제공
- 모바일단말 기반 보안 미들웨어용 암호 및 키관리
- 신뢰앱 및 사용자 인증 기반 분리된 보안영역에 대한 강력한 접근 통제
- 국제 표준 규격(FIPS-196) 준수를 통한 인증서 기반 상호인증 호환성

• **(세부기술 1) 경량 보안OS 기반 은닉형 보안플랫폼 기술**
  - 안드로이드OS와 분리된 보안영역에서 운영
  - 일반영역에서 호출된 보안 API 메시지를 해석 및 관리하는 기능을 포함
  - 보안영역 접근에 대한 2-Factor 인증(Admission) 기능, 보안영역 접근제어(Access Control) 및 메시지 관리 기능, KCMVP 대응 암호 알고리즘 및 키관리 기능, 안전한 저장관리(Secure Storage) 기능으로 구성

• **(세부기술 2) 보안플랫폼용 보안 API 및 추상화 기술**
  - 안드로이드OS의 보안서비스가 은닉형 보안플랫폼의 보안기능을 사용할 수 있도록 개발자에게 제공된 API와 일반영역 보안API의 구현을 제공하는 보안영역에서의 추상화 라이브러리로 구성
  - 일반영역에서의 보안플랫폼 활용을 위한 보안API 주요 기능, 보안영역의 보안서비스 추상화 기능, 일반영역 메시지 관리 기능으로 구성



[기술 및 서비스 적용 개념도]

□ 기존 기술과의 차별성

o (As-Is) 단일 운영환경 기반의 모바일 단말 구조로 모든 정보가 단일 운영환경에 공존하여 악성코드에 의한 중요 정보의 불법접근 및 유출 가능성 높음

o (To-Be) 분리된 운영환경 구조의 모바일 단말 보안 제공을 통해 일반 모바일 환경의 악성코드에 의한 중요정보의 불법접근 및 유출 방지 구조 제공

□ 기술의 활용 분야

o 정보유출 방지가 필요한 지휘용 보안단말, 군업무용 이동보안단말, 상황전파용 보안단말 등 **군용 보안단말 솔루션**

o 금융거래서비스, 의료관리서비스, 원격관리서비스 등 안전한 인증 및 데이터 보호가 필요한 **원격서비스의 신뢰 보안단말 솔루션**

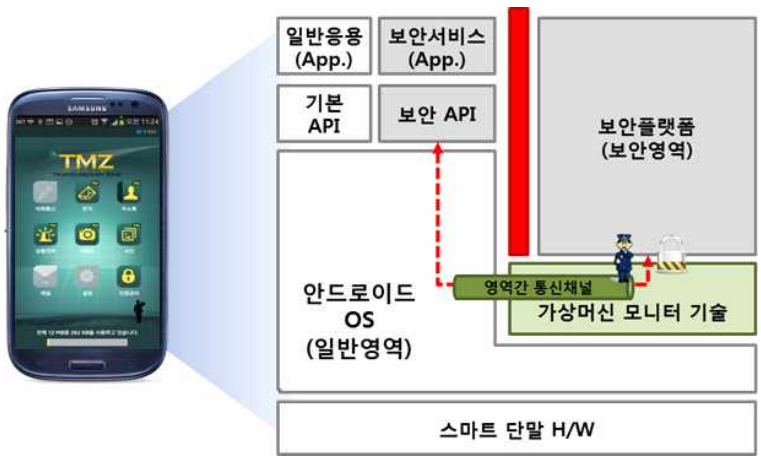
27 스마트단말 보안플랫폼용 TYPE-2 가상머신 모니터 기술

□ 기술소개

o **(배경 및 필요성)** 악성 코드의 지능화 및 진화로 인해 악성 코드에 의한 스마트 단말 내의 정보 유출 피해가 급증하는 환경에서, **정보 유출 방지 및 보안 연산에 대한 신뢰된 운영환경 제공**을 위한 **운영환경 분리 기술이 필요**함

o **(주요기술)** 본 기술은 분실 및 도난의 가능성과 악성코드 위협이 높은 스마트단말 환경에서 모바일 OS(안드로이드OS)가 동작하는 일반영역과 보안기능을 제공하는 보안영역으로 **운영환경을 분리하는 TYPE-2 기반의 가상머신 모니터** 기술임

- 스마트단말 등을 포함하는 모바일 시스템을 위한 마이크로 가상 머신 모니터
- 기존 상용 단말 위에서 게스트 운영체제로 uCOS-II 구동
- 호스트 운영체제와 게스트 운영체제와의 통신 지원



[기술 및 서비스 적용 개념도]

□ 기존 기술과의 차별성

o **(As-Is)** 모바일 단말 내의 운영환경 분리에 집중되어 있고, 분리된 영역 간의 메시지 교환이 불가능하여 분리된 영역을 독립된 운영환경으로 구축해야 됨

o **(To-Be)** 분리된 영역간 메시지 교환 기능을 제공하여, 최소한의 운영환경을 게스트 운영체제로 활용할 수 있고, 모바일 단말 내에 TEE(Trusted Execution Environment) 운영 환경 구축을 가능하게 함

□ 기술의 활용 분야

o 정보유출 방지가 가능한 원천적인 아키텍처가 요구되는 군 및 공공 서비스용 **보안 강화형 스마트 단말 솔루션**

28 화이트박스 암호를 이용한 무인항공기 보안기술

□ 기술소개

o **(배경 및 필요성)** 무인항공기와 같이 공격자에 의해 탈취 가능성이 존재하는 응용에서는 기기내의 암호 비밀키의 유출 가능성에 대한 대비가 있어야 함.

o **(주요기술)** 탈취 가능성이 있는 기기에 대하여 암호 비밀키의 보호를 위하여 화이트박스 암호를 이용하는 기술임.

- 기존 화이트박스 암호에 대한 대수적 공격에 대한 취약점 개선
- 코드리프팅 공격을 방어하기 위해 테이블 탈취 취약성 대응기법

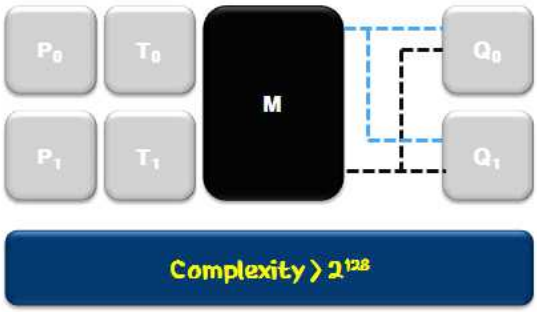


그림 23 대응기법의 개념도

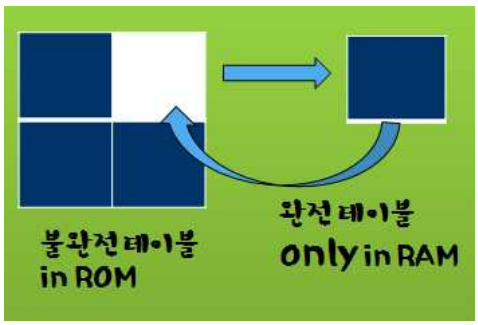


그림 24 테이블 탈취 방지 기법의 개념도

□ 기존 기술과의 차별성

o **(As-Is)** 기기(디바이스)가 수집하는 비밀 정보를 보호하기 위해 암호를 채택하고 있으나, 기기 탈취시 비밀정보를 해독할 수 있는 비밀키에 대한 방어기법이 존재하지 않았음.

o **(To-Be)** 기존 화이트박스 암호가 가지는 대수적 공격에 대한 취약점을 개선하고, 테이블 탈취(코드리프팅) 공격을 방어하기 위해 마스크를 이용한 방어 기법을 개발 하였음.

□ 기술의 활용 분야

o 무인항공기와 같이 보호하고자 하는 비밀키가 기기내에 존재하고, 이 기기가 공격자에 의해 탈취 가능성이 존재하는 응용.

o 화이트박스 암호를 이용해 비밀키를 보호하고 코드리프팅 공격을 방어하고자 하는 응용.

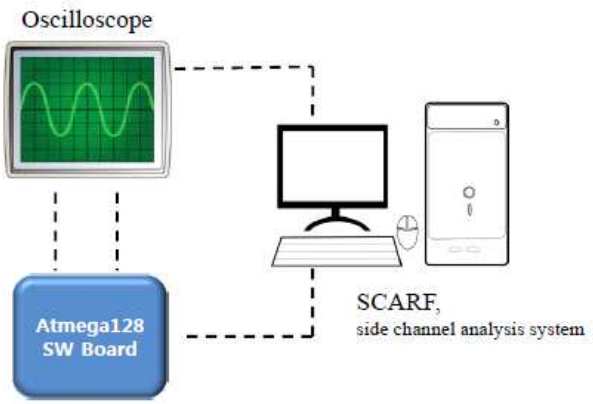
29 스마트 디바이스 키누출 HEB 검증 보드(KLA-SCARF)

□ 기술소개

o **(배경 및 필요성)** 스마트카드, OTP 기기, 보안 토큰과 같은 소형 디바이스에서 암호 알고리즘이 구동되는 동안 발생하는 다양한 부가적인 정보(전력소모, 전자기파 등)을 이용하여 비밀키를 추출하는 부채널 공격이 현실적이 위협이 되고 있음.

o **(주요기술)** 본 기술은 하드웨어(FPGA)로 구현된 암호 알고리즘이 구동되는 동안 발생하는 전력 소모를 활용한 부채널 공격에 대한 안전성을 검증하는 기술임.

- 디바이스에서 발생하는 전력 소모 수집 및 파형 생성
- 전력 및 전자기파 파형에 대한 신호 전처리 및 부채널 분석



□ 기존 기술과의 차별성

o **(As-Is)** 제품 생산이전에 FPGA로 구현된 암호에 대한 부채널 안전성 검증 방법이 없었음.

o **(To-Be)** FPGA로 암호를 구현하고, 제품 출시 이전에 이를 부채널 안전성에 대한 검증이 가능해짐.

□ 기술의 활용 분야

o 보안 디바이스의 부채널 안정성에 대한 시험 및 인증

o 중소 보안 디바이스 제조 업체의 보안성 인증 사전 테스트

30 ~ 32 스마트 디바이스 키누출 검증 시스템(KLA-SCARF)

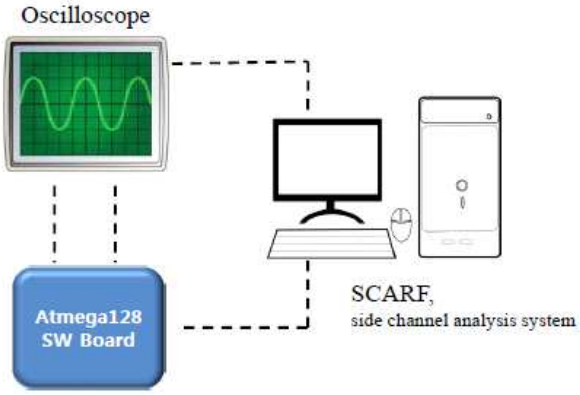
□ 기술소개

o (**배경 및 필요성**) 스마트카드, OTP 기기, 보안 토큰과 같은 소형 디바이스에서 암호 알고리즘이 구동되는 동안 발생하는 다양한 부가적인 정보(전력소모, 전자기파 등)을 이용하여 비밀키를 추출하는 부채널 공격이 현실적인 위협이 되고 있음.

o (**주요기술**) 본 기술은 소프트웨어 또는 하드웨어로 구현된 암호 알고리즘이 구동되는 동안 발생하는 전력 소모나 전자기파를 활용한 부채널 공격에 대한 안전성을 검증하는 기술임.

- 디바이스에서 발생하는 전력 소모, 전자기파 수집 및 파형 생성
- 전력 및 전자기파 파형에 대한 신호 전처리 및 부채널 분석

- **(세부기술 1) KLA-SCARF 시스템 기술**
  - 개발된 보안 솔루션에 대한 키누출 공격 취약성을 사전에 미리 검증하는 시스템
  - 파형 수집 기능, 파형 전처리 기능, 파형 부채널 분석 기능, 프로젝트 관리 및 프로그램 설치 기능으로 구성
- **(세부기술 2) CEB 보드 기술**
  - 접촉식 카드타입 검증보드에 탑재된 분석 대상(AES, DES, SEED, RSA 등의 보안 알고리즘) 등을 SPA, DPA, CPA 등의 분석 방법으로 안전성을 검증
  - 접촉식 카드타입 보안 디바이스 부채널 검증을 위한 카드리더 겸용 보드
- **(세부기술 3) C2EB 보드 기술**
  - 비접촉식 카드타입 검증보드에 탑재된 분석 대상(AES, DES, SEED, RSA 등의 보안 알고리즘) 등을 SPA, DPA, CPA 등의 분석 방법으로 안전성을 검증
  - 비접촉식 카드타입 보안 디바이스 부채널 검증을 위한 카드리더 겸용 보드



□ 기존 기술과의 차별성

o (As-Is) 다양한 암호 구현에 대한 검증이 불가능하며, 단일 프로세서에 기반하여 성능이 제한적임.

o (To-Be) 다양한 형태의 검증보드(소프트웨어, 하드웨어, 컨택스마트카드, 컨택리스 스마트카드)와 일차 및 이차 차분분석이 가능함. 멀티 프로세서 및 분산 컴퓨팅을 활용하여 분석 성능이 뛰어남.

□ 기술의 활용 분야

o 보안 디바이스의 부채널 안정성에 대한 시험 및 인증

o 중소 보안 디바이스 제조 업체의 보안성 인증 사전 테스트

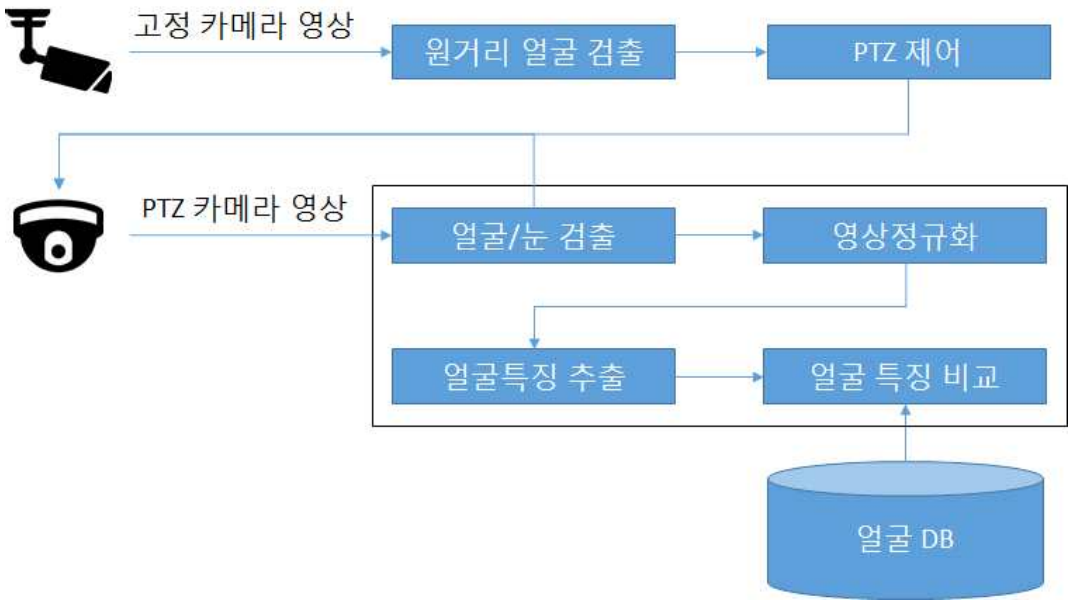
33 ~ 34 Human Identity를 위한 원거리 얼굴인식 기술

□ 기술소개

o **(배경 및 필요성)** 기존 출입통제용으로 사용되어 왔던 얼굴인식 기술이 최근 사회 안전영역으로 확대되어 용의자 검색 등의 요구사항이 증가하고 있으며, 사용자의 일상생활 중에서 지속적으로 신분을 파악할 수 있는 기술 필요

o **(주요기술)** 본 기술은 실내 원거리(15m 이내)에서 2대의 IP 카메라(고정형, PTZ)를 연동해서 사람의 얼굴을 확대, 검출하고 인식하는 기술
- 실내, 원거리 환경에서 사람의 얼굴 영역을 검출
- PTZ 카메라를 이용해서 얼굴 영역을 확대하고 영역을 재검출하고 인식

