제33회 한국정보처리학회 춘계학술발표대회 논문집 제17권 제1호 (2010. 4)

스마트 디지털 TV에서의 제3자 개발 애플리케이션을 위한 보안 요구사항 분석

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

A Study on Access Control Mechanism for 3rd Party Applications Process on Smart Digital TV

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

요 약

최근 스마트폰의 대중적 확산으로 인해 소프트웨어 및 콘텐츠에 대한 관심이 빠르게 증대되고 있으며, 제3자 개발자들이 애플리케이션 및 콘텐츠들을 개발하여 시장에 진입할 수 있는 앱스토어와 같은 제3자 애플리케이션 마켓도 함께 증가하고 있다. 이에 따라 제3자 개발 애플리케이션이 스마트기기에 설치되어 동작할 때 발생 가능한 보안 위협 및 이에 대한 대응 기술 연구가 주목받고 있다. 본 연구는 임베디드 리눅스 기반의 디지털 TV 환경에서 제3자 애플리케이션이 구동될 때 발생 가능한 보안 위협에 대응하기 위해서 필요한 보안 요구사항을 분석하고, 제3자 개발 애플리케이션의 전체 생명 주기를 고려한 보안 정책 관리 방법을 제안한다.

1. 서론

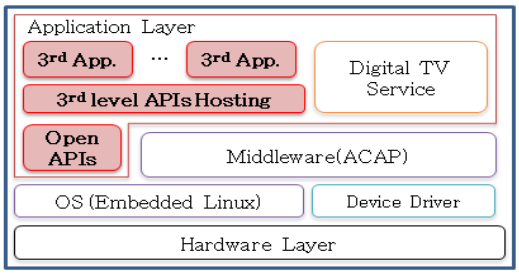
최근 스마트폰의 대중적 확산으로 인해 스마트 단말을 위한 다양한 애플리케이션들에 대한 관심이 늘어가고 있다. 이로 인해 스마트폰은 기존 하드웨어 산업 위주의 국내 IT 시장을 소프트웨어 및 콘텐츠 산업의 확대로 방향을 전환할 수 있는 시발점 역할을 할 것으로 기대되고 있다. 그리고 이러한 소프트웨어 및 콘텐츠 산업 발전에 대한 기대는 스마트폰뿐만 아니라 다양한 휴대 기기, 디지털 TV, AV 등의 여러 가전 영역에 적용될 수 있을 것으로 예상하고 있다. 이는 최근 2010 CES에서 삼성전자가 공개한 “삼성앱스” 계획을 통해서도 알 수 있다. 특히 TV와 인터넷의 결합, 디지털 TV를 통한 콘텐츠 소비, 다른 기기들과의 연동 등과 같은 TV의 진화가 예상되고 있어, 향후 디지털 TV는 TV의 단순 기능을 넘어서서 스마트 TV로서 가전제품들의 허브이자 다양한 콘텐츠 소비를 이끌어낼 기기가 될 것으로 전망된다.

삼성전자, LG전자 등과 같은 주요 디지털 TV 업체들을 통해 최근 출시되고 있는 TV들은 대부분 스마트 TV로서의 역할을 수행할 수 있도록 충분한 기능들을 탑재하고 있다. 예를 들어, LG전자의 디지털 TV들은 임베디드 리눅스와 같은 운영체제를 탑재하고, 인터넷 및 다양한 응용 소프트웨어를 지원할 수 있는 ACAP 미들웨어 등을 기본 탑재하고 있으며, TV에 인터넷 라인을 바로 연결하여 인터넷을 통해 콘텐츠 구매가 가능하도록 하는 소프트웨어 등도 탑재하고 있다. 이러한 디지털 TV의 기능을 최대한 사용하여 콘텐츠 소비를 극대화하기 위한 가장 효과적인 방법은 디지털 TV 애플리케이션 및 콘텐츠를 위한 오픈마켓을 형성하는 것이다. 즉, 스마트폰의 앱스토어와 같은 형태의 애플리케이션 스토어를 구축하는 것이다. 현재 삼성전자, LG전자 등은 디지털 TV를 위한 다양한 콘텐츠, 애플리케이션, 펌웨어 등을 위한 앱스토어를 구축 또는 계획 중에 있다. 앱스토어를 통해 다양한 제3자 개발자들이 개발한 애플리케이션을 디지털 TV에 설치하여 실행할 때 발생할 수 있는 가장 큰 문제는 보안 문제이다. 제3자 개발자는 보안 관점에서 신뢰할 수 없는 개체이며, 이들이 개발한 애플리케이션은 악의적 또는 개발자 실수에 의해 보안 문제를 일으킬 수 있다.

