스마트 TV 와 애플리케이션 스토어 간의 상호 인증과 암호 통신 적용 방안 연구

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

A Study on Methodology for Applying Mutual Authentication and Secure Communication between Smart TV and Application Store

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

요 약

디지털 TV 기술과 소프트웨어 기술의 발전은 스마트 TV 라는 TV 의 새로운 패러다임을 도래하게 하였다. 스마트 TV 는 네트워크를 통해 애플리케이션 스토어에 접속하여 다양한 콘텐츠들을 다운로드 하여 설치/이용하게 될 것이다. 본 연구는 이러한 과정에서 발생할 수 있는 보안 위협들 중에서 콘텐츠의 불법 다운로드 및 기기 인증 우회 등으로 인해 발생할 수 있는 피해를 예방하기 위한 방법으로서 공개키 기반 상호 인증 및 키 분배 방식과 암호 통신 방법을 제안한다.

1. 서론

디지털 TV 기술과 소프트웨어 기술의 발전은 스마트 TV 라는 TV 의 새로운 패러다임을 도래하게 하였다. 스마트 TV 는 네트워크를 통해 애플리케이션 스토어에 접속하여 다양한 콘텐츠들을 다운로드 하여 설치/이용하게 될 것이다. 현재의 애플리케이션 스토어(이하 앱스토어 또는 AppStore)은 스마트폰용 애플리케이션에 국한되어 있지만 점차 디지털 TV 용 앱스토어가 등장하고 있으며, 구글 안드로이드 기반의 TV 와 같은 스마트 TV 에 대한 이슈가 대두되면서 향후에는 스마트 TV 앱스토어가 대중화될 것으로 보인다.

앱스토어를 통해 TV 용 콘텐츠들을 다운로드 받아서 이용하게 될 경우에는 다양한 보안 위협에 노출 될 수 있다. 앱스토어의 이용구조가 네트워크를 기반으로 하기 때문에 기존의 폐쇄적 특징을 갖는 TV 가 향후에는 보다 다양한 위협에 노출될 수 있음은 사실 자명하다. 비록 피해 정도가 컴퓨터 네트워크나 스마트폰에서의 피해보다 약할 수 있더라도 TV 서비스는 이미 우리 생활에 가장 중요한 부분을 차지하고 있기 때문에 보안 위협에 충분히 대비해야 할 필요가 있다. 본 논문은 스마트 TV(이하 STV)와 앱스토어가 인터넷을 통해 연결된 환경에서 안전한 통신을 위해 필수적으로 필요한 기기 인증 및 암호 통신을 위해 필요한 보안 요구사항을 분석하고 공개키 인증서 기반의 기기 인증과 키 분배 메커니즘과 암호 통신 방법을 제안한다.

본 논문은 2 장에서 공개키 인증서 분배 메커니즘, 3 장에서 세션키 분배 및 암호 통신 메커니즘을 설명한 뒤 4 장에서 결론과 향후 연구에 대해 설명한다.

2. 스마트 TV 공개키 인증서 분배 절차

공개 키 메커니즘은 STV 와 서버 상호 인증뿐만 아니라 세션 키의 안전한 분배를 위해서도 사용된다. 공개 키 암호화 방식을 안전하게 이용하기 위해서 사용하는 것이 공개 키 기반구조이다. 공개 키 기반구조를 통해 모든 개체들일 고유한 공개 키 인증서를 발급받기 위해서는 각 STV 마다 STV 식별을 위한 고유 식별 정보(UDN: Unique Device Number)가 필요하다. 이 UDN 과 DTV 모델 정보를 조합하여 PKI 에서 사용할 DN(Distinguished Name)을 생성하게 된다. 이 DN 은 공개 키 인증서를 이용하기 위해서 반드시 필요하며, 또한 권한 관리 구조(PMI)에서 속성인증서를 이용한 권한 관리 수행 시 개체 식별을 위해서도 반드시 필요하다.

STV 의 UDN 을 설정하면 STV 공개키 인증서를 발급받을 준비가 완료된 것이다. 공개키 인증서를 발급받기 위해서는 간단한 인증 절차가 필요하다. 이는 인증서의 요청이 유효한 것인지 검증하기 위해서 필요한 절차이다. 이 단계에서 STV 의 UDN 을 등록하게 되는데, 표면적으로 이 과정이 애플리케이션 스토어 회원가입 및 STV 단말의 등록 과정이 된다.

