임베디드 운영체제에서의 접근제어기법

송승호 ○, 허신
한양대학교 컴퓨터공학과
glukjeoluk@osnn.hanyang.ac.kr, shinheu@cse.hanyang.ac.kr

Access Control Techniques for Embedded Operating System

Seung-Ho Song ○, Shin Heu
Department of Computer Science and Engineering, Hanyang University

요 약

임베디드 시스템은 MP3 Player, PMP, PDA 등 우리 생활의 일부분으로 자리 잡고 있으며, 이 외에도 로봇 시스템, 공장자동화 시스템, 군사기기 및 센서 노드 등에도 내장되어 사용 되어지고 있다. 이러한 임베디드 시스템은 앞으로도 나날이 발전을 하여 각 개인이 최소 하나 이상씩은 휴대를 할 정도로 임베디드 기기에 대한 의존도가 높아 질것이며, 이렇게 임베디드 기기에 대한 의존도가 높아질수록 더 많은 개인 정보들이 임베디드 기기에 저장이 될 것이다. 이에 따라 임베디드 기기내의 개인 정보 보호가 급격히 대두 될 것이다. 본 논문에서는 이러한 임베디드 기기내의 개인 정보 보호와 시스템 자원 보호를 위하여 사용자 인증과 접근제어기법에 대해 알아보도록 하겠다.

1. 서 론

전통적인 정보 보호의 기법들은 데스크톱 PC나 엔터프라이즈 급 서버의 보안을 위해 개발, 발전되어 왔다. 그러나 이러한 보안 기법들을 제한된 시스템 성능과 가용 자원을 가지는 임베디드 시스템에 그대로 적용하기에는 적합하지가 않다. 특히 임베디드 시스템은 MP3 플레이어, PDA, PMP, 디지털 카메라, 휴대폰 등 우리 일상 생활과 밀접한 관계를 가지고 있고 응용 범위 또한 매우 넓다. 그래서 임베디드 시스템의 응용 시장이 매우 빠르게 발전하고 요구사항 또한 급증 하고 있는 추세이다. 이러한 시장의 요구사항이 날로 커짐에 따라 그에 따른 여러 서비스 관련 기술들이 개발되어 현재에는 데스크톱 PC에서 가능했었던 인터넷 뱅킹, 홈쇼핑 결재 등의 사용이 임베디드 시스템에서도 가능해지고 있는 추세이다. 이에 임베디드 시스템을 사용하는 사용자들은 개인의 중요한 정보를 해당 장비에 저장을 해놓음에 따라 임베디드 운영체제에서의 보안 기술은 시간이 지날수록 중요해 질 것이다. 특히, 임베디드 시스템의 특성상 사용 목적 및 용도에 따라 기능 또한 다양해지고 특정 임베디드 시스템의 목적에 맞추어 구축할 수 있는 재구성 및 설정 기능도 요구되고 있다.[1]

본 논문에서는 보안 기법중의 하나인 접근 제어 기법에 대해서 알아 보고, 개인 정보 보호와 임베디드 시스템의 자원의 보호를 위하여 사용자 인증과 접근 제어 기법에 대해 설명 하겠다.

2. 접근제어 기법

접근 제어 기법은 일반적으로 임의적 접근 제어 (Discretionary Access Control), 강제적 접근 제어 (Mandatory Access Control), 직무 기반 접근 제어 (Role Based Access Control)로 구분되며, 사용자의 신분 및 직책, 역할, 소속그룹 등에 의해 시스템 자원에 접근 가능하도록 하여 악의를 품은 불법적인 사용자들로부터 시스템 자원을 보호할 수 있다.

2.1 임의적 접근제어(Discretionary Access Control)

임의적 접근 제어 기법은 시분할 시스템에서 한 사용자가 다른 사용자와 시스템 자원을 전체 혹은 부분적으로 독립적으로 접근 하기 위하여 소개되었다. 임의적 접근 제어는 TCSEC(Trusted Computer Security Evaluation Criteria)에서 정의하고 있으며, ISO(International Standard of Organization)에서는 신원 기반 접근 제어 기법(Identity-Based Access Control)과 동일하다. 임의적 접근 제어는 전통적인 유닉스 시스템에서 파일 접근 방법인 사용자의 신분에 근거하여 시스템 자원에 대한 접근을 제한하는 방법이다. 임의적 접근 제어 기법은 표 1과 같이 Access Control Matrix에 의해 접근이 이루어 지며, 열은 객체에 접근하고자 하는 주체(Subject)를 나타내며, 행은 객체(Object)를 나타내며, 각 요소(Element)들은 접근 권한을 나타낸다.

