한국항행학회 논문지 제13권 제3호 2009년 6월

온라인상의 콘텐츠 오남용 방지를 위한 보호기술 기준에 대한 연구

A Study on Protection Technology Criteria for Preventing Contents Abuse on On-line

홍성혁*, 윤은준**, 한재홍***, 박종혁*

Sung-Hyuk Hong*, Eun-Jun Yoon**, Jae-Hong Han*** and Jong-Hyuk Park*

요 약

급속한 통신의 발달로 지식과 정보가 디지털화 되고 유통이 활발히 이루어지고 있으나 디지털자산의 오남용 및 보안문제가 빈번히 발생되고 있다. 본 논문에서는 콘텐츠의 오남용사례와 콘텐츠 보호기술을 분석하며 이를 통해 온라인상의 콘텐츠 오남용 방지를 위한 보호기술을 위한 중요 항목을 제안한다. 본 중요 항목은 기술기준 수립을 위한 중요 요소로 활용 될 수 있을 것으로 기대된다.

Abstract

Due to fast development of communications, knowledge and information have been become digitalized and distributed actively. However, the misuse and abuse of digital properties and security problems frequently take place. In this paper, we analyze the cases of the misuse and abuse of contents and the contents protection technology. We propose important items for protection technology to prevent contents from misuse and abuse based on results of the analyses. These important items are expected to be used as important factors for establishing protection technology standards.

Key words : Digital Contents Protection, Preventing Contents Abuse

I. 서 론

통신환경의 급속한 발달로 지식 · 정보가 디지털화되고 있다. 따라서, 현대사회는 지식정보의 효율적인 관리 및 신속한 전달 등 여러 가지 장점을 가지고 있지만, 콘텐츠의 대량 복제나 저작자의 동의 없는 무단 변형, 디지털 자산의 오남용, 프라이버시 침해 등 온라인 보안 문제가 사회적 문제로 대두되고 있다. 이러한 사회적 요구로 인해 고부가가치의 디지털 콘텐츠에 대한 불법복제방지 기술과 오남용 방지에 대한 중요성이 날로 부각되고 있는 추세이다.

현재 방송에서는 CAS (Conditional Access System) 기술을 이용하여 지상파, 위성, 케이블, IP를 통해 전송되는 디지털 콘텐츠를 안전하게 보호하고 유료 가

* 경남대학교 컴퓨터공학부
** 경북대학교 전자전기컴퓨터학부
*** 한국 정보보호 진흥원 u-IT서비스보호팀
· 교신저자(Corresponding Author) : 박종혁
· 투고일자 : 2009년 5월 1일
· 심사(수정)일자 : 2009년 5월 4일 (수정일자 : 2009년 6월 3일)
· 게재일자 : 2009년 6월 30일

입자에 한하여 콘텐츠를 제공하고 있으며, 통신 환경에서는 DRM (Digital Rights Management) 기술을 이용하여 디지털 콘텐츠의 지적 자산에 대한 권리를 허가받지 않은 사용자로부터 콘텐츠의 접근 및 이용을 불가능하게 통제하고 있다. 하지만, 그 외의 콘텐츠의 불법복제 방지기술 및 콘텐츠의 오남용 방지를 위한 법적 제도적 장치가 미비한 상황이다.

본 논문에서는 온라인상에서 사용되는 디지털 콘텐츠의 오남용을 방지하고 디지털 콘텐츠의 안전한 보호를 위한 정보보호 기준을 위한 중요 항목을 제안한다.

본 논문은 2장에서 콘텐츠 오남용 사례에 대해 기술하고, 3장에서 콘텐츠 보호 기술을 분석하며, 4장에서 콘텐츠 보호 기술기준을 위한 중요 항목을 도출하고, 5장에서는 결론 및 향후 방향을 제시한다.

Ⅱ. 제 2 장 콘텐츠 오남용 사례

본장에서는 온라인상의 콘텐츠 오남용사례를 6가지의 경우에 대해 살펴본다.

2-1 악성코드

악성코드는 포털사이트나 검색엔진, UCC 동영상, P2P를 통한 상용 프로그램 다운로드 등 다양한 배포 루트를 통해 유포되고 있다. 게시물에 악성코드를 숨겨 놓고 사용자가 클릭하면 사용자의 PC로 자동으로 다운로드 되게 하는 방식을 사용하여 숙주 서버에 자동 접속되도록 하거나 개인정보를 불법적으로 탈취하여 사용하는데 이용한다 [1].

