[첨부 제4호]

스마트단말용 가상화 기반 보안플랫폼 기술

임재덕 (jdscol92@etri.re.kr)

시스템보안연구그룹

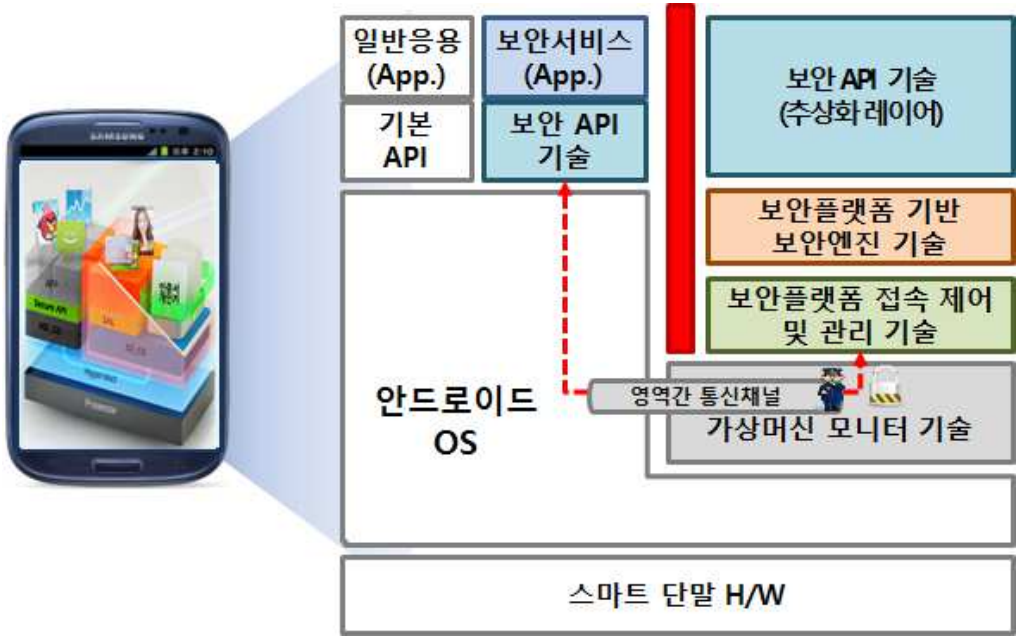
ETRI 한국전자통신연구원
www.etri.re.kr
초연결통신연구소 / 정보보호연구본부

목 차

1. 기술의 개요

▣ 스마트단말용 가상화 기반 보안플랫폼 기술

❖ 분실 및 도난의 가능성과 악성코드 위협이 높은 스마트단말 환경에서 가상머신 모니터를 통해 모바일 OS(안드로이드OS)가 동작하는 일반영역과 보안기능을 제공하는 보안영역으로 운영환경을 분리하여, 스마트단말 내의 민감 정보를 보호하고 처리하는데 있어 안정한 운영환경을 제공하는 가상화 기반 보안플랫폼 기술



2. 기술이전 내용 및 범위(1/6)

▣ 기술이전 내용

❖ A. 보안플랫폼 기반 보안엔진 기술

- 안드로이드OS와 분리된 보안영역에서 운영되는 “보안플랫폼 기반 보안엔진 기술”은 분리된 보안영역에서 데이터 처리를 수행하는 보안엔진으로 KCMVP 대응이 가능한 경량형 암호알고리즘, 화이트박스 기반의 키관리, 데이터의 기밀성과 무결성을 제공하는 안전저장 기능으로 구성됨