접근 제어 모델에서 현재 접근 집합 P = (S × O × A) 로 나타낼 수 있으며, S는 주체들의 집합, O는 객체들의 집합, A는 접근 모드의 집합을 나타내며, Matrix의 접근 권한과 일치한다.

표 1. Access Control Matrix

Object / Subject	F1	F2	F3	F4
U1	r	-	rwa	rwae
U2	r	rwa	rw	-
U3	rwae	rw	-	r

Subject : U1, U2, U3 Object : F1, F2, F3, F4

Access Right : r(읽기), w(쓰기), a(기록), e(수행)

임의적 접근 제어는 접근을 요청하는 사용자의 식별에 기초하며, 어떤 시스템 자원에 대해 사용자가 접근권한을 추가 및 철회할 수 있다. 이것은 소유권을 통한 관리적 제어가 분산됨을 의미한다. 그러나 임의적 접근 제어는 중앙 집중관리에서는 적합하며, 이러한 경우 권한 부여는 시스템 관리자에 의하여 관리될 것이다.

임의적 접근제어 기법이 갖는 일반적인 속성을 살펴보면 3가지로 요약할 수 있다.[2]

- 임의적 접근제어 기법은 허가된 주체에 의하여 변경 가능한 하나의 주체와 객체간의 관계를 정의한다.
- 한 주체가 어느 한 객체를 읽고 그 내용을 다른 어느 한 객체로 복사하는 경우에 처음의 객체에 내포된 접근제어정보가 복사된 객체로 전파되지 않는다.
- 임의적 접근제어 기법은 모든 주체 및 객체들 간에 일정하지 않고 하나의 주체/객체 단위로 접근제한을 설정할 수 있다. 즉, 임의적 접근제어 기법이 어느 한 주체로 하여금 특정 비밀등급의 한 객체를 접근하지 못하게 할지라도, 그 주체는 다른 주체가 그러한 비밀등급을 갖는 다른 객체들을 접근하는 것일 방지할 수 없다.

위와 같은 임의적 접근제어 기법의 일반적인 속성으로 인하여 내재적으로 상속되는 결점이 있는데, 첫째, 임의적 접근통제 정책의 속성상 통제는 주체의 신분에 전적으로 근거를 두며, 메커니즘은 데이터의 의미에 대한 아무런 지식도 갖고 있지 않으면, 이에 근거하여 결정할 것도 없다. 둘째, 이와 같이 주체의 신분이 매우 중요하므로 만약, 다른 사람의 신분을 사용하여 행위가 이루어진다면 임의적 접근제어 기법은 파괴될 수 있다. 셋째, 트로이 목마에 대하여 취약하며, 메시지 내용의 비밀 유지가 어렵다.

2.2 강제적 접근제어(Mandatory Access Control)

임의적 접근 제어 기법은 트로이 목마로부터의 공격에 취약하며, 메시지 내용의 비밀 유지가 어렵다. 강제적 접근제어 기법은 이러한 직간접적인 불법적 공격으로부터의 접근을 제한하며, ISO의 규칙기반 접근제어 기법과 동일한 개념이다.

강제적 접근 제어 기법은 객체에 포함된 정보의 비밀성과 이러한 비밀성의 접근 정보에 대하여 주체가 갖는 권한에 근거하여 객체에 대한 접근을 제한하는 방법이다. 강제적 접근 제어 기법은 사용자 및 대상 별로 부여된 기밀 분류에 따른 정책(MLP, Multi-Level Policy)과 조직 내의 각 부서별로 구분된 기밀 허가에 따르는 정책(CBP, Compartment-Based Policy)으로 분류할 수 있다.[2]

강제적 접근제어 기법은 각 등급의 시스템 데이터와 각 등급의 사용자간에 강력한 보호를 위하여 요구되는 많은 정보를 적용한다. 데이터에 대한 접근은 주체와 객체가 갖는 보안등급의 정의를 통한 강제적인 정책에 의해 결정된다. 객체 보안 등급의 2가지 주요특성을 포함하고 있는 정보를 반영한 허용등급과 객체 정보가 언급하는 응용분야의 범주로 구성된다.

