임베디드 OS에서의 역할기반 접근제어 적용

Appplication of Role-based access control in Embedded OS

임재덕*, 은성경† , 김기영‡ , 김정녀¶, 이철훈§
JaeDeok Lim*, SungKyong Un† , KiYoung Kim‡ , JeongNyeo Kim¶, ChoelHoon Lee§

Abstract - Recently, the security requirements of the embedded system which were not considered when the embedded system is independently deployed are being increased because the embedded system is connected to an internet. The connection to the internet of embedded system is the meaning that it is exposed to the various kinds of external attack and can be a victim to these attacks in anytime. Particularly, it is trend that the user-related information is stored into the personal terminals and/or electrical appliances such as PDA, home gateway for home network, settop boxes and so on. So it is needed the security mechanism which protects the user information from the malicious accesses. Accordingly, the coverage of the system security is being expanded from the general server to the embedded system. And it is not enough that the embedded system supports only its inherent functions and it becomes the essential element to provide the security function to the embedded system. This paper applies the RBAC(role-based access control) function to the embedded linux OS and tries to strengthen the security of the embedded linux OS. RBAC is implemented as a loadable kernel module with LSM(Linux Security Module) security framework for user's flexibility.

Key Words : 임베디드 OS, 접근제어, RBAC, Qplus, LSM

1. 서론

특정한 목적을 수행하는 단말의 요구 증가로 임베디드 시스템 시장이 점차 커짐과 동시에 임베디드 시스템의 응용 범위가 넓어짐에 따라 필요한 많은 기능을 충족시켜주기 위한 범용 운영체제 기반의 임베디드 OS에 대한 요구가 증가하고 있다[1]. 임베디드 리눅스는 이러한 요구 속에 꾸준히 성장해 왔다. 임베디드 리눅스는 기존의 전통 임베디드 RTOS들 보다 많은 기능을 지원하고 공개 소스를 이용하여 개발 속도가 빠르며 비용이 상대적으로 적게 드는 장점을 가진다. 최근 인터넷 환경에서 운용되는 임베디드 시스템이 증가함에 따라 독립적으로 운용되었을 때 고려되지 않았던 보안 요구 사항이 증가하고 있다. 이는 인터넷을 통한 외부 침입의 가능성이 높아지고 개인 휴대 단말이나 셋탑 박스 등의 중소형 단말에 사용자 정보와 이용 기록 등의 민감한 개인 정보가 임베디드 시스템에 저장되는 추세와 맞물려 개인 정보 유출의 가능성을 높이고 있다. 실제로 휴대폰이나 PDA 등에는 바이러스 침입으로 피해가 속출하고 있다.

본 논문은 앞으로 다양한 환경에 적용될 임베디드 시스템의 OS로 보편적으로 사용될 임베디드 리눅스에 역할기반 접근제어(Role-based access control, 이하 RBAC) 기능을 적용하여 임베디드 시스템의 보안성을 강화하고자 한다.

임베디드 리눅스는 ETRI에서 개발 배포하는 Qplus를 사용하였다. Qplus는 사용자 개발 환경인 Target Builder 툴킷을 제공하여 개발자로 하여금 보다 편리하고 빠른 기간 내에 임베디드 시스템 개발을 가능하게 해 준다[2].

RBAC은 운영체제의 보안 기능을 강화하기 위해 적용된 접근제어 모델 중 하나로 역할(Role)에 기반한 강화된 접근제어 기능을 제공한다[3,4]. RBAC는 객체에 대한 주체의 접근을 개별적인 신분이 아닌 각 주체의 역할에 따라 결정된다. 그리고 DAC(Discretionary Access Control), MAC(Mandatory Access Control) 등과 같은 접근제어와 달리 정책 관리자에게 많은 융통성과 관리의 편리성을 제공해 주는 접근제어 모델이다. 역할은 다양한 작업에 대한 처리의 기능으로 정의된다. 임의의 처리를 수행하는 허가(permission)는 임의의 역할에 할당되고, 시스템 사용자들은 임의의 역할을 할당 받는다. 사용자는 할당받은 임의의 역할을 기반으로 시스템에 정한 역할 정책을 통해 시스템 내에서 작업을 수행한다. 즉, 사용자는 임의의 작업에 대한 허가를 직접적으로 할당받지 않고 임의의 작업에 대한 허가를 가진 임의의 역할을 할당받음으로써 시스템 접근제어 정책의 영향을 받는다. 이는 시스템 운영/보안 정책이 변경되었을 경우 사용자에게 직접 할당된 접근제어 정책을 관리하기 보다는 사용자에 할당된 역할을 관리함으로써 보다 더 효율적인 시스템 운영/보안 정책을 가능하게 해 준다. 구현된 RBAC 기능은 Qplus 임베디드 리눅스 OS에 커널 모듈 형태로 추가되어 Intel PXA270 프로세서 기반의 X-Hyper270A 임베디드 시스템에 이식되었다.