2-2 불법콘텐츠 유포

불법 콘텐츠 유포는 P2P나 웹하드, 카페나 블로그 등을 통해 단시간내에 유포 및 삭제되기 때문에 불법 콘텐츠 방지가 쉽지 않다. 불법콘텐츠의 유포 방지 및 차단을 위해서는 워터마킹(watermaking), 핑거프린팅(FingerPrinting), 네트워크 모니터링, 매크로 프로그램, P2P 프로토콜 조작, 페이크(Fake) 파일 유포 등의 기술들이 사용된다.

2-3 개인정보유출

연예인 및 일반인에 대한 개인정보 유출 심각하다. P2P나 웹 하드 등을 통해 연예인 사생활 콘텐츠는 쉽게 구할 수 있으며, 심지어 포털사이트를 통해 중/고등학교 생활기록부와 주민등록번호 등도 알 수 있다.

P2P나 웹 하드를 처음 사용해 보거나 익숙하지 않은 사용자의 경우 파일 공유 폴더를 자신의 PC에 잘못 설정하여 개인정보가 유출되는 사례도 적지 않다.

또한, 공공기관 홈페이지와 기업의 홈페이지를 통해 개인정보가 유출되는 경우가 많아 인터넷 홈페이지를 통해 쉽게 개인정보를 접할 수 있다 [2].

2-4 악성 댓글

악성 댓글에 의해 많은 사람들이 정신적인 피해를 입으며, 언론이나 악성댓글에 의해 자살을 시도한 연예인도 쉽게 찾을 수 있을 정도로 악성 댓글의 피해는 심각하다. 악성 댓글이 자살의 원인이라고 단정할 순 없지만 악성댓글로 인해 자살을 결심하게 되는 원인이 되기도 한다 [3].

악성 댓글뿐만 아니라 스팸댓글로 인하여 홈페이지 서비스 속도 저하를 가져와 사용자 및 시스템, 네트워크 관리자의 불편을 초래한다. 이런 스팸 댓글은 제품이나 사행성 도박 사이트와 성인 사이트 홍보를 목적으로 한 상업용 스팸 댓글이 대다수이며, URL의 사이트로 유도해 악성코드를 배포하기도 한다.

2-5 청소년 유해 콘텐츠

최근 청소년들은 인터넷과 게임에 대부분의 여가시간을 보낸다. 이러한 환경에서 청소년들은 인터넷을 통해 불법콘텐츠를 쉽게 접할 수 있다. 인터넷을 통해 쉽게 접할 수 있는 성인/폭력 동영상의 지나친 음란성과 폭력성으로 인해 청소년의 사회문제로 대두되고 있으며, 청소년의 게임 및 인터넷 중독 문제는 2000년대 초반부터 끊임없이 문제가 되어 왔다.

2-6 IPTV 콘텐츠 불법 사용

IPTV에서 제공하는 VOD 영화, 드라마, 뮤직비디

오 등 유료 콘텐츠가 PVR (Personal video Recorder)을 통해 P2P나 웹하드 등을 통해 불법 배포되고 있다. 이파일의 명칭은 'IPTV'나 'IPTVRip' 등으로 누구나 IPTV를 통해 불법 복제된 파일임을 알 수 있으며, IPTV 업체들이 제공하는 EPG 정보나 연령제한 표시 등이 그대로 적용되어 있어 국내 3개 IPTV 서비스 사업자들을 통해 불법복제 되었음을 확인할 수 있다. 현재 P2P나 웹하드를 통해 배포되는 불법 콘텐츠는 IPTV 서비스를 통해 보는 것보다는 시청 방법이나 비용면에서 절대적으로 유리하다. 따라서 그동안 DVD 나 지상파 방송 프로그램을 통해 배포되었던 불법 콘텐츠가 IPTV를 통해서도 불법 유통될 수 있어 디지털 콘텐츠 오남용 사례가 되고 있다 [4].

Ⅲ. 콘텐츠 보호 기술 분석

본장에서는 콘텐츠 보호 기술에 대해 간략히 살펴보며 콘텐츠의 오남용 방지를 위한 보호 기준 중요 항목을 위해 기술요소를 분석한다.