각 주체와 객체는 객체의 허용등급을 나타내는 기밀수준과 범주의 집합으로 구성된 보안등급을 할당한다. 이 2개의 요소는 시스템에서 주체 및 객체의 역할과 대응된다. 주체의 등급은 그 주체에 할당될 수 있는 신뢰의 정도를 나타내고 객체의 등급은 정보의 부당한 사용에 의한 손상 정도를 고려한 객체에 포함된 정보의 기밀성을 반영한다.

접근권한 전송과 관련하여 할당된 권한은 변경될 수 없고 권한을 갖는 관리자에 의해서만 수정이 허용된다. 이것은 접근제어 시스템상의 모든 권한 제어가 권한을 갖는 보안관리자에 의해서 유지됨을 의미한다.

강제적 접근제어 기법은 임의적 접근제어 기법에 비하여 일반적으로 다음과 같은 특성을 가진다. 첫째, 강제적 접근제어 기법은 객체의 소유자가 변경할 수 없는 주체들과 객체들 간의 접근제어 관계를 정의한다. 둘째, 한 주체가 한 객체를 읽고 그 내용을 다른 객체에게 복사하는 경우에 원래의 객체에 내포된 강제적 접근통제 제약사항이 복사된 객체에 전파된다. 셋째, 강제적 접근제어 기법은 모든 주체 및 객체에 대하여 일정하며, 어느 하나의 주체/객체 단위로 접근 제한을 설정 할 수 없다. 즉, 강제적 접근제어 기법은 어느 한 객체를 접근하지 못하면, 이때에 그 주체는 이러한 특정의 비밀 등급을 갖는 모든 객체들을 접근하는 것이 금지된다.

2.3 직무 기반 접근제어(Role Based Access Control)

직무 기반 접근 제어 기법은 Ravi S. Sandhu에 의해 처음 소개되었다. 직무 기반 접근 제어 기법은 현대의 컴퓨터 시스템 환경에서 특히 가치가 있는 접근 제이 기법으로 임베디드 시스템에 많이 적용되고 있는 기법이다. 직무 기반 접근 제어는 정보에 대한 사용자의 접근이 개인신분에 따르는 것이 아니라 조직 내에서 개개인의 직무(또는 직책)에 따라 결정된다.

그림 1은 Ravi S. Sandhu의 직무기반 접근제어 모델로 사용자의 권한과 역할간의 관계를 나타내고 있다. 직무기반 접근제어 모델은 개념적으로 보면 사용자(U), 역할(R), 권한(P)로 구성된다. 일반적으로 사용자는 해당 직무에 속한 사람을 나타내며, 역할은 사용자와 권한의 집합으로 구성되며, 조직내의 작업 함수 혹은 작업의 제목을 나타낸다.

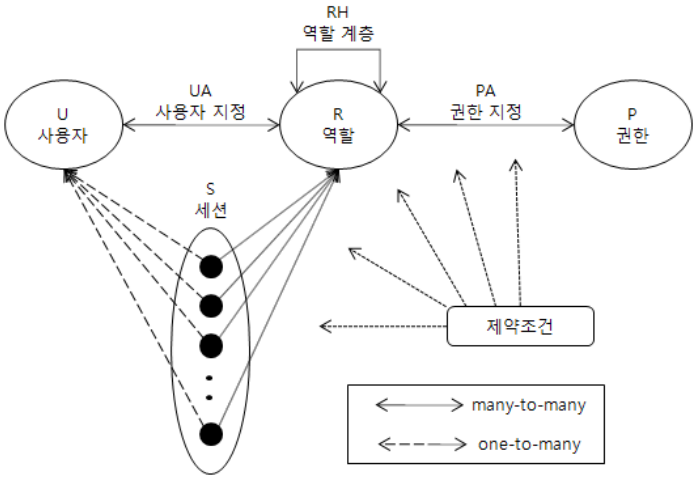

그림 1. RBAC 모델

권한은 자원에 대한 특정한 접근권한을 나타내며, 하나 혹은 그 이상의 자원에 적용될 수 있다. 세션(S)은 사용자가 속해있는 역할에서 부분집합을 활성화시킬 때 생성이 되기 때문에 일시적이다. 사용자는 자격과 책임을 기반으로 역할에 지정되고, 하나의 역할에서 다른 역할로 쉽게 재 지정될 수 있으며, 여러 가지의 역할을 할당 받을 수도 있다. 사용자와 권한의 관계는 일시적이며, 역할은 특정한 작업을 수행할 수 있는 능력과 특정한 위치에 지정됨으로써 가질 수 있는 권한 및 책임으로 표현된다. 따라서 사용자는 역할의 지정됨에 따라 그 역할에서 특정 작업을 수행할 수 있는 권한을 갖게 된다.

