DRM 기술로 보호된 컨텐츠의 융통성 있는 공유를 위한 멤버/그룹 라이선스 메커니즘

장 혜 진†

요 약

라이선스 메커니즘은 DRM(Digital Rights Management) 시스템의 핵심 요소 중의 하나이다. 라이선스 메커니즘은 DRM 시스템의 자원(resources), 자원의 사용 주체(principals), 자원에 대한 사용 규칙(usage rules) 등을 명확하게 식별하고 강제하기 위한 핵심적인 기능을 담당하도록 설계된다. 하지만 기존의 라이선스 메커니즘들은 가정이나 회사의 어떤 부서와 같은 그룹 내의 멤버들이 어떤 컨텐츠를 공유하고자 할 때 공유에 관련된 융통성이 부족하다. 본 논문은 그룹에 등록된 여러 명의 멤버들이 DRM 기술로 보호된 디지털 컨텐츠를 안전하고 융통성 있게 공유할 수 있도록 하는 새로운 라이선스 메커니즘을 제안한다. 본 논문이 제안하는 멤버/그룹 라이선스 메커니즘은 그룹 라이선스, 멤버 라이선스, 허가들(grants)간의 파생 관계 등의 개념들을 도입하여 기존의 라이선스 메커니즘을 확장한다.

Member/Group License Mechanism for Secure and Flexible Sharing of Protected Contents in DRM Systems

Hai Jin Chang†

ABSTRACT

License mechanisms are the key elements in almost all DRM(digital rights management) systems. The license mechanisms are designed for the clear identification and enforcement of contents, principals, and usage rules in DRM systems. But current license mechanisms are lacking in the flexibility for the secure and efficient sharing of the contents among the members of a group such as a family or a part of an enterprise. This paper suggests a new license mechanism for efficient and secure sharing of contents in DRM systems among the members of a group. We named it member/group license mechanism. The mechanism extends the current license mechanisms by introducing new concepts such as group licenses, member licenses, and derivation relationships between licenses.

키워드 : DRM, 권리 기술(Rights Management), 라이선스(License), 컨텐츠 공유(Content Sharing), 식별(Identifier), 권리 언어(Rights Language), MPEG-21

1. 서 론

IDC의 DRM 전망 보고서[1]에 의하면, DRM 기술이란 "합법적인 사용 및 사용자로 디지털 컨텐츠의 사용을 한정하고, 컨텐츠의 전체 생명주기를 통하여 디지털 컨텐츠의 사용의 결과를 관리하기 위한 하드웨어, 소프트웨어 서비스 및 기술들의 체인"이며, DRM 산업은 고속 성장이 예상되는 중요한 산업이다. DRM 기술은 DOI(Digital Object Identifier)[2], URI(Uniform Resource Identifier)[3]와 같은 디지털 컨텐츠의 식별(identification) 기술, 공개키 암호(public key cryptography) 기술[4]과 같은 디지털 컨텐츠의 보호를 위한 보안 기술, 다양한 디지털 컨텐츠의 효과적인 압축 및 재생(play)을 위한 기술, 디지털 컨텐츠의 배포와 판매에 관련한 네트워크 기술 및 유통 관련 기술 등의 다양한 기술들의 통합을 필요로 하는 종합적 기술이다.

라이선스 메커니즘은 DRM 시스템의 핵심 요소이다. DRM 시스템에서는 일반적으로 디지털 컨텐츠에 대한 허가(grants)를 명확하게 표현하기 위하여 라이선스 메커니즘을 사용한다. DRM 시스템의 권리 기술 언어(rights description language)의 표준으로 자리매김하고 있는 XrML(eXtended rights Markup Language)[5]을 기준으로 표현한다면, 라이선스는 라이선스 발급자(issuer) 정보와 허가 정보 등으로 구성되며, 허가 정보는 주체(principal), 자원(resource), 조건(condition), 권리(right)로 구성된다.

컨텐츠를 사용자들의 그룹 단위로 구매하여 그룹 내의 멤버들 간에 융통성 있게 공유할 수 있다면, 본 논문의 제 2장

※ 본 연구는 상명대학교 2004년도 교내연구비 지원에 의하여 연구되었음.
† 정 회 원 : 상명대학교 컴퓨터소프트웨어 교수
논문접수 : 2004년 5월 3일, 심사완료 : 2004년 8월 31일

에서 기술되는 바와 같이, 컨텐츠 구매에 관련한 총비용의 절감, 컨텐츠의 사용의 편리, 그리고 컨텐츠 사용을 위한 멤버의 신원 확인의 용이함 등의 장점이 생길 수 있다. 하지만 기존의 라이선스 메커니즘은 컨텐츠를 그룹 단위로 구매하여 그룹 멤버들 간에 효과적으로 공유하는 것을 지원하지 못한다. 예를 들어보자. 컨텐츠 c를 필요로 하는 3명의 멤버 p_1, p_2, p_3로 구성된 어떤 그룹 G가 존재한다고 하자. 그룹 G의 멤버들이 컨텐츠 c를 융통성 있게 총 10회 사용할 수 있는 사용 권한을 라이선스로 표현하려고 한다고 하자. 예를 들어 c를 총 10회까지 사용할 수 있지만 p_1이 총 5번, p_2가 총 3번, p_3가 총 2번 사용할 수도 있고, p_1이 총 3번, p_2가 총 2번, p_3가 총 5번 사용할 수도 있어야 한다고 하자. 이렇게 3명의 멤버 p_1, p_2, p_3 각자 최대 10회까지 c를 사용할 수 있지만 그룹 G의 멤버들의 c의 사용의 총 횟수는 10회 이내가 되어야 하는 .융통성 있는 허가를 어떻게 표현하고 강제할 것인가. XrML과 같은 기존의 라이선스 언어나 라이선스 메커니즘에서는 위와 같은 허가를 표현하기 어렵다. 왜냐하면 라이선스에 그룹 내의 주체들 간의 자원의 공유에 관련된 동적인 상호 관련성을 표현하기 어렵기 때문이다.

