디지털 콘텐츠의 정보보호 분석 모델

윤석규* · 장희선**

요 약

본 논문에서는 디지털 콘텐츠에 대한 안전하고 신뢰성 있는 유통, 전달, 취약성 점검을 위한 정보보호의 자동분석 방법을 위한 네트워크 구조와 분석 모델을 제시한다. 제시된 네트워크에서는 firewall과 IDS(Intrusion Detection System)를 이용하며, 자체적인 위협을 평가하기 위한 에이전트를 활용하는 방안을 제시하며, 주요 기능으로는 보안 범위 선정, 관련 데이터 수집/분석, 수준 평가 및 대책 제시 등을 포함한다. 효율적인 자동화 분석 모델을 개발하기 위해서는 콘텐츠의 상호 유통과 웹서버-사용자간 트래픽 분석에 기초한 네트워크의 설계와 정보보호 및 자동분석 알고리즘의 개발 그리고 효율적인 DRM/PKI 등의 도구 개발이 필요함을 알 수 있다.

An Information Security Model for Digital Contents

Seuk-Kyu Yoon* · Hee-Seon Jang**

ABSTRACT

The network architecture and analysis model for evaluating the information security are presented to distribute the reliable and secure multimedia digital contents. Using the firewall and IDS, the function of the proposed model includes the security range, related data collection/analysis, level evaluation and strategy proposal. To develop efficient automatic analysis tool, the inter-distribution algorithm and network design based on the traffic analysis between web-server and user are needed. Furthermore, the efficient algorithm and design of DRM/PKI also should be presented before the development of the automatic information security model.

Key words : DRM(Digital Rights Management), Contents Security

접수일 : 2010년 6월 14일; 채택일 : 2010년 9월 12일

* 평택대학교 컴퓨터학과
** 평택대학교 e-비즈니스 및 창업

1. 서 론

최근 컴퓨터와 정보통신 기술의 급속한 발전으로 인해 기존 텍스트 위주의 사용자 환경에서 벗어나 이미지, 그래픽, 오디오 및 비디오 데이터 등을 제공하는 멀티미디어 사용자 환경으로 변하고 있다. 인터넷의 대중화, 무선 네트워크의 활성화, 그리고 모바일 기기의 활용 증대와 함께 다양한 서비스와 디지털 콘텐츠의 융합에 따른 디지털 콘텐츠 서비스 기술이 하루가 다르게 발전하고 있다. 국내 디지털 콘텐츠 산업의 매출 규모는 조사를 처음 시작한 2003년 5조 7,721억 원을 기록한 이래 연평균 14.7%의 높은 성장률을 기록하며 2007년에는 10조 67억 원에 이른 것으로 나타났다[8, 9]. 이는 이전에 비해 성장률이 크게 둔화된 것으로 나타나고 있으나, 국내 전체 경제 성장률이 4.7%임을 감안하면 여전히 높은 성장세이며 금액적으로 매출 규모 10조원을 돌파하였다는데 큰 의미를 가지고 있다.

이러한 디지털 콘텐츠 산업의 발전과 더불어 크게 이슈화되고 있는 것이 멀티미디어 콘텐츠 보안이다. 디지털 정보는 여러 번의 복사에도 원본과 동일한 품질 상태를 유지할 뿐만 아니라 초고속망을 통해 광범위한 지역으로 신속하게 배포가 가능하고, 정보의 변경이 용이하다는 특성으로 인해 불법 복제 및 위/변조 등과 같은 각종 보안 위협에 쉽게 노출되어 있어 이에 대한 보안이 주요 이슈가 되고 있다. 최근 국내외에서 발생되고 있는 일련의 전산망 보안 침해 사고들에 대한 대책을 응용 기술의 발전에 맞추어 준비해야 할 문제임은 틀림이 없다[1, 3]. 인터넷 활용의 증가에 따른 편리함에 비례하여 역기능 요소 또한 증가해 이에 따른 보안관리가 체계적으로 이루어져야 한다. 미국을 비롯한 정보 선진국들의 주요 기관에서는 응용 환경에 적합한 안전성과 보안 수준 유지를 위해 보안관리 도구를 개발하여 활용하고 있고, 이에 관한 기술요건과 요구사항을 문서화하여 보안 관리의 정책과 모든 정보자원 보안 관리의 지침으로 활용되고 있다. 반면, 국내의 경우는 정보원에 대한 보안 관리 정책과 보안 관리 도구, 그리고 보안 분석 방법 등 보다 적극적이고 광범위한 보안 관리 방안이 매우 미흡한 실정이다[7].

