[정보보호] 트랜스코더블(Transcodable) 정보보호 동향

방송서비스를 네트워크를 통하여 전송함에 있어서, 중요한 점은 실시간성을 보장할 수 있느냐는 것이다. 전통적인 암호처리 방식은 모든 콘텐츠를 일률적으로 암호를 적용하여 처리하는 것이다. 즉 입력되는 패킷에 대하여 콘텐츠의 환경은 고려되지 않고 일방적인 암호처리가 적용되는 것이다. 이러한 방식은 용량이 비대한 멀티미디어 콘텐츠를 실시간적으로 전달하는 데에는 많은 문제점을 일으키고 있다.

또한 유무선 통합의 IPTV 환경이나 모바일 IPTV 환경에서의 HE(Head End)에서 전송되는 콘텐츠가 여러 종류의 단말에 적응적(Adaptive)으로 전달하는 것이 네트워크 관리 효율성 측면에서 필요하다. 즉 OsMu(One Source Multi Use)의 개념이 구현된 SVC(Scalabel Video Codec)을 사용하여 단말 화면의 크기, 대역폭 그리고 화면의 질에 따라 다양한 형태의 서비스가 제공되는 것은 네트워크의 효율성 측면에서는 필수적인 것이다.

방송, 통신 서비스의 융합으로 인하여 방송콘텐츠의 통신인프라를 통한 전달은 새로운 융합서비스의 창출을 보이고 있다. 이러한 서비스의 환경 변화에 따라 정보보호 메커니즘도 변화하고 있으며, 방송의 콘텐츠 보호 기술인 CAS(Conditional Access Service)와 통신의 콘텐츠 보호 기술인 DRM(Digital Right Management)의 연동, 통합 그리고 융합을 요구하고 있다.

이러한 시점에서 CAS와 DRM을 융합할 수 있는 핵심 정보보호 기술로서 선택적(Selective) 암호 메커니즘을 기반으로 하는 E2E(End-to-End) 정보보호 기술이 IPTV 콘텐츠 보호에 핵심기술로 떠오르고 있다. 즉 네트워크 상에서 콘텐츠를 재전송(Store, Copy and Rebroadcast)을 연속하여 하는 것에 무관하게 E2E 정보보호 서비스를 제공할 수 있다면, 그리고 실시간성을 유지할 수 있다면 IPTV 서비스 제공에 있어서 매우 중요한 역할을 할 수 있는 기술이라고 사료된다.

다음은 ITU-T에서 2008년 9월 승인된 워크아이템인 X.iptvsec-2 문서 관련하여, 지난 2009년 6월 IPTV-GSI 회의에서 정보보호 요구사항에 대하여 합의된 내용이다.

IPTV 트랜스코딩 정보보호 요구사항

안전한 트랜스코딩 정보보호를 제공하기 위해서는 다음과 같은 요구사항이 필요하다.

• Cryptographic and Perceptual Security

전통적인 암호알고리즘과 같이 암호알고리즘 자체의 보안 강도 역시 중요하다. 즉 암호알고리즘 자체의 보안성이 강해야 하며, 그에 따라 운용되는 암호키도 보안성이 강해야 한다. 그러나 이들의 강한 보안성으로 인하여 멀티미디어의 실시간성을 저해해서는 안된다. 그러므로 전통적인 방식이 아닌 선택적 암호 메커니즘을 적용하면서 보안성을 유지해야 한다. 반면 암호 알고리즘은 강한 보안성을 갖고 있을지라도 선택적 암호메커니즘을 콘텐츠에 적용하면 콘텐츠가 부분적으로 암호화가 된다. 이는 다음에 설명되는 Format compliance의 요구사항과 연관시키면, 암호화된 상태로 재생이 가능해야 한다. 그러면 암호화되지 않은

부분이 화면에 재생될 때, 이러한 상황에서 사람의 인지(Perceptual) 능력으로 희미한 영상에 대하여 해독을 할 수 있게 된다. 만약, 이와 같이 부분적인 정보로 전체를 연상할 수 있게 된다면 암호화의 목적을 달성하지 못하게 되므로, 사람의 인지를 뛰어넘는 수준을 맞추기 위하여 암호 메커니즘(파라미터)이 재설정되어야 한다.

• Efficiency

멀티미디어 콘텐츠 전송에 있어서 실시간성을 제공하기 위하여, 콘텐츠를 선택적으로 암호화를 실시해야 한다. 그렇게 하여 콘텐츠 암호화가 경량화되고, 추가적인(재전송적, 시스템적 등등) 복잡성을 피할 수 있다.

• Compression ratio

멀티미디어 콘텐츠 암호 메커니즘은 압축율을 감소시켜서는 안되며 또는 압축률에 영향을 주더라도 작은 범주 안에서 유지되어야 한다.

• Format compliance

암호화된 비디오 데이터는 표준 디코더와 호환성을 유지해야 한다. 즉, 어떤 표준 디코더라도 암호화된 비디오 데이터를 복호(Decrypt)하지 않고 재생(Decode)할 수 있어야 한다. 이러한 특성은 안전한 트랜스코딩 제공에 필수적인 요소이다.

• Error tolerance/Robustness

멀티미디어 콘텐츠 암호 메커니즘은 오류 허용성/오류 강인성을 지원해야 한다. 이것은 전송 중에, 암호 비트스트림의 한 비트의 오류가 발생할 경우, 복호화(Decryption) 과정에서 많은 다른 비트의 오류를 만들어낼 수 있다. 이것은 더 나아가 재생(Decoder)에서 오류 또는 영상 찌그러짐으로 확대의 원인이 된다.

• End-to-End security

전통적인 트랜스코더는 콘텐츠를 복호화, 트랜스코딩, 그리고 다시 암호화하는 과정에서 정보보호 위협을 야기시킨다. 그러므로 중간의 트랜스코딩 노드는 복호화하지 않고 트랜스코딩을 해야 한다.

• Adaptive resolution

트랜스코더블 암호 메커니즘은 다양한 전송대역, 화질, 화면크기의 단말을 지원할 수 있어야 하며, 이에 상응하여 정보보호 메커니즘은 보안 강도의 수준을 조절 할 수 있어야 한다.

향후 전망

방통융합서비스인 IPTV는 방송서비스와 통신서비스의 융합으로 탄생된 서비스이다. 그리고 방송과 통신서비스 정보보호의 공통점을 추출하고 이에 걸맞는, 즉 E2E를 지원하고, 이동성을 지원하며, 다양한 단말의 지원이 용이한 트랜스코더블(Transcodable) 정보보호 메커니즘의 필요성이 인식되고 있으며, 이에 대한 기술표준이 SVC(Scalable Video Codec) 기반의 IPTV 정보보호 메커니즘 표준화로 집중되고 있다.

나재훈 (한국전자통신연구원 지식정보보안연구부 팀장, jhnah@etri.re.kr)