안전한 트랜스코딩 메커니즘을 위한 보안 정책 모델

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

Security Policy Model for Secure Transcodable Mechanism

Yong-Hyuk Moon*, Hyeokchan Kwon*, Dong-Il Seo*, and Chan-Hyun Youn**
*Electronics and Telecommunications Research Institute (ETRI)
** Korea Advanced Institute of Science and Technology (KAIST)

요 약

본 고에서는 최근 주목 받고 있는 비디오 스트리밍 보안 기술과 관련한 ITU-T 표준화 내용에 대하여 살펴보고자 한다. 특히, SVC (Scalable Video Coding) 기술을 위해 제안된 안전한 트랜스코딩 메커니즘 (Secure Transcodable Mechanism)을 위한 보안 정책 모델에 대하여 논의한다.

1. 서론

최근 단말의 성능 및 네트워크 조건에 따라 비디오 데이터의 실시간 가변성 (Real-time Transcoding)을 지원할 수 있는 기법에 대한 연구 및 표준화 활동이 활발하게 진행되고 있다. 특히 비디오를 재인코딩 하지 않고, 일부 Bit Streams 을 추출함으로써, '영상 크기, 프레임 전송 비율 및 영상 품질'과 같은 3 가지 관점에서 다양한 영상 변환을 지원할 수 있는 SVC (Scalable Video Coding) 비디오 압축 알고리즘 [1]이 개발됨에 따라, 한번의 인코딩만으로 보다 최적화된 스트리밍 서비스 품질을 제공할 수 있는 기술적 수단이 마련되었다. 그러나, 상대적으로 비디오 변환의 안전성 담보할 수수 기법에 대한 연구 노력은 부족한 실정이다. 한편, ITU-T 표준화 기구에서는 IPTV 와 같은 환경에서 안전한 비디오 변환 기능을 구현할 수 있도록 관련 요구사항, 기능블록 및 프레임워크에 대한 규격 [2]을 제공하고 있어, 본 고에서는 해당 ITU-T 표준 내용 중 안전한 트랜스코딩 메커니즘의 구동 방식을 결정하는 보안 정책 모델에 대해 논의하고자 한다.

2. 안전한 트랜스코딩 메커니즘

ITU-T 표준 문건에서 제안하고 있는 안전한 트랜스코딩 메커니즘 (Secure Transcodable Mechanism)은 기본적으로 선택적 암호화 방식 및 SVC 비디오 압축 알고리즘을 채용하고 있다. 따라서, SVC 의 Extraction 기능을 활용하여 암호화된 비디오 데이터일 경우에도 여타의 조작 (예: 복호화, 디코딩, 재인코딩) 없이 단말 및 네트워크 요구사항에 따라 필요한 부분만을 보호가 유지된 형태로 추출하여 서비스할 수 있는 기술적 장점을 제공한다. 더불어, 종래의 영상 변환 기술과 달리 복호화를 통한 원본 데이터의 확보가 요구되지 않기 때문에 권한이 없는 제 3 자가 비디오 데이터를 취득하더라도 비디오와 관련된 일체의 조작이 불가능하여, 스트리밍의 서비스 안정성을 크게 높일 수 있다. 안전한 트랜스코딩 메커니즘은 아래와 같이 크게 3 가지 단계로 동작한다.

(1) 보호된 비디오 생성: 비디오 전체를 암호화 (Wholesale Encryption) 방법과 달리, 영상학적으로 중요한 의미를 내포하는 일부 부분만을 암호화 (Selective Encryption)하는 방식으로 안전한 영상 변형이 가능한 비디오를 생성하는 과정을 의미한다.

(2) 비디오 추출: 본 기능에서는 암호화된 비디오 데이터의 일부 스트림을 추출하거나 버리는 방식을 통해 디코딩, 복호화 및 재인코딩 없이 안전한 비디오의 변환을 수행 한다.

(3) 비디오 복호화: 사용자 단말에서는 안전하게 변환된 비디오 데이터를 서비스 공급자로부터 수신한 보안 정책에 근거하여 복호화 한 뒤 이를 소비한다.

3. 보안 정책 관리 모델

3.1 보안 정책의 필요성

안전한 트랜스코딩 메커니즘은 '인코딩 규칙, 암호화 방법, 암호화 될 비디오 영역, 기타 암호화 관련 알고리즘, 키 관리 프로토콜 및 비디오 배포 방식' 등을 고려해야 할 필요가 있다. 보다 구체적으로, 안전한 트랜스코딩 매커니즘이 수행되기 전에 비디오 스트리밍 성능에 영향을 미칠 수 있는 지표들에 대한 이해와 선정이 중요하다. 또한, 서비스 공급자가 일관된 방법에 의해 사용자의 단말로 서비스를 지속하기 위해서는 안전한 트랜스코딩 메커니즘 및 비디오 소비의 전반에 걸친 일관된 프로토콜 (또는 규약)이 요구된다. 즉, 비디오 서비스 제공자는 상기 고려사항들을 잘 정의된 Configuration 형태로 관리하고 이를 이용하여 요구사항 별로 상이한 정책을 생성함

으로써, 보다 단말의 성능 및 네트워크에 적합하고, 안정된 방법으로 비디오 스트리밍 서비스를 제공할 수 있게 된다.

3.2 보안 정책 구성

서비스 공급자는 생성된 정책들을 관리하기 위해 별도의 데이터베이스를 구성할 수 있으며, 정책의 상세한 구성 방법은 표 1 와 같이 실시될 수 있다.

