플랫폼 독립적 스마트 콘텐츠 공유 모델

문용혁*, 권혁찬*, 서동일*, 윤찬현**
*한국전자통신연구원
**한국과학기술원
e-mail : {yhmoon, hckwon, bluesea}@etri.re.kr; chyoun@kaist.ac.kr

A Platform-independent Smart Content Sharing Model

Yong-Hyuk Moon*, Hyeokchan Kwon*, Dong-Il Seo*, Chan-Hyun Youn**
*ETRI
**KAIST

요 약

본 고에서는 다양한 공유 환경에서 사용자의 콘텐츠 이용을 저해하지 않으면서, 콘텐츠의 중립적 사용과 안정성을 동시에 충족시킬 수 있도록 고안된 플랫폼 독립적 콘텐츠 공유 시스템에 대하여 논의한다. 특히, 본 시스템은 별도로 정의된 Bytecode 형태의 보안 코드를 플랫폼 독립적으로 해석하는 기능의 Secure Virtual Machine 기반으로 구현되는 제안상의 특징이 있다.

1. 사업자 중심의 콘텐츠 보호 기술의 한계

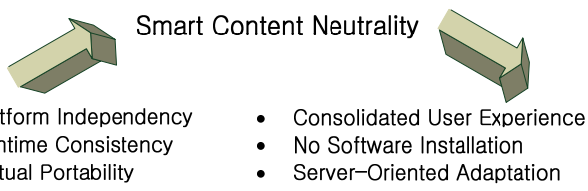
최근 디지털 미디어 시장은 발 빠르게 변화하고 있다. 대표적인 예로서, IPTV 및 Smart TV 와 같은 신규 서비스들이 산업계의 주요 사업으로 등장하고 있고, 콘텐츠의 다양한 소비형태를 지원할 수 있는 여러 Display 단말들이 등장함에 따라 N-Screen 와 같은 서비스 환경이 도래하고 있다. 또한, SNS 서비스의 폭발적인 확산에 따라, 비디오 스트리밍 서비스가 가장 많은 인터넷 트래픽을 유발하고 있는 실정이다.

그러나 다양한 기기에서 콘텐츠를 소비하고자 하는 사용자의 기본적인 욕구를 충족시킬만한 기술적 대안에 대한 요구와 사업자의 콘텐츠 Ownership 에 대한 제어 및 통제는 여전히 그 간격을 좁히는데 어려움을 겪고 있는 것 또한 사실이다. 최근, DLNA 와 같은 콘텐츠 공유기술을 통해 댁내에서 다양한 가전 기기간의 실시간 영상 공유가 가능한 서비스가 가전사의 제품을 중심으로 상용화 된 바 있다. 그러나 본 기술은 특정 기업의 제품간의 DLNA (Digital Living Network Alliance) 프로토콜을 통해서만 제한적으로 공유될 수 있는 문제점을 안고 있다. 더불어, 대표적으로 사용되는 디지털 콘텐츠 저작권 보호 기술인 DRM 의 경우, OMA, CORAL, MPEG-21, DMP 와 같은 대표 표준단체의 노력에도 불구하고, 플랫폼 종속적 보안성 제공모델의 한계에서 벗어나지 못하고 있는 실정이다. 실제로 DRM (Digital Right Management) 또는 Finger Print 은 사업자 중심의 콘텐츠 보호기술이다. 또한 소비를 강제하기 위한 갖가지 조항에 기초하고 있는 것이 사실이다. 그러나 이제는 콘텐츠 이용자를 믿지 않는 데서 출발하는 콘텐츠 보호 패러다임에서 벗어나 이용자들이 콘텐츠를 자유롭게 나누고 표현하도록 돕는 기술적 대안에 대한 요구가 커지고 있다. 그러므로, 본 고에서는 콘텐츠 중립성의 관점에서 이와 같은 문제를 분석하고 이를 위한 기술적 대안 모델에 대하여 논의하고자 한다.