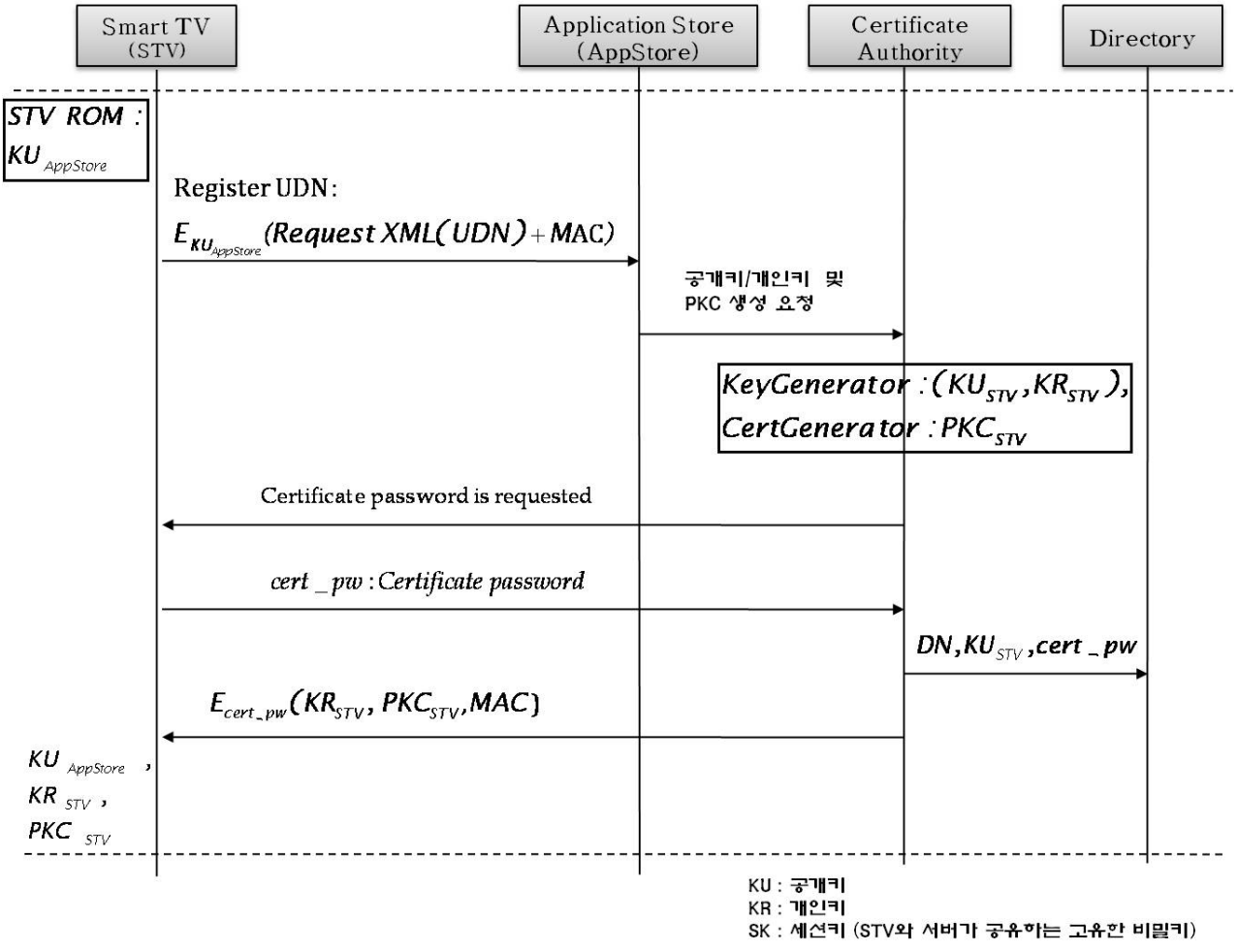
초기 인증 및 UDN 등록 과정에서 인증 및 등록 절차를 안전하게 수행하기 위해서 이 단계에서도 암호화 및 무결성 검증 과정이 필요하다. 암호화 및 무결성 검증에는 STV 에 내장된 AppStore 의 공개키가 이용된다. UDN 등록을 위한 xml 문서에 해쉬알고리즘이나 대칭 키 블록 암호화(DES 또는 AES 이용) 알고리즘의 CBC 모드 적용을 통해 무결성 검증 코드를

생성하여 xml 문서 데이터에 연접하여 STV 에 내장된 AppStore 공개키를 이용하여 암호화 한다. 이 암호화 된 데이터는 AppStore 개인키로만 복호화가 가능하기 때문에 AppStore 웹 서버 외에 아무도 그 내용을 확인할 수 없다.