이러한 상황 하에서 본 논문에서는 최근 그 사용량이 폭발적으로 대두되고 있는 사용자와 웹 서버 사이의 멀티미디어 정보에 대한 디지털 콘텐츠 정보보호 방법론을 제시하고 이에 대한 보안성을 자동으로 분석할 수 있는 자동분석 도구의 설계 방법론을 제시하고자 한다. 제시된 분석 방법 도구를 이용하여 자산분류 평가, 위협 평가, 취약성 평가, 위험 측정, 보안 대책 선택 및 비용 효과 분석 등의 기능을 처리할 수 있다.

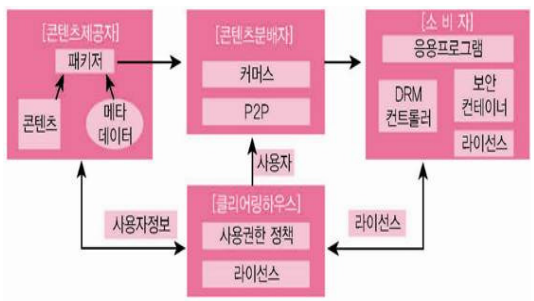
2. 정보보호 기술

정보보호란, 정보통신망의 마비, 개인정보의 유출, 불건전 정보의 유통 등 정보통신 환경을 저해하는 위협과 부작용에 대응할 수 있도록 정보통신 시스템 및 데이터의 기밀성(정보유출 방지), 무결성(데이터 위조 및 변조 방지)을 유지하고 시스템의 가용성을 보장하는 기술을 의미한다[5]. 정보보호 기술은 사용자 측면에서 개인정보 및 프라이버시 제공, 서비스 및 디바이스 측면에서 안전한 신뢰 서비스 제공, 인프라 환경 측면에서 끊김 없고 이동성이 지원되는 안전한 인프라를 제공하는 기술로 제공된다. 그 분류는 보는 관점에 따라 다양하게 분류(관리적 보안, 물리적 보안, 기술적 보안)된다. 네트워크/응용 보안 기술은 다양한 IT 인프라, 디바이스 및 서비스에 대한 안전성 및 신뢰성을 제공하기 위한 기술을 의미하며, 사용자의 접근 제어, 권한 관리, 유출 방지 및 데이터 암호화의 주요 기능을 수행한다. 여기서 대표적인 유출방지 기술에는 DRM(Digital Rights Management), 워터마킹,

finger printing, steganography의 형태로 나눈다.

DRM은 암호화 기술을 이용하여 디지털 콘텐츠의 지적 자산에 대한 권리를 지속적으로 관리 및 보호하는 기술로 허가되지 않은 사용자로부터 콘텐츠의 접근 및 이용을 불가능하게 통제하는 수단을 제공한다. DRM은 (그림 1)과 같이 패키저, 컨테이너, 클리어링 하우스, 컨트롤러 등으로 구성되어 있으며 주요 기능을 요약하면 다음과 같다[8].

- 패키저(packager) : 콘텐츠를 메타 데이터와 함께 배포 가능한 단위로 묶는 기능으로 보안 컨테이너로 포장된다.
- 보안 컨테이너(secure container) : 원본을 안전하게 유통하기 위한 전자적 보안 장치이다.
- 클리어링 하우스(clearing house) : 콘텐츠 배포 정책 및 라이선스의 발급을 관리한다.
- 컨트롤러(controller) : 배포된 콘텐츠의 이용권한을 통제한다.



(그림 1) DRM 구성도

DRM의 대표기술인 워터마킹(Watermarking)[2, 4]은 텍스트, 이미지, 비디오, 오디오 등의 데이터에 원 소유주만이 아는 마크를 사람의 육안이나 귀로는 구별할 수 없게 삽입하고 이를 네트워크에서 제공한다. 만약 사용자들이 멀티미디어 디지털 정보를 불법 복제하여 정당한 대가나 허락 없이 상업용 혹은 기타 용도로 사용되었을 때는 자신의 마크를 추출함으로서 자신의 소유임을 밝힐 수 있다. 디지털 콘텐츠의 권리 관리 분야에 대한 기술 요소 및 내용을 요약하면 <표 1>과 같다.