- **(세부기술 1) Human Identity를 위한 원거리 얼굴 검출 기술**
  - 실내, 원거리 환경에서 사람의 얼굴 영역을 검출하는 기능 및 PTZ 카메라를 이용해서 얼굴 영역을 확대하고 영역 재검출하는 기능으로 구성
- **(세부기술 2) Human Identity를 위한 얼굴 인식 기술**
  - 실내, 원거리 환경에서 얼굴 인식



[기술 개요]

□ 기존 기술과의 차별성

o (As-Is) 기존 출입통제용으로 사용되는 얼굴인식 기술의 경우, **근거리**에서 동작하며 사**용자가 의도적으로 카메라를 응시**하여야 함

※ 원거리 얼굴인식의 경우, 거리에 따른 해상도 문제와 외부 노이즈 증가에 의한 성능 저하 문제가 있음

o (To-Be) 고정카메라와 PTZ 카메라를 실시간으로 연동하여 고화질 얼굴을 재검출함으로써 실내 원거리(15m)에서 사용자 얼굴을 인식 가능

※ 사용자가 의도적으로 카메라를 응시하지 않더라도 원거리에서 얼굴 검출 및 인식이 가능

□ 기술의 활용 분야

o CCTV, DVR, NVR, CMS 등 지능형 영상보안 관련 분야에서 **원거리 얼굴인식 솔루션/서비스**

o 지하철 역사, 공항 등 위험상황 또는 사고 발생 시 대형피해가 발생될 수 있는 장소에서의 **영상 보안 서비스 인프라**

35 ~ 37 악성코드 비정상 행위 동적 분석 및 시각화 기술

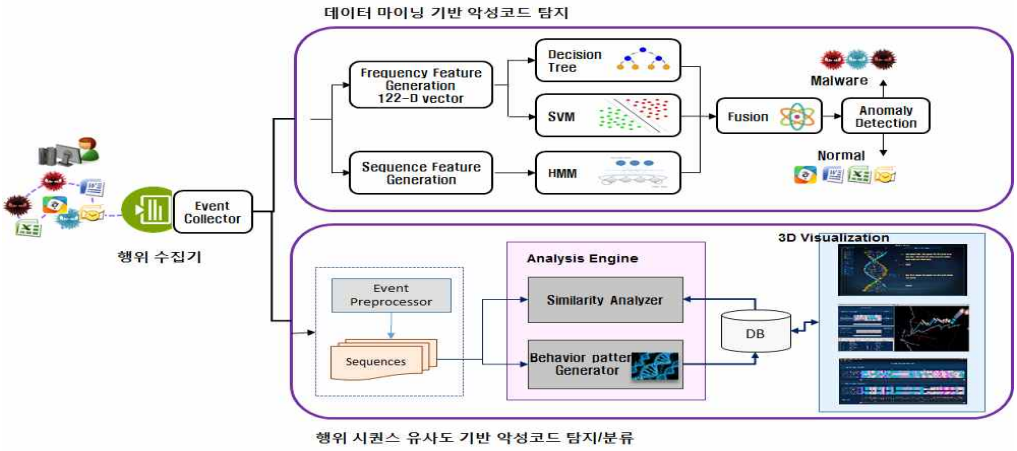
□ 기술소개

o **(배경 및 필요성)** 최근 악성코드 신종/변종의 수가 급증하고, 사이버 테러가 빈번이 발생함에 따라, 알려지지 않은 **악성코드를 탐지**하고, 행위기반의 **악성코드 그룹을 분류 및 시각화**할 수 있는 기술 필요

o **(주요기술)** 본 기술은 호스트에서 발생하는 **프로세스의 행위정보**를 **데이터 마이닝 기법**과 **다중서열정렬 (Multiple Sequence Alignment:MSA) 알고리즘**을 적용하여 **악성코드를 탐지 및 분류**하고 이를 **시각화**하는 기술

- 호스트에서 발생하는 프로세스 행위정보 수집
- 수집된 행위정보 기반 기계학습 및 데이터 마이닝 기술을 활용한 신종 악성코드 탐지
- 악성코드 그룹별 행위패턴 정의 및 행위시퀀스 유사도 분석을 통한 악성코드 분류 및 시각화

- **(세부기술 1) 호스트 프로세스 행위정보 수집 기술**
  - 호스트에서 실행되는 모든 프로세스의 행위정보를 API 후킹에 의해 실시간 수집
  - 40종 이상의 특성인자 수집
- **(세부기술 2) 호스트 행위기반 악성코드 분석 기술**
  - 데이터 마이닝 기반 악성코드 탐지
  - 프로세스의 행위패턴을 표현할 수 있는 특징벡터로 재구성
- **(세부기술 3) 사이버게놈 기반 악성코드 행위 분석 및 시각화 기술**
  - 악성코드 그룹별 고유 행위 패턴(사이버게놈) 생성 및 분류
  - 사이버게놈 기반의 시퀀스 유사도를 통한 악성코드 탐지
  - 프로세스 행위 특성인자 및 비정상 행위 분석 결과 시각화



[기술 구성도]

□ 기존 기술과의 차별성

o **(As-Is) 데이터 마이닝**을 활용한 비시그니처 방식과 **시퀀스 유사도 기반의 탐지/분류** 기술은 **학술적 연구단계**에 머물러 있음

※ 대부분의 보안 솔루션들은 시그니처 기반 악성코드 탐지에 초점을 두고 있으며, 데이터 마이닝과 시퀀스 유사도 기반의 악성코드 탐지/분류 및 시각화 기술을 제공하는 제품은 부재한 현황임.

o **(To-Be)** 데이터 마이닝 기반 악성코드 탐지 기술은 **기존 방식에 비해 성능이 우수**하고, 유사도 기반의 악성코드 분류 기술을 통해 **악성코드 계보관리로 사이버 공격의 사전 대응에 활용** 가능

※ 악성코드 탐지 성능 (탐지율 98.7%, 오탐율 4.05%, Decision Tree 경우) 측정.

※ 악성코드 그룹별 계보관리로 악성코드 제작자나 해킹그룹, 유포지, 공격지, 공격 목적 등을 빠르게 추정.

□ 기술의 활용 분야

o 사이버 공격 인지 및 대응 분야의 **악성코드 탐지·대응 솔루션/서비스**

38 ~ 39 호스트 행위기반 악성코드 탐지 기술

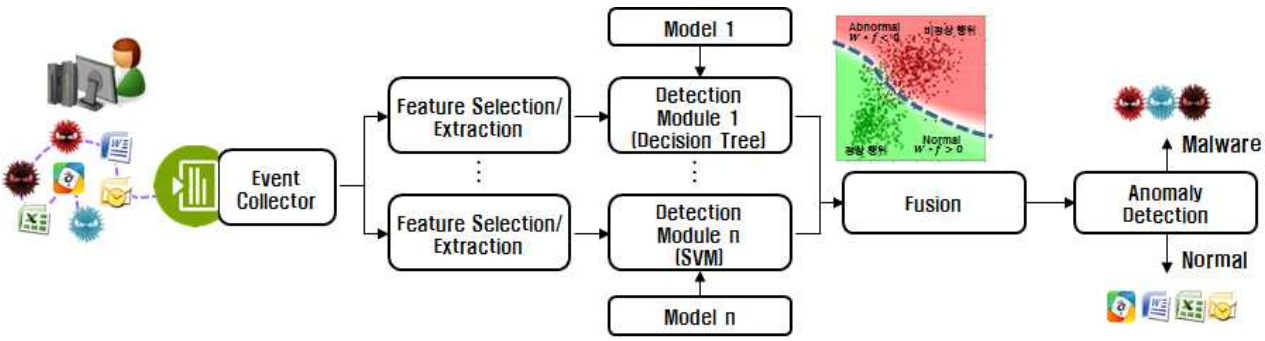
□ 기술소개

o **(배경 및 필요성)** 기존 시그너처 기반 악성코드 탐지 기술은 Zero-day 악성코드와 같은 알려지지 않은 **신종/변종 악성코드를 탐지하는데 한계**가 있기 때문에, **악성코드의 행위를 기반으로 탐지**할 수 있는 기술 필요

o **(주요기술)** 본 기술은 비 시그너처기반 악성코드 탐지에 관한 것으로, 호스트에서 발생하는 다양한 **행위 이벤트 정보를 수집**하고, 수집된 행위정보를 **데이터 마이닝 방법에 적용하여 악성코드를 탐지**하는 기술

- 호스트 PC에서 실행하는 동안 발생되는 프로세스의 행위 정보 수집
- 프로세스 별 행위 정보 프로파일링 및 데이터 마이닝 기반 악성코드 탐지

- **(세부기술 1) 호스트 프로세스 행위정보 수집 기술**
  - 호스트에서 실행되는 모든 프로세스의 행위정보를 API 후킹에 의해 실시간 수집
  - 40종 이상의 특성인자 수집
- **(세부기술 2) 호스트 행위기반 악성코드 분석 기술**
  - 데이터 마이닝 기반 악성코드 탐지
  - 프로세스의 행위패턴을 표현할 수 있는 특징벡터로 재구성



[기술개요]

□ 기존 기술과의 차별성

o **(As-Is)** 시그너처 기반 악성코드 탐지기술이 대부분이며, 학계를 중심으로 데이터 마이닝 기술을 활용한 행위기반 악성코드 탐지 기술이 제시되고 있으나, **실험실 수준의 연구결과**를 보임. 특히, **높은 오탐율로 인하여 상용화된 사례가 없음.**

※ 대부분의 데이터 마이닝 기술을 활용하는 행위기반 악성코드 탐지 연구들은 최신 악성코드의 특성을 반영하지 못하는 데이터베이스(KDD CUP 99 DB 등)를 사용하고 있는 실정이며, 본 기술은 최신 악성코드 행위에 대한 수집/표현/탐지 방법을 확보함

o **(To-Be)** 호스트에서 발생되는 행위에 대한 모델링을 통해 악성코드를 판단하여, 상용 수준의 성능으로 **신종/변종 악성코드 탐지** 가능

※ 10000 여개 악성코드와 8000여개의 정상프로세스를 대상으로 시험한 결과, 약 95%의 팀지율과 약 5%의 오탐율을 확인

□ 기술의 활용 분야

o APT 대응 분야에서 보안제품으로써 **신/변종 악성코드 대응 솔루션/서비스**

o 빅데이터 마이닝 기술을 이용하는 **차세대 SIEM 제품** 및 **사용자 행위분석 보안 제품**

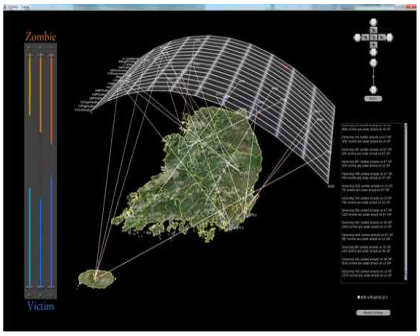
40 ~ 42 인터넷레이더 3D 시각화 기술

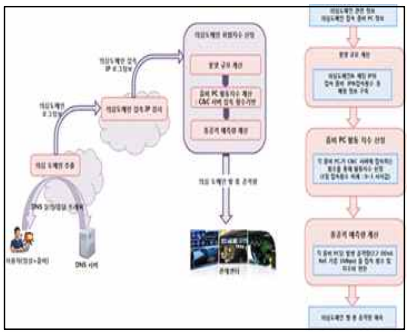
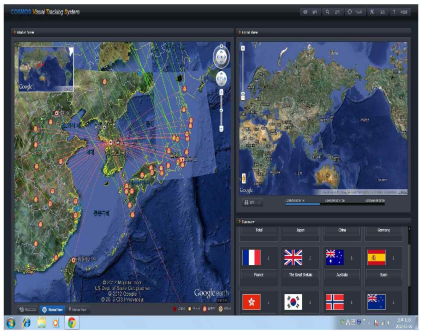
□ 기술소개

o **(배경 및 필요성)** 사이버공격의 지능화, 고도화, 전역화로 발전하면서 국가적으로 심각한 위협이 되고 있으므로, 이를 **전역 네트워크** 차원에서 효과적으로 방어할 수 있는 **체계적이고 종합적인 실시간 보안제어** 기술이 필요함

o **(주요기술)** 본 기술은 ISP(Internet Service Provider)와 같은 독립적인 도메인에서의 **사이버 공격 상황**을 3D 시각화 기술을 통하여 전역관점에서의 **네트워크 위협요소를 사전에 탐지하고 추적**하는 기술
- 공격 발생 가능성을 정량화하여 공격 규모 산정 및 악성도메인 탐지 기술
- 실시간으로 악성코드를 배포한 공격 근원지 추적 기술

- **(세부기술 1) 보안상황 3D 시각화 기술**
  - 보안이벤트 수집분석에 의한 공격상황정보 분류 축약
  - 공격상황 3D 시각화
  - 공격 내역을 표현하는 돔 구조와 공격 대상 지역을 지리정보와 연계하여 표현
- **(세부기술 2) 네트워크 위협 인지 기술**
  - 다양한 사이버위협 발생 전 봇넷 형성 및 행위 탐지
  - C&C 서버와 봇 간의 통신 모니터링에 의한 액티브 봇 행위 탐지
  - DNS 트래픽 감시에 의한 비정상 호스트 탐지 및 비정상도 정량화
  - 공격 징후 정량화에 의한 위험등급 및 발생가능 공격 규모 산정
- **(세부기술 3) 공격 근원지 추적 기술**
  - 웹 기반 파일 공유 사이트 기반의 추적로그 생성을 위한 업로드/다운로드 이벤트 수집
  - 추적로그 전달 프로토콜



< 주요 기술 구성도 >

□ 기존 기술과의 차별성

o (As-Is) 일반적인 이벤트 정보와 보안 이벤트 정보와의 상호 연관성 분석과 같은 **유기적인 공격분석 기술 부족**으로 조기 공격 예측 및 **종합적인 위협 상황 파악이 어려움**

o (To-Be) 위협요소 및 **위협상황 정량화**를 위해 요구되는 빅데이터 플랫폼 기반의 다중소스 데이터 수집 기능을 제공하며, 고유의 공격특성 정보를 추출하고, **데이터 마이닝 기반의 연관성 분석** 및 **위협행위의 근원지를 추적**함

□ 기술의 활용 분야

o **통합위협관리시스템** 및 망 관리시스템에 Add-On 모듈로 활용

o 사이버 보안 사고의 법률적 증거자료 강화 및 자동화된 범죄수사를 위한 **네트워크 포렌식 기술에 활용**

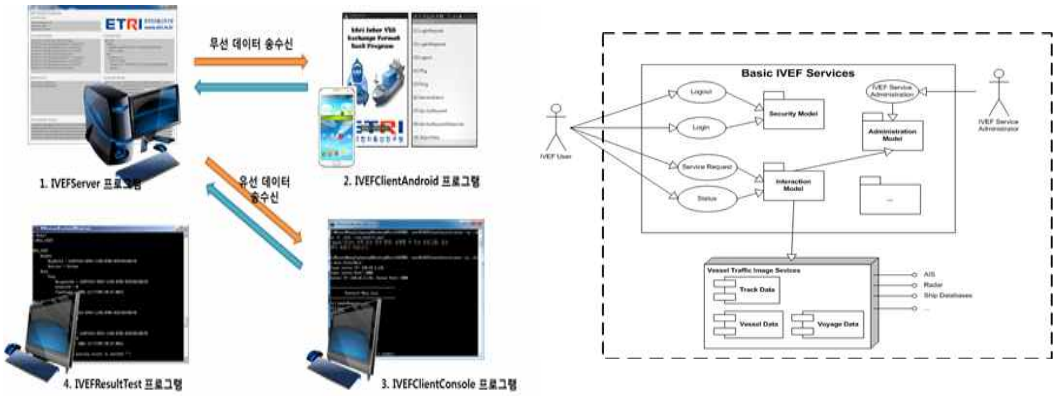
43 IALA 공통포멧(IVEF)기반 관제정보 교환 기술

□ 기술소개

o **(배경 및 필요성)** 관제정보시스템으로 정보 또는 제공하여 상호 교환하거나, 이해관계자의 시스템이 관제시스템으로 부터 정보를 주기적으로 받아 이용하기 위한 정보교환 기술이 필요

o **(주요기술)** 국제적 관제시스템간 상호 정보교환을 위하여 IALA(국제항로표지협회)에서 관련 표준(IVEF)을 제정, 표준에 기반하여 선박 등 관제정보를 관련 관제 시스템 특성에 맞는 정보를 제공 또는 주기적으로 전달 받기 위한 정보를 상호 교환하는 서비스 기술