3-1 디지털 콘텐츠 보호 기술

• DRM 기술 : DRM은 디지털 콘텐츠의 저작권을 보호・관리하는 기술이다.

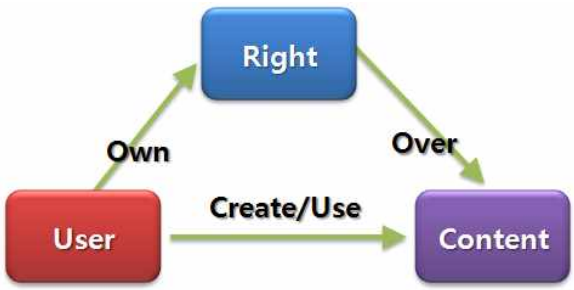

그림 1. 사용자, 권한, 콘텐츠의 관계
Fig. 1. relation of User, Right and Contents.

DRM의 기본적인 세 가지 구성 요소인 사용자, 콘텐츠, 권한 들 간의 관계를 그림 1에서 볼 수 있다.

사용자는 콘텐츠에 대해 창작, 판매, 구입, 소비, 등에 대한 행위를 할 수 있다. 콘텐츠는 지적자산의 가치가 있는 정보이며, 허가되지 않은 사용자로부터 보호해야할 대상이다. 권한은 콘텐츠별로 정해진 허가와 조건에 의해 콘텐츠의 이용 결정된다 [5].

• CAS 기술 : CAS는 가입자 관리 시스템(SMS: Subscriber Management System)과 함께 유료방송 서비스를 위한 필수적인 구성 시스템으로 가입자에게 원하는 프로그램을 제공하고, PPV (Pay-Per-View) 및 VoD (Video on Demand) 등과 같은 다양한 부가 서비스를 지원한다. 또한, 제공되는 서비스에 대한 보안성을 책임져야 하는 시스템이다. CAS는 방송 사업자가 콘텐츠에 스크램블(Scramble)을 걸어 Cable, 위성, 지상파, 인터넷, 휴대이동 방송망을 통해 시청자에게 전송하면 제한수신 모듈이 시청자가 유료 가입자인지, 어떤 서비스에 가입했는지 등을 확인하여 콘텐츠를 디스크램블링(Descrambling) 하게 된다. 이러한 CAS 기술은 방송 사업자에게 무자격자의 불법 시청을 방지할 수 있게 하고, 가입자의 시청 성향 등 마케팅 자료를 제공함과 동시에 이를 바탕으로 한 타깃 마케팅 등의 다양한 마케팅을 가능하게 한다. 콘텐츠 보호를 위한 CAS은 방송사업자의 가입자 인증시스템 및 셋톱박스의 암호해독시스템, 고객정보를 수록한 스마트카드와 가입자 모듈로 구성될 수 있다. 특히 암호해독 시스템만을 CAS라고 부르기도 한다 [6].

• 디지털 워터마킹(digital Watermaking) 기술 : 디지털 워터마킹 기술은 디지털 콘텐츠에 워터마크를 삽입・배포하며 저작권 분쟁이 발생하면 워터마크를 추출하여 저작권을 보호하는 방법이다. 저작권 주장, 온라인상의 콘텐츠 위변조 판별, 무단 배포 방지(복사 제어), 사용자 제어 등에 사용된다 [7].

3-2 개인정보유출 보안 기술

• 웹 프라이버시 기술 : 웹 프라이버시 기술은 웹사이트 이용자가 의도적이거나 부주의하게 웹사이트에 게재하는 개인정보를 사전에 차단하거나 지속적으로 점검함으로써 웹사이트에 개인정보가 노출되어 발생하는 명의도용 등의 사고를 최소화하도록 하는 기능을 제공하는 모든 형태의 기술을 의미한다. 따라서 이 기술은 게재되는 개인정보의 민감도에 따라 웹사이트의 개인정보 게재 시점에서 사전에 차단함으

로써 노출을 방지하는 기능(필터링 기능)과 웹 사이트 게재 이후에 점검함으로써 관리자의 판단에 따라 개인정보 삭제 여부를 판단하여 관리하는 기능(스캐닝 기능)이 두 가지로 구분된다 [8].