〈표 1〉 디지털 콘텐츠 보호 요소 기술

구 분	요소 기술	세부 기술
접근 차단 보호	콘텐츠 패키징	콘텐츠 패키징 구조선언 파일 포맷 설계 복합 콘텐츠 패키징 콘텐츠 암호화 및 키 관리
	권리 표현	권리 데이터 사전 XML 기반 동적 사용규칙 범용 REL 파서 설계 구현 저작권 관계 표현 권리 정보 저장 및 관리
	복제 방지	디바이스 인증 비밀키 교환
	도메인 내 권한 관리	도메인 합류/탈퇴 처리 가상 도메인 구성
저작권 보호	워터 마킹 핑거프린팅	실시간 핑거프린팅 삽입 공격 및 평가
연동 관리	IPMP 인터페이스	표준 인터페이스 DRM adaption
	콘텐츠 식별	식별자 구문 구조 및 전환 식별 메타데이터 관리
	DRM 도메인간 상호연동	상호 인증 처리 DRM 모듈 폐기 처리

한편, DRM의 표준화가 본격적으로 거론되기 시작한 시점은 2000년 초부터라고 할 수 있다. 당시 인터넷의 급속한 확산과 온라인 음악 및 e-Book의 전자상거래가 새로운 디지털 콘텐츠 산업의 수익원으로 부상하게 되자 많은 DRM 제품이 시장에 출시되었다. 그러나 DRM 업체들은 각각 고유한 기술을 이용하여 제품을 내놓았기 때문에 제품 간의 호환성이 제공되지 않았다. MPEG-21, OeBF, SDMI 등은 DRM 제품간 상호 호환성이 갖추어 지지 않고는 시장의 활성화가 어렵다고 판단되어 DRM의 표준화를 위해 설립된 국제적 표준화 단체이다.

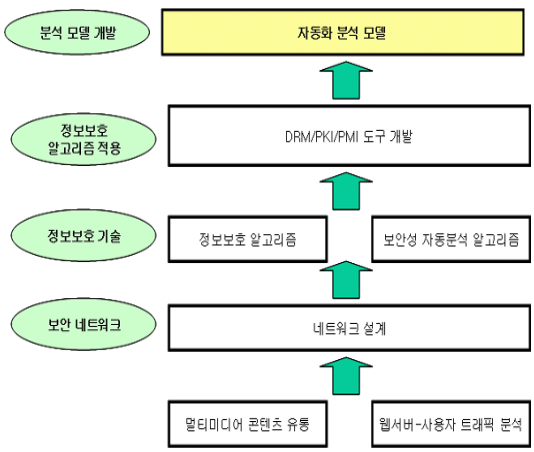
지금까지의 DRM 표준화 진행 현황을 요약하면 <표 2>와 같다[1, 4, 6].

〈표 2〉 DRM 표준화 현황

기술 분야	표준 단체	주요 내용
Copy Protection	CPTWG	DVD, 디지털 방송 분야의 복제 방지기술 표준화 포럼
	Smart Right	디지털 홈 환경에서의 디지털 콘텐츠 복제 방지 기술
	SVP	디지털 홈 환경에서의 디지털 콘텐츠 복제 방지 기술
	AACP	HD DVD의 복제 방지 기술
	OpenCable CPT	케이블 방송의 복제 방지 기술
	4C CPPM/ CPRM	저장장치에 저장되는 디지털 콘텐츠의 복제 방지 기술
	5C DTCP	디지털 전송 채널을 통해 디바이스 간에 전송되는 디지털 콘텐츠의 복제 방지 기술
	HDCP	디지털 디스플레이 장치로 전송되는 디지털 영상신호의 복제 방지 기술
	DVD CCA	DVD의 복제 방지 기술
CAS	NGNA	차세대 디지털 케이블 기술 규격 개발
	DVB CA	디지털 방송 콘텐츠의 보호를 위한 수신권한 제어 기술
	ATSC CAS	지상파 디지털 방송 콘텐츠의 수신권한 제어 기술