라이선스 표현 언어는 다양한 종류의 허가를 융통성 있게 표현할 수 있도록 설계되어야 한다. 왜냐하면, DRM 시스템의 다양한 사용자들은 여러 종류의 자원들의 사용에 대한 여러 가지 조건의 다양한 종류의 허가들을 요청할 것이기 때문이다. 허가에 대한 제약된 표현력을 갖는 라이선스 체계는 DRM에 관련된 비즈니스 모델들을 다양하게 지원할 수 없다.

본 논문은 그룹 라이선스, 멤버 라이선스, 허가간의 파생 관계(derivation relationship) 등의 새로운 개념들과 자원의 공유에 필요한 관련된 절차들의 도입을 통해 기존 라이선스 메커니즘을 확장하여 그룹에 의해 구매된 자원을 그룹의 멤버들이 융통성 있게 공유할 수 있도록 하는 허가를 지원하는 라이선스 메커니즘을 제시한다. 제시한 메커니즘에서, 멤버 라이선스는 발급 요청이 있을 때마다 그룹 라이선스로부터 파생되어 생성되며 생성된 각 멤버 라이선스의 허가는 개념적으로 그룹 라이선스의 허가의 범위를 넘지 못한다. 본 논문의 제 2장은 관련 기술들 및 기존 라이선스 메커니즘의 문제점에 대한 내용이다. 제 3장은 제안하는 멤버/그룹 라이선스 메커니즘의 근거를 이루는 개념들을 규정한다. 제 4장은 제 3장의 개념들을 기반으로 하여 제안한 라이선스 메커니즘의 동작 절차 및 구현에 대하여 논의한다. 제 5장은 결론 및 향후 연구에 대해 기술한다.

2. 관련 기술 및 기존 라이선스 메커니즘에서의 컨텐츠 공유 문제

라이선스 메커니즘을 지원하기 위한 권리 표현 언어는 허가(grant)를 명확하게 표현할 수 있어야 한다. 라이선스의 주체와 자원은 명확히 식별될 수 있어야 하며, 컨텐츠의 사용에 관련된 조건 및 권한도 모호함이 없이 표현되어야 한다. 허가의 주체는 사람일 수도 있고 장비일 수도 있다. 권리 표현 언어의 개발 및 표준화를 위해 활동하고 있는 단체에는 MPEG-21 그룹과 OMA(Open Mobile Alliance), METS (Metadata Encoding & Transmission Standard) 위원회 (www.loc.gov/standards/mets/), CreativeCommons(www.creativecommons) 등이 있다[6, 7]. MPEG-21그룹은 XrML 버전 2.0[8]에 근거한 표준 권리 표현 언어를 제안하고 있으며, OMA는 ODRL(Open Digital Rights Language)[9]에 근거한 모바일 환경을 위한 권리 표현 언어를 제안하고 있다. CreativeCommons는 HTML 문서, 디지털 오디오 파일들과 같은 공개된 웹상의 자원들에의 접근을 위한 권리 표현 언어를 제안하고 있으며, METS 위원회는 디지털 객체들의 라이브러리를 관리하기 위한 언어인 METSRights 언어[10]를 제안하고 있다.

XrML과 ODRL은 범용 권리 표현 언어이며 권리 표현을 위한 풍부한 어휘를 지원한다. XrML은 처음에 표준화 단체가 아닌 ContentGuard사(www.contentguard.com)에 의해 개발되었지만, 표준화 절차를 통해 현재 권리 표현 언어의 실제적인 표준으로 자리매김하였다. XrML은 마이크로소프트 등의 다양한 업체들의 DRM 시스템에서 사용되고 있다. XrML은 강한 표현력을 제공하며, 호환성이 높으며, 잘 설계된 권리 표현 언어(right expression language)로 평가되고 있다. ODRL은 처음에 IPR Systems 사에서 개발되었으나 현재는 여러 협력 조직들에 의한 공동 프로젝트 형태로 개발되고 있다. OMA의 권리 표현 언어는 모바일 환경을 위한, ODRL의 부분 집합이라고 볼 수 있다.

DRM 시스템에서 사용되는 컨텐츠와 라이선스는 불법적인 사용이나 위조를 방지하기 위하여 암호, 전자 서명, 워터마크(watermark)등의 보안 기술들로 보호되어야 한다. 예를 들어, OMA의 DRM 규격을 살펴보면, 컨텐츠의 보호를 위하여 대칭 및 비대칭 암호, 축약, 전자 인증서 등의 보안 기술이 사용되고 있다. XrML, ODRL 그리고 METSRights 언어와 같이 XML에 근거한 권리 표현 언어들은 XML의 표현력과 확장성 등의 장점들을 그대로 계승받을 수 있으며, W3C에서 제정한 XML에 대한 전자 서명과 암호화 표준인 XML 서명(XML Signature) 기술[11]과 XML 암호(XML Encryption) 기술[12]을 사용할 수 있다. 보호된 컨텐츠에 대한 표준 기술로는 IETF(the Internet Engineering Task Force)의 표준 문서 rfc 3369[13] 등이 있다.

권리 표현 언어는 주체, 자원, 조건, 권리에 대한 다양한 의미들을 모호성 없이 표현할 수 있어야 한다. 하지만 ODRL과 같은 기존의 권리 표현 언어들은 아직 충분한 형

식 의미(formal semantics) 체계를 갖고 있지 못하다[14]. 본 논문은 허가의 구성 요소인 조건과 권한의 관계를 술어 논리(predicate logic)를 사용하여 정형화하여 표현하고 그에 관련 용어들을 정의한다.