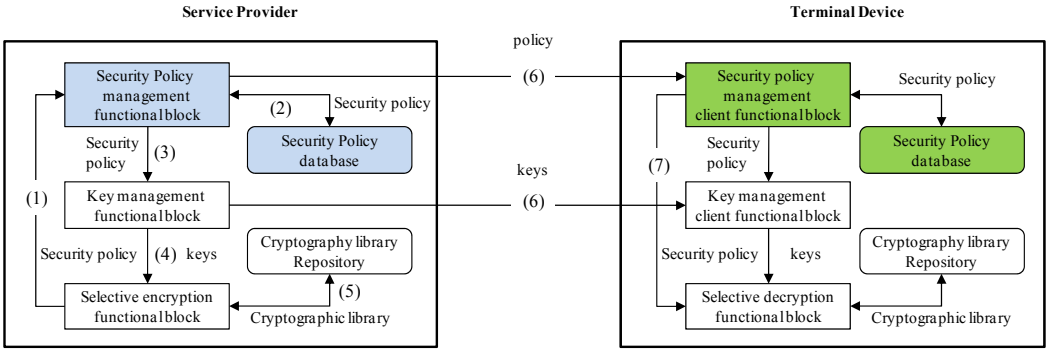
<표 1> 보안 정책의 구성요소 분류 [2]

Field		Items
Encryption method		- *ISE*: Incompression-based selective encryption - *PSE*: Postcompression-based selective encryption - *HSE*: Hybrid-type selective encryption
Encryption type		Incompression-based selective encryption - *I_type1*: IPM encryption - *I_type2*: Texture sign encryption - *I_type3*: MVD encryption - *I_type4*: Texture sign + MVD encryption Postcompression-based selective encryption - *P_type1*: SPS encryption - *P_type2*: SPS+PPS encryption - *P_type3*: SPS+PPS+Payload encryption Hybrid-type selective encryption - *Any combination types above are applicable*
Encryption layer		(*EL_start*, *EL_end*)
Cryptographic Parameter set	Encryption algorithm	*3DES, SEED, IDEA, AES_CBC, etc.*
	Key size	*128, 168, 192, 256 bits, etc.*
	Key lifetime	Time in seconds

다음은 상기 표 1 에 제시된 내부 데이터로 구성될 수 있는 보안 정책의 한가지 Configuration 이다. 본 예에서, 해당 비디오 데이터는 'id00001'이라는 콘텐츠 아이디를 부여 받고, 비디오 인코딩 과정 중 선택적 암호화 기법으로 보호되며, 암호화 계층 및 영역은 기본 계층의 'Texture Sign Bits'로 규정되고 있다는 것을 의미한다. 또한 암호화 알고리즘 및 방식은 192 비트의 AES (Advanced Encryption Standard)의 CBC(Cipher Block Changing) 모드를 활용하며, 암호화 키의 생명 주기는 10,000 초로 명시하고 있다.

- id00001: a content identity
- ISE: incompression-based selective encryption
- (I_type2): texture sign bits as a part to be encrypted
- {0, 0}: base layer as a layer to be encrypted
- AES_CBC (192bits): AES encryption algorithm, CBC encryption mode, 192 bits key size
- 10,000: key life time (seconds)

실제로 상기 정책이 사용자 단말로 전달될 때는 "{*id00001*, *ISE*, *I_type2*, {*0*, *0*}, *CP_set*{*AES_CBC*, *192*, *10000*}…}"와 같이 각 구성요소를 나열 (Enumeration)하는 형식으로 구성될 수 있는 것으로 ITU-T 표준 문건은 제시하고 있다.



(그림 1) 보안 정책 협상 모델 [2]

3.3 보안 정책 구동

서비스 공급자와 사용자 단말 간의 보안 정책 협상 모델은 그림 2 와 같은 기능 블록 레벨로 표현될 수 있으며, 협상을 수행하는 프로세스는 하단과 같이 7 단계로 요약될 수 있다.

(1) 신규 정책 데이터 생성 또는 검색·수신
(2) 특정 비디오에 적합한 형태 정책 구성
(3) 암호화 키 생성 및 키 생명 주기를 설정
(4) 정책 및 암호화 키를 암호화 기능블록에서 수신
(5) 암호화 라이브러리 저장소로 관련 암호 알고리즘 수신 후 정책에 따라 선택적 비디오 암호화 수행
(6) 비디오 복호화 키 및 정책을 사용자 단말로 전송
(7) 수신 비디오를 보안 정책에 따라 복호화·소비

이와 같은 정책 연동의 주요한 효과는 사용자 단말에서 서비스 공급자가 규정에 방법에 의해서만 비디오를 소비하도록 강제 (Policy Enforcement)하는 기술적 수단으로 제공할 수 있다는 것이다.

4. 결론

본 고에서는 ITU-T 에서 표준화가 진행되고 있는 안전한 트랜스코딩 메커니즘과 관련된 주요 기능 블록인 보안 정책 관리 생성 및 배포에 대하여 논의하였다.

참고문헌

[1] Heiko Schwarz, Detlev Marpe, and Thomas Wiegand, "Overview of the Scalable Video Coding Extension of the H.264/AVC Standard". IEEE Transaction on Circuits and Systems for Video Technology, VOL. 17, NO. 9, September 2007.
[2] ITU-T Draft Recommendation X.iptvsec-2 (TD 903): Functional requirements and mechanisms for secure transcodable scheme of IPTV.