3. 자동화 분석 모델

멀티미디어 콘텐츠 정보 보안 분석을 위해 정량적인 방법(위협 평가, 취약성 평가 등)과 정성적인 방법으로 크게 나눌 수 있다. 위협 평가는 각 위협들의 발생 빈도 및 위협 정도를 측정하는 것으로 위협 요소의 발생빈도, 충격을 주는 자산의 범위, 그리고 시스템에서 평가된 자산 가치와 위협이 발생하였을 때 입는 자산의 손상율에 의해 결정되며, 평가의 결과는 보안 대책의 수립에 기초가 된다. 반면, 보안의 취약성은 자산, 위협, 위협에 따른 영향 등과 밀접한 관련을 갖는다. 따라서 취약성 평가시 위험분석의 타 평가와 연관성이 고려되어져야 하며, 양적 및 질적 평가가 동시에 결정되어야 한다. 이런 정량적 분석 방법은 위협 발생이 피해 정도를 산술적으로 산출할 수 있다는 장점이 있으나, 정확한 정량화 수치를 구하기 어렵다는 단점을 갖고 있다. 반면, 정성적 방법에는 위험을 수량화하지 않은 기술변수로 나타냄으로서 수량화가 가져오는 오차를 줄이고 분석 과정에서 전문가의 의견을 최대로 반영할 수 있다는 장점이 있다. 디지털 콘텐츠의 정보보호 자동 분석을 위한 개발 절차를 요약하면 (그림 2)와 같다.



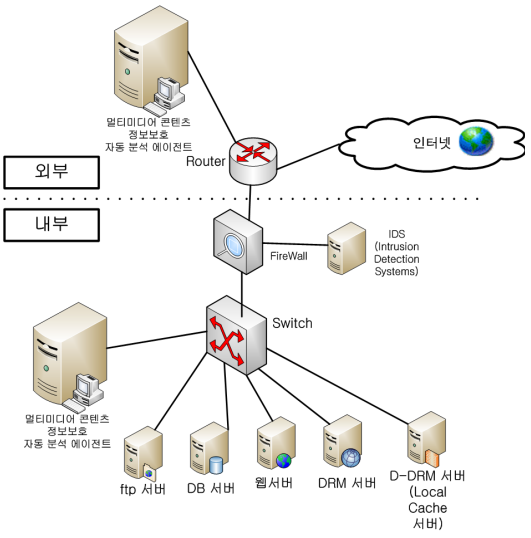
(그림 2) 자동화 분석 모델 개발 절차

크게 두 가지 정보보호 기술은 정보보호 알고리즘 개발과 보안성 자동분석 알고리즘 개발을 포함한다. 디지털 콘텐츠 유통을 위한 네트워크 경로상에서 웹서버와 사용자 사이의 트래픽에 대한 정보보호 알고리즘은 운영중인 네트워크의 구조를 분석하고 분석 결과를 토대로 DRM/PKI/PMI 등의 도구를 개발하며, 보안성 자동분석 알고리즘을 적용하여 효율적인 자동화 분석 모델을 개발하여야 한다. 자동화 분석 도구에서는 향후 보안 관련 표준화 기관에서 요구하는 다양한 보안 분석 기준이 제시된다면 이 기준을 만족하는 분석 도구로서 수정되어 국내 정보보호 산업과 정보 시스템 보안

관리 체계를 수립하는데 기여할 수 있다. 정보보호를 위한 자동화 분석 도구의 주요 기능을 요약하면 <표 3>과 같다[7-9].

〈표 3〉 자동화 분석 도구의 기능

분석 모듈	주요 기능
범위 선정	◦ 위험 분석 대상 선정 ◦ 전산망의 규모 파악 ◦ 자동화 자산 식별 ◦ 데이터베이스 지정
데이터 수집	◦ 정보 시스템 활용 ◦ 자동검색, 취약성 항목 설정 ◦ 취약성 검사 방법 설정
자료 분석	◦ 자동화된 자료 취합 ◦ 취약성 평가 정보 수집 ◦ 자동화된 자료 취합 알고리즘
기법 적용	◦ 자산가치 평가 ◦ 보안성 및 취약성 평가 ◦ 보안대책 효과 평가
수준 평가	◦ 보안대책 항목 설정 ◦ 자동 검색, 접근 통제 보안
대책 제시	◦ 네트워크 관리 보안 대책 ◦ 사용자 인증 보안 ◦ 익명 보안 대책



(그림 3) 정보보호 구조

본 논문에서 제시하고 있는 디지털 콘텐츠의 정보보호를 위한 시스템 구조를 나타내면 (그림 3)과 같다.

