The Journal of Digital Policy & Management 2013 May; 11(5): 1-11

DRM 소프트웨어의 보안성 품질평가 모델

이하용*, 김중규**
서울벤처대학원대학교 융합산업학과*, 호서대학교 글로벌창업대학원 창업학과**

Quality Evaluation Model for Security of DRM Software

Ha-Young Lee*, Jung-Gyu Kim**
Dept. of Fusion Industry, Seoul Venture University*
Dept. of Entrepreneurship, Graduate School of Global Entrepreneurship, Hoseo University**

요 약 DRM 기술이 디지털 콘텐츠의 저작권을 적절하게 보호할 수 있도록 하기 위해서는 DRM SW가 고품질을 갖추고 있어서 디지털 콘텐츠에 DRM을 부여했을 때 결함이 발생하지 않아야 한다. 따라서 DRM SW의 품질평가 모델을 개발하는 것은 디지털 콘텐츠의 저작권을 효과적으로 보호하기 위한 기초가 된다고 할 수 있다. 그 중에서도 DRM SW의 보안성은 DRM SW가 갖추어야 할 가장 핵심적임 품질특성이라고 볼 수 있으므로 본 논문에서는 DRM SW의 보안성 품질을 측정할 수 있는 방법에 관한 연구를 수행하였다.

주제어 : 디지털저작권관리, 기능성, 평가모델, 품질평가, 디지털 콘텐츠

Abstract To make the DRM technology protect adequately the copy right of digital contents, DRM software should have high quality and no defects when DRM is added to digital contents. It can be a basis for the effective protection of the copyright of digital contents to develop a quality evaluation model of DRM SW. First of all, the security of DRM SW is the most critical quality characteristic that DRM software must have. In this paper, we conducted research on how to measure the quality of security of DRM SW.

Key Words : Digital Right Management, Functionality, Evaluation Model, Quality Evaluation, Digital Contents

1. 서론

디지털 콘텐츠가 쉽게 복제된다는 특성 때문에 디지털 콘텐츠 저작권 보호 기술에 관심이 모아지고 있다. 또한 많은 콘텐츠 소유자들이 콘텐츠 유료화에 관심을 보임에 따라서 저작권을 보호할 뿐만 아니라 인터넷을 통하여 안정된 수익 모델을 촉진할 수 있는 기술적 장치에 대한 관심이 높아지고 있다.

디지털 콘텐츠 저작권 보호 기술로는 디지털 워터마킹 같은 저작권 추적 기술과, 사용 권한(use rights)을 획득하지 못한 사람에게는 콘텐츠를 사용하지 못하게 하는 저작권 관리 기술들로 대별될 수 있다. 저작권 추적 기술의 디지털 워터마킹 적용은 간단한 반면 저작권을 적극적으로 보호하지는 못하는 단점이 있다.

Received 1 May 2013, Revised 20 May 2013
Accepted 20 May 2013
Corresponding Author : Jung-Gyu Kim(Graduate School of Global Entrepreneurship, Hoseo University)
Email: lhyazby@suv.ac.kr

ISSN: 1738-1916

암호화 기술을 응용한 저작권 관리 기술들은 저작권자가 대가를 지불한 사용자에게만 사용권한을 줄 수 있어 좀 더 적극적인 저작권 보호 기술이다. 하지만 이런 암호화 기술들은 암호화 키의 관리를 어떻게 하느냐에 따라 보안성이 떨어지기도 하여, 암호화 키를 안전하게 저장하기 위한 기술을 덧붙인 기술들이 개발되어 왔다.

다른 한편으로는 이런 기술들이 전자상거래에서 활용되기 위해서는 사용권한을 좀 더 다양한 방법으로 제어할 필요가 있으며, 이를 위한 기술들도 개발되고 있다. 초기에는 특정 사용자에게 콘텐츠를 사용할 수 있는 모든 권한을 부여하는 단순한 방식에서 최근에는 콘텐츠를 볼(view) 수는 있으나 인쇄(print)는 못하게 한다든지, 사용할 수 있는 기간이나 횟수를 제어 할 수 있도록 하는 등 실 상거래에서 발생할 수 있는 다양한 방식의 사용권한 제어를 시도하려는 DRM(Digital Rights Management) 기술이 개발 상용화 되고 있다.