본 논문은 디지털 TV 환경에서 제3자 개발 애플리케이션이 구동될 때 애플리케이션 프로세스가 안전하게 실행될 수 있도록 하기 위해서 필요한 접근제어 요구사항을 분석하고, 제3자 개발 애플리케이션 프로세스 보안 정책 관리 방법을 제안한다. 본 논문은 2장에서 DTV 애플리케이션 프로세스 접근제어를 위한 요구사항을 분석하고, 요구사항 분석 결과를 토대로 제3자 개발 애플리케이션의 보안 관리를 위한 프로세스를 3장에서 소개한다. 그리고 마지막으로 4장에서 본 논문의 결론과 향후 연구 계획을 소개한다.

2. DTV 애플리케이션 프로세스 접근제어 요구사항

DTV 애플리케이션 프로세스 접근제어를 위한 요구사항 분석에 앞서 우선 DTV 시스템의 내부 구조에 대해 소프트웨어 관점의 아키텍처 이해해야 한다. (그림 1)은 DTV 시스템의 논리적 구조를 설명하는 그림이다.



(그림 1) DTV 시스템의 논리적 구조

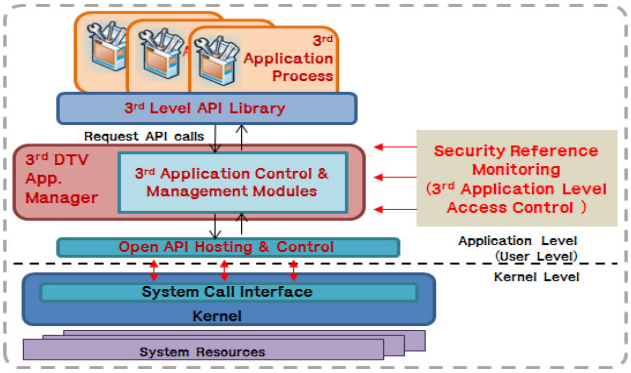
(그림 1)에서 “Open APIs”, “3rd level APIs Hosting”이라고 설명된 박스는 DTV 소프트웨어의 제3자에 의한 개발을 위해서 필요한 오픈 API들의 관리를 위해서 필요한 모듈을 설명한다. 이는 SDK(Software Development Kit)에 의해서 제공되는 외부 API들로 개발된 제3자 애플리케이션이 DTV에서 구동될 수 있도록 API들을 호스팅해주는 기능을 제공한다. 이러한 API 호스팅 구조에서는 제3자 개발자가 직접 시스템 콜 라이브러리를 사용하거나 시스템에 그 이상 가깝게 접근할 수 어떠한 행위도 할 수 없어야 한다. 이는 개발자에겐 시스템 구조에 대한 투명성을 제공하는 동시에 DTV 시스템의 보안성을 유지할 수 있는 장점을 가진다.

하지만 반대로 제3자 개발 애플리케이션이 제3자 개발자들을 위해 제공되는 API만이 아닌 시스템 콜 라이브러리에 직접 접근하려는 시도를 하려고 하거나, 또는 비록 제3자 개발자 API를 사용하지만 해당 애플리케이션의 기능을 넘어서는 수준으로 여러 API를 사용하려고 하는 경우 보안적 관점에서 권한 남용 및 침해가 발생하게 되어 문제가 될 수 있다. 따라서 제3자 개발 애플리케이션에게 적절한 권한을 설정 또는 부여하고, 이 권한에 따라 동작하는지 적절하게 제어를 해야 한다. 일반적으로 제3자 개발 애플리케이션은 바이너리 실행파일 형태로 배포가 되므로 소스코드 레벨에서의 보안 검증 및 권한 제어는 어렵다. 따라서 본 연구에서는 바이너리 실행파일 형태로 배포가 된 이후 상황에서 애플리케이션이 동작할 때 적절하게 접근제어를 수행하기 위해 필요한 보안 고려사항들을 분석하고자 한다.

<표 1> DTV 접근제어 구성 요소

구성요소	해당 항목
주체	애플리케이션 프로세스
객체	재생 미디어, 디바이스 장치, 파일과 네트워크 I/O 등의 장치 자원, 애드온 S/W 관리자가 유지하는 데이터 및 자료구조들,
동작	Open API들의 호출 (프로세스 동작을 위한 객체 접근 및 오퍼레이션 수행)

<표 1>은 DTV의 제3자 개발 애플리케이션 API 호스팅 환경에서 고려해야 하는 접근제어 구성 요소들을 주체(Subject), 객체(Object), 동작(Action)으로 분류하여 정리한 것이다.