본 논문이 제안하는 멤버/그룹 라이선스 메커니즘과 같이 그룹 단위로 구매한 컨텐츠에 대한 그룹 멤버들의 융통성 있는 공유를 지원하는 라이선스 메커니즘이 필요한 이유는 고객들이 그런 방식의 컨텐츠 구매를 원할 수 있기 때문이다. 개인 뿐 아니라 기관, 회사와 같은 단체들도 DRM 시스템의 중요한 사용자일 것이며, 단체 사용자의 경우 구매한 컨텐츠들을 단체 내에서 융통성 있게 사용하기를 원하는 경우가 있을 것이다. 라이선스 메커니즘이 지원하는 허가에 대한 표현력이 강할수록 DRM에 관련된 보다 다양한 비즈니스 모델들을 지원할 수 있다.

기존의 권리 표현 언어나 라이선스 체계를 이용하여 그룹의 멤버들 전체가 어떤 컨텐츠를 공유하여 사용하도록 하려면 그룹의 멤버 각각에게 개인별로 그 멤버가 필요로 하는 허가(grant)를 규정하는 라이선스를 발급해주는 방법을 사용하거나, 그룹의 멤버중 하나가 어떤 이름(즉 명확히 식별되는 자신의 이름, 법인 이름, 또는 그룹 이름 등)으로 컨텐츠를 구매하고 그룹 내의 멤버들이 그 이름으로 그 컨텐츠를 사용하도록 하는 방법 등을 사용해야 할 것이다. 하지만 그런 방법들은 다음과 같은 문제점들을 가질 수 있다.

2.1 문제점 1 : 총 구매 비용의 낭비 문제

그룹의 멤버들에게 개인별로 라이선스를 발급해주는 방법은 구매한 총 사용 권한이 낭비될 수 있으므로 결과적으로 총 구매 비용이 낭비될 수 있다는 문제점을 갖는다. 왜냐하면 라이선스의 속성상 멤버 각각에게 정확한 내용의 허가를 주어야 하지만 멤버 각각에게 필요한 허가의 범위를 정확하게 예측하기 어려운 경우가 많기 때문이다. 모든 멤버에게 필요한 허가의 범위에 대한 예측이 틀리는 경우 어떤 멤버는 자신에게 주어진 허가를 다 사용하지 못할 것이지만 어떤 다른 멤버는 자신에게 주어진 허가가 부족한 경우가 발생할 수 있을 것이다.

2.2 문제점 2 : 라이선스 상의 주체와 사용자의 불일치 및 컨텐츠 사용의 불편 문제

만일 그룹의 멤버들 중 한사람을 라이선스의 주체로 하여 그룹의 멤버들이 함께 사용할 컨텐츠 사용 권한을 구매하도록 한다면 주체와 사용자의 불일치 문제 및 컨텐츠 사용의 불편 문제가 야기될 수 있다. 왜냐하면 DRM 시스템이 불법적인 컨텐츠 사용을 방지하기 위하여 주체만 제시할 수 있는 패스워드 같은 어떤 비밀을 이용하여 컨텐츠 사용자의 신원 확인 절차를 수행하는 경우, 라이선스의 주체가 아닌 멤버는 컨텐츠를 사용할 때마다 신원 확인 절차가 요구하는 비밀을 제공하기 위하여 라이선스 주체의 도움을 받아야 하기 때문이다. 이런 경우 주체와 사용자가 일치하지 않는 현상도 발생한다.

2.3 문제점 3 : 사용자의 식별에 관련된 보안 문제

만일, 멤버 모두에게 라이선스 주체에 대한 신원 확인에 필요한 정보를 공유시킨다면 보안적인 문제가 생길 수 있다. 왜냐하면, 주체의 신원 확인은 일반적으로 패스워드, 지문 또는 개인키(private key)와 같이 그 주체만 보유한 어떤 비밀의 직접 또는 간접적 제시 능력 여부를 확인하는 과정을 통해서 이루어지므로, 컨텐츠의 공유를 위하여 그런 비밀을 그룹의 멤버들에게 공유시켜야 한다면 그 비밀의 엄격한 기밀성 유지가 어렵다. 이런 경우 엄격히 통제하지 않으면, 라이선스의 주체가 아닌 구매자가 원하지 않는 제삼자가 컨텐츠를 불법으로 사용하는 경우가 생길 수 있다. 또한 DRM 시스템이 라이선스 주체의 식별을 위해 지문과 같은 생체인식 메커니즘을 사용하는 경우나 장비 ID등의 식별을 통하여 신원 확인 절차를 수행하는 경우에는 멤버 각각에게 주체의 신원 확인에 필요한 정보를 공유하는 방법을 적용할 수 없다.

기존 라이선스 메커니즘들에서 하나의 라이선스에 여러 개의 허가를 담거나, 하나의 허가에 여러 주체들에 대한 권한을 표현하는 것은 가능하다. 예를 들어, XrML로 표현된 라이선스는 허가의 그룹을 표현하는 GrantGroup 요소를 구성 요소로 가질 수 있으며, 주체 요소는 주체들의 집합을 표현하는 allPrinciple 요소를 가질 수 있다[4]. 하지만 기존 라이선스 메커니즘들에서는 제 1장에서 언급한 바와 같이 주체들의 집합내의 주체들 각각의 자원의 사용의 총합이 10번이어야 한다는 것과 같은 융통성 있는 허가를 표현하기 어렵다.

일반적으로, XrML과 같은 권리 표현 언어에서 허가 정보를 구성하는 요소인 조건(condition)과 권리(right)는 별개의 원소(element)로 표현된다. 본 논문이 제안하는 메커니즘에서는 조건과 권리를 술어 논리식을 사용하여 규칙(rule)의 형태로 표현한다. 한 장의 라이선스에 여러 개의 조건 요소들과 여러 개의 권리 요소들을 표현하고자 할 때 규칙은 조건과 권리들을 명확하게 관련지을 수 있는 방법의 하나이다.