- 정보교환 포맷에 맞는 호환성을 가진 정보교환 체계
- 주어진 특정 포맷에 따라 정보를 입력, 전달, 수신처리하여 화면에 처리하는 기술



[기술 개요]

□ 기존 기술과의 차별성

o **(As-Is)** 관제정보는 독립된 정보로서 정보교환되지 않고 특정지역 관제만을 활용하여 왔으며, 연계되는 지역은 필요성을 가지고 정보교환 필요성을 인식하고 있으나, 연계에 적용되지 않고 연구단계에 머물러 있었음

o **(To-Be)** 관제 정보 또한 표준이 형성되는 시장으로 표준화되어 표준기반 정보 전달, 상황식별, 상호 공동 위험대응 형태로 상호 **집중 분석이 필요한 대상을 자동 식별하여 활용** 가능

□ 기술의 활용 분야

o 관제시스템의 한 분야로 납품, 정보교환 기본기술로 활용, 관제보안기술 등

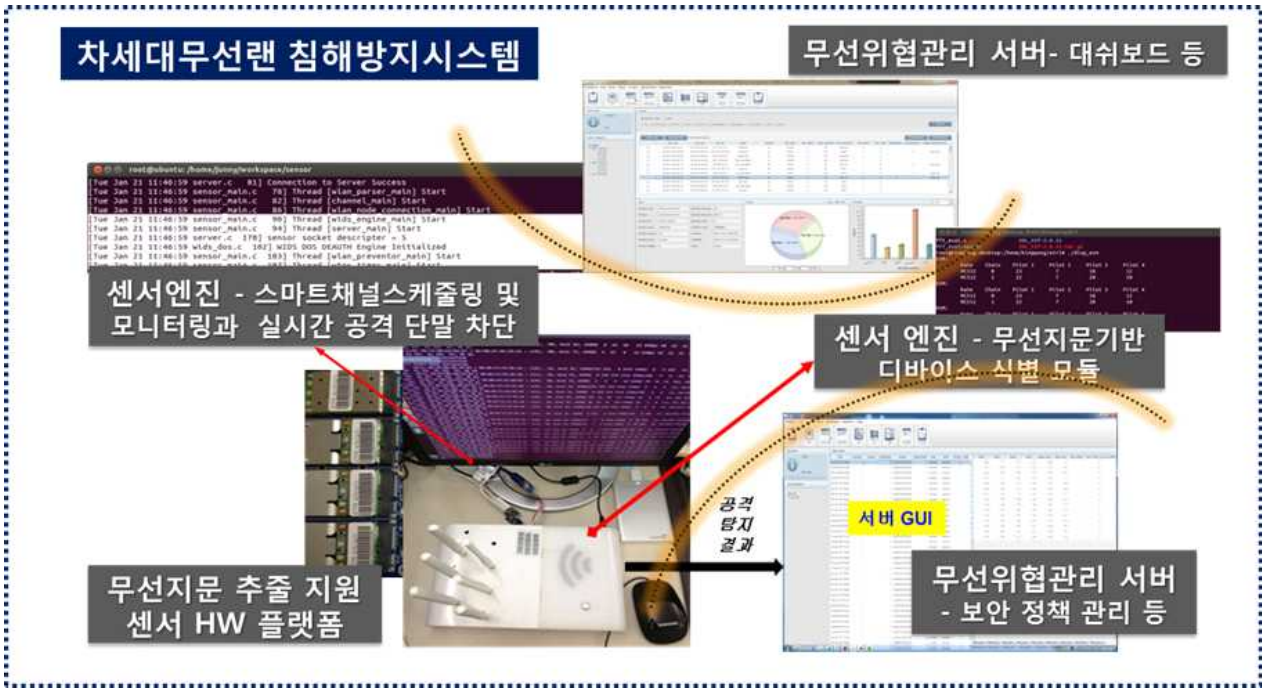
44 ~ 47 차세대 무선랜 침해방지 시스템 V1.0

□ 기술소개

o (배경 및 필요성) 무선 해킹에 취약한 802.11g/n/ac무선랜 환경에서, **복제(clone)·위장(Rogue) AP/단말을 이용한 무선 공격 위협을 실시간으로 탐지/분석**하여 차단할 수 있는 무선 침해 방지기술 필요

o **(주요기술)** AP/단말의 고유한 무선 지문(핑거프린트)을 이용하여 **불법복제 AP를 탐지하고 차단하는 무선랜 침입방지 시스템(센서, AP 및 서버) 기술**
- 스마트 무선 채널 감시 스케줄러 및 무선 침입 이벤트 수집/분석/차단
- EVM, RSSI등 물리적 무선 특성 추출 HW센서 및 무선지문기반의 디바이스 식별
- 무선랜 위협관리 서버 및 휴대형 무선랜 취약성 분석 도구(w-SCAN)

- **(세부기술 1) 무선침해방지 센서엔진 기술 - 스마트 채널 스케줄링 및 모니터링과 실시간 공격 단말 차단 모듈**
  - 다중 채널 공격 감시를 위한 스마트 채널 스케줄링 기능
  - 관리/제어/인증 패킷 파싱 및 무선 침해공격 분석 기능
  - 채널 스케줄링 연동 실시간 무선 침해공격 차단 기능
- **(세부기술 2) 무선침해방지 센서엔진 기술 - 무선지문 기반 디바이스 식별 핵심 모듈**
  - 무선지문 정보 수집 및 분석 기능
  - 기계 학습 기반 위장 무선 디바이스의 실시간 탐지 기능
  - 위장디바이스 식별 분석을 위한 서버 인터페이스
- **(세부기술 3) 무선지문 추출 지원 센서 HW플랫폼 및 디바이스 드라이버 기술**
  - 센서 HW 플랫폼 기능
  - 무선지문 추출 디바이스 드라이버 기능
- **(세부기술 4) 무선위협관리 서버 기술**
  - 서버 보안 관리 기능
  - 서버 보안 정책 및 센서 관리 기능
  - 서버 보안 이벤트 관리 기능



[기술 개요]

□ 기존 기술과의 차별성

o **(As-Is) MAC 주소를 불법 복제한 클론/위장 AP를 이용한 공격 탐지 및 차단에 한계**가 있어, 물리적인 무선 특성을 지문으로 디바이스를 식별하는 기법이 제시되고 있으나 학술적 연구단계 수준에 있음

※ 조지아텍, Bell Labs, 윈스콘신대학 등 : 무선 지문(Wireless Fingerprint) 검출 및 분석기법과 핑거프린트를 이용한 무선침입탐지 성능 개선, 무선단말의 실내위치인식 및 시각적 위협 관리 기법 등의 기술 연구

o **(To-Be) 무선랜 단말/AP의 고유한 특성(EVM, RSSI)을 추출/분석하고 디바이스를 식별함으로써 MAC을 복제한 클론/위장 공격AP 탐지**

□ 기술의 활용 분야

o 안전한 무선랜 서비스를 제공하는 **무선침입방지 및 무선위협분석/관리 솔루션**

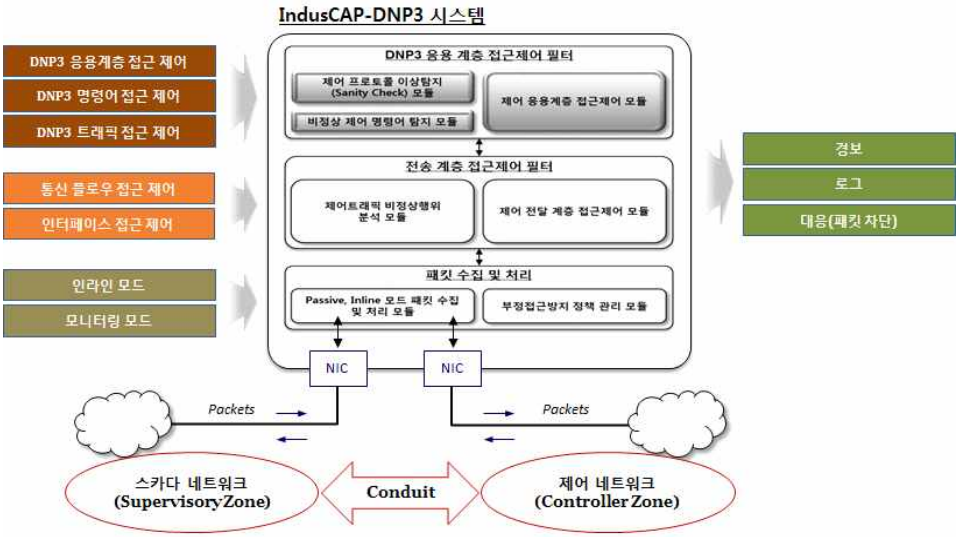
48 DNP3 방화벽 : IndusCAP-DNP3

□ 기술소개

o **(배경 및 필요성)** 악의적인 사이버 공격으로부터 **제어시스템 내부위협이 증가**함에 따라, 이를 보호하기 위한 기술에 대한 관심이 급속하게 증가하고 있음

o **(주요기술)** 본 기술은 DPI(Deep packet inspection)을 통해 대표적인 제어 프로토콜인 DNP3 프로토콜에 대한 **제어 응용 프로토콜의 취약점을 이용한 공격을 차단**하는 기술임

- 비인가 명령어, 유효하지 않은 필드 값, 비정상 트래픽을 탐지 및 차단
- 비인가 시스템 및 서비스 접근제어에 대한 다중 접근 제어 필터 제공



[기술 개요]

□ 기존 기술과의 차별성

o **(As-Is)** 산업체를 중심으로 여러 제품들이 출시되고 있으나, **단순한 형태의 화이트 리스트 정책**에 의한 DNP3 방화벽 기법들이 제시되고 있음

※ 대부분의 보안 솔루션들은 단순한 명령어 제어에만 초점을 맞추어, 본 기술과 같이 자동화된 접근 제어 시그니처 생성 및 제어 시스템 가용성을 위협하는 서비스 거부 공격에 대응하는 제품은 부재한 현황임

o **(To-Be) 반자동 형태의 White-list 기반 접근 제어 제공과 제어 프로토콜 필드 값들에 대한 유효성 검사 및 통신 흐름 추적을 통한 서비스 거부 공격 차단** 가능

□ 기술의 활용 분야

o 제어시스템 운영기관에서 독립적인 형태의 산업용 네트워크 방화벽으로 활용

o 보안 솔루션기업에서 기존 산업용 보안 플랫폼에 DNP3 보안 모듈 추가 탑재

49 ~ 50 Modbus 기반 제어 어플리케이션 방화벽 어플라이언스 기술

□ 기술소개

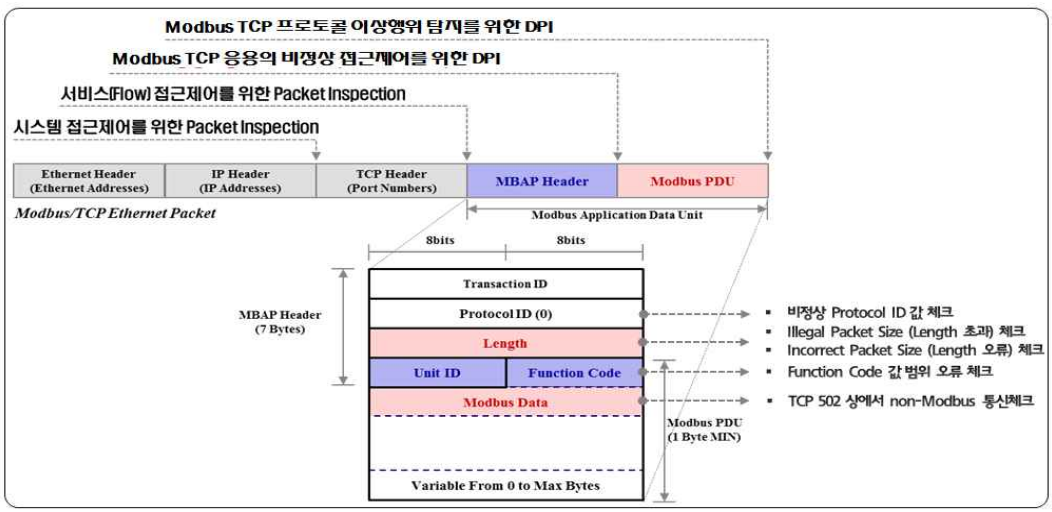
o **(배경 및 필요성)** Modbus 프로토콜은 인증 및 암호화 부재로 **위변조 등의 패킷 조작이 용이**함에 따라, 비인가 명령어 제어, 필드 값 유효성 검사 또는 비정상 트래픽을 탐지하여 이를 차단할 수 있는 기술 필요

※ Modbus : 자동화 디바이스 간 통신을 위한 산업용 통신 프로토콜임

o **(주요기술)** DPI(Deep packet inspection)을 통해 **Modbus 응용계층 레벨**에서의 다양한 비인가 접근 탐지 및 차단

- 비인가 명령어, 유효하지 않은 필드 값, 비정상 트래픽을 탐지 및 차단
- 비인가 시스템 및 서비스 접근제어에 대한 다중 접근 제어 필터 제공

- **(세부기술 1) 산업용 모드버스 방화벽 시스템 (IndusCAP-Modbus) 기술**
  - Function code 기반의 비인가 명령어 접근제어 설계 및 구현 기능
  - 제어 프로토콜 이상탐지 (Sanity Check) 설계 및 구현 기능
  - 서비스거부공격 대응을 위한 비정상 제어 명령어 탐지 설계 및 구현 기능
  - 사용자 인터페이스 기반 부정접근방지 정책 관리 설계 및 구현 기능
- **(세부기술 2) 산업용 네트워크 모니터링 시스템 (IndusCAP-Agent) 기술**
  - 네트워크 구성관리 모니터링 설계 및 구현 기능
  - 통신 프로토콜 모니터링 설계 및 구현 기능
  - 네트워크 트래픽 모니터링 설계 및 구현 기능



[기술 개요]

□ 기존 기술과의 차별성

o **(As-Is)** 산업체를 중심으로 여러 제품들이 출시되고 있으나, **단순한 형태의 화이트리스트 정책**에 의한 Modbus 방화벽 기법들이 제시되고 있음

※ 대부분의 보안 솔루션들은 단순한 명령어 제어에만 초점을 맞추어, 본 기술과 같이 자동화된 접근 제어 시그니처 생성 및 제어 시스템 가용성을 위협하는 서비스 거부 공격에 대응하는 제품은 부재한 현황임

o **(To-Be)** Modbus 응용계층 레벨에서의 비인가 명령어, 필드 값 유효성 검사 또는 비정상 트래픽 차단과 **통신 흐름 추적을 통한 서비스 거부 공격 차단** 가능