• 정보보호 포렌식 기술 : 정보보호 포렌식 기술은 근래 정보보호 유출에 따른 법/제도적 실효성을 부여하기 위한 대표적인 기술이다. 콘텐츠의 오남용의 사유로 개인정보보호 피해를 입었다면, 피해 경로를 역추적하고 피해 사실과 증거를 입증할 만한 디지털 증거(Forensics)를 확보하는 것이 중요하다. 이러한 이유로 근래는 디지털 포렌식(Digital Forensics)을 기반으로 하는 정보보호 포렌식 기술 연구가 진행되고 있다. 콘텐츠에 포함된 악성코드나 콘텐츠 유출에 따라 범죄자가 보유한 디지털 콘텐츠를 분석하여 유효한 증거를 수집/확보하는 기술이다. 시스템에 저작된 콘텐츠를 분석하거나 이메일과 사이트 접속 이력 등 다양한 부분에서 보안 기술이 요구된다.

3-3 디지털 콘텐츠 필터링

• 음원 필터링 : 현재 대형 포털 사이트를 통해 불법 배포되고 있는 대표적인 콘텐츠가 바로 MP3와 같은 음원 콘텐츠이다. 현재로서는 게시물에 링크되거나 업로드 되는 파일에 대해서 필터링을 하는 기술이 가장 효율적인 기술로 평가받고 있다. '인기 음원명' '가수 및 앨범명' '음원명과 다운로드' '음원명과 MP3' 등 음악 관련 키워드중심으로 불법으로 공유될 위험이 있는 게시물을 검색 대상에서 제외시킨다. 첨단 음원 및 동영상 필터링 기술을 도입은 불법 공유 목적 게시물을 차단하는데 그 목적이 있다. 네이버는 키워드 기반의 필터링 기술의 적용뿐만 아니라 보다 고도화된 음원 저작권 보호 시스템인 '음원 저작권 필터링 시스템'을 서비스 하고 있다. 음원 저작권 필터링 서비스는 블로그나 카페 등에 포함된 음원의 일부 특징을 추출하여 저작권 데이터베이스에 있는 원본 음원의 NDA와 비교하여 저작권 위반 여부를 확인하는 기술로서 이러한 기술을 오디오 지문인식 (Audio Fingerprinting) 기술이라고 부른다. 이러한 기술을 기반으로 저작권 위반으로 판단되는 음원을 다운로드나 재생을 자동으로 제한하는 기술이다 [9].

• 유해 콘텐츠 분류 기술 : 유해 콘텐츠 분류 기술에 대해 다양한 연구가 되고 있으며, 가장 근접해 있는 기술은 텍스트, 이미지, 음원이나 동영상 콘텐츠를 분별하고 필터링하는 기술이다. 이는 다양한 디지털 콘텐츠의 유형을 분류하고 해당 콘텐츠의 유해 정도를 판별하여 디지털 콘텐츠의 오남용 사례를 방지하기 위함이다. 이렇게 다양한 형태의 유해 정보를 막기 위해서는 정보의 기본 요소인 텍스트와 이미지의 유해성을 판단하고 차단하는 기술이 필요하다. 특히 인터넷의 통신 속도 향상과 미디어 저장 용량의 증가로 인해 유해 정보의 콘텐츠 유형이 문자 형태에서 이미지 형태로 급속히 변화되고 있는 상황과 전 세계에 산재한 외국의 유해 사이트를 효과적으로 차단하기 위해서는 언어에 대한 종속성을 갖는 텍스트 기반의 유해 정보 분류 기술보다 이미지 기반의 유해 정보 분류 기술 개발이 시급하다.

3-4 IPTV 콘텐츠 보호 기술

IPTV 환경에서 가장 중요한 기술 중의 하나가 제공되는 정보를 불법시청이나 불법 대량 복제 등을 막기 위한 콘텐츠 보안기술이다.

현재 가장 많이 사용되고 있는 방식으로는 정보의 수신을 제한함으로써 시청 자격이 있는 이용자들만 시청하도록 하는 CAS와 제공되는 콘텐츠의 이용 권한을 관리함으로써 콘텐츠를 보호하는 DRM 방식 등이 있다. 이들 방식은 각기 장단점을 가지고 있어, IPTV 콘텐츠 보호 기술에서는 병행하여 사용하고 있다 [10].