❖ B. 보안플랫폼 접속제어 및 관리 기술

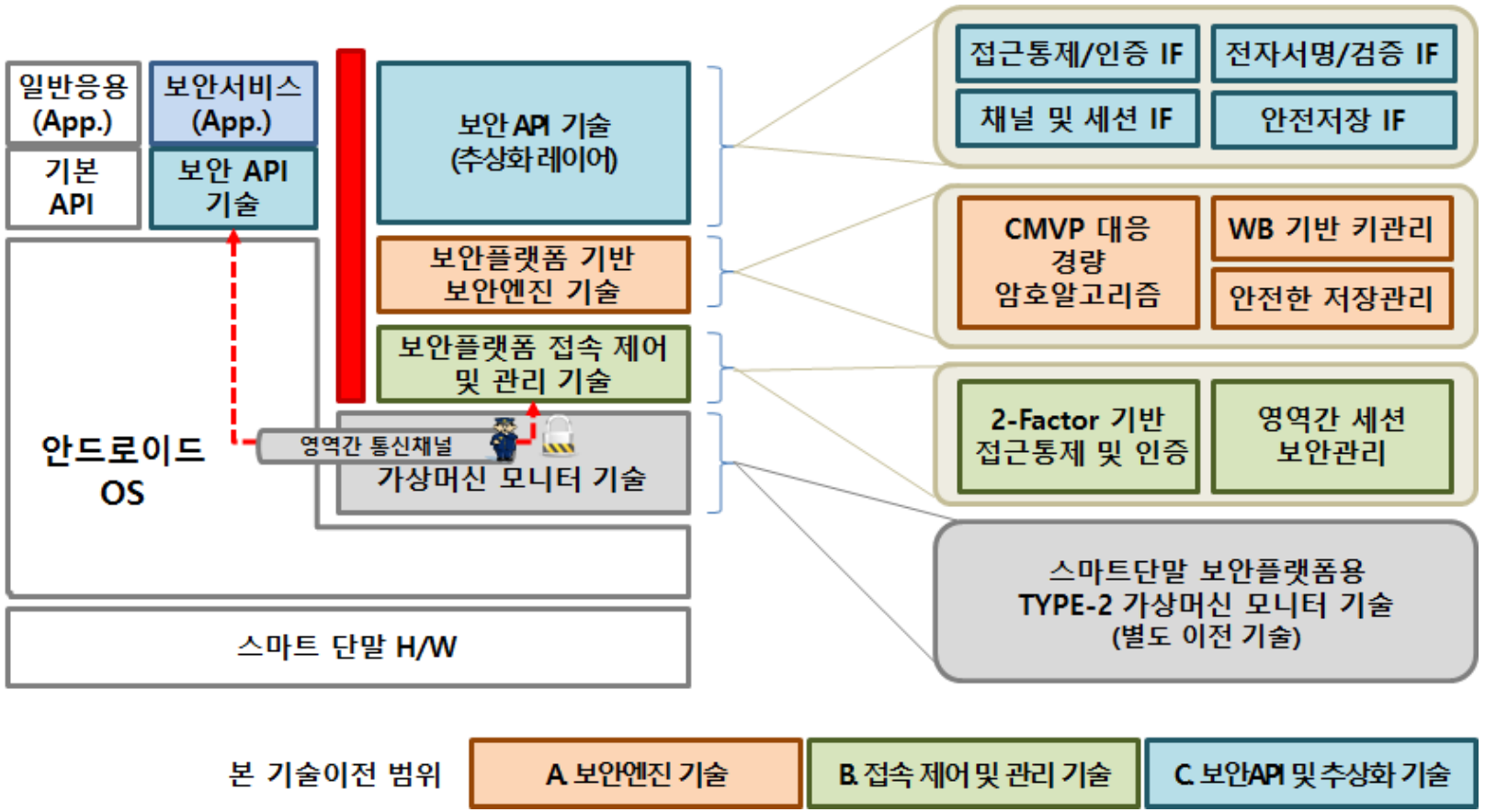
- 안드로이드OS와 분리된 보안영역에서 운영되는 ”보안플랫폼 접속제어 및 관리 기술”은 분리된 보안영역으로의 접근 제어 및 접근 관리를 위해 인증 및 접근제어, 메시지 관리 등의 기능으로 구성됨 (일반영역에서 호출된 보안 API 메시지 해석 및 관리 기능 포함)

❖ C. 보안플랫폼용 보안 API 및 추상화 기술

- 일반영역(안드로이드OS)의 보안서비스(앱)가 분리된 보안플랫폼의 보안 기능을 사용할 수 있도록 개발자에게 제공된 API와 일반영역에서 제공된 API의 실제 구현을 제공하는 보안영역(보안플랫폼)에서의 추상화 라이브러리로 구성됨

