

*IT R&D Global Leader*

[첨부 제4호]

# IoT 기기 권한관리 기술



임재덕 (jdscol92@etri.re.kr)

시스템보안연구그룹

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



## 목 차

---

1. 기술의 개요
2. 기술이전 내용 및 범위
3. 경쟁기술과 비교
4. 기술의 사업성
  - 활용분야 및 기대효과
5. 국내외 시장 동향

# 1. 기술의 개요



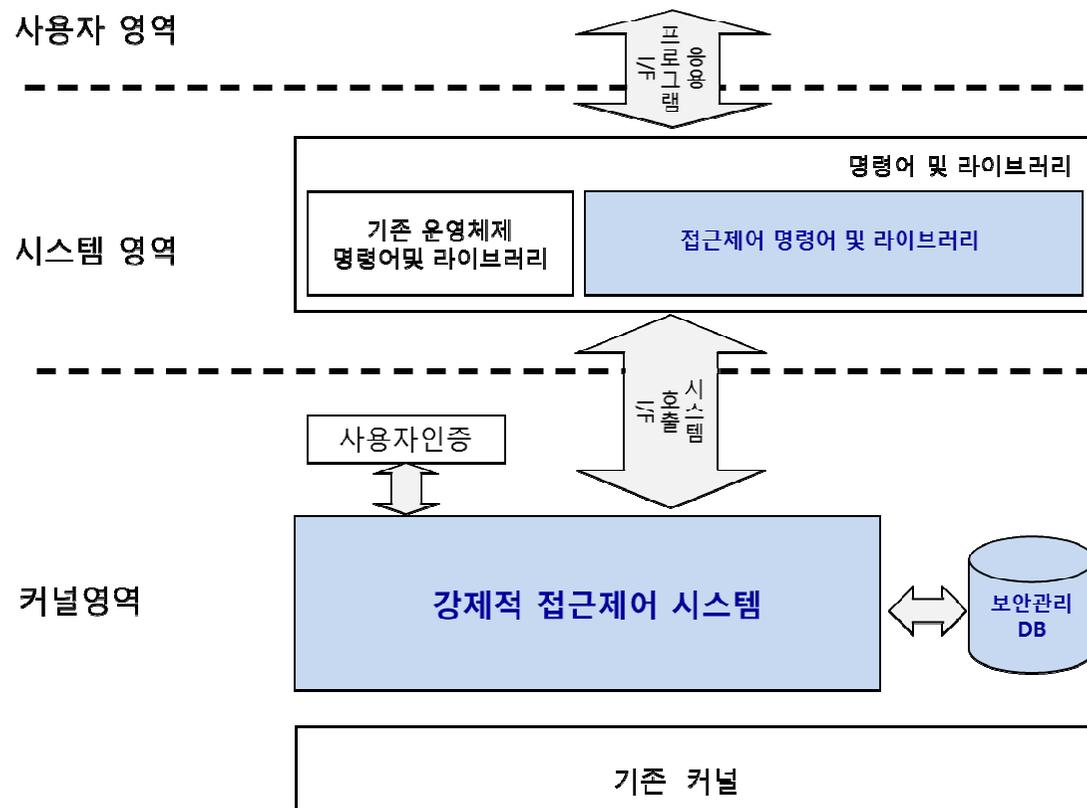
## ■ IoT 기기 권한관리 기술

- ❖ 기존 운영체제는 사용자가 루트 권한을 가질 경우 시스템 내의 모든 객체를 접근할 수 있는 막강한 권한을 가짐에 따라 내재된 보안 기능이 무력화될 수 있어, 버퍼오버플로우 등의 운영체제의 취약점을 통한 루트 권한 획득에는 무방비 상태임
- ❖ 본 기술은 루트가 가지는 막강한 권한을 분리할 수 있는 **최소 권한 분리 기능을 제공**하여 루트 권한을 가지더라도 별도의 접근 권한을 가지지 않을 경우 자원에 접근이 제한되어 해킹에 의한 루트 권한 획득 공격에 대응할 수 있음
- ❖ 본 기술은 시스템 운영체제 수준에서 발생하는 자원 접근과정에 있어 접근권한이 주어진 주체에 대해서만 접근을 허가하는 기능을 제공하며, 보다 구체적으로는 객체에 주어진 보안등급 및 범주를 기반으로 객체에 접근하는 주체의 속성을 확인하여 접근을 허용하는 **강제적 접근제어(MAC, Mandatory Access Control) 기능을 제공함**