저자 소개
* 임재덕 : 한국전자통신연구원 정보보호연구단 선임연구원
† 은성경 : 한국전자통신연구원 정보보호연구단 선임연구원
‡ 김기영: 한국전자통신연구원 정보보호연구단 책임연구원
¶ 김정녀 : 한국전자통신연구원 정보보호연구단 책임연구원
§ 이철훈 : 충남대학교 컴퓨터공학과 정교수

본 논문에서 제공되는 RBAC 기능은 리눅스 커널에서 제공하는 LSM(Linux Security Module) 인터페이스를 기반으로 한다. LSM은 리눅스 커널 2.6 부터 제공되는 커널 레벨의 보안 프레임워크이며, 총 88개의 hook을 가지고 있어 프로그램 로딩, 파일 접근, IPC 사용 등 보안 검사가 필요한 곳에서 LSM 모듈에서 제공하는 함수를 호출할 수 있도록 한다[5]. 의도적인 침입에 의한 불법적인 시스템 자원 접근은 물론이고 사용자 콘텐츠 내에 이식되어 배포되는 악성 코드에 대한 불법적인 시스템 자원 접근은 본 논문에서 제공되는 RBAC 기능을 통해 방어할 수 있어 인터넷 환경에서 제공되는 임베디드 시스템의 보안성을 강화할 수 있다.

본 논문은 총 4장으로 구성되어 있으며 2장에서 LSM 기반의 RBAC 구조를 설명하며 3장에서 X-Hyper270A 타겟 시스템으로의 이식에 대해 설명한다. 그리고 4장에서 결론 및 앞으로의 과제에 대해 설명할 것이다.

2. LSM-based RBAC 구조

RBAC은 리눅스 커널에 위치하며 LSM(Linux Kernel Module) 형태로 구성된다. RBAC 모듈은 라이브러리를 통해 요청된 사용자 명령(관리요청)을 처리하고 커널 내의 LSM hook에서 요청된 접근제어 요청을 처리한다. 그림 1은 LSM 기반으로 구성된 RBAC 모듈의 운용을 보여준다. RBAC 모듈은 크게 정책 관리 부분과 정책 결정 및 적용 부분으로 구분된다.

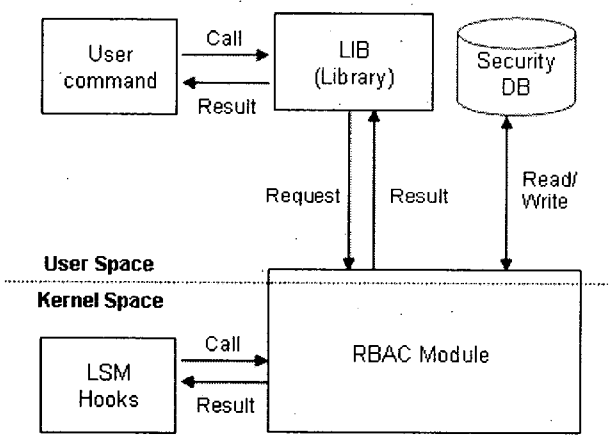

그림 1. LSM 기반의 RBAC 모듈 운용

정책 관리 부분은 RBAC 처리를 위한 정책 설정 부분이라고 할 수 있다. 시스템 운용 과정 중에 발생하는 접근제어 처리를 정책 관리 부분에서 설정한 접근제어 정책에 따라 이루어진다. 정책 설정 과정은 다음과 같다. 관리자는 정책 관리 기능에 해당하는 명령어를 통해 정책 설정을 RBAC 모듈에게 요청한다. RBAC 명령은 명령 처리를 위해 RBAC 라이브러리를 호출하고, 라이브러리는 RBAC 모듈 내의 RBAC 시스템 콜을 호출한다. RBAC 시스템 호출은 전달된 명령에 대한 적절한 처리를 수행하면서 필요시 보안 DB와 연결되어 필요한 정보를 저장 혹은 삭제 등의 처리를 수행한다. 예를 들어 시스템에 임의의 역할 "R"을 추가하고자 할 경우, 시스템 역할 추가 명령을 관리자가 수행하면 역할 추가 라이브러리, 역할 추가 시스템 콜이 차례로 호출되어 추가한 "R" 역할은 보안 DB에 저장되고, 시스템이 사용할 수 있은 역할로 설정된다. 정책 관리 부분에서 수행하는 기능은 다음과 같다.