DRM은 디지털 콘텐츠의 불법 사용방지 및 저작권 보호를 위한 기술로서 암호기술, 트랜잭션 처리기술, 분산처리 기법 등 다양한 요소들이 복합되어 운영되는 기술이며[1], 저작권 보호 및 복제방지 기술의 프레임워크를 제공하여 디지털 콘텐츠의 신뢰성 있는 유통과 투명한 권리보호를 뒷받침하는 기술이라 할 수 있다[2].

DRM 기술이 디지털 콘텐츠의 저작권을 적절하게 보호할 수 있도록 하기 위해서는 DRM 소프트웨어가 고품질을 갖추고 있어서 디지털 콘텐츠에 DRM을 부여했을 때 결함이 발생하지 않아야 한다. 따라서 DRM 소프트웨어의 품질평가 모델을 개발하는 것은 디지털 콘텐츠의 저작권을 효과적으로 보호하기 위한 기초가 된다고 할 수 있다.

그 중에서도 DRM 소프트웨어의 보안성은 DRM 소프트웨어가 갖추어야 할 가장 핵심적임 품질특성이라고 볼 수 있으므로 본 논문에서는 DRM 소프트웨어의 보안성 품질을 측정할 수 있는 방법에 관한 연구를 수행하고자 한다.

본 논문의 2장에서는 DRM 소프트웨어 관련 동향에 대해 살펴보고 3장에서는 DRM 소프트웨어 기반 기술과 기능성에 관한 품질 요구사항을 분석하며 3장에서는 DRM 소프트웨어의 기능성에 관한 품질특성에 따른 평가 모델을 구축하고 5장에서 결론과 향후 연구과제를 제시하였다.

2. DRM 소프트웨어 관련 동향

2.1 DRM 소프트웨어 시장동향

Web 2.0, UCC, DMB 등 연관 기술 분야의 발전에 따라 다양한 제품 및 서비스의 출현과 더불어 급성장이 예상된다.

DRM 분야의 매출 전망을 살펴보면, 2006년 매출액은 118억원으로 전년도 78억원에 비해 40억원이 증가해 51.6%의 높은 증가율을 보였다. 또한 CAGR이 24.28%로 전망되는 등 2011년에는 286억원 규모의 미출 성장이 이루어 졌다.

〈Table 1〉 Sales Trends of Contents Security Fiend

Year / Division	2006	2007	2008	2009	2010	2011	CACR(%)
DRM	11,784	15,796	19,006	22,215	25,425	28,634	24.28
Total	32,554	37,779	42,202	46,624	51,047	55,469	12.52

(Note) CACR : Compound Annual Growth Rate

2.2 DRM 소프트웨어 관련 표준화 동향

DRM이 적용된 콘텐츠를 처리하기 위해서는 서비스 사업자별로 독립적인 권리정보를 처리하기 위해 사용자 기기에도 별도의 응용프로그램이 필요하게 됨을 의미한다. 이는 서비스업체, 기기제조업체, 솔루션 제작업체, 사용자들 모두의 불편으로 귀결된다[3][4][5].

2.2.1 TTA PG506

DRM분야(PG506)에서는 디지털 콘텐츠(동영상·MP3 등)불법복제 방지 및 지재권 보호, 이기종 DRM 플랫폼 간에 상호운용성 기술, IPTV 및 휴대폰 등 에서의 디지털 미디어 보호기술들을 표준화할 계획이다.

TTA PG506 표준화 활동은 크게 DRM과 핑거프린팅 인터페이스(WG 5061), DRM 상호연동기술(WG 5062), CAS+DRM 연동기술(WG 5063) 표준화를 추진중에 있다.

