[첨부 제4호]

TeeMo:
가상화 기반 안전실행엔진 구현기술 (v4.0)

김정녀 (jnkim@etri.re.kr)

모바일보안연구실

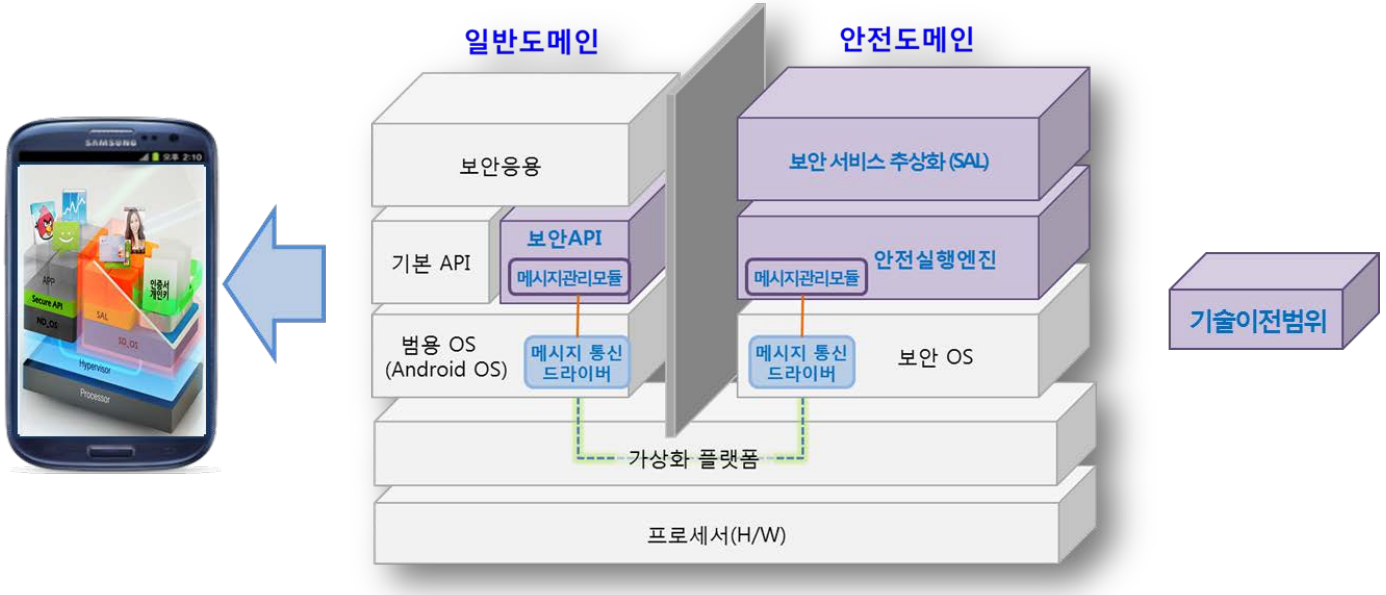
ETRI 한국전자통신연구원
www.etri.re.kr
사이버보안연구단

목 차

1. 기술의 개요

▣ 가상화 기반 안전실행엔진 기술

- ❖ 분실 및 도난의 가능성이 높은 모바일 단말 환경에서 가상화 기반의 도메인 분리 실행 기술을 이용, 기업 정보를 보호하고 불법 사용자의 접근을 차단하여 서비스의 안전성을 보장하는 기술
- ❖ 사용자 중심의 모바일 단말 환경에서 요구되는 다양한 보안 서비스 제공 가능



2. 기술이전 내용 및 범위(1/7)

▣ 기술이전 내용

❖ A. 보안 API 및 보안서비스 추상화 기술

- 일반도메인의 보안서비스(앱)가 분리된 안전실행엔진의 보안 기능을 사용할 수 있도록 개발자에게 제공된 API와 일반도메인에서 제공된 API의 실제 구현을 제공하는 안전도메인에서의 보안서비스 추상화 라이브러리로 구성됨
- 일반도메인에서 호출된 보안 API 내용을 분리된 안전도메인에 전달하고 수행된 결과를 보안서비스(앱)에게 전달하는 메시지를 관리하는 기능을 포함하고 있음.