(그림 2) 제3자 개발 애플리케이션 프로세스 접근제어 적용 레벨

(그림 2)는 DTV 제3자 개발 애플리케이션 프로세스 레벨에서 접근제어를 구현하기 위한 보안 참조 모니터의 적용 포인트에 대한 개념도이다. 제3자 애플리케이션 프로세스는 Open API 라이브러리 호출을 기반으로 동작하며, Open API 라이브러리들의 호출은 제3자 DTV App. System Manager 모듈 내부의 제3자 Application Control & Management 모듈을 통해 Open API Hosting & Control 모듈에 전달되며, 여기에서 DTV 애플리케이션 핸들링, 미디어 재생, 호스트 디바이스의 제어, DTV 장치 내 파일에 대한 입출력, 네트워크 장치 입출력 등의 기능들을 수행하게 된다. 이러한 제3자 애플리케이션 프로세스 동작 흐름을 고려할 때, 제3자 애플리케이션 프로세스 접근제어를 수행하기 가장 좋은 위치는 프로세스가 호출하는 Open API들을 제어·관리 하는 3rd DTV App. Manager 모듈이 된다. 이 위치에서 프로세스들이 호출하는 API들을 각 프로세스에 해당하는 정책에 따라서 제어하면서, 정책에 위배되는 API 호출은 Open API Hosting & Control 모듈로 해당 API 호출을 하지 않고 잘못된 API 호출에 대한 결과값을 리턴하고, 프로세스의 이상 종료나 다른 프로세스 및 자원에 영향을 주지 않도록 처리해야 한다. 경우에 따라서 정책에 위배되는 API 호출을 한 프로세스를 강제 종료해야 할 경우가 있을 수 있다. 이러한 경우에 프로세스의 강제 종료에 따른 연쇄적 반응으로 인해 동시에 동작하고 있던 다른 프로세스에 영향을 주거나 향후 3rd DTV App. Manager의 동작에 영향을 주면 안 되기 때문에 접근제어 시행 위치는 3rd DTV App. Manager 내부 모듈들과 함께 위치하여 프로세스 관리 모듈과 프로세스 처리 관련 데이터를 주고받을 수 있도록 구현되어야 한다.

3. 제3자 애플리케이션 보안 정책 관리 프로세스

제3자에 의해 개발된 애플리케이션은 호스팅 플랫폼 관점에서 신뢰할 수 없는 프로그램(Untrust Program, 이후 UTP로 기재함)이다. UTP의 의미는 간단하게 프로그램이 원래 수행해야 하는 기능을 안전하게 수행하는지 보장할 수 없다는 의미이다. 반대의 관점으로 해석하면 프로그램이 원래 제공해야 하는 기능 외의 다른 동작을 수행할 수도 있는 가능성이 있다는 의미이다. 원래 프로그램이 수행

해야 하는 기능 외의 동작을 수행하면서 시스템에 아무 영향을 주지 않을 경우는 이러한 경우를 무시할 수 있지만, 시스템 자원이나 동시에 구동되고 있던 다른 프로세스에 영향을 주게 될 경우 이러한 UTP로 인해 시스템의 안정성과 보안성이 크게 침해당할 수 있게 된다. 따라서 UTP를 설치하여 이용하는 플랫폼 환경에서는 시스템의 안정성과 보안성을 지키면서 이들을 이용하기 위한 대응책을 마련해야 한다.

제3자 개발 프로그램의 비 신뢰성으로 인한 문제의 해결은 단순히 하나의 솔루션으로 이루어질 수 없으며, 개발부터 배포 및 설치에 이르기까지 각 단계별로 적합한 솔루션들을 유기적으로 연계하여 적용해야 한다. 즉, 단순하게 특정 시점에서 적합한 특정 솔루션을 적용한다고 해결되는 문제가 아니며, 개발 단계, 배포 단계, 실행 단계 각각에 해당하는 적합한 대응책이 함께 어우러져서 적용되어야만 궁극적으로 제3자 개발 프로그램의 비 신뢰성으로 인한 문제들을 해결할 수 있다. 따라서 애플리케이션 라이프 사이클 특징을 분석하고, 이를 기반으로 각 단계에서 적합한 보안 메커니즘을 설계 및 구축해야 한다. 그리고 각 단계별로 보안 메커니즘 시행의 기준 역할을 하기 위한 보안 정책이 올바르게 수립되고 적용되어야 한다.