2.2.2 DRM 포럼

DRM 포럼은 디지털 콘텐츠의 중요성과 유료화가 대두됨에 따라 DRM 관련 기관의 전문가 50여명이 모여 2000년 12월에 결성되었다. 2007년은 DRM 포럼이 활동 7년차로 주로 워크샵, 해외 동향분석을 위주로 활동하였으며 또한 기업들의 정보교류 및 기술개발 지원을 위하여 분과별로 DRM 기술 표준화 작업을 진행하고 있다.

DRM 포럼은 국내외 표준화 활동, 기술 동향 연구, DRM 기능 연구 및 표준안 제시, DRM 워크샵 및 분과회의 개최 등의 활동을 수행하고 있다.

3. DRM 소프트웨어의 보안성 품질 요구사항

이 절에서는 DRM 소프트웨어의 보안성 품질에 관한 특성을 분석하여 DRM 소프트웨어가 갖추어야 할 품질 요구사항을 확립하고자 한다.

3.1 핵심 기술요소별 보안성 요구사항

3.1.1 암호화 기술

암호화 기술에서 요구되는 사항으로는 다음과 같은 것들이 있다.

- 콘텐츠별로 요구되는 보안 레벨 및 콘텐츠 서비스 환경에 따라 암호화 알고리즘이나 메시지 축약 알고리즘 등과 같은 보안기법들에서 제공되는 보안변수들을 협의(선택) 및 조정함으로써 콘텐츠 품질 및 보안레벨을 보장할 수 있는 보안 프레임웍을 제공해야 함
- 암호화 부분을 최소화함으로써 무선 단말 환경의 제약으로부터 발생 가능한 성능 및 품질 저하를 방지해야 함. 특히 콘텐츠 서비스 시 발생 가능한 지연(Latency)을 최소화해야 함
- 사용자 단말에서 이뤄지는 디코딩 프로세싱의 효율성을 고려한 콘텐츠 멀티미디어 실시간 암호 알고리즘을 적용해야 함
- 무선 단말의 제약된 환경을 고려한 사용자/단말기 인증 프로토콜 지원
- 목표 보안 레벨 및 성능 Trade-off를 고려한 암호화 기법을 적용해야 함
- 암호화 기술을 이용하여 사용이 허가되지 않는 사용자에게는 디지털 콘텐츠의 접근을 차단해야 함
- 접근제어 방식은 암호화 기술을 이용하여 콘텐츠를 암호화한다고 하더라도 허가된 사용자에겐 암호화된 콘텐츠를 복호화하여 원본 콘텐츠를 제공하기 때문에 콘텐츠의 지속적인 보호가 불가능하다는 한계점을 지니고 있으므로 지속적인 보호가 가능한 기술을 제공해야 함
- 비대칭키 방식은 암호화할 때의 키와 복호화할 때의 키가 서로 다르기 때문에 키를 효과적으로 분배할 수 있다는 장점이 있으나, 연산시간이 오래 걸린다는 단점이 있다. 반면, 암호화키와 복호화 키가 동일한 DES, SEED, AES 등의 대칭키 암호방식은 비대칭키 방식에 비해 연산시간이 빠르지만, 키 분배에서의 문제점을 드러내고 있다. 이러한 특성을 고려하여, 용량이 큰 디지털 콘텐츠의 경우, 대칭키 암호화 방식을 이용하여 암호화함으로써 연산 속도를 줄이고 있는지, 동시에 비대칭키 방식을 활용하여 대칭키를 분배함으로써 DRM 시스템의 보안성을 높여야 함
- 암호화 알고리즘으로 많이 알려진 DES와 3-DES 알고리즘에 취약점이 드러나 있으므로 최근에 많이 사용되는 AES(Advanced Encryption Standard) 알고리즘을 채용하고 있어야 함
- 암호화/복호화 과정을 거친 후 정상적으로 동작
- 콘텐츠가 사용자에게 배포될 때 수신자의 고유 정보를 이용해서 콘텐츠를 암호화해야 하기 때문에 콘텐츠를 유통하는 서버의 부담이 크게 증가하게 되므로 이를 피하기 위해 콘텐츠의 pre-packaging 및 super-distribution이 가능한 기술을 지원해야 함
- 암호화 및 복호화를 위해 사용되는 키 배포 및 관리의 부담을 사용자가 떠맡게 되는데 암호화에 대한 지식 이해도가 떨어지는 사용자로 하여금 키 배포 및 키 관리의 책임을 맡기는 것은 편리성 및 안전성 측면에서 많은 문제점을 내포하게 되므로 키 배포 및 관리가 사용자의 인식 없이 투명하게 처리될 수 있어야 함
- 암호화된 콘텐츠가 수신자 측에서 일단 복호화되어 평문 형태로 이용되게 되면 콘텐츠 제공자의 의도와 무관하게 콘텐츠가 재배포되거나 변형될 수 있다. 또한, 콘텐츠의 내용에 다라 콘텐츠 사용자의 이용권한을 자동화할 수 있어야 하는데, 이 방식은 콘텐츠의 권리정보를 제어할 수 있는 방법을 제공하지 않는다. 일부 전용 뷰어에서는 사용자에게 허락되는 기능만을 제공함으로써 의도되지 않은 콘텐츠의 불법복제를 방지하고 있지만 이것은 사용자의 권한에 따른 제어가 아니라 모든 사용자에게 동일한 제약을 가하게 된다. 이를 해결하기 위해서는 콘텐츠 제공자로 하여금 지정된 수신자가 지정된 권한 내에서만 콘텐츠를 이용할 수 있도록 권한 설정이 가능해야 하며, 콘텐츠 이용자는 지정된 권한 내에서 콘텐츠의 이용을 지속적으로 통제받을 수 있어야 함