❖ B. 가상화 기반 안전실행엔진 기술

- 보안서비스 프리미티브 기능 즉, 인증 및 접근제어, 암호알고리즘, 안전저장, 메시지 관리 등의 기능으로 구성됨
- 일반도메인에서 전달된 보안 API에 해당하는 보안서비스 추상화 라이브러리를 호출할 수 있도록, 일반도메인에서 호출된 보안 API 메시지를 해석 및 관리하는 기능을 포함하고 있음.

2. 기술이전 내용 및 범위(2/7)

▣ 기술이전 내용

❖ A. 보안 API 및 보안서비스 추상화 기술

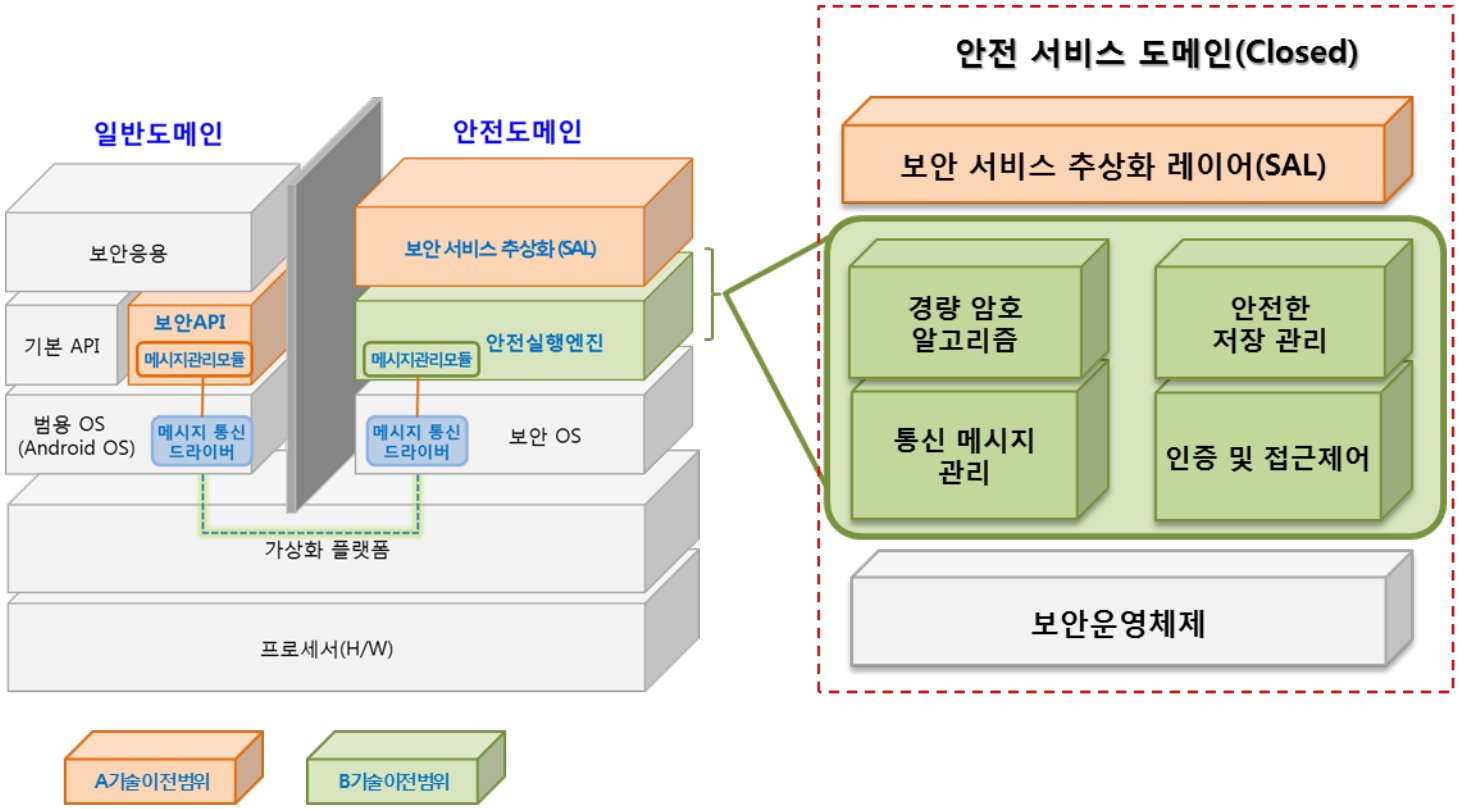
- 일반도메인의 보안서비스(앱)가 분리된 안전실행엔진의 보안 기능을 사용할 수 있도록 개발자에게 제공된 API와 일반도메인에서 제공된 API의 실제 구현을 제공하는 안전도메인에서의 보안서비스 추상화 라이브러리로 구성됨
- 일반도메인에서 호출된 보안 API 내용을 분리된 안전도메인에 전달하고 수행된 결과를 보안서비스(앱)에게 전달하는 메시지를 관리하는 기능을 포함하고 있음.