## 2. 기술이전 내용 및 범위(1/4)

### ■ 기술이전 내용

#### ❖ 운영체제 수준의 자원 접근권한관리를 위한 접근제어 기술

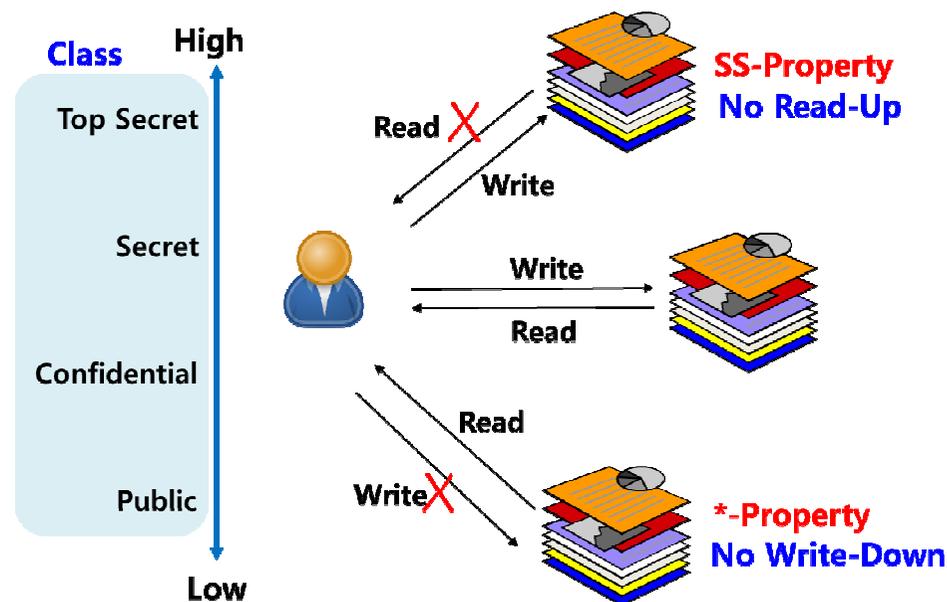


## 2. 기술이전 내용 및 범위(2/4)

### □ 기술이전 내용

#### ❖ MAC(강제적 접근제어) 기반 자원 접근 권한관리 기능

- MAC 정책 DB 관리
- Bell-LaPadula(BLP) 보안 모델 기반의 Simple Security & Modified \*-Property 를 적용
- 주체(사용자, 프로세스)와 객체(파일, 폴더)의 보안 등급 및 범주 기반의 접근권한(RWX) 수행



## 2. 기술이전 내용 및 범위(3/4)



### □ 기술이전 범위

- ◆ 접근제어시스템 설계문서 중 강제적 접근제어(MAC) 부분
- ◆ 접근제어시스템 블록별 설계문서 중 강제적 접근제어(MAC) 부분
- ◆ 접근제어시스템 시험문서 중 강제적 접근제어(MAC) 부분
- ◆ 접근제어시스템 소스 코드 프로그램 중 강제적 접근제어(MAC) 부분

## 2. 기술이전 내용 및 범위(4/4)

### ■ 기술 개발 현황

#### ❖ 기술 성숙도(TRL: Technology Readiness Level) 단계 : (3) 단계

구분	단계	정의	세부 설명
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	시험생물을 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	파일럿 규모 시작품 제작 및 성능 평가	파일럿 규모(복수 개~양산규모의 1/10정도)의 시작품 제작 및 평가가 완료된 단계 파일럿 규모 생산품에 대해 생산량, 생산용량 불량률 등 제시 파일럿 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 파일럿 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

- ❖ 운영체제 수준에서 다양한 자원접근권한 기능을 통해 시스템 내의 최소 권한 분리 환경을 제공할 수 있으므로, 루트 권한을 획득한 해커 등의 악성 코드에 의한 불법 자원 접근을 방지할 수 있어, 시스템 자원을 보호할 수 있음
- ❖ MAC(Mandatory Access Control) 기능을 통해 시스템 내의 보호 자원에 대한 보호 등급과 범주를 강제적으로 지정하도록 하여, 임의로 루트 권한을 획득한 경우에도 정당한 접근 등급과 범주를 획득하지 못할 경우 자원 접근을 통제하는 기능을 제공함

