제 3 자 개발 애플리케이션 접근제어에 대한 연구

박선호*, 박민우*, 정태명**
*성균관대학교 전자전기컴퓨터공학과
**성균관대학교 정보통신공학부
e-mail :{shpark, mwpark}@imtl.skku.ac.kr*, tmchung@ece.skku.ac.kr**

A Study on Access Control for Applications Developed by 3rd party

Seon-Ho Park*, Min-Woo Park and Tai-Myoung Chung**
*Dept. of Electrical and Computer Engineering, Sungkyunkwan University
**School of Information & Communication Engineering , Sungkyunkwan University

요 약

본 논문은 향후 임베디드 단말 기기에 탑재되어 실행되는 응용 애플리케이션들이 제 3 자에 의해 개발되어 앱스토어를 통해 배포될 경우, 신뢰성 및 보안 문제 해결을 위해 제 3 자 개발자에 의해 개발된 애드온 애플리케이션들의 접근통제 메커니즘에 대해 연구하였다. 본 논문에서는 태스크-플로우 기반 메쏘드 접근제어 모델을 제시하고, X.509 기반의 권한 관리 구조를 통해 임베디드 단말에서 애드온 프로세스의 접근 통제를 위한 구조를 디자인하였다.

1. 서론

최근 임베디드 시스템 기술의 발달로 핸드폰, PDA 등의 휴대 단말부터 가정용 전자기기까지 다양한 분야에서 실시간 임베디드 기술을 적용하여 활용하고 있다. 이미 모바일 분야에서는 노키아의 심비안 운영체제, 국내의 WIPI 플랫폼, 자바의 J2ME 등을 통해 모바일 단말을 위한 다양한 응용프로그램을 개발하여 이용할 수 있으며, 최근에는 가정용 디지털 TV 분야에서도 플래시 기반의 게임과 같은 텔레비전용 엔터테인먼트 응용 프로그램들이 개발되어 이용되고 있다.

이와 같은 임베디드 실시간 시스템을 위한 플랫폼들의 개발로 인해 다양한 응용프로그램들의 개발이 가능해지면서, 최근에는 플랫폼의 개방을 통해 보다 많은 제삼자 개발자들을 통해 더욱 다양한 응용프로그램을 개발하여 공유할 수 있도록 하고 있는데 대표적인 사례가 앱스토어이다. 모바일 분야에서는 이미 애플, 구글, 마이크로소프트, 삼성전자, SKT, LG 전자 등이 앱스토어 시장에 진출해 있다. 또한 최근 삼성전자는 누리삼 사이트(www.nurisam.com)를 통해 디지털 텔레비전을 위한 애플리케이션들을 유/무료로 배포하고 있으며, 향후 모바일에서의 앱스토어와 같은 형태로 발전될 전망이다[1].