직무기반 접근제어 모델의 구성요소를 간단히 정리하면 다음과 같다.

- U, R, P, S : 사용자, 역할, 권한, 세션의 집합
- PA ⊆ P × R : 권한과 역할지정 관계 (many-to-many)
- UA ⊆ U × R : 사용자와 역할지정 관계 (many-to-many)
- RH ⊆ R × R : 역할계층이나 역할의 유전 관계를 부분 순서로 나타냄

3. 임베디드 운영체제 접근제어 기법

앞 장에서 각각의 접근제어 기법들에 대해 살펴보았다. 그러나 이러한 접근 제어 모델은 데스크톱 PC나 엔터프라이즈 급 서버에 적용되는 기법들로서 임베디드 시스템에 바로 적용하기에는 어렵다.

이번 장에서는 임베디드 시스템에 적용 가능한 접근제어 기법에 대해서 살펴보도록 하겠다.

3.1. 사용자 인증

임베디드 시스템에서 사용자는 로그 인을 하지 않는다. 이러한 특성은 임베디드 시스템의 자원을 다른 사용자로부터 보호하지 못하는 특성을 가지게 된다.

사용자는 임베디드 시스템에서 운용할 수 있는 응용프로그램을 개발하는 개발자, 임베디드 장비를 테스트할 장비 관리자, 임베디드 장비를 사용할 사용자로 구분을 할 수 있다. 이러한 각각의 사용자들이 자신의 업무 범위에 맞게끔 임베디드 시스템의 자원을 이용가능 해야 하며, 사용이 인증되지 않은 불법사용자로부터 시스템 자원을 보호해야 한다.

임베디드 시스템을 사용하고자 하는 사용자는 인증을 통해서 시스템의 사용 범위가 결정 되도록 하고, 이에 맞는 적절한 시스템 자원을 사용하도록 한다.

3.2. 접근 제어 모듈

임베디드 시스템에서 운용되는 응용 프로그램들이 시스템 자원에 접근하기 위해서 그림 2와 같이 접근 제어 모듈을 통해 현재 사용자가 어떠한 권한과 역할을 가지고 있는지를 확인을 하고 시스템 자원에 접근을 한다.

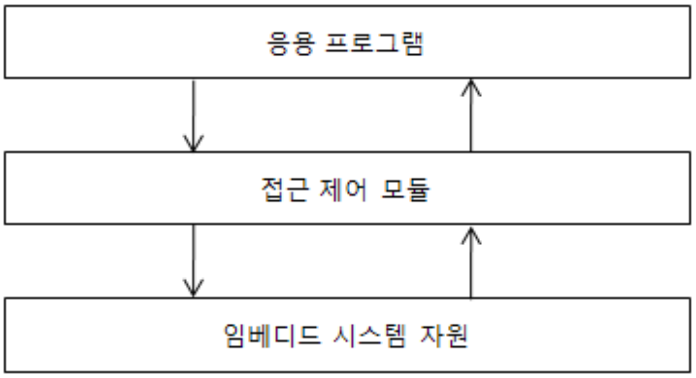

그림 2. 임베디드 시스템 접근 제어

접근 제어 기법은 RBAC에 근간을 두고 이루어진다. 이러한 접근 제어 모듈을 통하여 불법 사용자의 접근을 차단하며, 시스템 자원뿐만 아니라 개인의 중요한 정보 역시 보호할 수 있다.

접근 제어 모듈은 다음과 같은 기능들을 가진다.

- 사용자가 속한 그룹 및 권한 확인
- 시스템을 사용하는 사용자 로그 파일 작성
- 시스템 자원에 접근하는 응용프로그램의 로그 파일 작성
- 접근 권한 프로파일 작성

접근 제어 모듈은 그림 3과 같이 시스템을 사용하고자 하는 사용자 혹은 응용 프로그램의 정보를 먼저 확인을 하여 인가된 사용자인지 인가되지 않은 사용자인지를 확인한다. 만약 인가되지 않은 사용자가 접근을 하면 악의적인 목적으로 접근을 하는 경우이기 때문에 시스템 자원에 접근 할 수 없도록 차단을 한다. 인가된 사용자인 경우에는 현재 사용자의 권한과 역할을 확인하고 그에 맞는 시스템 자원의 접근 범위를 결정한 후 시스템 자원에 접근 가능 하도록 허용을 한다.