❖ B. 가상화 기반 안전실행엔진 기술

- 보안서비스 프리미티브 기능 즉, 인증 및 접근제어, 암호알고리즘, 안전저장, 메시지 관리 등의 기능으로 구성됨
- 일반도메인에서 전달된 보안 API에 해당하는 보안서비스 추상화 라이브러리를 호출할 수 있도록, 일반도메인에서 호출된 보안 API 메시지를 해석 및 관리하는 기능을 포함하고 있음.

2. 기술이전 내용 및 범위(3/7)

▣ 기술이전 내용



A. 보안 API 및 보안서비스 추상화 기술
B. 가상화 기반 안전실행엔진 기술

2. 기술이전 내용 및 범위(4/7)

▣ 기술이전 범위

◈ **A. 기술명 : 보안 API 및 보안서비스 추상화 기술**

- 시스템설계서 중 해당 기술 부분
- 보안서비스 및 API 블록 상위 설계서
- 보안서비스 및 API source code
- 시스템 시험계획서 중 해당 기술 부분
- 시스템 시험절차서 중 해당 기술 부분
- 시스템 시험결과서 중 해당 기술 부분

◈ **B. 기술명 : 가상화 기반 안전실행엔진 및 보안서비스 추상화 기술**

- 시스템설계서 중 해당 기술 부분
- 안전실행엔진 블록 설계서
- 보안엔진 프로그램 source code
- 시스템 시험계획서 중 해당 기술 부분
- 시스템 시험절차서 중 해당 기술 부분
- 시스템 시험결과서 중 해당 기술 부분

2. 기술이전 내용 및 범위(5/7)

▣ 기술이전 세부 내용

❖ A. 보안 API 및 보안서비스 추상화 기술

- **안전실행엔진용 일반도메인 보안 API 주요 기능**
  - 사용자 인증용 RSA 서명 생성 및 검증용 IF
  - G-PKI 연동용 KCDSA 서명 생성 및 검증용 IF
  - G-PKI 연동용 인증서 및 개인키 관리용 IF
  - 안전저장을 위한 File I/O IF
  - 안전도메인 채널 및 세션 생성 IF

- **보안서비스 추상화 기능**
  - 사용자 인증용 RSA 서명 생성 및 검증 구현
  - G-PKI 연동용 KCDSA 서명 생성 및 검증 구현
  - G-PKI 연동용 인증서 및 개인키 관리 구현
  - 안전저장을 위한 File I/O 구현
  - 안전도메인 채널 및 세션 생성 구현