본 논문이 제안하는 라이선스 메커니즘은 기존 라이선스 메커니즘의 기본적 개념들이나 체계를 무시하거나 변경하지 않는다. 제안하는 메커니즘은 기존의 라이선스 메커니즘에 몇 가지 개념들과 절차들을 추가하여 그룹의 멤버들이 보안적으로 안전하면서도 융통성 있게 컨텐츠를 공유하기 위한 방법을 제공한다. 기존의 라이선스 관련 기술들은 그룹의 멤버들이 보안적으로 안전하면서도 융통성 있게 컨텐츠를 공유하기 위한 구체적 방법을 제시하고 있지 못하다.

3. 멤버/그룹 라이선스 메커니즘 개념 정의

잘 정의된 라이선스 메커니즘을 구축하려면 라이선스 메커니즘에 대한 정형화가 필요하다. 이 장에서는 술어 논리(predicate logic)를 이용하여 멤버/그룹 라이선스 메커니즘에 필요한 개념들과 절차들의 정의를 시도한다. 술어 논리는 수학, 철학, 인공 지능, 연역 데이터베이스(deductive database) 등의 분야에서 이론적 근거로 사용되는 전통적 논리 이론이다[15]. PROLOG 등의 프로그래밍 언어에서도 일차 술어 논리가 사용되고 있다.

3.1 개념 정의

먼저, 제안하고자 하는 라이선스 메커니즘이 사용하는 어떤 공리들(axioms)의 집합 A가 존재한다고 가정하자. 이 공리들의 집합의 구체적인 내용은 구현에 따라 달라질 것이다. 다음의 [정의 1]은 사용 규칙(usage rule)에 대하여 정의한다. 사용 규칙은 허가의 조건과 권리를 규정한다. 사용 규칙의 정의는 이후에 허가(grant)를 정의하는 데 필요하다. 사용 규칙의 정의에는 논리 내포 연산자(implication operator) → 가 사용된다.

[정의 1] 사용 규칙

사용 규칙이란 공리들의 집합 A상에서 참이나 거짓으로 판정될 수 있는 논리적 내포 C → R이라고 정의한다. 여기서, C와 R은 논리합 연산자 ∨, 논리곱 연산자 ∧, 부정 연산자 ¬, 그리고 술어들(predicates)로 구성된 논리식(predicate logic expression) 이다. ■

조건과 권한을 표현하는 술어들을 논리 연산자들로 조합하면 사용 규칙을 표현할 수 있다. 예를 들어, permit이 권리를 행사할 수 있음을 표현하는 술어 심벌(predicate symbol)이고, today가 현재 날짜와 인자를 비교하여 같으면 참 아니면 거짓을 반환하는 술어 심벌이고, view와 print가 각각 보는 동작과 프린트 하는 동작을 나타내는 술어 심벌들이라고 가정하면, 볼 수도 있고 프린트할 수도 있다는 권리를 permit(view) ∧ permit(print)와 같이 표현할 수 있으며, "2003년 3월 15일에는 볼 수 있고 2003년 3월 16일에는 프린트할 수 있다"라는 사용 규칙은 다음과 같이 표현될 수 있다.

(today(03-3-15) → permit(view)) ∧ (today(03-3-16) → permit (print))

사용 규칙들의 구체적인 형태와 의미는 공리들의 집합 A 및 술어들의 구체적 구현에 의해 결정된다. 다음의 [정의 2]는 라이선스를 정의하는 요소의 하나가 될 허가(grant)에 대한 정의이다. 허가의 정의에서는 무한의 정수를 나타내는 기호 ∞가 사용된다.

[정의 2] 허 가

허가란 튜플 <P, S, R>이라고 정의한다. 여기서, P는 주체(Principal)를 표현하는 1개 이상의 심벌들의 집합이며, S는 자원(reSource)을 표현하는 심벌과 자연수 또는 ∞의 쌍의 튜플(tuple)이며, R은 1개 이상의 사용 규칙들의 논리곱(conjunction)이다. ■

위 정의에서 허가를 구성하는 요소들 P, S, R을 각각 허가의 주체부, 자원부, 사용 규칙부라고 부르기로 하자. 사용 규칙부는 하나 이상의 사용 규칙들의 논리곱으로 구성된다. 자원부는 자원과 그 자원에 대한 최대 사용 회수를 나타내는 값으로 구성된다. 예를 들어 자원부 <c, 3>은 자원 c에 대한 3회의 사용 권한을 표현하며, <c, ∞>는 자원 c에 대한 무제한 회수의 사용 권한을 표현한다. 예를 들어, p_1과 p_2가 주체를 나타내는 심벌들이고, c_1과 c_2가 자원들을 나타내는 심벌들이고, today와 permit이 사용 규칙에 사용되는 술어 심벌들이라면 다음 (그림 1)의 g_1, g_2, g_3는 허가들이다.

g_1 : <{p_1, p_2}, <c_1, ∞>, (today(03-1-17) ∨ today(03-1-18) → permit(view)) ∧ (today(03-1-17) → permit(print))>
g_2 : <{p_1}, <c_1, 5>, (today(03-1-17) ∨ today(03-1-18) → permit(view))>
g_3 : <{p_1, p_2}, <c_2, 6>, (today(03-1-17) ∨ today(03-1- 18) ∨ today(03-1-19) → permit(view))>

(그림 1) 예제 허가들

허가 g_1, g_2, g_3의 해석은 각각 공리 집합 A의 구체적 구현에 영향을 받는다. 허가 g_1은 "주체들 p_1과 p_2가 컨텐츠 c_1을 무제한 회수로 2003년 1월 17일과 18일에 볼 수 있으며 무제한 회수로 2003년 1월 17일에 프린트할 수 있다"고 해석된다고 하자. 허가 g_2는 "주체 p_1이 컨텐츠 c_1을 5번까지 2003년 1월 17일과 18일에 볼 수 있다"는 허가라고 하자. 허가 g_3는 "주체들 p_1과 p_2가 컨텐츠 c_2를 모두 합쳐 6번 이내에서 2003년 1월 10일, 11일, 그리고 12일에 볼 수 있다"는 의미라고 하자. 허가 g_1이나 g_3와 같이 주체부의 원소의 개수가 2 이상인 허가들은 주체들 간에 자원을 효과적으로 공유하기 위한 허가를 표현한다.