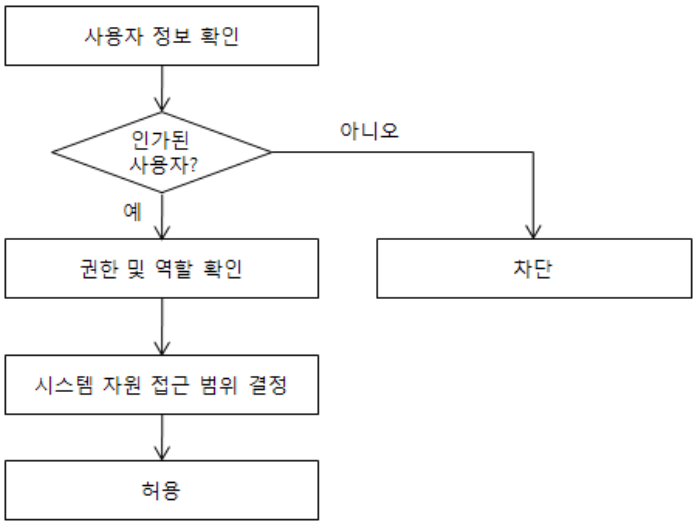

그림 3. 시스템 자원 접근

접근 제어 모듈에서 작성되는 로그 파일들은 인가되지 않은 사용자나 악의적은 응용프로그램이 시스템 자원에 접근하는지 분석하는 용도로 이용된다.

3.3. 접근 권한 프로파일

접근 제어 모듈에서 작성된 접근 권한 프로파일은 다양한 임베디드 시스템에 현재의 정책이 빠르게 적용할 수 있도록 하여 임베디드 시스템의 확장성과 신뢰성을 제공한다.

4. 결론

임베디드 시스템은 전세계적으로 많은 분야에 이용되고 있는 추세이다. 이에 임베디드 시스템 사용자는 더 많은 개인의 중요한 정보를 임베디드 시스템에 저장할 것이며, 임베디드 운영체제의 보안 기법은 향후 더 많이 기술들을 요구 할 것이다. 현재 많은 보안 기술들은 일반 데스크톱 PC나 엔터프라이즈 급 서버들을 위해 개발되었으나 임베디드 시스템은 이와 달리 한정된 자원을 사용하고, 여러 사용자들이 사용하는 것이 아니라 한 명의 사용자만이 시스템을 사용한다는 특성을 가지고 있다. 이러한 특성은 악의를 품은 불법 사용자로부터 시스템 자원을 보호해주지 못한다. 악의적인 사용을 사전에 방지 하기 위하여 사용자 인증 및 접근 제어 기법을 이용하여 불법 사용자로부터 임베디드 시스템의 자원을 보호하고 개인의 중요한 정보를 보호할 수 있다. 본 논문에서는 사용자 인증과 접근제어 기법만을 설명하였으나 향후 파일 암·복호화 기법과 프리빌리지 관리 기능 및 감사 관리 기능을 추가하여 임베디드 시스템의 자원과 개인의 중요한 정보를 불법적인 사용자로부터 더욱 견고하게 지킬 수 있으며 더운 안정되고 신뢰성 있는 임베디드 운영체제를 개발 할 수 있다.

참 고 문 헌

[1] 정영준, 임동혁, 서영빈, 김재명, “임베디드 운영체제 보안 기술 동향”, ETRI, 제23권, 제1호, 2008.2.

[2] 홍기융, 김재명, 홍기완, “Secure OS 보안정책 및 메커니즘”, 정보보호학회, 제13권, 제4호, 2003.8.

[3] Ravi S. Sandhu, “Role-Based Access Control Models”, IEEE Computer, Volume 29, Number 2, February 1996

[4] Ahmad Ubaidah Omar, “Trusted Computer System: Understanding and Issues”, SANS Security Essentials GSES Practical Assignment Ver 1.3, 25 March 2002

[5] Charles P. Pfleeger, Shari Lawrence Pfleeger, “Security in Computing Third Edition”

[6] Matt Bishop, “Computer Security : Art and Science”