STV 의 인증 및 단말 등록 등의 과정은 AppStore 서버와 AppStore PKI 의 RA 서버 인터페이스에서 수행한다. AppStore 서버에서는 사용자 회원 가입 시 기기 단말을 요청해야 하며, 이 때 STV 제품별 시리얼 번호의 유효성 검증 모듈을 이용하여 사용자가 입력한 STV 제품 시리얼 번호의 유효성을 검증해야 한다. 그리고 향후 애플리케이션 서버의 이용을 위한 공개키 인증서 발급을 위한 과정을 수행하기 위해 RA 에도 기기의 등록을 수행한다. RA 의 인터페이스는 애플리케이션 스토어 웹 페이지와 연동하여 사용자 입장에서 보안 서비스를 위한 기술적• 구조적 내용들에 대해 투명성을 제공하도록 해야 한다.

모든 등록 과정이 끝나면, 사용자가 느끼지 못하는 과정에서 STV 내장 브라우저 또는 PC 브라우저의 PKI 클라이언트 모듈이 AppStore CA 에게 인증서 발급을 요청하는 과정을 시작하게 된다. 이 과정은 애플리케이션 스토어 웹 서버와 함께 구동되는 RA 인터페이스에서 RA 에게 인증서 발급에 필요한 내용을 전달하게 되고, RA 는 인증서 발급을 위해 필요한 CSR(Certificate Signing Request) 메시지를 작성하여 AppStore CA 에게 전달하게 된다. AppStore CA 에서는 해당 STV 의 공개키/개인키를 생성하고, 공개키 인증서 내용을 완성한 후에 자신의 개인키로 서명하여 공개키 인증서를 완성한다. 이후 개인키는 대칭 키 암호화 방식으로 암호화하고, 공개키 인증서를 함께 STV 에게 전달하게 되며, 동시에 CA 는 인증서를 디렉토리 서버에 게시한다. 그림 1 은 AppStore 서버에 STV 를 등록하고, 공개키 인증서를 요청하여 공개키 인증서와 개인키를 발급 받는 전체 과정의 프로세스 흐름을 보여주는 시퀀스 다이어그램이다.

모든 과정이 완료되면 STV 에는 AppStore 서버의 공개키, STV 의 개인키, STV 의 공개키 인증서가 저장된다. 이 때 STV 브라우저나 AppStore 서버 공개키 인증서 발급 프로그램은 공개키 인증서 저장의 선택이 가능하도록 해야 한다. 사용자 편의를 고려하여 STV 자체에 저장하거나 USB 에 저장하는 것을 선택할 수 있도록 해야 한다.