Ⅳ. 콘텐츠 보호 기술기준 항목

본 장에서는 디지털 콘텐츠 오남용 방지를 위한 콘텐츠 보호 기술 기준을 위한 중요 항목을 도출한다.

4-1 악성 코드 방지 기술

현재 인터넷 콘텐츠를 통한 악성코드에 대한 방지 기법은 대부분 백신이나 실시간 감시 기능 및 OS 보

안 업데이트 등 수동적인 방법에 국한하고 있다. 실질적으로 악성코드를 발견하는 방법은 너무도 다양하기 때문에 본 연구에서는 악성코드 방지 기술 혹은 기법에 대한 가이드라인 차원에서 기술 기준을 위한 중요 항목을 아래와 같이 고려할 수 있다.

- 악성코드가 의심되는 특정 사이트 필터링
- 사용자 PC 실시간 감시
- 사용자 PC 보안 설정 기능
- 악성코드 탐색 기능
- 악성코드 삭제 처리 기능
- 악성코드 분류 기능
- 특정 포트 차단 기능
- OS 보안 패치(업데이트) 기능
- 기타 보안 요구사항

4-2 불법콘텐츠 유포 방지 기술

현재 DRM과 같은 불법콘텐츠 유포 방지 기술 등에 대한 기술 기준은 전무한 상태이며, MPEG이나 OMA와 같은 표준을 따라 개발하거나 MS DRM(WMRM)등과 같은 산업적 표준 모델을 기반으로 개발되어 서비스 되고 있다. 콘텐츠 오남용 사례가 대부분 P2P나 개인 블로그, 카페 등을 통해 유출되어 전파되는 만큼 관련 서비스에서는 불법 콘텐츠 유포 방지 기술을 반드시 적용해야할 것으로 판단된다.

본 논문에서는 불법콘텐츠 유포 방지 기술기준 항목은 DRM을 기준하며 아래와 같이 고려할 수 있다.

- 암호화 기술 (Encryption/Decryption)
- 콘텐츠 식별체계 (Identifier)
- 권한 통제기술 (Right Enforcement)
- 사용내역 관리기술 (Event Reporting)
- 키 관리 기술 (Key Management)
- 콘텐츠 메타데이터 (Metadata)
- 템퍼링 방지기술 (Tamper Resistance)
- 인증폐기 (Revocation)
- 콘텐츠 패키저 (Secure Container)
- 권리표현기술 (Right Expression)
- 인증기술 (Authentication)
- 인증 취소 (Renewability)
- 유통 보안 (Security)
- 권한정책관리 (Policy Management)

4-3 필터링 기술

현재 필터링 기술의 대부분은 웹 콘텐츠나 게시물에 대한 필터링과 콘텐츠의 접근 제어 등을 이용한 기술이 대부분이다. 하지만 디지털 콘텐츠의 형태가 다양하고 그에 따른 기술 또한 어느 한가지로 단정지어 정의할 수 없기 때문에 현재 연구개발 되고 있는 기술을 토대로 중요 항목을 다음과 같이 고려한다.

- 유해 콘텐츠 판별 기술
- 인터넷 유/무해 정형화 기술
- 규칙 기반 텍스트 분류 기술
- 학습 기반 텍스트 분류 기술
- 유해 콘텐츠 전처리 기술
- 유해 콘텐츠 특징 추출 기술
- 유해 콘텐츠 처리 및 관리 기술

4-4 IPTV 콘텐츠 보호 기술

현재 IPTV와 관련된 표준화는 TTA 등을 통해 활발히 진행되고 있다.

본 논문에서는 콘텐츠 오남용을 방지하기 위한 기술로서 CAS에 한하여 기술기준 중요 항목을 다음과 같이 고려한다.

- 제한 수신 모듈의 식별
- 채널 복제 방지 기술
- 콘텐츠 자원 관리
- 복제 방지(Copy Protection)
- 제한수신모듈 펌웨어 업그레이드
- 단말 및 사용자 인증
- 복사방지 장치
- 보안 전송 프로토콜
- 상호인증/메시지 프로토콜
- 보안 요구사항

Ⅴ. 결론 및 향후계획

지식정보의 디지털화는 정보의 효율적 관리 및 신속한 전달 등 여러 가지 장점을 가지고 있지만, 콘텐

츠의 오남용 및 프라이버시 침해 등 온라인 보안문제를 발생시키고 있다.