□ 기술의 활용 분야

o 제어시스템 운영기관에서 독립적인 형태의 산업용 네트워크 방화벽으로 활용

o 보안 솔루션기업에서 기존 산업용 보안 플랫폼에 Modbus 보안 모듈 추가 탑재

51 LEA 암호 알고리즘

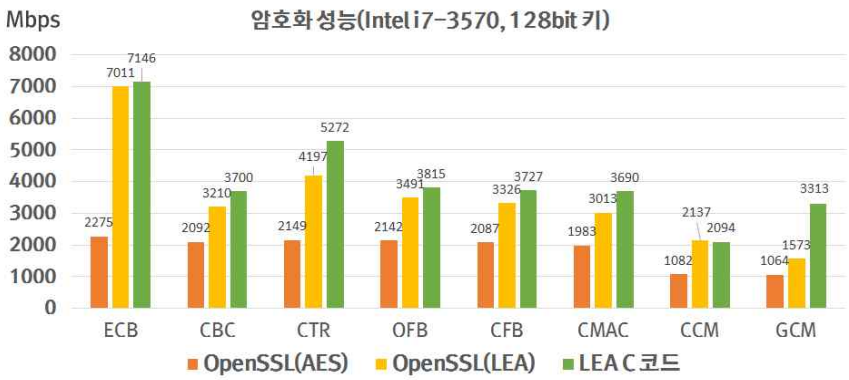
□ 기술 소개

o BIC(Big data, IoT, Cloud)와 같은 신규 ICT 환경의 등장에 따라 이에 적합한 암호기술이 요구되고 있음

o 암호기술 적용으로 인한 서비스 가용성 저하를 최소화하기 위해 경량, 고속 암호 알고리즘이 필요함

o 주요 특징

- 128비트 블록암호 LEA
  - · 기존 블록암호(AES, ARIA 등)와 동일 규격
    (블록 길이 : 128비트, 키 길이 : 128비트/192비트/256비트)
  - · 고속 연산이 가능한 ARX 기반 신규 구조
  - · 한국정보통신기술협회(TTA) 표준으로 등록(TTAK.KO-12.0223, 2013)
- 우수한 안전성 및 효율성
  - · 각종 암호학적 공격에 대하여 안전하며 취약점이 존재하지 않음
  - · LEA는 다양한 SW 환경에서 국제 표준암호 AES 대비 1.5배~2배 성능



[보급용 LEA 코드 성능]

□ 기술의 차별성

o ARX(덧셈, 비트 순환, Xor) 기반 신규 구조

o AES, ARIA, SEED 등 기존 블록암호와 기능은 동일

o 우수한 LEA의 성능은 적용 제품의 성능으로 직결

※ 他 암호 알고리즘 적용 제품 대비 성능 우위

□ 기술의 활용 분야

o 금융, 클라우드, 빅데이터 분야 등 고속 암호화 분야에 활용
- 클라우드/빅데이터 서비스 보안을 위한 암호 기능 개발에 활용
- 금융 데이터 배치 작업(암복호화) 등 대용량 데이터의 단시간 내 처리가 필요한 분야에 적용(금융 DB 보안 솔루션 개발)
- 디스크 암호화 등 저장 데이터 실시간 암복호화 솔루션 개발에 활용

o 모바일 기기 등 저전력 암호화 처리 필요 분야에 활용
- 암호 사용으로 인한 배터리 소모 최소화가 필요한 분야
- 모바일 기기에서 저장 데이터 보호 및 mVoIP 등 전송 데이터 보호를 위한 앱 개발에 활용
- 스마트그리드 보안 제품 개발에 활용(소형 스마트미터 탑재 등)

o 국가·공공분야 적용을 위한 암호 제품 개발에 활용
- LEA는 암호모듈 검증제도 신규 검증대상으로 포함됨(2015.06)
- 국가·공공분야 보안 시장에서 기존 검증대상 암호 알고리즘 (SEED, ARIA 등)이 적용된 암호모듈 및 암호제품 대체

[암호모듈 검증제도]

암호모듈 검증제도(KCMVP)
○국내 국가·공공분야에 암호모듈을 적용하기 위해서는 암호모듈 검증제도의 검증을 받아야 하며, 검증제도 보호함수 목록에 포함된 암호 알고리즘을 구현해야 함

52 고속 해시함수 LSH

□ 기술 소개

o 암호학적 해시함수(Cryptographic Hash Function)

- 디지털 데이터의 고유값을 생성하는 암호 알고리즘으로서 디지털 핑거프린터 등으로 불림
- 데이터의 변조 유무를 확인할 수 있는 기능(무결성)을 제공함
- 이외에 전자서명, 키 공유, 난수발생기 등 다양한 암호학적 응용에 사용됨
- 주요 해시함수로는 외국에서 개발된 MD-4, MD-5, SHA-1, SHA-2, SHA-3 등이 있음
  - ・2000년대 중반 MD4, MD5, SHA1에 대한 취약성이 알려진 후 해시함수 국제 공모사업을 통해 SHA3가 선정되었음

o 고속 해시함수 LSH

- 2014년에 개발된 ARX(덧셈, 비트 순환, XOR) 논리 기반 해시함수
- Wide-pipe Merkle Damgaard 구조
- 우수한 안전성 및 효율성
  - ・충돌쌍 공격, 역상 공격 등 모든 해시함수 공격에 대하여 안전
  - ・SW 환경에서 국제 표준(SHA-2/3) 대비 2배 이상 성능

국제 표준(SHA-2/3)과 LSH의 성능 비교

□ 기술의 차별성

o ARX(덧셈, 비트 순환, Xor) 기반 신규 구조

o SHA-2, SHA-3 등 기존 해시함수와 기능은 동일

o 우수한 LSH의 성능은 적용 제품의 성능으로 직결

※ 他 암호 알고리즘 적용 제품 대비 성능 우위

□ 기술의 활용 분야

o 금융, 클라우드, 빅데이터 분야 등의 분야에서 대용량 데이터의 무결성 검증에 활용

o 실시간 서비스에서 데이터 무결성 검증에 활용

- 화상회의 등 암호학적 보호가 필요한 대용량 멀티미디어 데이터의 스트리밍 서비스 등

o 모바일 앱 무결성의 효율적 검증

- 앱의 배포, 설치, 구동 시 위변조 여부 확인

o 해시함수 기반 인증기술 및 서비스에 활용

- 타임스탬핑 서비스, Merkle-tree, 일회용 전자서명 등

o 암호제품에서 사용자 인증, 전자서명, 키 유도함수, 난수발생기 등의 구현에 활용

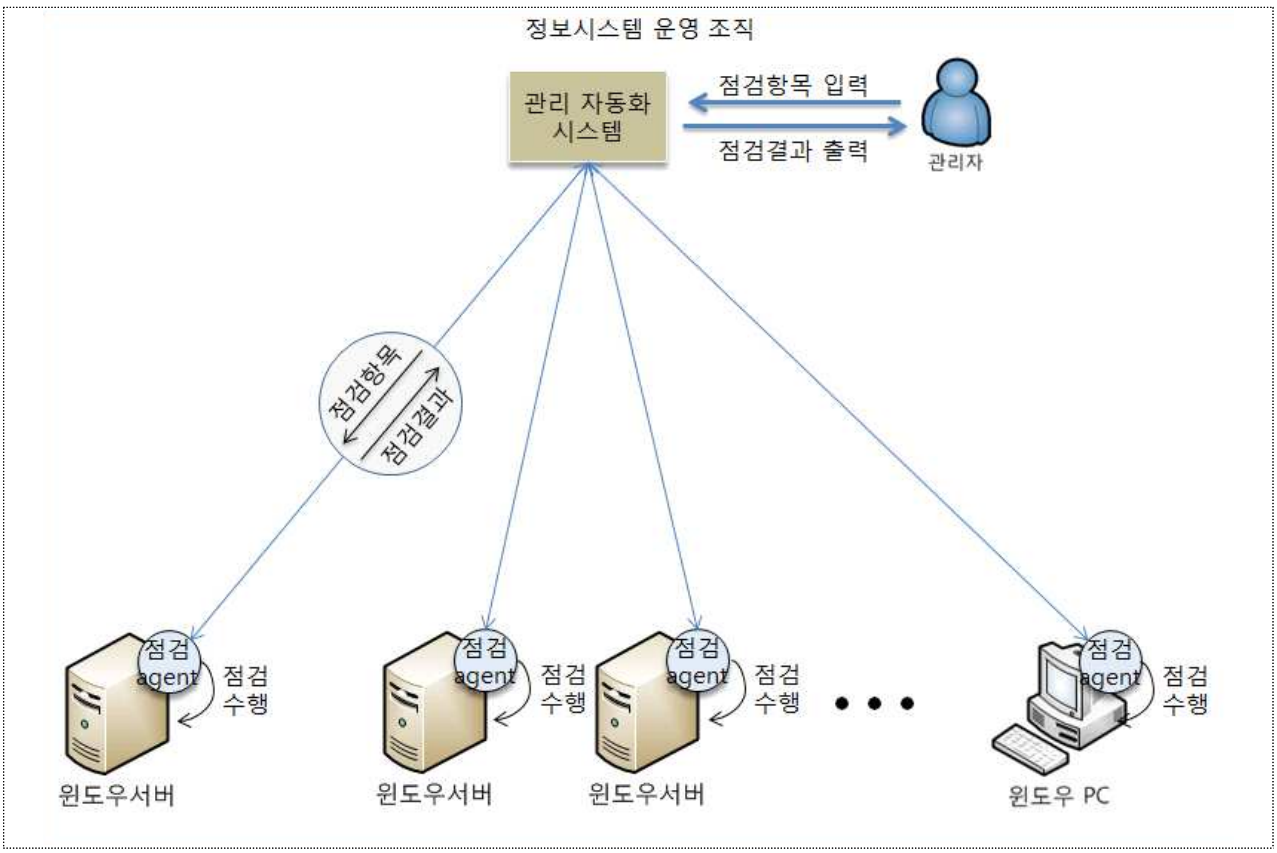
53 Windows 보안기능 설정 점검 기술

□ 기술개요

o Windows 보안기능 설정 점검 기술

- 윈도우 운영체제가 설치된 정보시스템의 보안수준을 강화하기 위해서 필요한 설정의 현재 상태를 확인하고 안전하지 않은 설정값을 안전한 상태로 변경하는 기능을 제공
- 이전 대상 기술은 정보시스템 설정 관련 표준인 SCAP(Security Content Automation Protocol), XCCFD(Extensible Configuration Checklist), OVAL(Open Vulnerability and Assessment Language)에 따라 윈도우 설정 상태를 점검 및 변경

o 기술 구성도



□ 관련 특허

o 해당사항 없음

□ 기술성

o 기존의 보안설정 점검 기술 주로 PC 제품을 대상으로 비밀번호 재설정, USB 자동실행 차단, 화면보호기 설정 등 윈도우에서 설정 가능한 정보 가운데 일부에 대해서만 적용 가능

o 이전 대상 기술은 윈도우 서버 제품을 대상으로 보안 수준과 관련된 다양한 설정 정보를 점검 · 확인하고, 안전한 설정값으로 변경하는 기능을 국제표준에 따라 제공함

o 이전 대상 기술에서 지원하는 표준 및 점검항목 현황

구 분	세부 구분	지원 표준	점검항목 개수
OS	Windows 7	XCCDF 1.2 / OVAL 5.4 / SCAP 1.0	213개
	Windows 2003	XCCDF 6 / OVAL 5.3 / SCAP 1.0	126개
	Windows 2008	XCCDF 6 / OVAL 5.3 / SCAP 1.0	180개
	Windows 2008R2	XCCDF 1 / OVAL 5.3 / SCAP 1.0	246개
	Windows 2012	XCCDF 6 / OVAL 5.3 / SCAP 1.0	212개
Internet Explorer 8(추가 제공)		XCCDF 1.1 / OVAL 5.4 / SCAP 1.0	111개

o 조직의 보안 요구사항에 따라 설정 항목을 다양하게 변경하여 사용 가능하며, 별도의 설치 없이도 동작이 가능하기 때문에 보안 상태 점검 등 다양한 용도로 활용이 가능

□ 시장성

o 관련 시장 현황

- 보안관리 기술 분야 전세계 규모는 지속적으로 성장하고 있는 시장
- 매출 1위 업체의 점유율이 13.8%에 지나지 않을 정도로 독보적인 1위 업체는 없는 상태이며, 상위 10개 업체 이외 업체의 성장률이 높아 기술이전 후 진입후 경쟁력 확보 가능
- 국내의 경우, 주요정보통신기반시설 취약점 분석 · 평가, 정보보안 관리 실태 평가, 정보보호 관리체계 인증(ISMS), 다양한 법 · 제도에서 요구사하는 보안수준 상태를 만족하기 위해서 보안관리 기술의 중요성이 점차 커지고 있는 실정임

o 관련 시장 규모

업체명	2012년 매출 (백만$)	2013년 매출 (백만$)	2013년 점유율 (%)	성장률 (%)
IBM	440.2	556.3	13.8	26.4
HP	355.1	368.0	9.1	3.6
EMC	219.9	253.5	6.3	15.3
Tripwire	126.4	150.0	3.7	18.7
McAfee	114.7	130.6	3.2	13.9
NetIQ	119.5	121.4	3.0	1.5
Symantec	129.5	116.8	2.9	-9.7
Qualys	86.9	102.6	2.5	18.0
Guidance Software	112.9	95.7	2.4	-15.3
Extreme Networks	85.7	89.6	2.2	4.6
소계	1,790.8	1,984.5	49.1	7.7
기타	1,864.4	2,044.4	50.9	12.7
합계	3,655.2	4,028.9	100	10.2

* 출처: IDC, 2014

□ 기술 응용 분야

o 조직에 사용하고 있는 서버급 정보시스템의 일괄적인 보안수준 관리를 통한 사이버보안 사고 조기예방

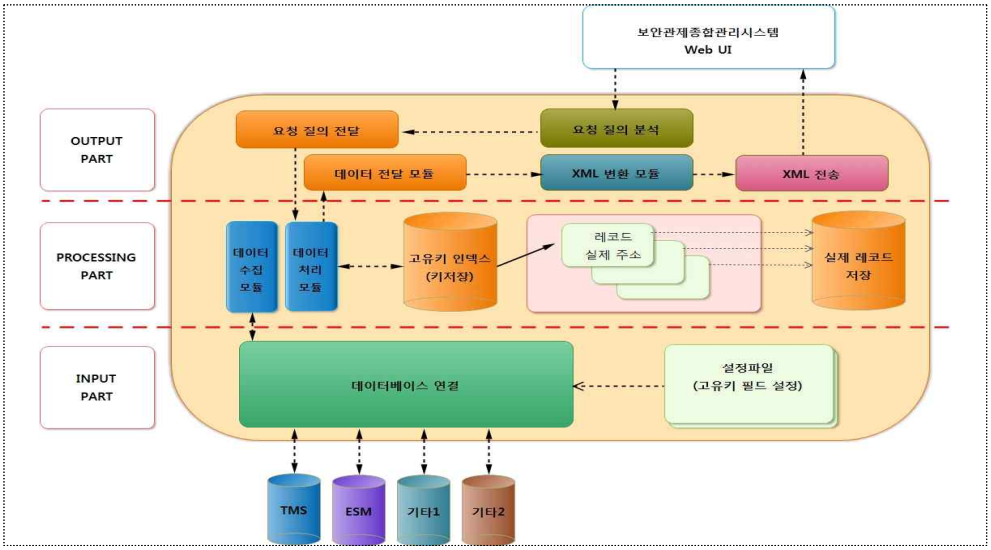
o 취약점 분석 · 평가 기준, 정보보안 관리실태 평가, 정보보호 관리체계 인증(ISMS) 등 법 · 제도에서 요구하는 기술적 요구사항 만족을 위해 활용 가능

54 보안관제종합관리시스템

□ 기술 개요

o 본 기술은 이기종 보안관제장비(TMS: Threat Management System, ESM: Enterprise Security Management)에서 탐지되는 대용량 보안관제 데이터 중 보안이벤트에 대한 검색 및 연관성 분석 업무와 침해사고 대응·관리 업무 수행 시 대응 시간 및 처리 절차를 단축할 수 있는 보안관제용 통합관리시스템을 개발 할 수 있는 기술임

o 기술 구성도



- 본 기술은 ①사이버 보안관제 업무절차/②보안관제종합관리시스템(SW)/③대용량 관제정보 고속검색 기술/④정탐 판단 개선을 위한 오탐이벤트 관리기술로 구분됨