2. 스마트 콘텐츠 중립성 문제

콘텐츠 중립성 문제에서는 그림 1 의 좌측 내용과 같이 콘텐츠의 플랫폼 독립적 사용 및 호환성을 제공함으로써 실행의 일관성을 제공해야 하는 것이 가장 주된 요구사항으로 이해될 수 있다. 즉 콘텐츠를 소비하는 환경 및 기기에 무관하게, 동일 콘텐츠를 이용하는 소비자로 하여금 일관된 경험을 갖도록 보장해 주는 것이 가장 핵심적인 사항인 것이다.

종래의 CP (Content Provider)는 자사 또는 특정한 단체 표준의 DRM 으로 보호된 콘텐츠를 제공하고 있는 실정이다. 따라서, 사용자는 콘텐츠 제공 주체가 누구냐에 따라 별도 DRM 을 중복 설치해야 하는 불편함을 감수해야 한다. 또한, DRM 기술 또한 특정 플랫폼에 종속된 형태로 구현되고 있어, CP 가 지원하는 일부 기기 이외에서 동일 콘텐츠에 대한 사용이 불가능한 단점이 존재한다. 그럼에도 불구하고, 여전히 CP 들은 자사만의 보안 루틴을 포함하고 있는 보안 기술을 콘텐츠에 적용하고자 하는 욕구를 가지고 있는 것으로 판단된다.



(그림 1) 스마트 콘텐츠 중립성 관련 요구사항

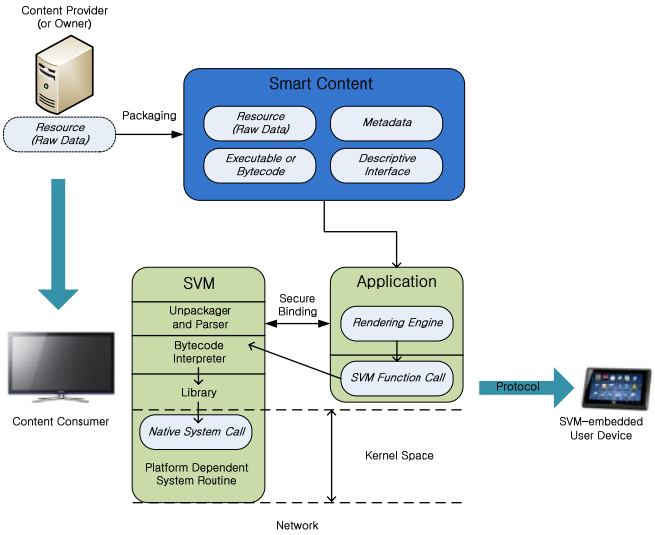
그러나 이것은 일관된 콘텐츠 소비를 가능하게 하기 위한 콘텐츠 중립성의 핵심사항과는 충돌을 피할 수 없다. 따라서, 종래의 DRM 과 달리 CP 간 상이한 콘텐츠 보호 기술이 적용되는 경우라도 이를 통합적으로 수용하여 소비할 수 있는 새로운 시스템 모델이 매우 크게 요구된다.

구체적으로, 1) 적용된 보호기술의 종류에 따른 별도의 사용자 프로그램 (예: Security Agent Software) 설치를 지양할 수 있는 구조이어야 한다. 동시에, 2) 단일한 CP 서버가 상이한 보안 루틴을 콘텐츠에 적용(Server adaptation)하여 배포할 수 있는 등의 보안 기술에 대한 유연한 구현 및 구조 변경을 지원할 수 있어야 한다. 그러므로, 일관된 사용 및 안전한 콘텐츠 이용 (콘텐츠 중립성)의 보장이라는 이 두 가지 특징이 만족되어 제공될 수 있는 콘텐츠를 본 고에서는 특히 “스마트 콘텐츠 (Smart Content)”라 정의한다.