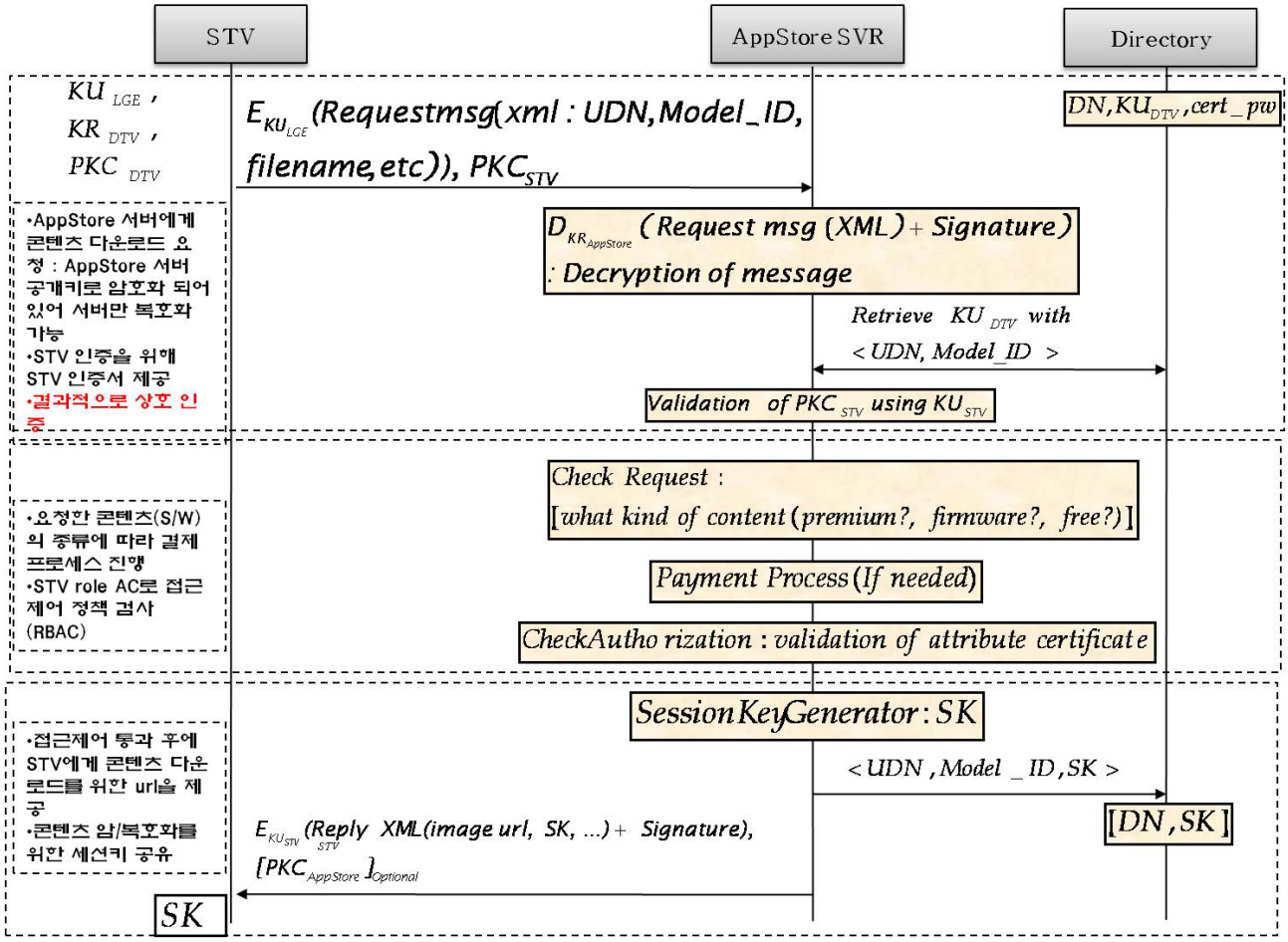
[그림 1] STV 공개키 인증서와 개인키 발급 프로세스 시퀀스 다이어그램