① 사이버 보안관제 업무절차 : DFD(Data Flow Diagram)기반의 9종 업무 절차서

② 보안관제종합관리시스템(SW) : 이기종 보안장비 관제정보 통합 및 연관성 분석 기술/ 침해사고 대응절차 간소화 및 자동화 기술

③ 대용량 관제정보 고속검색 기술 : 이기종 관제데이터 수집을 위한 인터페이스/고속 인덱싱 기술을 사용한 데이터 저장 방식

④ 정탐 판단 개선을 위한 오탐이벤트 관리기술 : 보안이벤트 중 식별된 오탐이벤트에 대한 표출 기술/오탐이벤트에 대한 오탐이벤트 학습 및 이력관리 기술

□ 관련 특허

o 10-1484186 (2015. 1. 13.) 보안 관제 데이터의 검색을 위한 인덱싱 장치 및 방법

o 10-1488271 (2015. 1. 26.) IDS 오탐 검출장치 및 방법

□ 기술성

o 대상기술은 보안관제센터 운영을 통한 實 보안관제 데이터 처리 기술을 반영하여 신속하게 사이버위협 대응 업무를 수행할 수 있도록 최적화 되어 있음

o 보안관제 데이터(TMS, ESM 로그) 검색 속도가 향상되고 이벤트별 그룹화를 통해 침해사고 분석 시간을 단축할 수 있음

o 이기종간 보안관제장비(TMS, ESM, 침해사고 관리시스템, 정보공유시스템) 간 데이터 연동 및 연관성 분석 기술을 통해 침해사고 대응 절차를 간소화 할 수 있음

o 보안관제 이벤트 수집 및 탐지 중심의 기존 기술과 달리 사이버위협 대응을 위한 정탐 탐지 개선 기술 등이 반영되어 있음

□ 시장성

o 본 기술은 상용 보안관제장비에 연동하여 사용이 가능하므로 범용성, 확장성이 높으며, 사이버위협 대응 및 보안관제센터 운영 기술을 기반으로 개발되어 시스템 활용도 높음

o 상용 제품에서 상당 부분을 차지하는 로그 수집 및 표출 요소를 배제하고 사이버위협 대응 요소만을 특성화하여 기존 제품 대비 30,000천원 절감 효과가 있어 가격경쟁력 높음

o 상용 보안관제 통합관리시스템은 로그 수집・분석・표출 형태의 제품이며, 보안관제 업무 프로세스에 기반하여 침해사고 대응 업무 수행에 체계화된 보안관제 통합솔루션은 아직 없음

□ 기술 응용 분야

o 국가·공공기관 보안관제센터

※ 본 기술에 대한 공공분야 소개 시, 본 시스템 도입 의사 등 확인

o 민간부문 보안관제 시스템 및 서비스 제공 업체

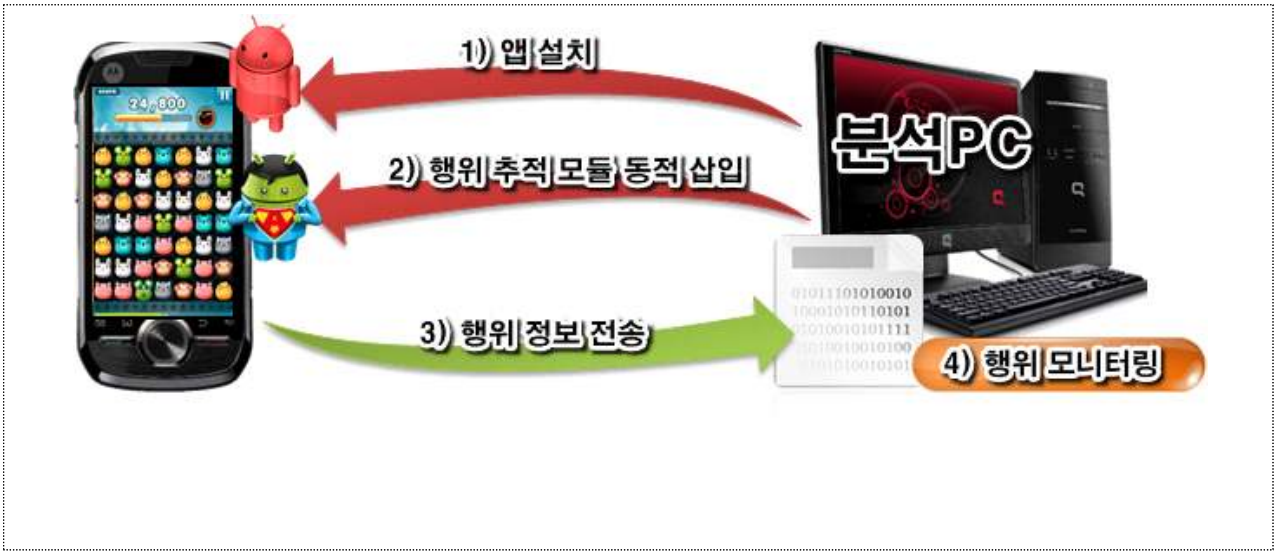
55 스마트폰 앱 행위 모니터링 기술

□ 기술 개요

o 스마트폰 앱 행위 모니터링 기술
- 루팅되지 않은 일반 스마트폰에 앱을 실행시켜 해당 앱의 행위를 실시간 추적 및 GUI를 통한 모니터링
- 앱 실행시 동적으로 DEX를 로딩하는 행위를 추적 및 대응하며, 자바 리플렉션 등 행위 모니터링 방해 기술에 대응
- 앱 모니터링 결과를 함수 단위로 그룹화하여 의미 분석

o 앱의 데이터 추적 기술
- 앱이 실행하며 사용하는 함수 인자, 타입, 이름, 데이터 등을 자동으로 추적
- 실시간으로 앱에서 생성한 파일을 추출하여 획득 가능

o 기술 구성도



□ 관련 특허

o 2015-0090559 (2015. 6. 25.) 안드로이드 플랫폼 기반의 어플리케이션 모니터링 장치 및 방법

□ 기술성

o 기존 모니터링 기술은 안드로이드 펌웨어를 수정하거나 루팅을 해야하며, API가 아닌 개발자가 개발한 함수는 모니터링이 불가능하나 본 기술은 일반 스마트폰에서 루팅없이 모든 API 및 개발자 함수도 모니터링 가능

o 기존에는 모니터링 기술을 만든 개발자가 정해놓은 함수와 데이터 만 추적 가능했으나 본 기술은 분석가가 원하는 함수와 모든 데이터를 추적 가능

o 특히 본 기술은 안드로이드의 Native 단의 행위 및 외부 서비스와의 연동 모두 추적 가능

기능		Scalpel	DroidBox	Anubis
행위 모니터링	플랫폼 변경	불필요	필요	필요
	앱 코드 수정	불필요		
안드로이드 API 추적		O	O	O
데이터 객체 추적		O		
Native 코드 추적		O		O
사용자 정의 메소드 추적		O		
선택적 행위 분석		O		

□ 시장성

o 안드로이드 앱 정적 분석 도구인 JEB(PNF Software)는 $1,000에 팔리고 있으며 국내 앱 분석하는 대부분의 사람이 사용하고 있음
- PC 정적 도구인 IDA 와 유사하여 선도적인 기술이 시장을 장악

o PC의 행위 모니터링 도구인 GFI Sandbox, Norman Sandbox는 수천만원을 넘고 있으며, 모바일에서의 행위 모니터링 도구는 아직 제품화되어 판매되지 않고 있음

o 모바일 악성코드 전용 분석 도구 확보로 모바일 분석 도구 시장 선점 필요
- 모바일 환경에 맞는 특화된 기능(앱과 Native 모듈 연동, 코드 은닉 대응 등)으로 공개 분석 도구 대비 경쟁력 확보

□ 기술 응용 분야

o 기본 API뿐만 아니라 앱 개발자에 의해 개발된 함수를 모니터링하여 앱의 모든 행위 분석

o OS와 앱 코드 수정 없이 앱의 내부 정보 추출 및 조작

56 악성도메인접근 식별 및 차단 기술

□ 기술개요

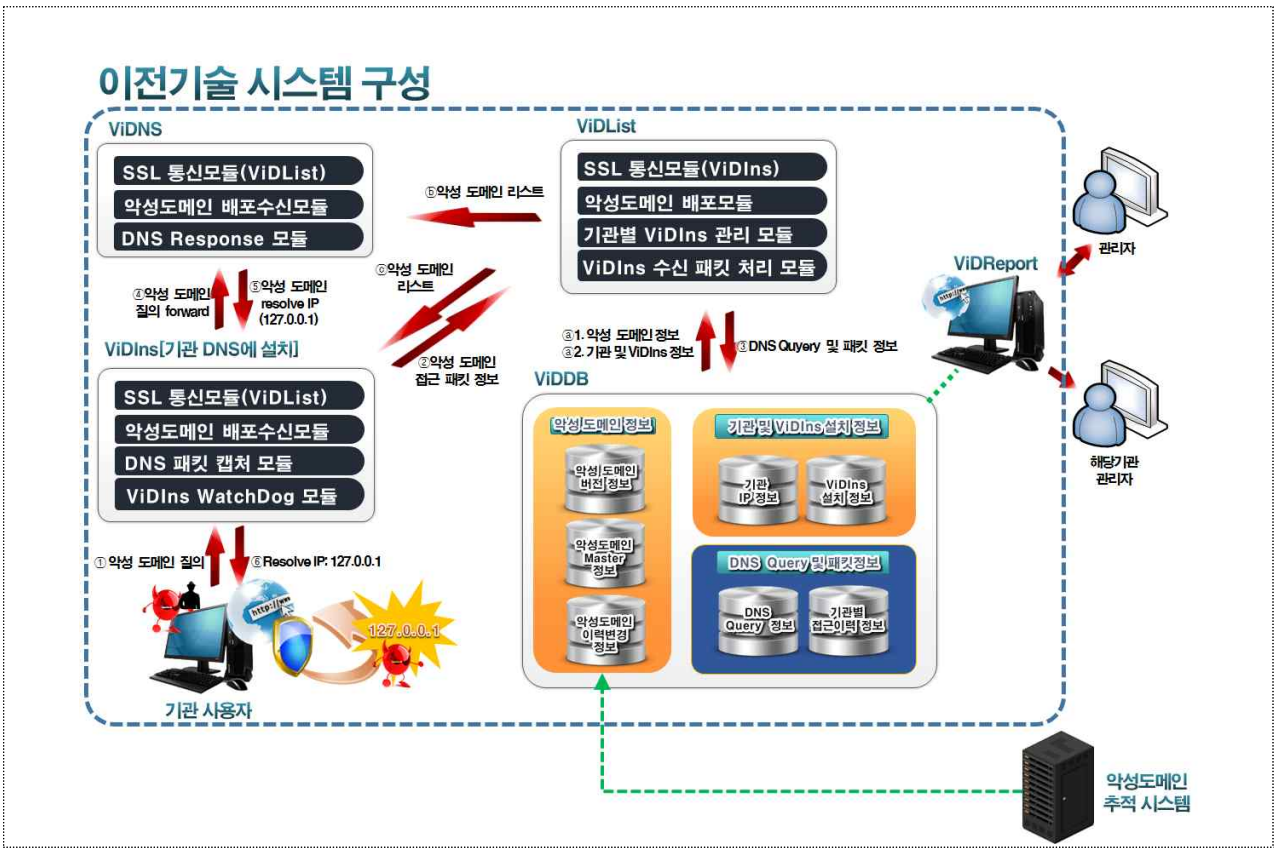
o 악성도메인접근을 시도하는 호스트 식별 및 차단 기술

- Open DNS(Bind DNS)기반의 악성도메인접근 시도하는 내·외부 호스트 식별 기술
- 악성도메인에 접근하는 호스트의 네트워크 정보를 추적·식별하고 악성도메인에 접근하는 시도를 기 지정된 유도서버로 Redirect시켜 악성도메인접근 네트워크 데이터 정보를 수집하는 기술
- 외부 악성도메인 접근이 차단된 내·외부 감염호스트에 대한 추가 보안조치를 수행함으로써 기관 내·외부에서 감염된 호스트에 의한 2차 피해를 줄이고 보안수준을 강화

o 악성도메인유지 및 이력관리 기술

- 악성도메인식별 및 차단을 위한 악성도메인의 이력을 관리하는 기술

o 기술 구성도



□ 관련 특허

o 2015-0074619 (2015. 5. 28.) 호스트의 악성도메인접근식별 방안과 탐지 정보에 기반한 탐지 효율성 개선 방법

□ 기술성

o 기술수준

질적 수준(핵심 기술내용)	기술수준	동 기술수준을 보유한 국가/기관
악성도메인접근 식별 및 차단 기술	우수	미국/ Cisco, 미국/ Infoblox, 한국/ KISA

o 기술의 독창성 및 신규성

구분	기술의 독창성과 신규성 내용
① 독창적인 신기술	- OpenDNS(Bind DNS)를 이용한 악성도메인접근 식별 및 차단기술 - 기관별 악성도메인접근 호스트 식별기술
② 기존기술의 개량/응용	- DNS 접근유도 기술 - 패킷 스니핑 및 프로세스 모니터링 기술
③ 기존기술의 융합	- DNS 질의권한 승계 기술

□ 시장성

o 국・내외 시장상황

- (국내) 2000년 초기부터 악성도메인에 대한 접근을 유도하는 DNS씽크홀이 KISA 및 ISP 업체를 중심으로 운영되고 있었으나, 단순 접근차단 목적으로 개발되어 있음. 악성 소프트웨어나 악성 웹 페이지를 통하여 감염된 호스트의 식별을 불가능하게 구성되어 국가・공공기관을 대상으로 사이버 안전수준을 높일 수 있는 시스템의 구축은 전무한 상태임
- (국외) Cisco와 Infoblox에서 DNS 방화벽 개념으로 박스형 보안장비로 개발되어 출시되고 있으나, 다수의 보안기능 탑재와 별도의 장비구축을 위한 네트워크 망 구성변경과 같은 부가적인 작업이 필요하며 운영중인 시스템 환경에 변경없이 적용하기 어려움

o 예상 수요처

- 국가・공공기관 보안관제센터
- 민간부문 보안관제 시스템 및 서비스 제공업체
- 국가・공공기관 및 민간부분 소규모 ISP 서비스 제공단위

o 시장 적용 및 성장성

- (기술적 측면) 旣 구축된 기관 DNS시스템과 호환되어 적용가능하며, 기관 내부의 악성감염 호스트를 직접 식별하고 후속조치를 할 수 있다는 장점과 약 1년 동안의 IDC 운영시험 결과를 통하여 안정성이 검증되어 기술적 안정성이 일정수준 보장됨. 또한 Linux, WIndows, Solaris, HP-UX와 같이 다수의 범용서버장비에서도 운영되는 BinD DNS Server를 대상으로 개발되었기 때문에 활용성이 뛰어남
- (가격경쟁력 측면) 상용 박스형 DNS보안장비는 그 기능에 따라 최소 수천만원에서 수억원이 넘고 있으며 BinD DNS 서버를 대상으로 한 악성도메인접근식별 및 차단 시스템은 아직 제품화되어 판매되지 않고 있음. 또한 자체 운영과 함께 서비스 제공의 개념으로 다수의 기관에 맞춤형 악성도메인접근 식별 및 차단 서비스를 제공하여 별도의 부가이익을 창출할 수 있음