DRM 시스템에서는 일반적으로 사용자가 컨텐츠 플레이어를 이용하여 보호된 컨텐츠를 사용하려면 컨텐츠 뿐 아니라 그 사용에 대한 라이선스가 필요하다. 라이선스 자체가 전자 서명 검증 실패 등의 이유로 유효하지 않거나 라이선스의 허가(grant)를 구성하는 주체, 자원, 조건, 권리가 현재의 사용 상황과 일치하지 않으면 컨텐츠 플레이어는 해당 컨텐츠를 재생하지 못한다. 다음은 라이선스에 대한 정의이다.

[정의 3] 라이선스, 그룹 라이선스, 멤버 라이선스

라이선스란 튜플 <u, g> 라고 정의한다. 여기서 u는 발급자

를 나타내는 심벌이고 g는 허가이다. 주체부의 원소의 개수가 2 이상인 허가를 갖고 있는 라이선스를 그룹 라이선스라고 정의한다. 주체부의 원소의 개수가 1인 허가를 멤버 라이선스라고 정의한다. ■

예를 들어, m이 어떤 발급자를 나타내는 심벌이고 p_1, p_2가 주체들이고 c가 자원을 나타내는 심벌이고 today와 permit가 술어 심벌이라면 (그림 2)의 L_1과 L_3는 그룹 라이선스이다. L_2는 멤버 라이선스이다.

L_1 : <m, <{p_1, p_2}, <c, 5>, (today(03-1-10) ∨ today(03-1-11) → permit(view)) ∧ (today(03-1-17) → permit(print))>>
L_2 : <m, <{p_1}, <c, 3>, (today(03-1-10) → permit(view))>>
L_3 : <m, <{p_1, p_2}, <c, 1>, (today(03-1-11) ∨ today(03-1-12) → permit(print))>>

(그림 2) 예제 라이선스들

하나의 라이선스에 여러 개의 허가들을 담을 수 있다. 하지만 본 논문에서는 논의의 간결함을 위해 라이선스가 하나의 허가만을 담는다고 가정한다. 이런 가정은 일반성을 크게 훼손하지 않는다. 왜냐하면 여러 개의 허가를 담은 라이선스는 하나씩의 허가를 담은 여러 장의 라이선스들로 표현될 수 있기 때문이다.

일반적으로, 라이선스에는 고유한 일련 번호나 발급자의 전자 서명을 넣어, 라이선스 발급자의 신원 확인 및 라이선스의 위조와 변조를 방지한다. [정의 3]은 필요하다면 발급자의 전자 서명과 일련 번호를 포함하는 라이선스에 대한 정의로 쉽게 확장될 수 있다.

다음 [정의 4]는 허가와 허가 사이에 존재할 수 있는 파생 관계(derivation relationship)를 정의한다. 허가 간의 파생 관계의 정의는 라이선스간의 파생 관계를 정의하는 데 필요하다.

[정의 4] 허가로부터 파생될 수 있는 허가

g_b와 g_d를 임의의 허가들이라고 하자. 만일 다음과 같은 조건이 만족된다면 허가 g_b로부터 허가 g_d가 파생될 수 있다고 정의한다.

① g_d의 주체부가 g_b의 주체부의 부분 집합이다.

② g_d의 자원부를 <r_d, n_d>라고 하고 g_b의 자원부를 <r_b, n_b>라고 하면, $r_d = r_b$이고 $n_d \leq n_b$이다(n_b, n_d는 자연수 또는 ∞이다).

③ g_d의 사용 규칙부가 g_b의 사용 규칙부로부터 논리적으로 함축된다. ■

(그림 1)의 예제 허가들 g_1, g_2, g_3에서 g_2가 g_1으로부터 파생될 수 있는 허가임을 [정의 4]로부터 알 수 있다. 왜냐하면 g_2의 주체부는 g_1의 주체부의 부분 집합이며, g_2의 자원부는 <c_1, 5>이고 g_1의 자원부는 <c_1, ∞>이며, g_2의 사용 규칙부(today(03-1-17) ∨ today(03-1-18) → permit(view))가 g_1의 사용 규칙부(today(03-1-17) ∨ today (03-1-18) → permit(view)) ∧ (today(03-1-17) → permit(print)) 로부터 논리적으로 함축되기 때문이다. 하지만 g_1과 g_3는 서로 다른 자원에 대한 허가들이므로 서로 파생될 수 없는 허가들이다.

파생 관계의 판정에는 사용 규칙부들간의 논리적 함축 관계의 판정이 필요하며, 사용 규칙부들간의 논리적 함축 관계의 판정에는 라이선스 메커니즘의 공리들의 집합 A가 사용된다. 따라서 허가를 구성하는 요소들의 구체적인 표현과 의미는 공리 A의 구현에 따라 결정된다고 할 수 있다. 이제, 라이선스 간의 파생 관계를 정의한다. 라이선스들 간의 파생 관계는 본 논문이 제안하는 멤버/그룹 라이선스 메커니즘의 핵심적 개념이다.