- 보안 DB 초기화 : RBAC 처리를 위한 정책이 저장되는 곳으로 사용자 관리 명령어를 통해 보안 DB를 초기화한다.
- 역할 관리 : 시스템에서 사용할 역할 생성 및 삭제, 각 역할에 대한 배타적 설정, 각 역할에 대한 최대 할당 가능치 등을 설정한다.
- 사용자 관리 : 시스템 사용자에 대해 역할을 할당 및 삭제한다.
- 프로세스 관리 : 현재 수행중인 프로세스에 대해 역할을 할당 및 삭제한다.
- 파일 관리 : 시스템에서 사용 중인 파일에 대해 역할을 할당 및 삭제한다.

정책 결정 및 적용 부분은 LSM 인터페이스를 통해 요청된다. 시스템 운용 중 프로세스가 시스템의 자원을 접근하고자 할 경우에 RBAC 모듈을 통한 접근제어를 통해 접근된다. 그림 2는 RBAC 적용 과정에서 정책 결정 및 적용 과정을 보여준다.

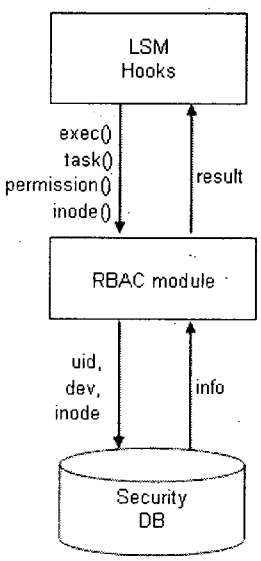

그림 2. RBAC 정책 결정 및 적용 과정

정책 결정 및 적용 부분은 LSM 인터페이스를 통해 요청된다. 커널이 LSM을 지원할 경우 시스템 운용 시 프로세스의 동작이나 객체에 대한 접근이 발생할 시 모든 작업은 LSM hook을 통하게 되어 있다. 그림 2에서 보듯이 바이너리 실행이나 작업 수행, 객체에 대한 접근 이벤트 등이 발생할 경우 LSM hook을 통해 구현된 작업을 수행한다. 본 논문은 이런 hook을 통해 RBAC 정책을 통한 접근제어를 수행하도록 구현하였다. LSM에서 제공하는 모든 hook에 대해 구현한 것이 아니라 RBAC 기능 제공에 필요한 부분만 사용하였으며 사용된 hook을 통해 접근제어 이벤트가 발생할 경우 RBAC 모듈을 통해 미리 설정된 보안 DB의 정책에 따라 접근을 제어한다. 예를 들어 프로세스가 파일에 접근할 경우

읽기 요청이나 쓰기 요청이 발생한다. 이 때 시스템은 open() 이라는 시스템 콜을 호출하고 이는 LSM hook을 통해 파일 접근 이벤트가 RBAC 모듈로 전달된다. RBAC 모듈은 LSM hook을 통해 전달된 이벤트의 정보 즉, open() 작업을 요청한 프로세스의 역할을 통해 보안 DB에 설정되어 있는 RBAC 정책 즉, open() 작업의 대상이 되는 역할에 부여된 권한을 비교하여 현재 open() 작업을 허가할지 말지를 결정한다. 만약 접근이 거부될 경우 RBAC 모듈은 해당 프로세스의 파일 접근을 거부시키며, 접근이 허용될 경우 open() 작업 수행을 계속 하도록 한다.

3. X-Hyper270A 타겟시스템으로의 이식

X-Hyper270A 임베디드 시스템은 Intel PXA270 프로세서가 탑재되어 저전력/고성능(520MHz)의 성능을 가지고 있어 모바일 관련 제품군에 이용될 수 있는 시스템이다. 리눅스 2.6.11을 지원하여 LSM 보안 프레임워크를 사용할 수 있는 장점도 있다.