- **일반도메인 영역 메시지 관리 기술**
  - 멀티 채널 지원 메시지 통신 구조 제공
  - 인증 세션 관리

2. 기술이전 내용 및 범위(6/7)

▣ 기술 이전 세부 내용

❖ B. 가상화 기반 안전실행엔진 및 보안서비스 추상화 기술

- 안전도메인 인증(Admission)/접근제어(Access Control) 기능
  - 사용자 패스워드 보호가 가능한 인증 및 접근제어 기능

- 암호 알고리즘
  - 대칭키 암호 : AES, SEED, ARIA (모드 : ECB/CBC/CTR/CFB/OFB)
  - 공개키암호 : RSA-1024, RSA-2048
  - 해쉬함수 : SHA1, SHA224, SHA256

- 안전한 저장관리(Secure Storage) 기능
  - 중요 데이터의 안전한(암호화) 저장/관리 기능

- 일반도메인 영역 메시지 관리 기술
  - 멀티 채널 지원 메시지 통신 구조 제공
  - 인증 세션 관리

2. 기술이전 내용 및 범위(7/7)

▣ 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

❖ 스마트 단말의 실행 환경을 두 개의 도메인으로 분리한 상태에서, 중요한 데이터의 저장 및 보안 기능을 안전 도메인 내에서 수행함으로써, 일반 도메인에서 루팅을 통한 중요 데이터의 유출 시도를 원천적으로 차단 가능

❖ 보안엔진내의 암호 기능에는 국산 암호알고리즘인 SEED, ARIA를 포함하고 있으므로, 국내의 기존 보안 시스템과의 연동에도 전혀 문제가 없음

▣ 기존 기술과의 비교

❖ 기존에는 모바일 단말의 중요한 데이터를 보호하기 위해 모바일 백신, 원격제어와 관련된 기술이 있으나, 이들 기술은 루팅 등을 통한 악의적인 공격으로부터 중요한 데이터를 보호하기 위해서는 부족한 면이 있음

❖ 하드웨어적인 실행환경 분리기술을 이용하지 않고, 소프트웨어적인 기법을 적용함으로써 비용 절감 및 배포의 용이성을 얻을 수 있음

4. 기술의 사업성

▣ 기술의 예상 적용 분야 및 조건

❖ 예상 응용 제품 및 서비스

- 재택근무, 홈오피스, 스마트워크 센터 등 스마트워크 환경의 단말
- 행정민원서비스, 현장지원서비스 등의 모바일 전자정부를 구축

❖ 사업성

- 스마트폰 보급이 향후 5년간에 5배 증가할 것으로 예상되므로, 모바일 단말 및 서비스 보안 시장 규모가 급증할 것으로 예상(출처: ABI Research, 2010)
- IDC에 의하면 세계적으로 모바일 보안 시장은 2011년 19억불에서 , 2015년 39억불로 성장을 예상

❖ 기술이전 업체 조건

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

❖ 사업화시 제약 조건

- 단말의 실행환경을 분리하는 가상화 기능은 업체가 담당

5. 국내외 시장 동향

▣ 기술현황 (모바일 단말 보안)

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

▣ 시장전망

- ❖ IDC에 의하면 세계적으로 모바일 보안 시장은 2014년 32억불에서 , 2018년 64억불로 성장을 예상

[표 1] Worldwide Mobile Security 2009-2013 Forecast and Analysis (단위: 억불)

관련 제품 /서비스	시장	1차년도 (2014년)	2차년도 (2015년)	3차년도 (2016년)	4차년도 (2017년)	5차년도 (2018년)	합계
스마트단말	해외	3,233	3,902	4,655	5,497	6,418	23,705
보안플랫폼	국내	167	223	288	362	445	1,485

감사합니다.

www.etri.re.kr

♣ 연락처 : 모바일보안연구실(사이버보안연구단), 김정녀 실장 (042-860-4884, jnkim@etri.re.kr)