[정의 5] 파생될 수 있는 라이선스

L을 임의의 라이선스 <u, g>이라고 하자. L'를 임의의 라이선스 <u', g'>이라고 하자. 이 때 만일 다음과 같은 조건이 만족된다면 L'가 L로부터 파생될 수 있는 라이선스라고 정의한다.

- u' = u
- g'는 g로부터 파생될 수 있는 허가이다. ■

위 [정의 5]에 따르면 (그림 2)의 예제 라이선스 L_2는 L_1에서 파생될 수 있는 라이선스이지만 L_3는 L_1에서 파생될 수 없는 라이선스이다.

4. 멤버/그룹 라이선스 메커니즘의 동작 및 구현

4.1 동작 절차들

멤버/그룹 라이선스 메커니즘은 제 3장의 정의들을 근거로 동작한다. 라이선스 발급자는 그룹 등록 요청 및 그룹 라이선스 발급 요청을 처리하며, 일단 그룹 라이선스가 발급되면 그로부터 파생될 수 있는 멤버 라이선스들의 발급 요청도 처리한다. 여기서 라이선스 발급자란 라이선스를 발급하는 시스템 또는 소프트웨어 모듈 등을 의미한다.

4.1.1 주체의 등록 및 신원 확인 방법

라이선스 메커니즘들은 컨텐츠의 불법적인 사용을 막기 위하여 허가에 포함된 주체들에 대한 어떤 신원 확인 방법을 필요로 한다. 멤버/그룹 라이선스 메커니즘에서 사용될 수 있는 신원 확인 방법의 하나는 주체의 공개키 인증서(public key certificate)와 그에 대응하는 개인키(private key)를 이용하는 다음과 같은 도전과 응전 방식(challenge and response method)이다. 여기서, 논스(nonce)란 필요시에 매번 새롭게 생성되는 큰 난수를 의미한다.

단계 1 : 라이선스 발급자가 논스를 생성하여 주체 p에게 보낸다.

단계 2 : 주체 p는 자신의 개인키로 논스에 대한 전자 서명을 생성하여 라이선스 발급자에게 보낸다.

단계 3 : 라이선스 발급자는 p가 보낸 논스의 전자 서명을 p의 공개키 인증서로 검증하여 p의 신원을 검증한다.

멤버/그룹 라이선스 메커니즘은 하나의 자원을 모든 멤버들이 공유하여 사용하려는 경우에도 그룹 멤버 각자가 자신의 개인키를 사용하여 자신의 신원을 증명하는 방법을 사용하므로 제 2장에서 언급한 신원 확인을 위한 주체의 비밀의 공유에 의한 문제가 발생하지 않는다.

개인키를 주체의 신원 확인의 근거로 사용하는 경우, 그룹의 멤버들 p_1, p_2, …, p_n의 공개키가 라이선스 발급자에게 등록되어야 한다. 그룹에 소속한 멤버들을 DRM 시스템에 등록하려면 다음과 같은 정보를 DRM 시스템에게 전달한다. 여기서 ID_G는 그룹의 고유한 이름이며, $Cert_{p1}$, $Cert_{p2}$, …, $Cert_{pn}$은 그룹 멤버 각각의 공개키 인증서들이라고 하자.

$$<ID_G, \{Cert_{p1}, Cert_{p2}, \cdots, Cert_{pn}\}>$$

위와 같은 정보를 전달받은 라이선스 발급자는 그룹 이름 ID_G의 유일성과 $Cert_{p1}$, $Cert_{p2}$, …, $Cert_{pn}$의 유효성(validity)이 검증되면 그룹 등록 정보를 저장한다.

4.1.2 라이선스의 발급 절차

하나의 자원을 2명 이상의 주체들이 효과적으로 공유하여 사용하고자 할 때 그룹 라이선스가 필요하다. 예를 들어, 3명의 멤버 p_1, p_2, p_3가 자원 c를 2003년 2월 3일과 4일에 총 10회 사용할 수 있는 허가에 대한 그룹 라이선스는 다음 (그림 3)과 같다. u는 라이선스 발급자라고 하자.

<u, <{p_1, p_2, p_3}, <c, 10>, (today(03-2-04) ∨ today(03-2-05) → permit(play))>

(그림 3) 예제 그룹 라이선스

라이선스 발급자 u는 그룹 라이선스의 발급 요청이 있으면 발급 요청을 검사하여 문제가 없으면 그룹 라이선스를 발급한다. 이 때 라이선스 발급 요청자의 신원 확인 및 요청 라이선스에 대한 비용 지불 여부 등이 검사될 수 있다. 일단 그룹 라이선스가 발급되면, 그 그룹 라이선스로부터 멤버 라이선스들이 발급될 수 있다. 멤버 라이선스는 그룹 라이선스를 근거로 하여 발급되며 멤버들 각각에게 필요한 허가를 담는 라이선스이다.

다음은 그룹 라이선스 L_G = <u, <{p_1, p_2, …, p_n}, <c, i>, r>>에 대한 멤버 라이선스 L_m = <u, <{p}, <c, j>, r'>>의 발급 절차이다. 여기서 i, j는 자연수 또는 ∞이며, p는 {p_1, p_2, …, p_n}의 원소이다.

단계 1 : 주체 p가 라이선스 발급자 u에게 멤버 라이선스 L_m의 발급을 요청한다. 이때, 해당 그룹 라이선스 L_G를 지정하기 위한 정보 및 발급을 요청하는 멤버의 소속 그룹에 대한 정보(예를 들어 그룹 고유 이름 ID_G)가 전달된다고 하자.

단계 2 : u는 p가 해당 그룹의 멤버인가를 확인하고, 멤버 라이선스 L_m이 그룹 라이선스 L_G로부터 파생될 수 있는 라이선스인가를 검사한다. 이 때 필요에 따라 p의 신원 확인을 위한 부수적 절차가 수행될 수도 있다.