2. 기술이전 내용 및 범위(2/6)

▣ 기술이전 내용



2. 기술이전 내용 및 범위(4/6)

▣ 기술 이전 세부 내용

❖ A. 보안플랫폼 기반 보안엔진 기술

- **KCMVP 대응 암호 알고리즘 및 키관리 기능**
  - 대칭키 암호 : AES, SEED, ARIA (모드 : ECB/CBC/CTR/CFB/OFB)
  - 공개키암호 : RSA-1024, RSA-2048
  - 전자서명: KCDSA_1048, KCDSA_2048,
  - 해쉬함수 : SHA224, SHA256, SHA384, SHA512
  - 난수생성기: HMAC_DBRG
- **화이트박스(WB) 기반 키 생성 알고리즘**
- **안전한 저장관리(Secure Storage) 기능**
  - 중요 데이터의 안전한(암호화, 무결성 검증) 저장/관리

❖ B. 보안플랫폼 접속제어 및 관리 기술

- **보안영역 접근에 대한 2-Factor 인증(Admission) 기능**
  - 보안영역 접근 허가앱 인증 및 사용자 PIN 인증
- **보안영역 접근제어(Access Control) 및 메시지 관리 기능**
  - 2-Factor 인증을 통한 영역 간 암호화 통신 채널 제공
  - 인증 정보 기반 세션 관리(생성/삭제/타임아웃/갱신)
  - 영역 간 송수신 메시지 관리 및 보안 서비스 호출 관리

2. 기술이전 내용 및 범위(5/6)

▣ 기술 이전 세부 내용

❖ C. 보안플랫폼용 보안 API 및 추상화 기술

- **일반영역에서의 보안플랫폼 활용을 위한 보안API 주요 기능**
  - 안전저장 및 메모리 관리용 IF
  - 사용자 접근제어용 PIN 관리 IF
  - 보안영역 채널 및 세션 생성 IF
  - FIPS-196 표준 규격 기반 RSA 서명 생성/검증용 IF
  - FIPS-196 표준 규격 기반 G-PKI 연동용 KCDSA 서명 생성/검증용 IF
- **보안영역의 보안서비스 추상화 기능**
  - 안전저장 및 메모리 관리 라이브러리 구현
  - 사용자 접근제어용 PIN 관리 라이브러리 구현
  - 보안영역 채널 및 세션 생성 라이브러리 구현
  - FIPS-196 표준 규격 기반 RSA 서명 생성/검증 라이브러리 구현
  - FIPS-196 표준 규격 기반 G-PKI 연동용 KCDSA 서명 생성/검증 라이브러리 구현
- **일반영역 메시지 관리 기술**
  - 멀티 채널 지원 메시지 통신 구조 제공

2. 기술이전 내용 및 범위(6/6)

▣ 기술 개발 현황

❖ 기술 성숙도(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	실용 목적의 아이디어 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

3. 경쟁기술과 비교

▣ 기술의 특징

- ❖ 진화하는 스마트 단말의 악성 코드로부터 단말 내 중요 정보의 유출을 방지할 수 있는 가상화 기반의 분리된 운영환경을 제공하는 보안 구조를 제공함
- ❖ 특히, 암호키, 인증서 등과 같은 민감 정보의 안전한 보호가 가능하여 관련 서비스의 신뢰도를 높일 수 있음
  - 인증 결과의 신뢰도 향상(신뢰 인증) / 암호 연산의 신뢰도 향상(데이터 보호의 신뢰도 향상)
- ❖ 보안엔진내의 암호 기능에는 국산 암호알고리즘인 SEED, ARIA를 포함하고 있으므로, 군 및 공공분야 활용 및 국내의 기존 보안시스템과의 연동에 문제가 없음