□ 기술 응용 분야

o 국가·공공기관 보안관제센터에 보급하여 기관 내부에서 발생할 가능성이 있는 사이버 위협에 대한 피해 사전 차단업무에 활용

o 국가·공공기관 내·외부에서 악성 프로그램에 감염되거나 악성도메인으로 유도되어 피해를 입을 수 있는 호스트에 대한 식별 및 대응에 활용

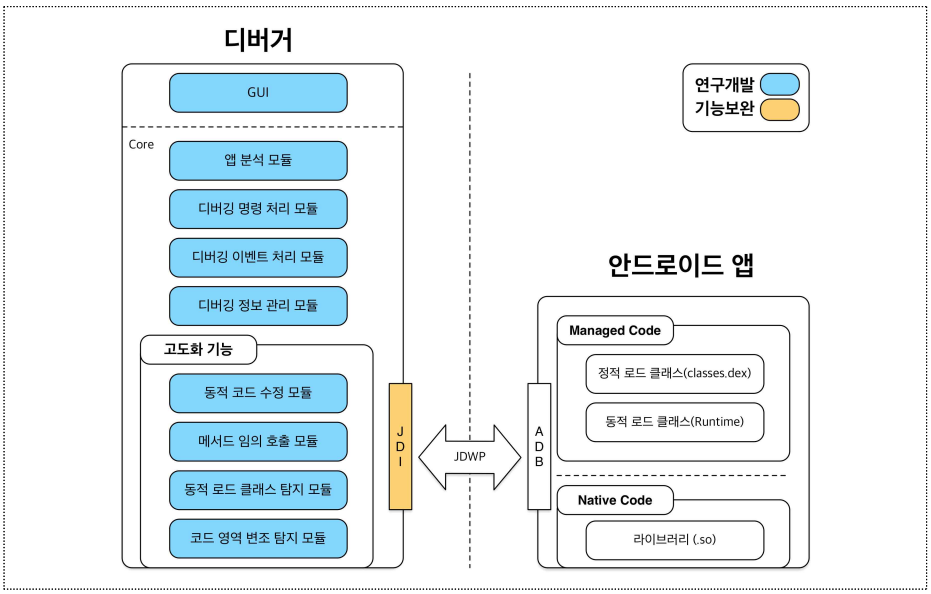
57 안드로이드 앱 역공학 관점 디버깅 기술

□ 기술개요

o 안드로이드 앱을 실시간으로 역공학 관점에서 디버깅하기 위한 기술

- 정적으로 추출한 실행코드가 아닌 실제 메모리상의 실행 코드를 디버깅하기 위한 기술로, 디버깅을 위한 안드로이드 실행 파일 해석 기술, 앱 디버깅 전처리 자동화 기술, 메모리상의 동적 변화를 실시간 반영 기술을 개발하여 고도화된 모바일 악성코드에 대응 가능한 기술임

o 기술 구성도



□ 관련 특허

o “동적 코드 확장을 이용한 앱 동적 분석 장치 및 그 방법” 출원 예정

□ 기술성

o 현재 시장에 나와있는 디버깅 기술은 정적으로 추출한 실행 코드를 디버깅에 활용하는 수준으로 동적으로 코드가 변경되는 악성코드에 대응 할 수 없음

o 본 기술은 실제로 실행되고 있는 실행 파일을 디버깅하여 메모리상의 변화를 탐지하여 반영하거나 분석가가 임의로 코드를 수정하는 등 현재 안드로이드 앱 디버깅을 위해 차용하고 있는 자바 디버거의 한계를 극복함

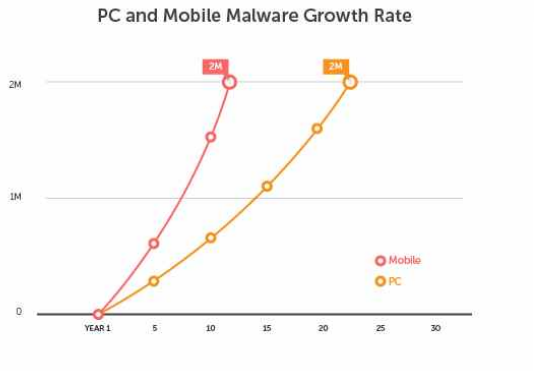
기능	DABiD	Smali-Debugging	IDAPro
디버깅을 위한 전처리 및 설정 자동화	O		
정적으로 추출한 DEX 디버깅	O	O	O
메모리에서 추출한 DEX 디버깅	O		
동적 코드 변화 탐지 (자가변조, 동적로딩)	O		
동적 코드 수정	O		

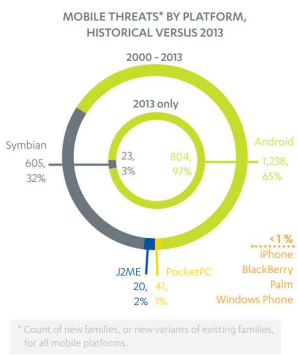
□ 시장성

o TrendMicro의 조사에 따르면 모바일 악성코드의 증가 속도는 PC 악성코드 증가 속도의 2배 이상으로 앞으로도 모바일 환경을 타겟으로 한 악성코드가 더욱 증가 할 것으로 예상됨

o 모바일 악성코드의 대부분은 안드로이드 악성코드로 2013년에는 97%의 모바일 악성코드가 안드로이드 플랫폼을 타겟으로 하고 있음

o 모바일 분야는 악성코드의 증가 속도 및 그로 인한 피해에 비하여 역공학을 위한 전용 분석 도구가 부족한 상황이며 따라서 전용 분석 도구의 수요가 높은 것으로 추정됨





□ 기술 응용 분야

o 백신업체 등 모바일 악성코드에 의한 사고 시 대응이 필요한 업체에서 앱 정밀 분석에 활용 가능

o 국가·공공기관, 군 등 모바일 앱 배포 기관에서 배포 전 앱 정밀 검사 시 활용 가능

o 통신사 등 앱마켓 운영 주체에서 배포 전 앱 정밀 검사 시 활용 가능

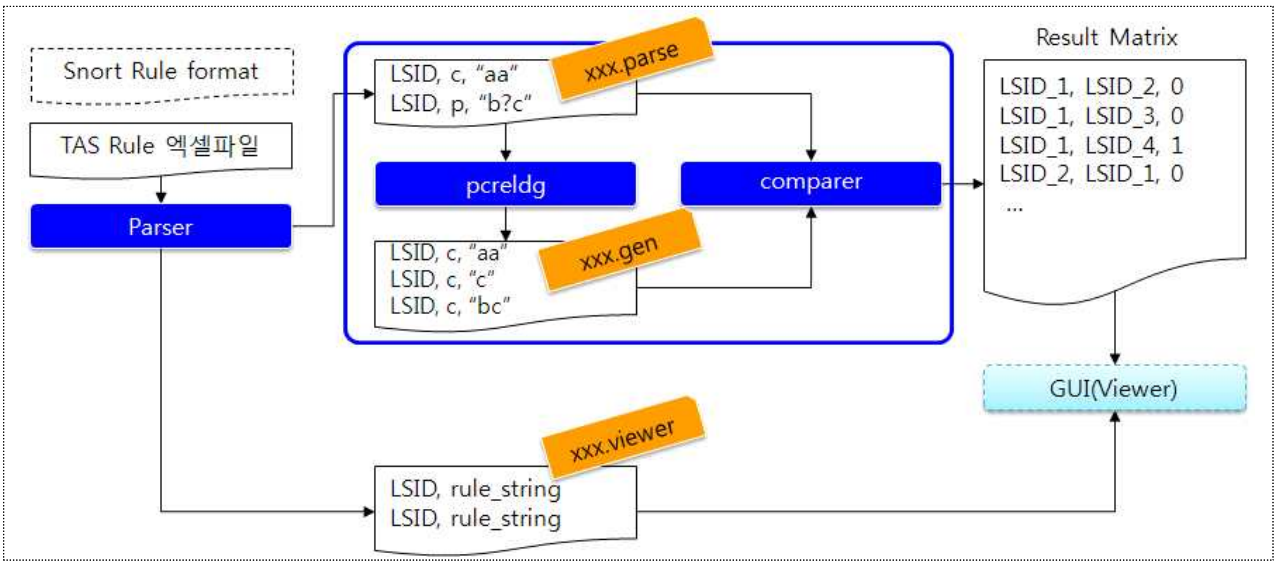
58 탐지규칙 유사도 검사 기술

□ 기술 개요

o 수많은 침입탐지 규칙을 자동으로 검사하여 유사한 탐지규칙을 판별할 수 있는 기술

- 사용자 정의 탐지규칙을 비교할 수 있는 휴리스틱 알고리즘을 사용한 탐지규칙 유사도 검사기술
- 탐지규칙 옵션 중 pcre와 content에 대한 유사도를 판별
  ※ R1 : content:"abc"; R2 : content:"abcd"; 인 경우 R1 ⊆ R2
  ※ R1 : content:"abc"; R2 : pcre:"/a?bc/"; 인 경우 R1 ⊆ R2
- 탐지규칙 헤더 중 IP 필드에 대한 유사도 판별
  : 출발지 IP, 목적지 IP에 대해 C 클래스 수준에서 유사도를 비교(any는 제외)
- 유사도 검사 결과 보고서 제공

o 기술 구성도



- 탐지규칙 유사도 검사 도구는 parser, pcreldg, comparer의 3 모듈으로 구성되며 이 모듈들을 제어하는 사용자 인터페이스인 viewer로 구성됨
- 입력파일로 사용자 정의 탐지규칙 파일 혹은 스노트 탐지규칙 파일을 입력
- parser는 입력된 사용자 정의 탐지규칙을 해석하고 탐지규칙 정규화를 수행
- pcreldg(pcre language dictionary generator)는 정규표현식을 문자열로 재구성

- comparer는 parser의 결과 파일과 pcreldg의 결과 파일을 읽은 후 탐지 규칙 간의 포함관계를 계산하고 그 결과를 저장
- viewer는 탐지규칙 유사도 검사 도구의 사용자 인터페이스를 제공

□ 관련 특허

o 10-1414061 (2014. 6. 25.) 침입탐지규칙 간의 유사도 측정 장치 및 그 방법

□ 기술성

o 기존 침입탐지시스템에 내장된 탐지규칙 중복 검사 기능은 탐지규칙을 단순 문자열로 간주하고 비교하는 방식으로, 탐지규칙의 탐지 범위를 비교하는 데 사용할 수 없음

o 본 기술은 정규표현식 간의 포함관계를 판단할 수 있는 휴리스틱 알고리즘에 기반하여 개발되었으며, 이 기술이 적용된 도구를 기존에 개발된 탐지규칙에 적용하여 유사한 탐지규칙을 판별하고 이 결과에 따라 불필요한 탐지규칙을 제거할 수 있음

o 또한, 신규 탐지규칙 생성시 기존 탐지규칙과 비교하여 유사한 탐지규칙을 제거하여 최적화된 탐지규칙을 생성할 수 있도록 도와줌

o 오프라인 혹은 온라인으로 사용자 정의 탐지규칙을 비교하여 유사도를 판단할 수 있음

□ 시장성

o 국내 정보보안 산업의 2014년도 총 매출규모는 1,695,755백만원 수준이며, 전년 대비 4% 증가

(참고자료: 2014 국내 정보보호산업 실태조사(지식정보보안산업협회, 2015. 3. 2.)

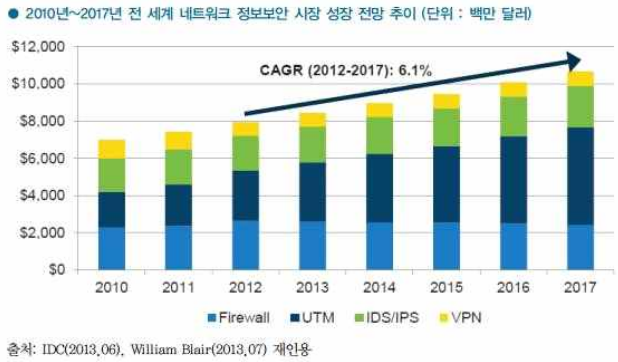
- 특히, 정보보안 제품군 중 본 기술의 해당분야로 판단되는 네트워크 보안분야는 2013년도 448,224백만원에서 2014년도 473,412백만원으로 5.6% 성장세를 보여, 전체 산업군 대비 높은 성장세를 보임
- 이밖에도 본 기술이 적용된 제품의 주요 활용기업인 보안컨설팅사업 및 보안관제사업의 매출성장 역시 각각 8.2%, 5.0% 상승하여, 정보보안 산업 전반의 지속적인 성장세를 보여주고 있음

o 정보기술(IT) 시장조사 기관인 IDC에 따르면, 전 세계 네트워크 정보보안 시장 역시 6.1% 수준으로 지속적인 성장세를 보일 것으로 전망함

[표 4-13] 정보보안산업 중분류 매출 현황 (단위 : 백만원, %)

구분		2013년	2014년(E)	성장률(%)
정보보안 제품	네트워크 보안	448,224	473,412	5.6
	시스템(단말) 보안	212,982	215,484	1.2
	콘텐츠/정보유출 방지보안	257,716	268,782	4.3
	암호/인증	126,761	126,792	0.0
	보안관리	97,542	111,350	14.2
	기타 제품	133,316	124,691	-6.5
	소계	**1,276,541**	**1,320,511**	**3.4**
정보보안 서비스	보안컨설팅	76,061	82,279	8.2
	유지관리	85,212	90,776	6.5
	보안관제	150,310	157,892	5.0
	교육/훈련	16	15	-6.3
	인증서비스	42,973	44,282	3.0
	소계	**354,572**	**375,244**	**5.8**
합계		**1,631,113**	**1,695,755**	**4.0**

[2014년도 정보보안산업분야 매출 현황]



출처: IDC(2013.06), William Blair(2013.07) 재인용

[전 세계 네트워크 정보보안 시장 전망 추이]