3.1.2 권한 통제(Right Enforcement)

권한 통제기술에 관한 요구사항으로는 다음과 같은 것들이 있다.

- 디지털 콘텐츠가 라이센스에 명시된 사용 권한과 사용 조건의 범위에서만 사용될 수 있도록 지속적으로 통제되어야 함
- 초기의 DRM 제품은 built-in 방식의 전용뷰어나 plug-in 방식을 주로 사용했으나 콘텐츠 포맷 지원에 한계가 있으므로 최근에는 API Hooking이나 File System Filter 방식과 같이 모든 애플리케이션에 범용적으로 적용할 수 있는 통제 기술을 적용하는 추세로 바뀌고 있으므로 이러한 최신 기술을 지원하는지를 검토해야 함
- 보안적인 측면에서 볼 대는 DRM Controller의 처리가 애플리케이션 내에서 처리되는 Built-in 방식과 API Hooking 방식이 높은 안정성을 보이고 있는 반면 공개 인터페이스를 이용하는 File System Filter 방식이나 VBA 제어방식은 보안상 취약점이 있으므로 보안성이 최우선적으로 고려되어야 하는 DRM인 경우 Built-in 방식이나 API Hooking 방식을 지원하고 있는지 검토되어야 함

3.2 도메인별 보안성 요구사항 분석

3.2.1 문서보안

가. 문서의 보안 전달

문서가 유통되는 중에 권한이 없는 사람이 열어 볼 수 없도록 믄서를 암호화하여 유통 시키고, 특정 조건 하에서만 복호화한다.

나. 문서의 보안 사용

문서가 사용되는 중에도 허용된 권한을 밖의 용도로 사용되지 않도록 프로그램(오피스)을 제어하여 임의로 문서를 사용하거나 복호화된 문서를 추출하지 못하도록 한다.

다. 문서보안 기술

문서보안을 위해 필요한 기술로는 <Table 2>와 같은 것들이 있다.