단계 3 : 만일, 파생 관계 검사 결과가 거짓이면 u는 멤버 라이선스 발급 불가 메시지를 출력하고 절차를 종료한다.

단계 4 : 파생 관계 검사 결과가 참이면, u는 p를 주체로 하는 멤버 라이선스를 발급하고, 만일 $i \neq \infty$이면 그룹 라이선스의 허가의 자원부 <c, i>를 <c, i-j>로 수정한다.

이런 절차는 그룹 라이선스로부터 멤버 라이선스가 발급될 때마다 반복되며, 멤버 라이선스가 발급될 때마다 해당 그룹 라이선스의 허가의 자원부는 수정될 수 있다. 단계 4에서, 멤버 라이선스가 파생될 수 있는 경우이므로 $j \neq \infty$이다.

4.1.3 멤버 라이선스 발급 예제

개념적으로, 하나의 그룹 라이선스로부터 파생되어 발급된 모든 멤버 라이선스들의 허가의 총 합은 그룹 라이선스의 허가의 범위를 넘을 수 없다. 그림 3의 그룹 라이선스에 대한 멤버 라이선스들의 발급 요청의 처리의 예를 살펴보자.

요청 1 : 멤버 라이선스 L_1 = <u, <{p_1}, **<c, 6>**, (today(03-2-04) ∨ today(03-2-05) → permit(play))>의 발급이 요청된다면 u는 그 멤버 라이선스를 발급할 것이다. 왜냐하면 멤버 라이선스 L_1은 (그림 2)의 그룹 라이선스로부터 파생될 수 있는 라이선스이기 때문이다. 그리고 멤버 라이선스 L_1의 발급 직후 그룹 라이선스의 허가의 자원부는 <c, 4>로 수정된다.

요청 2 : 이때 다시 새로운 멤버 라이선스 L_2 = <u, <{p_2}, <c, 3>, (today(03-2-05) → permit(play))>의 발급이 요청된다면 그 멤버 라이선스가 발급될 것이다. 왜냐하면 그 멤버 라이선스 L_2는 수정된 그룹 라이선스 <u, <{p_1, p_2, p_3}, **<c, 4>**, (today(03-2-04) ∨ today(03-2-05) → permit(play))>로부터 파생될 수 있는 라이선스이기 때문이다. 이제 c에 대한 총 1번의 사용 권한이 남아있는 상태이다.

요청 3 : 이때 다시 새로운 멤버 라이선스 L_3 = <u, <{p_2}, <c, 2>, (today(03-2-05) → permit(play))>의 발급이 요청된다면 그 멤버 라이선스의 발급은 거부될 것이다. 왜냐하면 자원 c에 대하여 사용 회수가 1번

남아있으나 2번의 사용 권한을 요청하였기 때문이다. 하지만 만일 L_4 = <u, <{p_2}, <c, 1>, (today(03-2-05) → permit(play))>의 발급이 요청되었다면 요청된 멤버 라이선스가 발급될 수 있다.

이 예제는 제안한 메커니즘이 그룹 라이선스와 그로부터 동적으로 파생되어 발급되는 멤버 라이선스들을 이용하여 그룹의 멤버들이 DRM 시스템으로부터 구매한 자원의 효과적인공유를 지원함을 보여준다. 만일 그룹 라이선스의 허가의 자원부가 <c, ∞>와 같은 형태로 주어진다면 멤버 라이선스가 발급될 때에 그룹 라이선스의 허가의 자원부의 수정이 발생하지 않는다.

4.1.4 라이선스 권한의 확인

사용자가 DRM 시스템의 컨텐츠를 사용하려면 라이선스에 그 사용에 필요한 권한이 기술되어 있는가를 확인해야 한다. 이런 확인은 일반적으로 보호된 컨텐츠를 재생하는 컨텐츠 플레이어에 의해 수행된다. 본 논문이 제안하는 메커니즘은 술어 논리에 기반을 두고 있으므로 라이선스의 권한의 확인을 위해 분해 반증 증명(resolution refutation proof) 방법[16]을 적용하는 것이 가능하다. 즉, 검증하고자 하는 술어식을 P라고 하면 $\neg P \wedge A$로부터 모순(contradiction)을 이끌어내는 과정을 통해 컨텐츠의 사용에 관한 사용자의 요청이 정당한 것인가를 판정할 수 있다. 여기서 A는 제 3.1절에서 설명된 공리들이다.

4.2 구현의 용이성

본 논문이 제안하는 메커니즘은 술어 논리 규칙들을 사용하여 라이선스의 조건과 권한의 관계를 표현한다는 특징을 갖는다. 술어 논리 규칙들은 전문가 시스템, 연역 데이터베이스(deductive database) 등의 다양한 응용 분야에서 사용되고 있다. 술어 논리를 사용하여 라이선스의 조건과 권한의 동적인 관계를 표현하는 것은 효과적인 방법이라고 할 수 있다. 왜냐하면, 규칙들을 사용하면 그들을 논리적으로 연결(chaining)하는 추론 엔진에 의해 새로운 사실을 동적으로 추론하거나 주어진 사실의 진위를 판정하는 것이 가능하기 때문이다.

본 논문이 제안하는 라이선스 메커니즘에서 사용되는 규칙들은 구현 및 수행의 복잡도가 비교적 크지 않다고 할 수 있다. 그 이유는 다음과 같다.

① 만일 라이선스의 구성 요소들인 주체(principal), 자원(resource), 조건(condition) 그리고 권리(right) 모두의 관계를 규칙의 형태로 표현하려고 한다면 매우 다양한 종류의 술어 심벌들과 복잡한 규칙들이 요구될 것이다. 하지만 본 논문이 제한하는 라이선스 메커니즘은 라이선스의 구성 요소들 중 주체와 자원을 제외한 조건과 권리의 관계만을 규칙의 형태로 표현하므로 규칙의 형태가 비교적 간단하고 의미가 명확하다.