3. 세션키 분배와 암호 통신

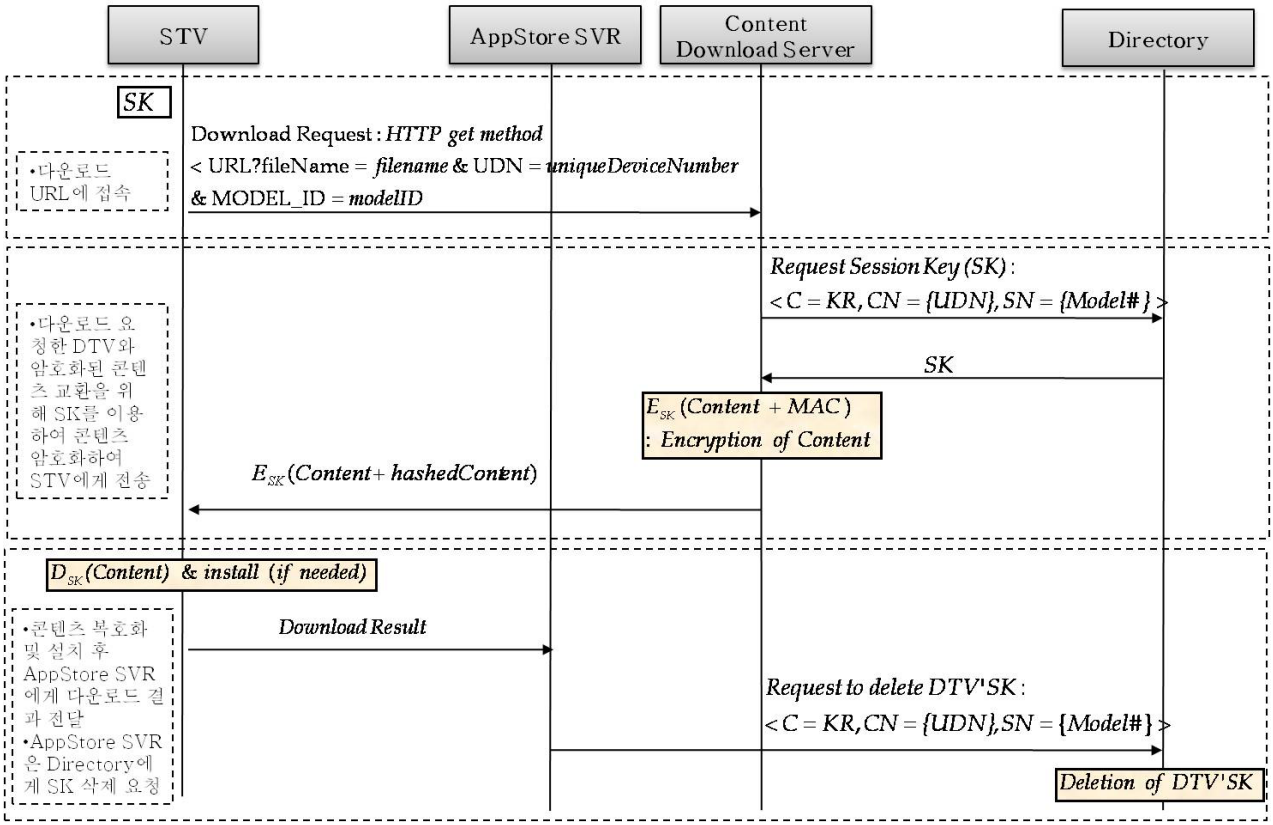
STV 마다 고유의 공개키 인증서를 발급받고 해당하는 개인키를 안전하게 장치에 저장해두면 세션 키의 안전한 키 분배를 위한 준비가 완료된 상태가 된다. 세션 키의 안전한 키 분배를 위한 사전 조건으로서 STV 는 AppStore 서버의 공개키, STV 의 개인키, STV 의 공개키 인증서를 필요로 한다.

우선 첫 단계에는 콘텐츠 다운로드 요청과 상호 인증을 포함한다. STV 는 AppStore 웹 사이트에 접속하여 원하는 콘텐츠나 애플리케이션을 선택하여 다운로드를 요청하게 된다. 이 때 다운로드를 요청하는 메시지는 XML 로 작성되어 HTTP 기반으로 Get 방식으로 전달된다. 이 XML 메시지에는 STV 를 식별하기 위한 UDN 과 모델 번호가 포함되며, 다운로드 받고자 하는 파일의 식별자 및 기타 다운로드 요청을 위한 정보들이 포함된다. 이 요청 메시지를 전송할 때 AppStore 서버의 공개키로 암호화를 하고, STV 의 공개키 인증서를 함께 AppStore 서버에게 전송한다. 이 때 STV 의 공개키 인증서가 LDAP 서버에 저장되어 있다면, STV 에서 보낼 필요 없이 UDN 과 모델 번호를 통해 LDAP 에서 공개키 인증서를 가져와서 이용할 수 있다. AppStore 서버는 전송 받은 공개키 인증서를 통해 STV 를 인증하게 되며, 또한 STV 가 AppStore 서버에게 전송한 요청 메시지는 AppStore 서버만 자신의 개인키를 가지고 복호화 해볼 수 있기 때문에 이후의 프로세스가 정상적으로 진행된다면 암묵적으로 AppStore 서버에 대한 인증이 완료되었다고 고려할 수 있다. 따라서 이 과정을 통해 결과적으로 상호 인증 효과를 얻을 수 있게 된다.