〈Table 2〉 The skills necessary for document security

Security technology	contents
Encryption of the document	- Perform file-level encryption at the same time as the creation and storage of electronic documents - Folder Encryption Support
Setting of usage right of document	- Setting of the detailed right such as setting the view of a document, the number of outputs and edit - support of setting of usage rights according to users, groups and document security level
Editing control	- interception of copy & paste and print screen function in a important document
Output control and insert the printer marking	- the control of use of printer according to User/group/PC - the control of print marking insertion in the output according to user/group - It is possible to insert some variety of different types of watermarks such as print Information, security levels, and a warning message
automatic discard of electronic documents	- Auto-destructive functions of important documents at expiration, exceeding the number of output and reading - Provides the function of destory which is not being recovered with a general document recovery program
support of safe external transfer of electronic documents	- creation of security file for an encrypted external transmit with a document usage right - Only users who have passed authentication can use the security file for external transfer
control of storing to the external storage medium	- write control to portable storage devices such as floppy disks(FDD), CD-RW, USB memory
logging (record)	- Management of all records for user authentication and the history of use of important documents - Management of all records for administrator authentication, policies, user management, etc.

3.2.2 온라인 콘텐츠의 보안성

가. 음악

음악은 mp3, wma, ogg 등 다양한 종류가 있으므로 PC에서 실행 가능한 다양한 종류의 음악 파일에 대한 DRM을 지원해야 한다.

음악에 대한 서비스 방식에 있어서도 스트리밍 서비스, 다운로드 서비스, 기간정액제 서비스 등 다양한 서비스 형식이 있으므로 사업자가 원하는 기능을 선택하여 DRM을 적용할 수 있는 기능을 제공해야 한다.

<Table 3>은 음악에 관한 DRM이 제공해야 할 기능에 대해 나타내고 있다.

〈Table 3〉 DRM function for music

Function Name	contents
Blocking Voice Capture	Blocking the capture program such as Sound Forge
Blocking URL link	Blocking of URL Copy and watch
Block runs after the illegal copying	Even if you copy a file, because of its encrypion, it will not run without the real-time authentication of operators
Blocking of Network Hooking	Blocking a copy method intercepting the data that is passed to the Internet line
Blocking of video memory copy	Blocking of illegal copies of the files that are copied to the user PC's video memory
Blocking of cache file copy	Protection of temporary files that are created in the process of running a file
Fingerprint Function	We can be tracked by the insertion of user-specific information on the file to download
Real-time control Function	Even if users already downloaded a file, disable it not to run by real-time control

나. 동영상

동영상은 avi, mpg, wmv, dat 등 다양한 종류가 있으므로 PC에서 실행 가능한 다양한 종류의 동영상 파일에 대한 DRM을 지원해야 한다. 동영상에 대한 서비스 방식에 있어서도 스트리밍 서비스, 다운로드 서비스, 기간정액제 서비스 등 다양한 서비스 형식이 있으므로 선택 적용할 수 있는 기능을 제공해야 한다.

<Table 4>는 동영상에 관한 DRM이 제공해야 할 기능에 대해 나타내고 있다.

〈Table 4〉 DRM function needed to provide for the videos

Function name	contents
ID Marking Function	Blocking copies to use a video camcorder by displaying of user ID on a video
Blocking of Capture Program	Blocking various video capture programs
Blocking URL link	Blocking of URL Copy and watch
Block runs after the illegal copying	Even if you copy a file, because of its encrypion, it will not run without the real-time authentication of operators
Blocking of cache file copy	Protection of temporary files that are created in the process of running a file
Real-time control Function	Even if users already downloaded a file, disable it not to run by real-time control

3.2.3 모바일

모바일 DRM의 요구사항은 다음과 같다.