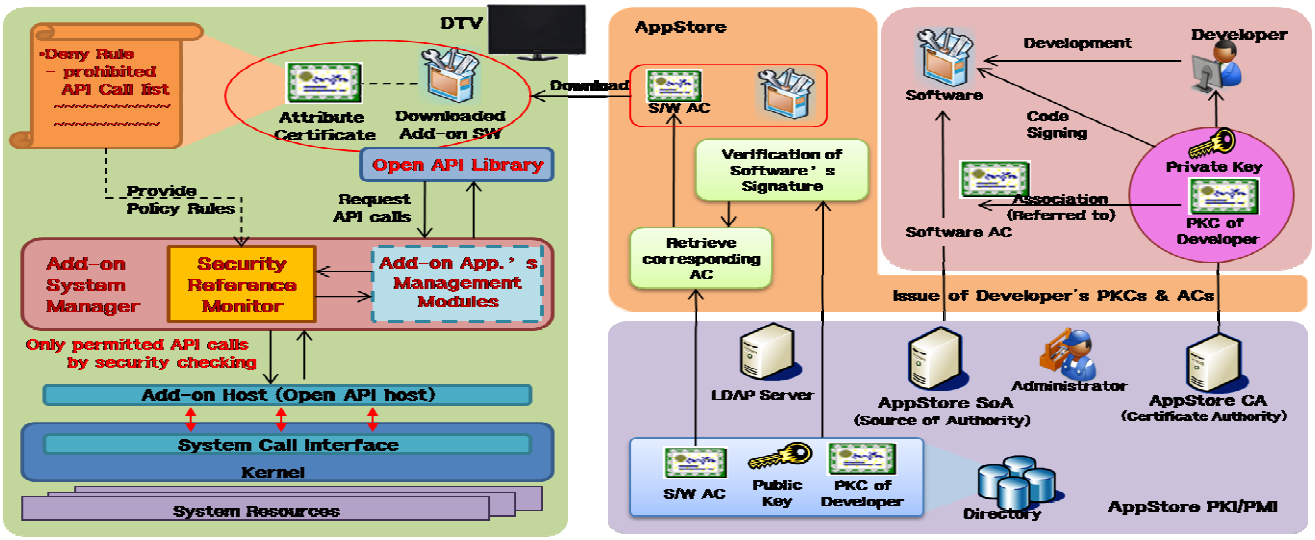
향후 제 3 자 개발자의 개발 소프트웨어를 오픈 마켓인 앱스토어에 등록하여 사용자들이 자유롭게 해당 콘텐츠를 구매하여 이용하게 될 경우에 문제되는 것이 바로 제 3 자 콘텐츠에 대한 신뢰성 문제이다. 무수히 많은 제 3 자 개발자들이 개발한 콘텐츠를 다운로드 받는 과정에서 이용자, 개발자, 배포자 간의 신뢰 관계를 유지하는 것은 매우 복잡하고 어려운 일이다. 제 3 자가 개발한 프로그램의 오동작으로 인한 피해는 앱스토어의 가치사슬 특성상 배포자 측인 앱스토어 운영사가 받게 되어 있다.

본 논문에서는 앱스토어를 통해 받게 될 제 3 자 개발 애플리케이션을 안전하게 실행하기 위한 방법에 대한 연구 결과를 소개하고, 태스크 기반 메쏘드 제어 모델을 제안한다. 본 논문은 디지털 텔레비전의 애드온 애플리케이션들의 안전한 실행에 주로 초점을 둔다. 본 논문은 2 장에서 DTV 애드온 프로세스 접근제어를 위한 고려사항 도출과 접근제어 메커니즘에 대한 상세 설명을 하고, 3 장에서 결론을 맺고 향후 연구 방향에 대해 논의한다.

2. DTV 애드온 프로세스 접근제어

본 논문은 리눅스 기반의 디지털 텔레비전 환경에서 제 3 자가 개발한 애드온 프로세스의 접근제어에 대한 연구에 초점을 맞춘다. 본 연구에서는 DTV 프로세스 접근제어를 위해 적합한 새로운 모델의 도출을 위해 DTV 애드온 구조의 분석을 바탕으로 몇 가지의 접근제어 고려사항 및 요구사항을 도출하였다.

우선 접근제어 구성 요소에서 주체는 애드온 소프트웨어 프로세스로 한정한다. 그리고 객체는 재생 미디어, 디바이스 장치, 파일&네트워크 등으로 한정하고, 오퍼레이션은 객체들에 해단 오퍼레이션 수행을 위해 제 3 자에게 공개되는 Open API 들이다. 내부 시스템 콜은 보안 상 제 3 자 애드온 애플리케이션 개발자들에게 공개되지 않는다고 가정한다. 마지막으로 접근제어 포인트는 애드온 애플리케이션 API 레벨로 한정한다. 이와 같은 고려사항들은 실제 디지털 텔레비전을 위한 애드온 애플리케이션 구조의 분석 결과이다.



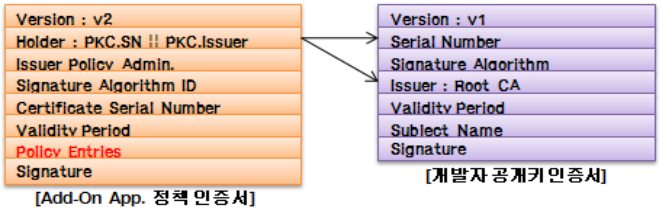
(그림 1) 제 3 자 애드온 프로세스 접근제어 메커니즘 전체 구조 개념도