3. 가상 머신 기반의 보안 콘텐츠 실행 모델

상기 논의한 특징 1)을 구현하기 위해서는 그림 2 와 같이 Security Bytecode Interpreter [1]의 고안을 선행해야 한다. 본 해석기는 CP 가 구현할 Executable/Script 또는 Bytecode 형태의 보안 실행 코드를 어떻게 정의하고 해석할 지에 대한 구체적인 체계(예: Syntax)를 제공하기 때문이다. 또한, 본 해석기는 보안 목적의 가상 머신(Security Virtual Machine, 이하 SVM) 구조를 가짐으로써, 다양한 보안 루틴을 수용하며 동시에 상이한 플랫폼을 범용적으로 지원할 수 있는 장점을 제공할 수 있다. 구체적으로, SVM 은 Application 영역의 Rendering Engine 요청에 따라 특정 Smart Container 를 언패키징하고, 콘텐츠에 대한 접근 유효성을 검증하는 상위 레벨과, 이후 보안 실행 코드를 해석하고, 포함된 루틴을 특정 단말 Platform 의 Native System Call 형태로 수행하는 하위 레벨 구조로 나누어 나뉘어 진다. 특히, SVM 이 처리해야 하는 실행 루틴은 보안코드 수행에 국한된 것으로 본다. 따라서, SVM 은 일관되고 안전한 콘텐츠 사용이라는 특수 목적의 Bytecode Interpreter 로 고려될 수 있으므로, 범용 VM 에 비해 그 구현의 범주가 넓지 않은 것으로 판단할 수 있다.

또한, 상기 특징 2)을 기술적으로 도입하기 위해서, 다음의 그림 2 와 같이 CP 가 상이한 보호기술을 적용시킬 수 있는 범용적 Smart Container 을 정의해야 한다. 컨테이너 내부에는 콘텐츠 자체 (Resource), 메타데이터를 포함할 수 있어야 하며, 해당 콘텐츠의 사용 권한 및 콘텐츠의 유효성을 검증하기 위한 보안 수단이 Executable code 또는 Bytecode 형태로 탑재될 수 있어야 한다. 추가적으로, 해당 데이터를 위한 Renderer 와의 바인딩을 위한 Descriptive interface 를 포함한다. 여기서 특히 보안코드는 콘텐츠 자가보호 (Self Protection) [2]를 위한 실행 루틴을 포함하고 있으며, 스마트 컨테이너를 통해 VM 을 통해 소비가 가능한 콘텐츠를 구성함에 따른 오버헤드는 매우 작도록 구현되어야 한다. 추가적으로, License 를 Smart container 에 자체 탑재하거나 별도의 License 관리 서버를 이용하는 등의 개별 CP 들의 보안 정책에 따른 다양한 운용 모델을 고려할 수 있다.



(그림 2) 콘텐츠의 중립적 공유를 위한 시스템 모델

4. SVM 보안성 및 범용성 지원 방안

SVM 의 Application 영역과 Kernel 영역간의 Interface 를 Bypass 하지 못하도록 하는 강력한 Binding 기술이 요구된다. 일례로, Rendering engine 이 SVM 으로 영상 데이터의 추출을 요청할 경우 상호 신뢰가 가능한 Binding Protocol 을 통해 데이터의 전달이 이뤄져야만 종래의 DRM 해킹으로 인한 데이터 유출과 같은 문제점을 방지할 수 있다. 더불어, 다양한 Video renderer 와의 Secure binding 이 용이하도록 범용 API 제공되어야 한다. 또한, Function (예: API) 수준의 Hardening manual 이 개발자에게 제공되어야 잘못된 동작내지 보안위협 등을 포함하지 않은 형태의 스마트 콘텐츠 구성 및 SVM 구축이 가능하다.

5. 결론 및 추후연구

본 고에서 논의한 콘텐츠 중립성은 크게 일관된 사용 및 안전한 사용의 보장이라는 두 가지 요구사항으로 이해될 수 있는데, 이러한 요구사항이 만족되는 콘텐츠를 특히, 스마트 콘텐츠라 정의하였다. 구체적으로, 합리적 스마트 콘텐츠 공유를 위한 방법으로, SVM 기반의 시스템 모델에 관하여 제안하였다.

Acknowledgement

“ 본 연구는 방송통신위원회의 Beyond Smart TV 기술개발사업의 연구결과로 수행되었음 (2011 년도 사업)”.

참고문헌

[1] Smith, James E. and Nair, Ravi, "The Architecture of Virtual Machines". Computer (IEEE Computer Society) Vol. 38 (5): pp32–38, 2005.

[2] Paul Kocher, Joshua Jaffe, Benjamin Jun, Carter Laren, and Nate Lawson, “Self-Protecting Digital Content”, published by Cryptography Research, Inc. (CRI).