- 암호화 부분을 최소화하여 무선 단말 환경의 제약으로 인한 성능 및 품질의 저하를 최소화해야 함
- 사용자 단말에서 이루어지는 디코딩 프로세싱의 효율성을 고려한 콘텐츠 멀티미디어 실시간 암호 알고리즘 적용
- 무선 단말의 제약된 환경을 고려한 사용자/단말기 인증
- 목표 보안 레벨 및 성능 Trade-off를 고려한 암호화 기법을 적용
- 제한된 자원 및 전력 환경에서 동작하기 때문에, 모바일 휴대기기에서 연산시간과 에너지 소모를 최대한 줄이면서 콘텐츠를 안전하게 보호할 수 있는 암호화 알고리즘이 요구

3.2.4 홈 네트워크

현재 DRM 기술은 콘텐츠와 플랫폼의 종류에 따라 적용되는 보호 기술이 다르고, 비즈니스 및 도메인별로 별도의 표준이 존재하고 있어 현재의 DRM 기술들을 그대로 홈네트워크에 적용하기는 어렵다. 다양한 플랫폼과 디지털 TV, 인터넷, 휴대단말기, 셋톱박스 등 다양한 기기를 사용하는 홈네트워크에서 DRM을 적용하기 위해서는 DRM간의 상호호환성이 보장되어야 하며 홈네트워크 서비스가 제대로 이루어지려면 사용자 인증이나 데이터 암호화 또는 콘텐츠 사용 제어와 같은 보안기술의 적용이 필수이다.

홈네트워크에서 사용되는 DRM 기술 중의 하나로 DTCP(Digital Transmission Control Protocol)가 있다. DTCP는 5C(Hitach, Intel, Matsushita, Sony, Toshiba)가 개발한 기술로 오디오/비디오의 콘텐츠를 IEEE 1394, USB 표준 및 IP 기반 홈네트워크와 같은 디지털 인터페이스로 전송할 때 불법복제, 가로채기 등으로부터 보호하기 위한 암호화 기반의 프로토콜이다. DTCP에서 복제방지를 위한 4가지 기본 요소는 다음과 같다.

- 인증과 키 교환(Authentication and Key Exchange)
- 콘텐츠 암호화(Content Encryption)
- 복제제어 정보(Copy Control Information)
- 시스템 갱신능력(System Renewability)

3.2.5 방송

방송콘텐츠의 불법복제와 재배포를 방지하기 위한 기

술 표준으로 DVB CPCM(Control Protection & Content Management)가 있으며, DVB CPCM이 핵심으로 하는 보호 기술은 Authorized Domain, Security Control, Content Handling이다.

4. DRM 소프트웨어의 보안성 품질특성

이 절에서는 DRM 소프트웨어의 공통 기술 요구사항을 바탕으로 DRM 소프트웨어의 보안성에 관한 특성을 분류하고 분석하고자 한다.

4.1 DRM 소프트웨어 전반의 보안성 품질특성

보안성이란 소프트웨어가 허가되지 않은 사람이나 시스템의 액세스를 방지하여 정보 및 데이터를 보호하는 능력을 의미하며 보안성에 관련된 DRM 소프트웨어의 공통적인 특성으로는 다음과 같은 항목들이 있다.

① 적법하게 license를 발급받은 자만이 license가 허용한 사용규칙에 따라 해당 콘텐츠를 이용할 수 있도록 제어할 수 있어야 함
② 불법적인 접근과 사용을 방지하여야 함
③ license 정보의 무단 변경을 방지하고 license 정보의 무결성을 보장
④ 거래내역을 수집·관리함에 있어서 사용자의 프라이버시를 보호하고, 거래내역 정보의 불법유출 및 내용변경에 대한 보안이 필요
⑤ 콘텐츠의 보호가 지속적으로 유지되기 위해서 Temper Resistance와 Trusted System이 필요. Temper Resistance는 해킹이나 역공학(reverse engineering)으로부터 DRM과 관련된 프로그램 및 정보를 보호. 예를 들면, 콘텐츠를 한달간 사용할 수 있도록 라이선스가 부여된 경우, 자신의 컴퓨터 날짜를 변경함으로써 콘텐츠의 사용기간을 변경하는 행위 등을 방지하는 기술이 요구됨
⑥ 암호화 기술을 이용하여 사용이 허가되지 않는 사용자에게는 디지털 콘텐츠의 접근을 차단해야 함
⑦ 콘텐츠 제공자로 하여금 지정된 수신자가 지정된 권한 내에서만 콘텐츠를 이용할 수 있도록 권한 설정이 가능해야 하며, 콘텐츠 이용자는 지정된 권한 내에서 콘텐츠의 이용을 지속적으로 통제받을 수 있어야 함
⑧ 디지털 콘텐츠의 암호화를 위해 사용된 암호화 대칭키(CEK)는 매우 안전하게 관리 및 배포되어야 함
⑨ 보안적인 측면에서 볼 대는 DRM Controller의 처리가 애플리케이션 내에서 처리되는 Built-in 방식과 API Hooking 방식이 높은 안정성을 보이고 있는 반면 공개 인터페이스를 이용하는 File System Filter 방식이나 VBA 제어방식은 보안상 취약점이 있으므로 보안성이 최우선적으로 고려되어야 하는 DRM인 경우 Built-in 방식이나 API Hooking 방식을 지원하고 있는지 검토되어야 함