② 일반적으로 XrML과 같은 기존의 권리 표현 언어들은 라이선스의 조건과 권리 요소들의 표현에 변수의 사용을 지원하고 않는다. 왜냐하면 라이선스에서의 조건과 권리의 표현에 변수의 사용이 그다지 필요하지 않기 때문이다. 마찬가지로 본 논문이 제안하는 라이선스 메커니즘에서도 라이선스의 사용 규칙들에 변수의 사용이 그다지 필요하지 않다고 판단된다. 기존의 권리 표현 언어들이 표현하는 조건과 권리들은 상수값들이므로 그대로 본 논문이 제안하는 라이선스 메커니즘에서 변수가 없는 사용 규칙들로 표현될 수 있기 때문이다. 변수들을 포함하지 않는 규칙들은 빠르고 효과적으로 처리될 수 있다.

기존의 권리 표현 언어나 라이선스 모델들[5, 8, 9, 14]은 술어 논리 등의 정형화 도구를 사용하지 않고 라이선스에 관련된 의미들을 규정한다. 하지만 본 논문이 제안하는 모델은 술어 논리 기반으로 정형화된 모델이며 모호성이 작다. 본 논문에서 제안된 그룹 라이선스, 멤버 라이선스, 그리고 파생 가능한 라이선스의 개념은 다른 연구들에 없는 새로운 개념이다. 본 논문이 제안하는 방식은 기존 권리 표현 언어들과 충돌하지 않으므로 기존 권리 표현 언어들을 사용하여 DRM 기술로 보호된 컨텐츠의 그룹 내에서의 안전하고 융통성 있는 공유 메커니즘을 구현할 수 있을 것이다.

5. 결 론

본 논문은 여러 명의 멤버들로 구성된 그룹이 DRM 기술로 보호된 디지털 컨텐츠를 융통성 있게 공유할 수 있도록 하는 새로운 라이선스 메커니즘을 제안하였다. 제안한 메커니즘은 그룹 라이선스, 멤버 라이선스, 허가간의 파생 관계 등의 개념과 절차들을 도입하여 기존의 라이선스 메커니즘 체계를 확장한다. 제안된 메커니즘은 개인 고객이 아닌 기업들이나 가정에서 DRM 기술로 보호된 컨텐츠를 효과적으로 공유할 수 있도록 하며, DRM 시스템을 운영하는 기업들에게는 DRM에 관련된 보다 다양한 비즈니스 모델들을 지원할 수 있을 것이다.

향후 연구로는 제안한 메커니즘을 홈 네트워킹 환경 등에서 XrML 등의 언어로 구현하여 구체적인 문제점들을 찾아내는 것과 라이선스 메커니즘에 관련한 개념과 절차들에 대한 정형화를 보다 확장하는 것 등이 필요하다.

참 고 문 헌

[1] Joshua Duhl, "The DRM Landscape : Technologies, Vendors and Markets," IDC, 2001.

[2] Piero Attanasio, "The use of DOI in eContent value chain

: The case of Casalini Digital Division and mEDRA," mEDRA, February, 2004.
[3] T. Berners-Lee, R. Fielding, U. C. Irvine, L. Masinter, "Uniform Resource Identifiers (URI) : Generic Syntax," RFC 2396, August, 1988.
[4] William Stallings, Cryptography and Network Security, 2nd Edition, Prentice Hall, pp.163-206, 1999.
[5] Content Guard, "XrML 2.0 Technical Overview version 1.0," March, 2002.
[6] 강호갑, "DRM 최신 국제 표준 기술 사양 분석 및 세계 유명 제품 동향과 전망에 대한 연구", 한국소프트웨어진흥원, Feb., 2004.
[7] Karen Coyle, "Rights Expression Languages," Library of Congress of US, February, 2004.
[8] Jan Bormans, Keith Hill, "MPEG-21 Overview v.5," ISO/IEC JTC1/SC29/WG11/N5231, October, 2002.
[9] Renato Iannella, "Open Digital Rights Language (ODRL) version : 1.1," IPR Systems Pty Ltd, August, 2002.
[10] METS community, "Draft Rights Declaration Schema," http://www.loc.gov/standards/mets/news080503.html, August, 2003.
[11] R. Housley, "Crypographic Message Syntax," RFC 3369, IETF, August, 2002.
[12] J. Reagle, "XML Signature Requirements," RFC 2807, IETF, July, 2000.
[13] Takeshi Imamura, Blair Dillaway, Ed Simson, "XML Encryption Syntax and Processing," W3C, December, 2002.
[14] Riccardo Pucella, Vicky Weissman, "A Fomal Foundation for ODRL," Proceedings of Workshop on Issues in the Theory of Security, Barcelona, Spain, pp.234-247, April, 2004.
[15] Stuart Russel, Peter Norvig, AI A Modern Approach, Prentice Hall, pp.185-216, 1995.
[16] George F. Luger, William A. Stubblefield, Artificial Intelligence and the Design of Expert Systms, Benjamin/Cummings, pp.416-418, 1989.

장 혜 진

e-mail : hjchang@smu.ac.kr
1985년 서울대학교 사범대학 수학교육과 (이학사)
1987년 서울대학교 자연과학대학 계산통계학과 전산학 전공(이학석사)
1994년 서울대학교 계산통계학과(이학박사)
1987년~1989년 한국전자통신연구소 근무
1994년~현재 상명대학교 공과대학 컴퓨터소프트웨어 전공 교수
관심분야 : 분산 에이전트 시스템, 통신 보안 시스템, DRM 시스템