▣ 기존 기술과의 비교

- ❖GP TEE 기술은 HW 기반의 SE의 내부안전실행환경인 TEE로부터 서비스를 보호하기 위한 기능 규격 및 API를 정의하고 있으나, 본 기술은 HW 보안칩 대신 S/W 가상화 기술을 이용하여 물리적 보안 칩셋이 없는 단말 환경에서도 TEE와 동일한 안전실행환경 제공 가능
- ❖삼성 KNOX는 갤럭시 시리즈에 적용된 보안 구조로, 하나의 운영환경에서 SEAndroid의 강제적 접근제어를 적용하여 KNOX 기반 앱과 일반 앱을 구분하는 방식으로 사용자 영역을 분리하고 있어 접근제어 기능을 우회할 경우 정보 접근이 가능하지만, 본 기술은 안드로이드 운영환경과 다른 운영체제 기반의 격리된 운영 환경을 제공하여 정보 유출를 방지하는 보다 원천적인 보안 구조 제공

4. 기술의 사업성

▣ 기술의 예상 적용 분야 및 조건

❖ 예상 응용 제품 및 서비스

- 스마트워크, 안전재난 서비스, 군 분야 등 보안이 철저히 요구되는 모바일 서비스 분야에서 신뢰된 사용자 인증 및 중요 정보 유출 방지를 위한 스마트 보안단말
- 특정 구성원 간의 문자/음성 정보의 안전한 전달 및 관리를 위한 스마트 보안단말

❖ 사업성

- 스마트폰 악성코드가 2014년 기준 2012년 대비 약 444%, 2013년 대비 약 14.2% 증가한 상황(AnLab 2015)에서 증가하고 지능화되는 악성코드에 대응할 수 있는 보안 단말의 요구가 증가할 것임
- IDC에 의하면 세계적으로 모바일 보안단말시장은 2015년 142억불에서 , 2019년 190억불로 전망 (모바일 오피스 보안단말, 보안통신용 스마트단말, 상황전파용 보안단말, 융합서비스 단말보안 등)

❖ 기술이전 업체 조건

- 모바일 단말에 대한 개발경험이 있는 업체가 유리
- 모바일 단말장치에 대한 소프트웨어 개발업무를 담당하는 연구인력 필요

❖ 사업화시 제약 조건

- 가상화 기반 보안플랫폼 기술은 가상머신 모니터 기반의 분리된 영역에서 운영되는 모듈로 가상머신 모니터 기술의 지원이 필요함

  (본 연구원에서 실시하는 "스마트단말 보안플랫폼용 TYPE-2 가상머신 모니터 기술"을 통해 해당 기능을 제공할 수 있음)

5. 국내외 시장 동향

▣ 기술현황 (모바일 단말보안)

❖ 악성코드 차단을 위한 백신 기술뿐만 아니라, 디바이스 보호, 개인데이터보호, 네트워크 접속 제어 기술 등을 포함하여 개발되고 있으며, 주로 MDM 기술 형태의 제한적인 솔루션으로 제공되고 있음

❖ 단말 보안 플랫폼으로는 삼성에서 갤럭시 시리즈에 적용한 KNOX 플랫폼이 있으며, 하나의 운영환경에서 SEAndroid의 강제적접근제어를 적용하여 KNOX 기반 앱과 일반 앱을 구분하는 방식으로 사용자 영역을 분리하고 있어 **접근제어 기능을 우회할 경우 정보 접근이 가능성이 존재함**

▣ 시장전망

(단위: 백만불, 억원)

관련 제품 /서비스	시장	1차년도 (2017년)	2차년도 (2018년)	3차년도 (2019년)	4차년도 (2020년)	5차년도 (2021년)	합계
보안강화형 스마트단말	해외	16,660	17,900	18,950	20,346	21,845	95,701
	국내	7,880	10,296	13,254	16,117	19,598	67,145
합계	해외	16,660	17,900	18,950	20,346	21,845	95,701
	국내	7,880	10,296	13,254	16,117	19,598	67,145

(해외시장) ※ IDC, Worldwide Mobile Enterprise Security Software 2015-2019 Forecast and Analysis, 2015.3 참고
(국내시장) 사이버보안 시장 규모에 대한 국내시장비율을 적용하여 추정(2015년 2.9%, 2016년 3.1%, 2017년 4.3%, 2018년 이후 CAGR 21.6% 적용, 한국산업기술평가관리원, 2013)

감사합니다.

www.etri.re.kr

♣ 연락처 : 시스템보안연구그룹/정보보호연구본부, 임재덕 책임 (042-860-1522, jdscol92@etri.re.kr)