4.2 DRM 소프트웨어 도메인별 보안성 품질특성

4.2.1 문서보안

① 문서보안의 경우, 다음 경로에 대해 필요한 경우, 차단되어야 한다.
- 복사/붙여넣기
- 원본저장
- 메일 보내기
- 스크린 캡쳐 등

② 문서 유통중 권한이 없는 자를 차단하기 위해 암호화하여 유통되어야 한다.
③ 허가된 사용의 경우에도 임의 사용이나 복호화된 문서의 추출을 방지해야 한다.
④ 문서보안에 관해 Persistent Protection(지속적인 보호)을 지원하여 비인가자에 의한 문서 이용 차단하고 불법 문서 유출 경로를 차단해야 한다.
⑤ 전자문서의 생성 및 저장과 동시에 파일 단위의 암호화 수행
⑥ 폴더 암호화 지원
⑦ 문서의 열람(횟수 설정), 출력(횟수 설정), 출력, 편집 등의 상세 권한 설정 지원
⑧ 사용자/그룹 별, 문서 보안등급 별 사용 권한 설정 지원
⑨ 중요 문서 내 Copy& Paste 기능 및 Print Screen 기능 차단
- 사용자/그룹/PC 별 프린터 사용 제어(옵션)
- 사용자/그룹/PC 별 출력물 내 프린트 마킹 삽입 제어
- 출력자 정보, 보안 등급, 경고 문구 등 다양한 워터마크 종류별 삽입 가능
- 출력정보 삽입시 글꼴, 크기, 농도, 회전각도 옵션 선택
- 다양한 이미지 파일 삽입 기능 지원
- 반투명, 불투명 지원 등으로 원본 문서의 가독성을 보장해야 함

- 기타 출력정보와 중복 삽입이 가능해야 함

⑩ 유효기간 만료, 열람 및 출력 횟수 초과 시 중요 문서 자동 파기 기능 제공 및 일반 문서 복구 프로그램으로 복구 불가능한 파기 기능 제공

⑪ 문서 사용 권한이 지정된 암호화 된 외부 전송용 보안 파일 생성하고 인증을 통과한 사용자만이 외부 전송용 보안 파일 사용 가능

⑫ 플로피디스크(FDD), CD-RW, USB 메모리 등의 이동 저장 장치로의 쓰기 기능 제어

⑬ 사용자 인증 및 중요문서 사용 이력에 대한 모든 기록 관리

⑭ 관리자 인증 및 정책 수립, 사용자 관리 등에 대한 모든 기록 관리

4.2.2 온라인 콘텐츠

가. 음악

① DRM을 무력화시키려는 다양한 시도에 대한 차단기능을 제공해야 한다.
- 음성 캡쳐 차단
- URL 링크를 통한 다운로드나 청취 차단
- 실시간 인증 없이는 실행되지 않도록 하여 불법복사를 통한 실행을 차단
- 네트웍 전송 데이터를 가로채서 복사하는 방법에 대한 차단 기능 제공
- 파일 실행시 만들어지는 임시파일의 복사를 차단하는 기능 제공
- 핑거프린트 기능을 통한 사용자 추적 기능 제공
- 파일 다운로드에 성공했더라도 권한이 없으면 실행할 수 없도록 함