제3자 개발 애플리케이션이 개발되어 단말 플랫폼에서 실행되기까지 과정을 크게 개발(Development) 단계, 배포(Deployment) 단계, 실행(Execution) 단계로 구분하고, 개발과 배포 단계는 각각 디자인/개발, 업로드/다운로드로 세분하여 그 특징을 분석하면 다음과 같다.

3.1. 디자인 단계

디자인 단계에서 제3자 개발자는 개발 목표 및 기능의 명세서 등을 포함하는 개발 제안서를 작성하여 앱스토어 관리자에게 먼저 제출한다. 앱스토어 관리자는 개발 제안서에서 개발하과 하는 개발품의 사업성 및 현실성, 제안 내용의 완성도 등 다양한 측면의 검토를 통해 개발 진행 여부를 결정한다. 제3자 개발자는 최종 도출될 개발품의 상세한 구조와 세부 모듈 설계서, 상세 기능 명세서 등이 포함된 개발 계획서를 작성하여 앱스토어 관리자에게 제출하고, 관리자는 제출된 개발 계획서의 개발 범위에 적합한 API들을 포함하는 SDK를 제3자 개발자에게 배포한다. 다음은 디자인 단계의 보안 고려사항이다.

- 제3자 개발자의 개발 제안서 및 계획서 내용에 근거하여 개발 요구사항을 도출해야 함
- 개발 요구사항에는 실행 플랫폼에서 안전한 구동이 가능하도록 최소권한 원칙에 근거하여 Open API Set을 정의하고, 보안 요구사항과 필수사항 등을 포함해야 함
- 제3자 개발자에게 개발을 위한 SDK(Open API Set), 개발 요구사항을 제공함
- 전체적인 개발 요구사항에 대한 준수 여부를 점검하기 위한 체크리스트를 작성하여 제3자 개발자에게 제공해야 함
- 개발될 애플리케이션을 위한 보안 정책을 설계 (기능 명세서를 기반으로 정책 초안 작성)

3.2. 개발 단계

제3자 개발자는 앱스토어로부터 제공받은 SDK를 이용하여 개발 계획서의 내용을 기반으로 애플리케이션을 개발한다. 개발 시 개발 명세서를 작성해야 하며 개발 중 개발 계획서의 내용에서 변경되어야 하는 사항이 생길 경우 앱스토어에 보고 및 개발 명세서에 해당 변경 사항을 반드시 포함해야 한다. 또한 제공된 SDK에 포함되지 않은 DTV Open API가 있거나 수정·확장이 필요할 경우 앱스토어에 요청해서 개발에 적합한 API를 제공받아야 한다. 다음은 개발 단계의 보안 고려사항이다.

- 제3자 개발자는 개발 과정에서 발생할 수 있는 개발 범위와 내용의 변경 사항을 앱스토어 측에 즉각 알려야 함
- 제3자 개발자는 개발 과정에서 앱스토어 측이 제공한 개발 요구사항에 대한 준수 여부를 체크리스트에 표기해야 함
- 제3자 개발자는 개발 과정에서 코딩오류 점검, 메모리 누수 점검 등과 같이 보안·성능을 고려하여 개발해야 함

3.3. 업로드 단계

제3자 개발자는 충분한 테스트와 성능/보안 검증을 완료한 개발품을 애플리케이션 스토어에 업로드 한다. 다음은 업로드 단계의 보안 고려사항이다.

- 업로드 과정에서 앱스토어 측은 애플리케이션 검증을 수행해야 함. 애플리케이션의 검증은 간단하게 개발 요구사항 체크리스트의 점검부터 바이너리 레벨 시뮬레이션 테스트, 정적 바이너리 검증(역 어셈블 분석) 등 상황과 조건에 맞는 검증 방법을 선택해서 수행해야 함
- 애플리케이션 검증 시 정적 바이너리 검증 시에는 검증의 효율성을 위해 Targeted Reassembly 정적 분석과 같이 특정 기능 영역에 초점을 둔 역어셈블 분석이 가능한 상용 도구를 이용하는 것이 바람직함
- 프로그램 인증 및 무결성 체크를 위해서 개발 프로그램을 서명하고, 프로그램과 서명을 함께 애플리케이션 스토어에 업로드 해야 함