□ 기술 응용 분야

o 침입탐지시스템에 내장하여 침입탐지 규칙의 최적화를 통한 시스템 성능 향상 도모

o 보안관제업체는 제작 및 관리 중인 침입탐지규칙에 대해 자동으로 유사한 탐지규칙을 판단 후 개선

59 ~ 61 FEA 암호알고리즘을 이용한 형태보존 암호화 기술

□ 기술 개요

o (세부기술 1) 형태보존 암호화를 위한 형 변환 기술

- n 자리 r 진수를 비트열로 변환 및 역 변환하는 기술
- r=2, r=10 인 경우에 대해 고속으로 변환 및 역 변환 하는 기술

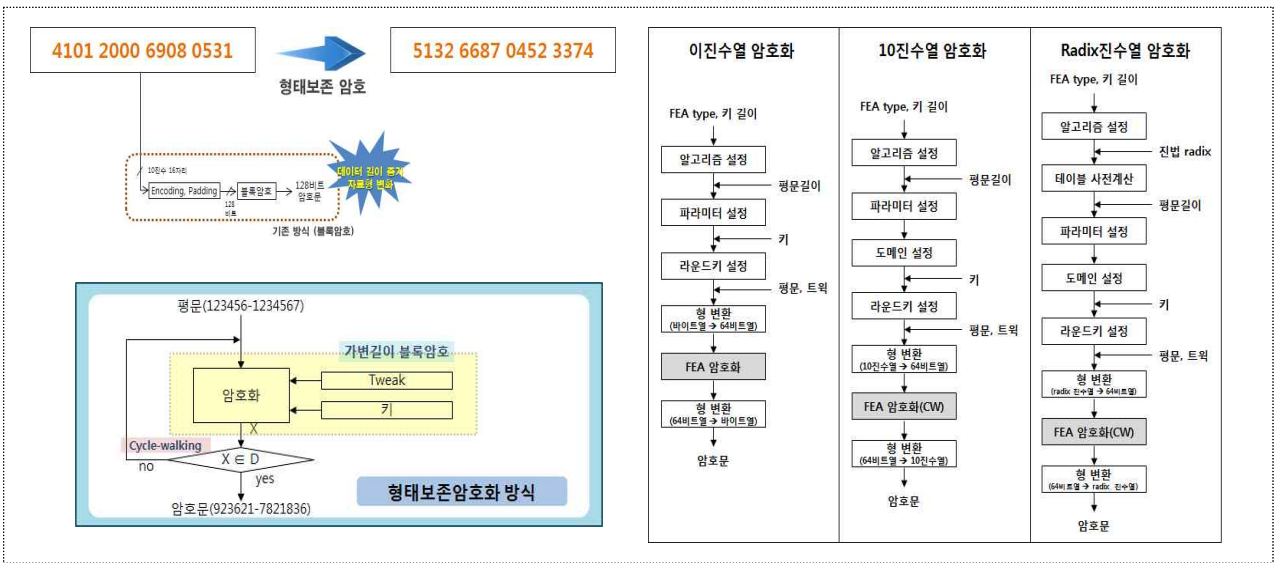
o (세부기술 2) 형태보존암호 알고리즘 FEA 고속구현 기술

- FEA 알고리즘의 고속구현 라이브러리 제공(64비트 프로세서 용)
- 라운드 함수의 고속화 기술
- 임의의 집합(ZN)내에서 암, 복호화가 수행되도록 하는 기술(Cycle-walking)

o (세부기술 3) 암호화 기능 구동 기술 및 인코딩 유지 암, 복호화 기능 개발 기술

- 제공되는 라이브러리를 이용하여 파라미터에 따른 암, 복호화 기능을 개발하는 기술
- 10진수 형태보존 암, 복호화 기능 개발 기술
- FEA를 이용하여 ASCII 인코딩을 유지하는 암, 복호화 기능 개발 기술
- 유니코드 등 기타 인코딩을 유지하는 암, 복호화 기능 개발 기술

o 기술 구성도



□ 관련 특허

o 해당사항 없음

□ 기술성

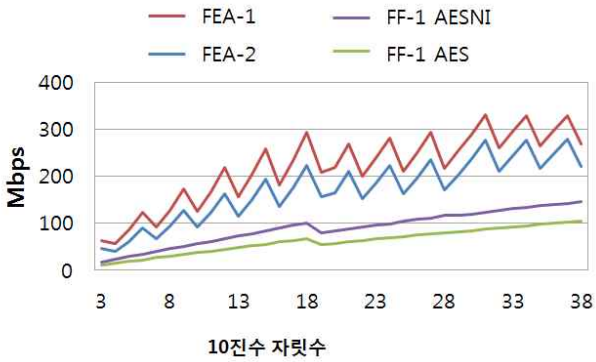
o 가변길이 블록암호와 Cycle-walking 방식을 융합하여 임의의 도메인에서 암호화 가능하도록 개발

- 이론적 안전성이 증명된 tweakable Feistel 구조를 기반으로 설계됨

o 형 변환 함수를 최적화하여 암, 복호화를 고속화함

- 형 변환에 필요한 나눗셈 연산의 횟수를 최소화 하는 기법을 적용
- 나눗셈 연산을 고속으로 구현하는 기술을 적용함

o 기존 기술(미국 NIST 표준 초안, FF-1) 대비 최고 3배의 성능



- FF-1은 기반 블록암호를 10회 이상 반복하는 블록암호 운용모드 방식으로 구성됨
- 블록암호 실행횟수가 많고, 매 반복마다 형 변환 함수를 구동하도록 설계되어 효율성이 떨어짐
- 본 기술은 비트길이를 보존하는 가변길이 블록암호를 기반으로 하여 연산량이 적음
- 형 변환 함수가 입력, 출력 시 2회만 구동되므로 효율성이 우수함

□ 시장성

o 2014년의 DB 암호 관련 매출은 64,093백만원으로 2013년 대비 5.6% 증가였고, 이 중 개인정보를 다루는 공공, 금융, 서비스 분야의 시장 점유율은 약 82%임

※ 2014 국내 정보보호산업 실태조사 보고서의 DB암호 매출 참조(지식정보보안산업협회 발간)

o 최근까지 지속적으로 발생하고 있는 대형 개인정보유출사고 및 DB 해킹 사고로 비추어 볼 때, 데이터베이스 암호화 시장은 지속적으로 성장할 것으로 판단됨

o 클라우드 및 스마트 모바일 환경의 확산으로 데이터베이스의 규모와 보안위협이 동시에 증가 하고 있어 데이터베이스 암호화의 중요성이 더욱 증대될 것으로 판단됨

□ 기술 응용 분야

o 데이터 형태의 유지가 필요한 데이터베이스 등의 암호화 기능 구현에 활용이 가능하며 특히 주민등록번호 등 개인정보의 암호화에 활용이 가능함

o SAP 등 DB 파라미터의 변경이 불가능한 시스템의 암호화에 활용이 가능함

o 동일 형태의 짧은 데이터의 송, 수신이 빈번한 금융관련 통신정보 암호화에 활용이 가능함

62 ~ 64 GPS 간섭완화 안테나 및 필터링 기술

□ 기술 개요

의도적인 GPS 전파간섭 환경에서 GPS 수신기의 위치/시각 서비스를 지속적으로 제공

o **(세부기술 1) 안테나 부가형 차폐 기술**

- 기존에 설치된 GPS 안테나에 부착하여 간섭완화를 수행하는 기술

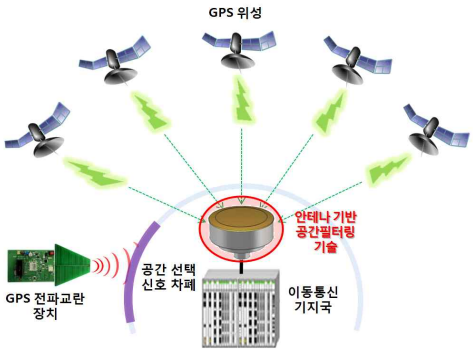
o **(세부기술 2) 단일 안테나 기반 간섭완화 기술**

- 기존 안테나를 대체하는 고성능 간섭완화 기술

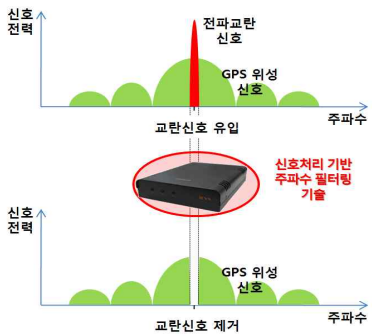
o **(세부기술 3) 신호처리 기반 주파수필터링 기술**

- 협대역 신호를 선택적으로 제거하여 GPS 위성 신호 수신을 가능케 하는 기술
- 시각/위치정보를 활용하는 고정/이동국에 활용 예상

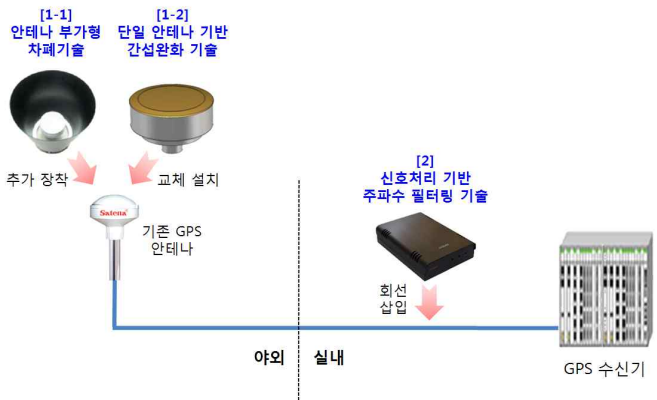
o 기술 구성도



[안테나 기반 공간필터링 기술]



[신호처리 기반 주파수필터링 기술]



[기술 운용환경]

□ 관련 특허

o 10-1447553 (2014. 9. 29.) 다중대역 GNSS 고정패턴 안테나 장치

o 10-1295643 (2013. 8. 6.) GPS 신호 수신 장치 및 그 방법

□ 기술성

o 이전기술의 성능

- 안테나 부가형 차폐기술

순번	성능 파라미터	성능
1	수평 간섭완화 성능(GP/G0) @ Absolute[1)]	23.2 dB
2	수평 간섭완화 이득 @ Absolute[2)]	16.5 dB
3	가시위성 범위 @ RHCP[3)]	100 o
4	가시위성 개수 비율[4)]	71.5 %
5	크기(하면 지름, 상면 지름, 높이)	142, 260, 210 (mm)

1) 안테나 절대수신패턴(Absolute Reception Pattern) 기준으로 이득 최고치(GP) 대비 수평면에서의 이득(G0) 간의 비율. G0는 방위각 360o 이내 최고치를 산정한 값
2) 대상 기술의 수평 간섭완화 성능(GP/G0)에서 ACE 안테나(GA-1575)의 수평 간섭완화 성능(6.7 dB)을 차감한 수치. 기존 설치 안테나 대비 상대적인 수평 간섭완와 성능을 산정한 값
3) 안테나 RHCP 수신패턴 기준으로 -5dBic 이상의 이득을 나타내는 각도
4) "ACE 안테나(GA-1575) 운용 시 가시위성 개수" 대비 "차폐기술 적용 시 가시위성 개수"의 상대적인 비율 (Legacy GPS 수신기 기준, 기준성능 측정 대상장비는 GDU)

- 단일 안테나 기반 간섭완화 기술

순번	성능 파라미터	성능
1	수평 간섭완화 성능(GP/G0) @ Absolute[1)]	31.7 dB
2	수평 간섭완화 이득 @ Absolute[2)]	25.0 dB
3	가시위성 범위 @ RHCP[3)]	110 o
4	가시위성 개수 비율[4)]	69.0 %
5	크기(하면 지름, 상면 지름, 높이)	322, 326, 215 (mm)

1), 2), 3), 4)에 대한 설명은 "안테나 부가형 차폐기술"과 동일

- 신호처리 기반 주파수 필터링 기술

순번	성능 파라미터	성능
1	간섭완화 성능 @ CW1)	39 dB
2	평상시 평균 C/N0 저하2)	1 dB 이하

1) GPS 중심주파수(1575.42 MHz)에 CW 신호 주입시 얻을 수 있는 간섭완화 성능(Legacy GPS 수신기 기준, 기준성능 측정 대상장비는 GDU)
2) 무간섭신호 환경에서, 대상기술 미적용시 평균 C/N0 값 대비 대상기술 적용시 평균 C/N0 저하 정도 (Legacy GPS 수신기 기준, 기준성능 측정 대상장비는 GDU)

□ 시장성

o 민간에서 자유롭게 활용 가능한 고성능·저비용 기술은 본 기술이 유일

o 군용 제품 대비 저비용(50% 수준)으로 제작 가능하며, 본 기술의 최대 수요처로 예상되는 이동통신 기지국 기술 도입 시 수익 창출이 가능할 것으로 예상됨

□ 기술 응용 분야

o 이동통신 기지국(Wibro), 전력망 및 SCADA시스템, 금융 분야 등 사회 기반 시설 적용

o 『신호처리 기반 주파수필터링 기술』은 선박 및 항공 분야, 군사용 무기체계 적용 가능

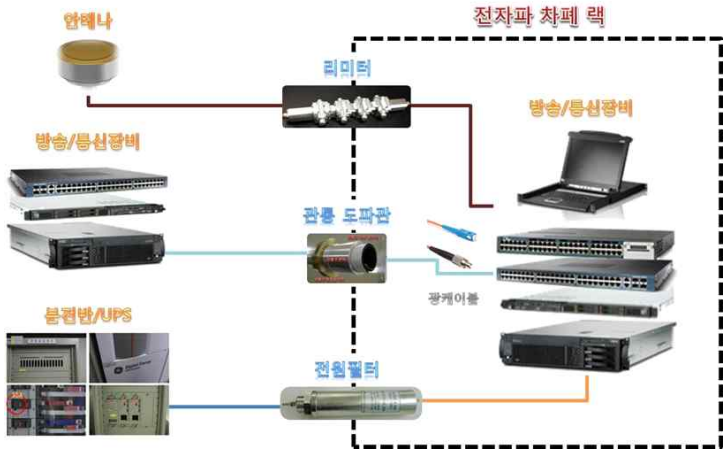
65 고전력 전자파 차폐 랙 설계 기술

□ 기술 개요

o 대상 기술은 광대역 주파수 범위의 고전력 전자파로부터 방송·통신 장비를 보호하기 위한 것으로서, 상용 허니컴이나 다수의 관통구를 대체할 수 있도록 하는 저비용 차폐 구조 설계 기술이며, 전산실과 유사한 환경에서 운용되는 방송·통신 장비를 외부의 광대역(0.1GHz~18GHz) 고전력 전자기파로부터 보호할 수 있는 기술

- 고전력 전자파 방호 개념 상 3차 방어(장비단위 차폐) 제품 설계 기술임

o 기술 구성도



[전자파 차폐 랙의 운용 환경 및 구성]

- 대상기술은 전산실 환경에서 운용되는 방송·통신 장비를 보호 대상으로 함
- 방송·통신 장비는 건물 내부 일반 랙에 설치되며, 일반 랙의 전/후면 도어는 다공면으로 구성되어 있기 때문에 외부 전자파에 의해 영향을 받을 수 있음
- 장비간 신호선 연결을 위해 도전성을 갖는 UTP 케이블이 이용되고, 전원선이 장비로 직접 연결되기 때문에 외부 전자파의 전도성 경로 차단 불가능함
- 대상기술이 적용되면 랙 외부와 연결되는 전원/안테나선은 전원 필터와 리미터를 통해 랙 내부 장비와 연결되고, 통신에 이용되는 UTP선은 광케이블로 변환되어 연결되어 외부 전자파로부터 방송통신 장비를 외부 전자파로부터 보호함

o 이전 대상 기술 시제품 형상

[고전력 전자파 차폐 랙 시제품 구성]

[고전력 전자파 차폐 랙 시제품 구성 부품]

□ 관련 특허

o 10-1319488 (2013. 10. 11.) 전자파 차폐 구조를 위한 환기구 구조체

o 10-1436910 (2014. 8. 27.) 전자파 차폐 랙

o 10-1521806 (2015. 5. 14.) 광대역 감쇠를 위한 관통도파관

□ 기술성

o 이전기술의 성능

순번	성능 파라미터	성능
1	전자파 차단 주파수 범위	100MHz~18GHz
2	전자파 차폐 성능	≥ 60 dB
3	방열 성능[1)]	≤ 5 kW
4	설계 가능한 차폐 랙 폭[2)]	≥ 600mm
5	광케이블용 관통구 직경[3)]	≤ 45mm

1) 전산실 온도 환경(20℃)을 기준으로 내/외부 온도차 15℃ 이하, 내부 온도 편차 10℃ 이하를 기준
2) 기존의 표준 전산 랙과 동일한 외각 폭으로 제작 가능, 기존 전산 랙 1:1 교체 가능함
3) 단일 광케이블용 관통구에는 최소 30개 이상의 광케이블이 동시에 설치 가능하며, 최대 설치 가능 관통구 개수는 2개 이상임

o 기존에 사용되던 전자파 차폐 환기구는 벌집 형태로 제작된 다수의 도체관이 2차원 배열된 형태인 허니컴(honecomb)이 사용되었으며, 높은 차폐 성능 확보를 위해 허니컴과 차폐 구조를 수작업에 의해 납땜하는 공정이 필요함에 따라 제작 단가 상승 요인으로 작용

o 이전기술은 상용 허니컴을 대체할 수 있는 환기구를 요구 차폐 성능에 따라 설계할 수 있도록 하고, 조립 및 양산이 용이하도록 함으로써 제조 원가 절감 가능하도록 하였음. 따라서, 적용비용이 중요한 민간운용 국가기반 시설 적용에 유리

□ 시장성

o 연구소 자체 조사에 따라, 관련 업계 주요기업 매출규모 및 시장점유율을 감안할 때, 랙 시장규모는 연 500억 규모로 추산되며, 차폐 랙 시장 규모는 그 중 10% 수준으로 추산됨(※연 50억 규모)