AppStore 서버에 대한 다운로드 요청 메시지 전송 및 상호 인증 과정이 완료되면 AppStore 서버는 요청 메시지의 내용을 분석하여 요청내용이 유료에 해당하는지, 무료에 해당하는지, 또는 펌웨어에 해당하는지에 따라서 과금 프로세스를 진행하게 되며, 과금 결과에 따라서 권한 부여가 이루어지고 이후 요청 트랜잭션 데이터를 생성하여 권한 검사를 수행함으로써 웹 서버 데이터에 대한 접근제어 과정을 수행하게 된다. 이 과정에서는 STV 의 role AC 를 기반으로 접근제어 정책을 검사하게 되며, 역할기반 접근제어 메커니즘을 이용한다.



[그림 2] Smart TV 와 애플리케이션 스토어 서버 간의 상호 인증과 세션키 생성과정



[그림 3] 세션키 분배와 암호화 데이터 다운로드 메커니즘 시퀀스 다이어그램

역할기반 접근제어를 이용한 접근제어의 자세한 과정은 본 논문의 범위에서 벗어나기 때문에 설명하지 않고 향후 다른 논문을 통해 소개하겠다. 접근제어 과정을 거쳐 STV 에게 콘텐츠나 애플리케이션을 다운로드 해줄 수 있는 상태가 되면, STV 에게 콘텐츠 다운로드를 위한 URL 을 제공해야 한다. 이 과정에서 AppStore 서버 측에서는 URL 제공 메시지 세션과 함께 콘텐츠 다운로드 시 암호화를 위한 세션 키를 보내게 된다. 이 때 세션 키는 AppStore 서버 측에 있는 세션 키 생성 모듈을 통해 생성하게 되고, 이 세션 키는 STV 외에도 콘텐츠 다운로드 서버에서 접근할 수 있는 디렉토리에 저장되게 된다. 이 때 디렉토리의 키 저장에 대한 접근제어가 반드시 이루어져야 한다.

STV 는 다운로드 URL 에 접속하게 되며, 이때 요청 메시지는 HTTP Get 방식으로 전달되며, 요청 메시지에는 파일 정보뿐만 아니라 UDN 과 모델 번호가 함께 전달된다. 콘텐츠 다운로드 서버는 이 정보들을 이용하여 디렉토리에서 해당 세션 키를 가져와 콘텐츠를 암호화하여 MAC 과 함께 STV 에게 전송하게 된다. 이후 STV 는 콘텐츠 복호화 후에 해당 애플리케이션 또는 콘텐츠를 설치하거나 이용할 수 있게 된다. 그리고 이 때 STV 는 AppStore 서버에게 다운로드 결과를 전달하게 되며, AppStore 서버는 다운로드가 성공적으로 완료된 경우 디렉토리 서버에 STV 세션 키를 삭제하도록 요청하게 된다.

5. 결론 및 향후 연구 계획

본 논문은 디지털 TV 및 스마트 TV 가 인터넷을 통해 TV 용 앱스토어에 접속하여 콘텐츠 및 애플리케이션을 다운로드 받는 환경에서 TV 와 앱스토어 서버 간의 안전한 통신 및 불법 접근 등을 예방하기 위한 방안으로 공개키 기반 기기 인증 및 키 분배 메커니즘과 암호 통신을 적용하는 방법에 대한 연구를 소개하였다. 본 연구는 향후 스마트 TV 환경 및 앱스토어 서버 등을 시뮬레이션 하여 PKI 구축 및 키 분배와 암호 통신을 실제 적용해보고 다양한 보안 위협 시나리오를 적용하고 보안성을 평가할 예정이다.

참고문헌

[1] William Stallings, " Cryptography and Network Security", Prentice Hall, 2003.

[2] 박선호, 박민우, 정태명, " 제 3 자 개발 애플리케이션 접근제어에 대한 연구", 제 32 회 한국정보처리학회 추계학술대회 논문집 제 16 호 2 호, 2009.11, pp.705-706.

[3] 박선호, 정태명, " 스마트 디지털 TV 에서의 제 3 자 개발 애플리케이션을 위한 보안 요구사항 분석", 제 33 회 한국정보처리학회 춘계학술발표대회 논문집 제 17 권 제 1 호, 2010.4, pp.820-823.