#### ■ 기존 기술과의 비교

- ❖ 보안운영체제 내의 자원 접근 권한관리 기술은 기본적으로 ACL, MAC, RBAC 개념을 적용하고 있음
- ❖ 본 기술은 ACL, MAC, RBAC 개념 중 MAC 기술을 적용하고 있으며, 관리의 편의성을 위해 다양한 관리 인터페이스와 이식성을 높이기 위해 모듈 단위로 기능을 제공함

## 4. 기술의 사업성



### ▣ 기술의 예상 적용 분야 및 조건

#### ❖ 예상 응용 제품 및 서비스

- 인증정보 보호를 위한 인증서버
- IoT 서비스 제공 서버 내의 중요 데이터 유출 방지를 위한 IoT 클라우드 서버
- 네트워크 운용 정보 위변조 보호를 위한 IoT 보안GW 및 네트워크 서버

#### ❖ 사업성

- 본 기술이 적용될 보안운영체제 시장은 운영체제 시장과 밀접한 관계가 있으며, 이를 기준으로 Gartner에서 분석한 세계 운영체제 시장을 살펴보면, 2011년 347억 달러 규모로 성장하였다가 2013년에는 344억 달러로 감소되었으나, 운영체제가 시스템의 기본이면서 핵심 SW임과 IoT 등 신기술 발전으로 클라우드 서버 등의 수요가 증가함을 감안하면 시장 규모가 증가할 것으로 예상됨

#### ❖ 기술이전 업체 조건

- 리눅스 혹은 BSD 계열의 운영체제/커널 등의 시스템 엔지니어링 및 임베디드 시스템 엔지니어링이 가능한 업체

#### ❖ 사업화시 제약 조건

- 본 기술은 운영체제 수준에서 동작하기 때문에, 본 기술을 적용하여 보호하려는 운영체제에 대한 자원 관리(자원 접근 등) 구조, 시스템 호출 구조 등의 파악을 통해 본 이전 기술의 접근권한 인터페이스와 연동 과정이 필요하며, 해당 부분은 업체가 담당함

## 5. 국내외 시장 동향

### ■ 기술현황 (기기 권한관리 기술)

- ❖ IBM, HP, SCO, Sum Microsystems, Miscosoft 등 서버 업체를 중심으로 자사의 운영체제에 다양한 보안 기능을 탑재하여 CC 인증을 획득하고 있음
- ❖ 구글은 자사 안드로이드 운영체제 내에 강제적 접근제어 구조가 적용된 SELinux를 채용하여 퍼미션 기반의 자원접근 권한을 관리하고 있음
- ❖ (주)시큐브, (주)시큐브레인, (주)테이스온넷, (주)레드게이트 등이 접근제어와 다중보안등급 등의 기능을 적용하여 PC 및 서버 보안 솔루션을 출시하고 있음
- ❖ 삼성은 모바일 운영체제인 Tizen 운영체제 내에 SMACK(Simple MAC for Kernel) 구조를 채용하여 모바일 환경에 적합한 강제적 접근제어를 제공하고 있음

### ■ 시장전망

(단위 : 백만불, 억원)

관련 제품 /서비스	시장	1차년도 (2018년)	2차년도 (2019년)	3차년도 (2020년)	4차년도 (2021년)	5차년도 (2022년)	합계
보안 운영체제	해외	14,078	14,979	15,939	16,959	18,045	80,000
	국내	2,082	2,111	2,140	2,170	2,200	10,703
합계	해외	14,078	14,979	15,939	16,959	18,045	80,000
	국내	2,082	2,111	2,140	2,170	2,200	10,703

- 출처 자료의 서버 및 PC OS 시장 규모에서의 CAGR(해외 6%, 국내 1%)를 반영하고, 보안OS 시장을 30% 비율로 산정함.

. 출처. 운영체제 시장동향 및 이슈 분석, 전자통신동향분석, 2014. 해당 출처는 Gartner의 "Market Share: Operating System Software, Worldwide 2009, 2010, 2011, 2012, 2013" 자료 및 StatCounter Global Stats 자료를 인용함. 인용된 자료에서는 OS 시장을 분석하였으며, 보안OS 시장을 20% 비율로 산정함

감사합니다.



[www.etri.re.kr](http://www.etri.re.kr)