3.4. 다운로드 단계

DTV 사용자는 DTV 브라우저 또는 PC를 통해 응용 프로그램이나 콘텐츠를 다운로드 받는다. DTV 브라우저를 통해 다운로드 받는 경우는 DTV가 네트워크를 통해 인터넷에 연결되어 있는 경우 자체 내장된 브라우저 프로그램을 이용하여 애플리케이션 스토어에 접속하여 원하는 애플리케이션을 선택하여 다운로드 받을 수 있다. PC를 통해 다운로드 받는 경우는 이동형 저장 장치(예: USB 메모리)를 이용하여 PC에서 다운로드 받은 애플리케이션을 DTV에 옮겨 저장하여 이용할 수 있다. 이때 이동형 저장 장치에는 DTV의 고유 식별 ID와 DTV 인증을 위한 인증 토큰(예: 공개키인증서)이 저장되어 있어야 한다. 이는 DTV 단말 자체의 인증을 위해서 반드시 필요하며, 이를 통해

유/무료 콘텐츠 및 기타 인증과 접근제어가 필요한 다운로드 요청을 제어할 수 있게 된다. 다음은 다운로드 단계의 보안 고려사항이다.

- 애플리케이션의 다운로드 시 반드시 프로그램의 서명 검증이 이루어져야 하며, 서명 검증을 위해 필요한 검증 모듈은 DTV 단말 자체에 내장된 브라우저에서 이용이 가능한 형태이어야 함
- 다운로드 애플리케이션의 안전한 실행을 위해서 해당 애플리케이션의 보안 정책을 함께 다운로드 받아서 DTV 내에 저장해야 함
- 정책 내용의 무결성이 반드시 보장되어야 함
- 정책은 해당 애플리케이션의 안전한 실행을 위해 작성한 것임을 증명할 수 있어야 함 (즉, 인증과 부인봉쇄 기능이 제공되어야 함)

3.5. 실행 단계

애드온 애플리케이션 구동 환경을 통해 다운로드/설치된 애플리케이션이 실행된다. DTV 리모컨(Remote Controller)을 통해서 애플리케이션이 제어되며, 애플리케이션의 종류에 따라서 단순히 미디어 자원만을 이용하거나 네트워크에 접속하여 검색이나 게임 등을 수행할 수도 있다. 다음은 실행 단계의 보안 고려사항이다.

- 앞서 수행된 개발 단계에서의 보안 메커니즘 적용이 DTV에서 애플리케이션이 안전하게 실행될 것이라는 것을 완벽하게 보장해주지는 않음
- 보안 검증, 시뮬레이션 테스트 등을 충분히 수행하였더라도 실제 구동 환경에서 예상하지 못했던 이벤트의 발생으로 인해 보안 정책 위배 및 DTV의 다른 프로세스들의 실행 방해 등의 보안 위협이 발생할 수 있음
- 애플리케이션 다운로드할 때 함께 저장한 보안 정책에 근거하여 애플리케이션의 실행 흐름을 모니터링하고, 보안 정책 위배 여부를 검사하고 제어해야 함
- DTV 애드온 애플리케이션의 모든 실행 흐름을 모니터링 하기 위한 보안 참조 모니터를 반드시 고려해야 하며, 보안 참조 모니터는 반드시 우회 불가능하고, DTV 운영체제가 구동되는 동안 무조건 구동되어야 하며, 최대한 경량으로 구동되어야 함

4. 결론 및 향후연구계획

본 논문은 향후 스마트 가전 관리의 핵심 허브 역할 및 소프트웨어 및 콘텐츠 산업 발전의 주요 기수 역할을 수행할 것으로 기대되고 있는 스마트 디지털 TV를 위한 제3자 개발 애플리케이션의 보안 정책 관리를 위해 필요한 보안 요구사항을 분석하고 보안 정책 관리 프로세스 및 방법론을 제시하였다. 본 연구는 DTV 내에서 실제 제3자 개발 애플리케이션 프로세스의 보안 모니터링을 위한 보안 참조 모니터의 개발 및 보안 정책 관리를 위한 PKI/PMI 결합 구조 등에 대한 연구를 수행하고, DTV 내에서 보안정책의 표현 및 이해를 위한 정책 기술 언어 연구에 대해 수행할 계획이다.

참고문헌

[1] CES 2010 - Latest Consumer Electronics Show nes - CNET. http://ces.cnet.com/

[2] Pablo Desar, A Graphics Software Architecture for High-End Interactive TV Terminals (Doctoral Dissertation Defense Presentation), Helsinki University of Technology, Finland, December 2005 (in print).

[3] SOC R&D Center, Software Architecture for Embedded System, 2004 추계 학술 발표회 Workshop, Samsung Electronics Co. ltd. 2004.10

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

(그림 3) DTV 제3자 애플리케이션 권한 관리 메커니즘 시퀀스