□ 기술 응용 분야

o 정부통합전산센터 및 국가지도 통신망, 전력망 및 SCADA 시스템, 금융분야, 민간 전산센터 등

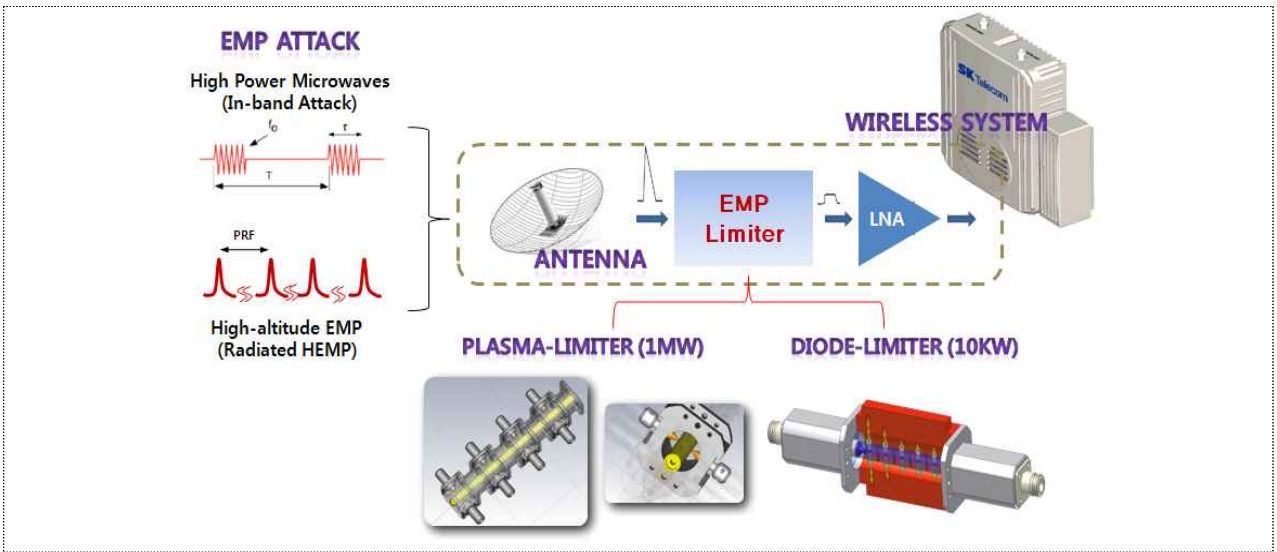
66 안테나선로용 EMP 차단 기술(플라즈마-반도체 리미터)

□ 기술개요

o 대상기술은 무선기반의 안테나를 사용하는 통신, 제어 및 레이더 시스템 등을 고출력 전자기파 펄스(EMP: Electromagnetic Pulse)로부터 안전하게 보호하는 목적으로 사용되는 동축선로 방식 모듈형 장치로서, 전자기파 테러 발생 시 안테나선로로 인입되는 EMP 펄스의 세기를 시스템 안전수준 이하로 제한하는 기능을 수행함

- 이전 대상 기술은 1MW급의 플라즈마 방식과 10kW급의 적층형 반도체 방식의 2종 기술로서,무선 시스템 및 시설의 환경 조건이나 중요도에 따라 10kW급 반도체방식 단독 적용 또는 1MW급 플라즈마 방식과 10kW급 반도체 방식의 연동 적용이 가능함
- “제2회 국제군사과학 신기술경진대회” 은상 수상 기술

o 기술 구성도



□ 관련 특허

o 10-1410765 (2014. 6. 17.) 적층형 다이오드 리미터

o 10-1506619 (2015. 3. 23.) 안테나선로 보호장치

□ 기술성

o 이전기술의 성능

순번	성능 파라미터	성능
1	주파수 대역	DC ~ 2.5 GHz
2	삽입 손실	< 2 dB
3	최대 입력 전력	1MW @ 1us, duty 0.1%
4	정재파 비	< 2.0
5	전력 차단성능, 1kW[1)]	최대 20 dB, 잔류전력 < 10W
6	전력 차단성능, 10kW[2)]	최대 30 dB, 잔류전력 < 10W
7	전력 차단성능, 1MW[3)]	최대 50 dB, 잔류전력 < 10W

1) 전력 차단 성능 1kW 성능 명세는 펄스폭 1us, duty 0.1%의 TWTA를 이용해 측정한 결과임
2) 전력 차단 성능 10kW 성능 명세는 펄스폭 1us, duty 0.1%의 TWTA를 이용해 측정한 결과임
3) 전력 차단 성능 1MW 성능 명세는 UWB 임펄스(출력 레벨 7.07kV, 상승시간 100-200ps, 펄스폭 1-2ns)를 1kHz의 반복주파수로 설정하여 측정한 결과임

o 스트리머 방전원리를 이용하여 기존의 동일 방식 리미터 부품 구조에 대해 나노초 이하의 임펄스 반응속도 성능을 구현하였으며, 이는 최초의 “1MW/ns 플라즈마 리미터 기술” 개발 사례임

o 전극의 구조적 특징상, 다단의 구조와 콘형상의 전극은 입력 펄스에 대해 큰 방전 전류 용량을 가질 수 있으며 확장성 측면에서도 용이. 또한, 입력부를 상용 N 커넥터로 설정하고, 고전압 방전부 및 다이오드로의 전류 도통 시 절연 파괴가 일어나지 않고 광대역 임피던스 정합이 되도록 하는 구조를 가짐으로써 기존 기술에 비해 상용 시스템과의 호환성이 매우 우수

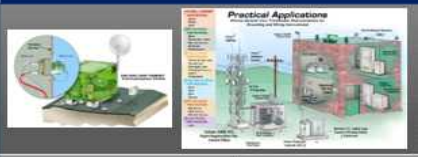
□ 시장성

o 국가 주요시설, 군 시설 및 민간의 주요 사회기반시설 등에 EMP 방호 구축 사업 추진에 따라 시장 확대 가능성
- 본 기술은 국내 최초 기술이자, 세계적으로도 상용화 사례가 없어, 시장 확보 시 시장지배적 경쟁력 확보 가능

□ 기술 응용 분야

o 기지국, IDC 센터, 방송·통신, 전력, 교통·항공, 금융 등 국가 및 사회 주요 기반시설의 EMP 방호시설 구축 사업 등에 활용

o 군의 EMP 방호사업을 시작으로 민간으로의 점진적인 전파가 예상됨

Applications	Contents	Examples
Military	- All the Wireless COM. Link (Mil. Shelter, OP.COM.Cent.)	
Communication	- CDMA/WCDMA M/W BS, Repeater - Microwave Com. Link (PtP, PtMP) - GPS BS	
Broadcast	- Satellite Broadcasting - M/W Broadcasting Link	
Traffic	- Traffic Control Radar - ILS, Landing Guidance for Aircraft - Etc.	

67 휴대용 고속 불법신호탐지 설계 기술

□ 기술개요

o 목적 및 활용분야

- 소형·저전력·휴대용의 특징을 갖는 고속 불법신호 탐지기술과 주장비와 연동한 신호 도래방향 추정 기술
- 국가·공공기관 및 국내·외 대도청 탐지업체 보급을 통해 대도청 탐지 관련 산업발전에 기여

o 세부기술

- 휴대용 탐지장비(무지향 안테나 및 유선용 탐지 프로브 포함) 설계/제작 기술
  - 주파수 변경, 저전력 운용을 위한 경로별 전력제어 등 펌웨어를 포함한 광대역(20MHz~6GHz), 저전력(4.2W), 경량(700g) RF 수신모듈 설계 기술
- 전자나침반을 내장한 광대역 지향성 안테나 설계/제작 기술
  - 동작 주파수 200MHz~6GHz의 광대역 단일 지향성 안테나 및 RF 수신모듈 연동 제어 모듈 및 프로토콜 펌웨어

o 기술 구성도

□ 관련 특허

o 10-1345748 (2013. 12. 20.) 지향성 안테나 및 전자나침반을 이용한 무선주파수 신호의 방향추정 장치

o 10-1403020 (2014. 5. 27.) 광대역 지능형 재밍 제어 장치 및 방법

□ 기술성

o 전자나침반을 활용하여 수신전력(RSSI)을 극좌표에 표시하여 수신신호 도래방향을 추정하고, 전화선/전원선으로부터 광대역 신호를 탐지할 수 있는 독창적 기술

o 특히, iPad/스마트폰을 이용하여 원격에서 WiFi를 통하여 장비를 운용할 수 있는 기술 적용

o 수신주파수 대역에 따른 전원제어, FPGA를 사용한 H/W와 S/W decimation 복잡도 최적화 등 기존기술 대비 소형·저전력화된 기술 구현

o FFT 알고리즘을 이용한 탐지속도 고속화 기술 구현

o 신호저장 기능을 이용하여 별도의 신호분석 장비와 융합하여 정밀한 분석 가능

□ 시장성

o 국내외 시장 상황

- 국내 유사제품은 전파감시용으로 출시되었으며, 대도청 탐지장비는 전량 수입에 의존하고 있어, 본 기술을 통한 국산화 및 수입대체효과 기대
- 국외에서 생산되는 제품으로 독일 R&S社의 'PR100' 장비가 있으며, 판매금액은 약 1억원 수준으로 상당한 고가임. 본 기술의 경우, 생산가격을 1,000만원 수준으로 낮출 수 있을 것으로 예상되는 바, 충분한 시장수요가 기대됨

o 우수한 기술성

- 낮은 생산가격에도 불구하고, 소형·휴대용으로서는 전대역 스캔속도(12GHz/sec), 스펙트로그램, 지향성 안테나, 유선용 프로브 등 세계 최고 수준의 기술력을 갖추어 높은 시장성을 기대할 수 있다고 사료됨

□ 기술 응용 분야

o 국가 외교안보 관련 부처, 공공기관, 지자체 및 대도청 탐지 업체 등

o 도청장치 판매나 통신 재밍이 자유롭게 시행되는 국가로의 수출 역시 기대됨

□ 기술개발 완료 시기

o 개발완료(현재 1개 업체 이전)

68 외부침투를 물리적으로 차단하는 신뢰성 있는 자료전송 기술

□ 기술 개요

o 망연계 구간에서의 보안강화가 관심을 받으며 물리적 단방향 장치에 대한 관심이 높아지고 있음

- 방화벽과 같은 기존 망연계구간 보안장치는 자체 취약점 및 관리자의 실수로 인해 외부에서의 침입이 발생할 수 있음
- 물리적 단방향 장치는 외부망에서 내부망으로의 데이터 전송이 원천적으로 불가능하여, 설정상의 오류 및 소프트웨어적 취약점이 발생하여도 외부에서 원격으로 침입할 수 없음

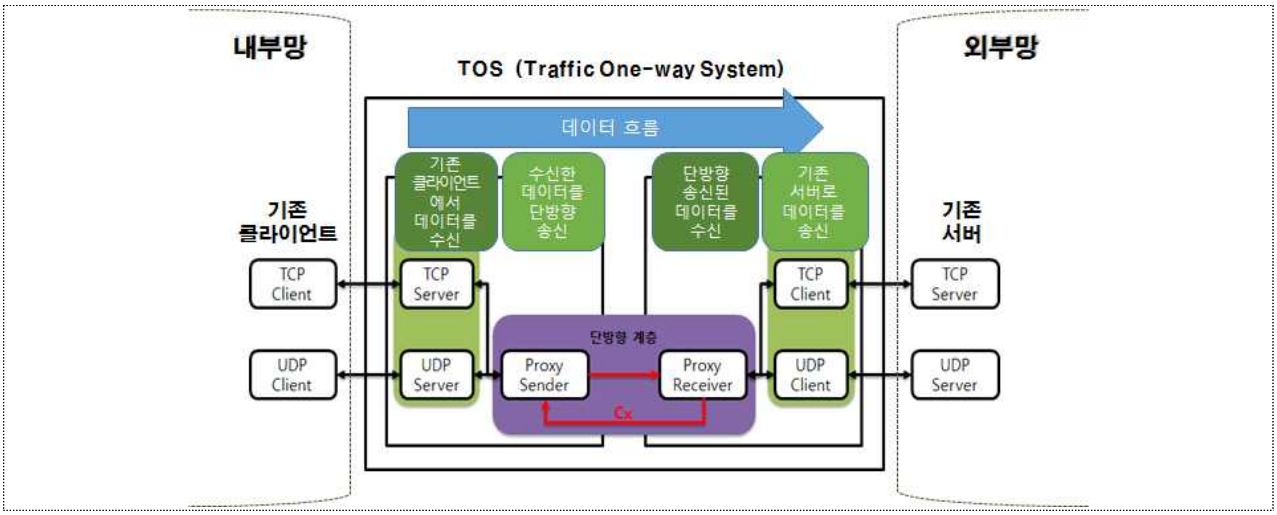
o 물리적 단방향 자료전송 구조를 이용하여 외부망에서의 침투를 원천적으로 차단할 수 있으나 지금까지의 기술적 한계로 인해 현장에서 널리 사용되지 못하고 있음

- 물리적 단방향 자료전송 방식의 구조적 한계에 의해 데이터 전송신뢰성을 보장하지 못함
- 기존 단방향 통신장치들은 신뢰성 확보를 위해 고성능의 장비 등을 활용하여 1개 채널 구축에 1억 이상의 비용이 소요

o **데이터 전송신뢰성을 보장하는 단방향 통신(Traffic One-way System, 이하 TOS로 약칭) 기술**

- 물리적 단방향 자료전송 구조를 유지하면서 전송신뢰성 확보
- 임베디드 보드를 이용한 제작단가 경감

o 기술 구성도



□ 관련 특허

o 2014-0029537 (2014. 3. 20.) 데이터 전달 장치 및 그 방법

o 10-1593168 (2016. 2. 2.) 단방향 통신 장치 및 방법

□ 기술성

o 물리적 단방향 자료전송 장치의 문제점 극복

구분	이전기술	본 기술
전송신뢰성	- 내부망에서 외부망으로 데이터를 전송한 이후에 데이터 전송 성공여부를 확인할 수 없음	- 전기신호를 이용한 데이터 전송 성공여부 확인 가능
	- 전송신뢰성 100%를 보장하지 못 함 (기존 장비들은 전송신뢰성을 높이기 위해 같은 데이터를 여러 번 보내는 방식을 사용)	- 전송신뢰성 100% 보장
도입 용이성	- 단방향 자료전송을 적용할 구간에서 사용하는 서비스마다 별도 개발이 필요(추가비용 발생) - 데이터 전송 실패 상황에 대한 알림 메시지가 없음	- TCP 프로토콜에서 ack 사용패턴에 대한 설정으로 서비스 지원 가능 - UDP 프로토콜 지원 - 파일전송(FTP) 및 전송 오류 (전송파일의 이름 겹침 등)에 대한 에러메시지 제공 서비스 지원
	- 1개 채널(서버-클라이언트) 구축시 1억원 이상의 비용 소요	- 임베디드 보드를 이용한 경량화를 통해 재료비 기준 100만원 이하

□ 시장성

o 데이터 전송신뢰도 확보 및 도입단가 절감을 통해 보급률 증가를 통한 시장확대 가능

- 국가기반시설 제어시스템의 경우 물리적 단방향 기술을 통한 망분리가 권고되어 있으나 고가의 도입 비용 및 전송신뢰성 미확보 등의 이유로 현재 보급률 저조
- 국가기반시설 제어시스템에 2,000여대 이상 도입될 것으로 추정

  ※ 2015년 1월 기준 국가기반시설 제어시스템 234개 시설

  ※ 시설별로 10여대 도입을 가정
- 국가기반시설 뿐 아니라 금융권, 산업제어시스템 등 다양한 영역에서 활용 가능

□ 기술 응용 분야

o 단방향 자료전송을 활용한 다양한 구간에서의 보안성 강화 가능

- 단방향 통신장치는 내부업무망과 외부망 간의 망연계 구간 뿐 아니라,
- USB사용금지된 PC에서 안전하게 파일을 다운로드할 수 있는 시스템 구축, 로그서버로의 원격침투 및 정보누출을 방지하는 안전장치 등 그 활용도가 높음

□ 기술개발 완료 시기

o 2014년 12월, 기술개발 및 시제품 제작 완료