본 논문에서는 악성코드, 불법콘텐츠 유포, 개인정보유출, 악성 댓글, 청소년 유해 콘텐츠, IPTV 콘텐츠 불법 사용 등의 콘텐츠 오남용 사례에 대해 살펴보았다. 또한, 악성코드 방지 기술, 인터넷 콘텐츠, 개인정보유출 방지 기술, 필터링, 청소년 유해 콘텐츠 방지 기술, IPTV 콘텐츠 보호 기술 등 콘텐츠 보호 기술을 분석을 통하여 온라인상의 디지털 콘텐츠의 오남용을 방지하고 디지털 콘텐츠의 안전한 보호를 위한 콘텐츠 보호 기술기준 중요 항목을 제안하였다. 향후 본 논문에서 수립한 중요 기술기준 항목을 바탕으로 보호기술 기준을 수립하면 보다 효율적이고 체계적인 기준이 될 것으로 기대된다.

참 고 문 헌

[1] 지디넷 코리아, http://www.zdnet.co.kr

[2] 세계일보, http://www.segye.com

[3] 뉴스엔, www.newsen.com

[4] 베타뉴스, http://www.betanews.net

[5] 경호갑, “국제 DRM 표준화 동향 분석 및 대응전략”, *정보과학 학회지*, 제23권 8호, pp. 15-24, 2005. 9.

[6] 정준영, 구한승, 권은정, 권오형 “제한수신 기술 및 표준화 동향 분석”, *ITFIND 주간기술동향*, 통권 1214호, pp. 1-14, 2005. 9.

[7] I. Cox, J. Killian, T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for multimedia”, *IEEE Trans. Image Processing*, Vol.6, pp. 1673-1687, Dec. 1997.

[8] 남기효, “웹 프라이버시 필터링 및 스캐닝 제품 분석”, *ITFIND 주간기술동향*, 통권 1284호, pp. 13-20, 2007. 2.

[9] 컴퓨터프로그램보호위원회, “SW IPReport”, *SW 지적재산권 동향*, 제46호, pp. 1-3, 2008. 12.

[10] KBS 방송기술연구, DTV 콘텐츠 저작권 보호기술 및 동향, pp. 9-27, 2007

홍 성 혁 (洪成赫)

2008년 2월 : 경남대학교 컴퓨터공학부 (공학사)

2008년 3월~현재, 경남대학교 컴퓨터공학부 석사과정

관심분야 : ISMS, 정보보증, DRM, RFID

윤 은 준 (尹恩準)

1995년 2월 : 경일대학교 컴퓨터공학과 (공학사)

2003년 2월 : 경일대학교 컴퓨터공학과 (공학석사)

2007년 2월 : 경북대학교 컴퓨터공학과 (공학박사)

2007년~2008년: 대구산업정보대학 컴퓨터정보계열 전임강사

2009년 3월~현재: 경북대학교 전자전기컴퓨터학부 계약교수

관심분야 : 암호학, 정보보호, 유비쿼터스보안 등

한 재 홍 (韓在鴻)

2006년 2월 : 한신대학교 컴퓨터공학과 (공학사)

2008년 2월 : 한양대학교 컴퓨터공학과(공학석사)

2007년 12월 ~ 현재 : 한국정보보호진흥원 주임연구원

관심분야 : RFID/USN 보안, 콘텐츠 보호, S/W 개발 보안

박 종 혁 (朴鍾爀)

2001년 2월: 순천향대학교 컴퓨터공학부 (공학사)

2003년 2월: 고려대학교 정보보호대학원 정보보호학과 (공학석사)

2007년 2월: 고려대학교 정보보호대학원 정보보호학과 (공학박사)

2002년 12월~2007년 7월: 한화에스앤씨(주) 기술연구소 선임연구원

2007년 9월~현재: 경남대학교 컴퓨터공학부 전임강사

관심분야 : 디지털포렌식, DRM, 접근제어, 유비쿼터스 컴퓨팅 & 보안, 지능형 홈 서비스, 멀티미디어 보안 및 서비스