그림 3은 RBAC 모듈 이식을 위한 시스템 구성을 보여준다.

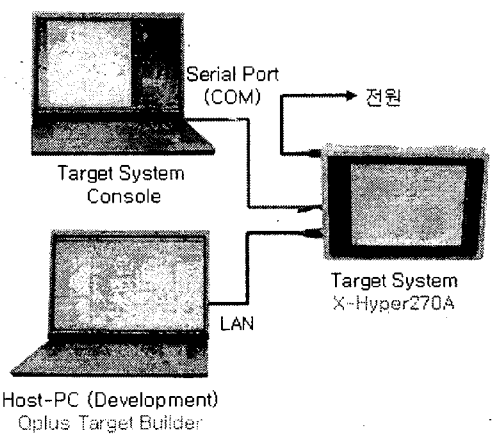

그림 3. RBAC 모듈의 타겟 시스템으로의 이식 환경

커널 설정/컴파일/이미지 제작 등의 개발은 호스트 PC 상의 Qplus Target Builder를 통해 이루어진다. 여기서 제작된 OS, 파일시스템 등은 네트워크를 통해 타겟으로 이식되고 타겟은 이식된 OS 및 파일시스템 이미지로 구동되게 된다. LSM은 리눅스 커널 옵션에서 "Security" 옵션이 정의되어야 사용 가능하며 이 옵션은 "Security Option -> Enable different security models" 항목을 선택하면 정의된다. RBAC 모듈은 타겟(intel PXA270)용 컴파일러를 이용하여 컴파일하여 타겟 파일시스템 이미지 내에 포함하여 파일시스템 이미지를 제작한다. 타겟 시스템에서의 구동 상황은 별도의 콘솔 시스템을 시리얼 연결을 통해 확인할 수 있다.

4. 결론 및 향후 과제

임베디드 시스템은 특정 목적을 위해 구동된 특별한 시스템이다. 이런 목적 때문에 인터넷 연결형 보다는 독립형태로 제공되어 시스템 자체의 기능 수행에 집중했었다. 하지만 인터넷 연결형 임베디드 시스템이 점차 증가하고 또 앞으로는 인터넷 연결이 필수 요소가 되면서 보안 기능이 없는 임베디드 시스템은 안전하지 않게 되었다. 특히 개인형 단말기에는 개인 신상 정보를 비롯한 금융 정보 등 민감한 정보들이 많이 저장되고 있어 언제든 악의적인 침입 및 우회적인 침입으로부터 공격당할 위험이 존재한다. 따라서 이들 침입으로부터 사용자 정보는 물론 시스템 자원을 안전하게 보호할 필요가 있다. 본 논문은 임베디드 시스템에 적용 가능한 간결한 개념과 용이한 관리 구조 등을 제공하는 역할기반 접근제어를 소개하고 타겟 시스템에 적용하는 과정을 제시하였다. 아직은 임베디드 시스템에서 접근제어 모델을 통한 자원 보호에 대한 구체적 사용 예가 없지만 본 논문이 제시한 RBAC 모델을 통해 다양한 환경에서의 임베디드 시스템을 보호할 방법이 제시될 수 있다. 향후에는 본 논문의 RBAC 모델을 통한 임베디드 시스템 보호 방법 모델을 연구하여 인터넷을 기반으로 한 임베디드 시스템 사용에 보안성 강화를 구체화해야 한다.

참 고 문 헌

[1] 이형석, 정영준, "임베디드 운영체제 커널 기술 동향", 전자통신동향분석 제21권 제1호, pp. 33-46, 2006. 2.

[2] Qplus distribution sites, http://www.qplus.or.kr/

[3] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, and Charles E. Youman. "Role-based Access Control models",IEEE Computer, 29(2):38-47, February 1996.

[4] D. Ferraiolo, J. Cugini, and D. R. Kuhn. "Role-based Access Control: Features and motivations", In Annual Computer Security Applications Conference. IEEE Computer Society Press, 1995.

[5] Chris Wright, Crispin Cowan, Stephen Smalley, James Morris, Greg Kroah-Hartman, "Linux Security Modules: General Security Support for the Linux Kernel", Proceedings of the 11th USENIX Security Symposium, pp. 17-31, August 2002.