정보보호 구조의 성능을 평가하기 위하여 디지털 콘텐츠 정보보호 자동 분석 에이전트는 외부⇒내부로 가상의 위협 메시지를 보내고 내부의 시스템과 네트워크들이 유기적으로 반응하는지를 조사하게 된다. 그리고 내부⇒내부에서는 에이전트로부터 각각의 서버로 특히 DRM 서버와 분산형 DRM (D-DRM) 서버로 위협 메시지를 처리하는 과정을 분석한다. 마지막으로 내부⇒외부로 시스템과 네트워크를 통한 위협 항목들을 점검하는 시나리오 형태의 디지털 콘텐츠 정보보호 자동분석 도구를 구현한다.

4. 결 론

최근 인터넷 활용이 증가함에 따라 국내외에서 발생되고 있는 일련의 시스템 보안 침해 사고들에 대한 보안관리가 중요한 문제가 되고 있다. 일반적으로 보안 정책 구현을 위한 보안 제품이 알려지지 않은 보안 취약점을 가지고 있을 경우, 이런 시스템을 사용하는 조직은 중요한 정보를 안전하게 보호하지 못하고 누출, 파괴, 위변조와 같은 예상치 못한 보안 문제가 발생할 수 있다. 국내의 경우는 보안 관리 방안이 미흡한 실정이며, 특히 보안관리 정책, 보안관리 도구, 보안 분석 방법 등을 포함한 전반적인 시스템, 네트워크 보안 관리 방안이 시급히 필요한 실정이다. 특히 정보통신 기술의 급속한 발전으로 인해 기존의 텍스트 위주의 환경에서 벗어나 이미지, 그래픽, 오디오 및 비디오 데이터 등을 제공하는 멀티미디어 사용자 환경으로 변화하고 있다. 이러한 디지털 멀티미디어 콘텐츠 시장의 발전과 더불어 크게 이슈화되고 있는 것이 바로 콘텐츠 보안이다. 디지털 정보는 여러 번의 복사에도 원본과 동일한 품질 상태를 유지할 뿐만

아니라 초고속망을 통해 광범위한 지역으로 신속하게 배포가 가능하고, 정보의 변경이 용이하다는 특성으로 인해 불법 복제 및 위변조 등과 같은 각종 보안 위협에 쉽게 노출되어 있다.

이러한 배경 하에, 본 논문에서는 디지털 콘텐츠에 대한 안전하고 신뢰성 있는 유통, 전달, 취약성 점검을 위한 정보보호의 자동분석 방법을 위한 네트워크 구조와 그 모델을 제시하였다. 콘텐츠의 정보보호를 위한 자동화 분석 도구를 위하여 보안 시스템 관리 자동화 도구 서버를 활용하는 방안을 제시하며, 여기에서는 외부에서 침입하는 위협 요소를 가상으로 설정하여 내부로 침입시 DRM과 D-DRM 서버의 취약성을 점검하고 보안 방어의 수준을 평가하는 방법을 제시하였다. 향후 제시된 도구를 통하여 융복합 서비스 및 다른 기기를 사용한 서비스를 상호 교환하는 환경과 정보보호 알고리즘을 이용한 콘텐츠의 정보보호 방안에 대한 연구가 필요하다.

참 고 문 헌

[1] AAP, Digital Rights Management for Ebooks : Publisher Requirements Version 1.0, 2000.

[2] BSI, BS 7799, Code of Practice for Information Security Management, 1997.

[3] Content Guard, Content Guard DRM Solution Overview, 2000.

[4] Danny Bradbury, “Decoding Digital Rights Management”, Computer and Security, Vol. 26, 2007.

[5] ISO/IEC JTC1/SC27, TR13335-1, Guidelines for the Management of IT Security(GMITS) : Part 1-Concepts and Models for IT Security, 1996.

[6] Joshua Duhl and Susan Kevorkian, Understanding DRM Systems : An IDC, White Paper, 2001.

[7] 김점구, 김태은, “CDN 환경에서 콘텐츠 보안 방법 연구”, 정보보안논문지, 제8권, 제3호, 2008.

[8] 손병희, 장종찬, 유비쿼터스 개론 : 개념과 기술, ITC, 2009.

[9] 김영철, “멀티미디어 정보보호”, 한국멀티미디어학회논문지, 제8권, 제5호, 2005.

윤 석 규

전북대학교 컴퓨터학과(공학박사)
현재 평택대학교 컴퓨터학과 교수
관심분야 : 컴퓨터 구조

장 희 선

KAIST 산업공학과(공학박사)
현재 평택대학교 경상학부 교수
관심분야 : 트래픽 엔지니어링