제 3 자 개발 애드온 프로세스 접근제어를 위해 다음으로 고려해야 할 사항은 접근제어 정책의 관리 및 시행에 관한 것이다. 접근제어 정책은 반드시 DTV 애드온 API 들을 기본단위로 이루어져야 하며, 이들의 호출 관계 및 순서 등에 대한 제어가 이루어져야 한다. 따라서 태스크-플로우(task-flow) 기반의 메소드 제어가 필요하다. 또한 관리 효율성을 고려하여 애플리케이션 개발자가 제출하는 기능명세서를 기반으로 앱스토어 측의 보안 정책 관리자에 의해서 접근제어를 위한 보안 정책이 수동적, 또는 자동화 도구에 의해서 생성되어야 한다. 이것은 일종의 계약서(contract) 기반 관리 개념과 유사하다[2]. 제 3 자 개발자가 애플리케이션의 기능 명세를 보안 관점에서 작성하며, 앱스토어 측의 보안 정책 관리자는 기능 명세서인 애플리케이션 계약서를 기반으로 보안 정책을 세우고, 이 보안 정책을 기반으로 디지털 텔레비전에서 애드온 애플리케이션의 실행시 보안 참조 모니터를 통해 Contract Policy Matching 메커니즘을 시행함으로써 애드온 애플리케이션이 보안적으로 안전하게 실행되는 것을 보장할 수 있게 된다.

태스크 플로우 기반 메쏘드 접근제어 모델은 메쏘드 호출(Open API 호출)을 접근 통제의 주요 대상으로 취급하며, API 들의 허용 리스트, 거부 리스트, API 호출 시퀀스 등을 이용하여 정책 설정 및 시행을 수행한다. 본 연구에서는 태스크-플로우 기반 메쏘드 제어를 위한 Security Automaton 을 정의하고, 이 Security Automaton 을 기반으로 애드온 프로세스를 위한 참조 모니터에서 contract-policy matching 을 수행하게 된다.

애드온 애플리케이션의 계약(보안 정책) 명세의 관리는 X.509 권한 관리 구조를 기반으로 한다. X.509 권한 관리 구조는 속성 인증서를 통해 권한 관리를 위한 주체의 속성 정보들을 관리하고, 이를 통해 권한 관리를 수행하는 인프라구조이다. 그림 1 은 제 3 자 개발 애드온 프로세스를 위한 접근제어 메커니즘의 전체 구조를 개념적으로 도식한 도이다.

제 3 자는 앱스토어에 개발 애플리케이션을 등록하기에 앞서 먼저 앱스토어 운영사가 루트 CA 가 되는 사설 공개키 인증서를 발급받는다. 그리고 앱스토어의 관리자는 개발자가 제출한 애플리케이션 보안 명세서를 기반으로 애플리케이션의 보안 관련 명세를 포함하는 계약서(보안 정책 명세)를 생성하고, 이를 포함하는 정책인증서(X.509 속성 인증서 이용)를 생성한다. 정책인증서는 개발자의 공개키 인증서와 바인딩된다. 그림 2 는 공개키 인증서와 정책인증서 사이의 바인딩 관계를 설명해준다. 정책인증서는 애플리케이션과 함께 DTV 에 다운로드 되며, 정책인증서에 포함된 보안 정책을 기반으로 애드온 애플리케이션의 보안 참조 모니터에서 수행되는 Contract Policy Matching 메커니즘에 의해서 해당 애플리케이션이 계약서에 명시된 보안 행위를 준수하면서 실행되는지 여부를 검사하게 된다.



(그림 2) 공개키 인증서와 정책인증서 관계

3. 결론 및 향후 연구 계획

본 논문은 DTV 환경에서 제 3 자에 의해 개발된 애플리케이션의 안전한 실행을 위한 참조모니터 시행을 위한 접근제어 메커니즘을 제안하고 관리 구조를 소개하였다. 본 연구는 향후 정책 표현 언어 및 Security Automaton 을 위한 정책 언어 개발을 수행할 것이다.

참고문헌

[1] 임언석, 김자원, 한영숙, "통신사업자의 애플리케이션 스토어 활용전략", KT 경제경영연구소, 2009.06.

[2] N. Dragoni, F. Massacci, and K. Naliuka, "Security-By-Contract (SxC) for Mobile Systems", Telektronikk, 2009.