나. 동영상

① 동영상의 DRM을 무력화시키려는 다양한 시도에 대한 차단기능을 제공해야 한다.
- 영상에 이용자 정보를 표시하여 캠코더를 이용한 복사를 차단
- 다양한 캡쳐 프로그램을 이용한 복사 차단
- URL을 복사해서 시청하는 경우를 차단
- 파일을 복사해도, 암호화 되어 있어 사업자의 실시간 인증 없이는 실행되지 않아야 함
- 파일이 실행될 때 이용자 PC의 비디오 메모리에 복사가 되는데, 이것의 불법 복사를 차단
- 파일을 실행하는 과정에서 만들어지는 임시 파일도 보호하며, 복사를 차단
- 이용자가 이미 파일을 다운로드 했더라도 실행하지 못하도록 실시간 제어가 가능

다. e_Book

① DRM이 적용된 전자책은 사용자가 임의로 배포 및 수정할 수 없는 상태로 만들어지며, 허가되지 않은 사용자 또는 사용 방법으로부터 콘텐츠를 보호해야 한다.

② 최신의 암호화 알고리즘을 사용하여 해킹이 어렵도록 구성되어야 한다.(예:AES((Advanced Encryption Standard) 알고리즘 사용)

4.2.3 홈 네트워크

① 홈네트워크 서비스가 제대로 이루어지려면 사용자 인증이나 데이터 암호화 또는 콘텐츠 사용 제어와 같은 보안기술의 적용이 필수이다.

4.2.4 DVD 등 광 미디어

가. 보안성

① Copying과 Ripping으로부터 콘텐츠를 보호(Ripping이란, 오디오나 비디오 콘텐츠를 하드 디스크로 복사하는 절차를 의미)해야 한다.

② 가능하다면, 다중의 복제방지 기술을 제공하여 여러 타입의 불법복제에 대응할 수 있어야 한다.

③ 복제방지는 Copying & Ripping 프로그램들을 감지하고 정상적으로 동작하는 것을 막아야 한다.

④ Active와 Passive 복제방지가 결합하여 소프트웨어 및 하드웨어 레벨에서의 복제를 방지해야 한다.

5. DRM 소프트웨어의 보안성 평가모델

DRM 소프트웨어의 보안성 평가모델은 기반이 되는 품질특성 체계[6][8]와 평가를 위한 메트릭(metrics, measure), 메트릭의 활용을 위한 품질검사표와 점검표 그리고 이를 종합한 시험모듈로 구성된다. DRM 소프트웨어의 보안성에 대한 특성은 소프트웨어 제품평가에 관한 국제표준인 ISO/IEC 9126과 ISO/IEC 12119의 품질특성 체계에 근간을 두고 있다.

두 표준에서는 품질특성으로서 기능성, 신뢰성, 사용

성, 효율성, 유지보수성, 이식성의 6가지 특성을 정의하고 있으며, 보안성은 기능성에 속하는 부특성 중의 하나이다. <Table 5>에 기능성에 관한 부특성을 보이고 있다.

〈Table 5〉 Quality Characteristics System of Functionality

Quality Characteritics	Quality Subcharacteritics	Concept
Functionality	Suitability	The capability of the software product to provide an appropriate set of functions for specified tasks and user objectives.
	Accuracy	The capability of the software product to provide the right or agreed results or effects.
	Interoperability	The capability of the software product to interact with one or more specified systems.
	Security	The capability of the software product to protect information and data so that unauthorised persons or systems cannot read or modify them and authorised persons or systems are not denied access to them.
	Compliance	The capability of the software product to adhere to standards, conventions or regulations in laws and similar prescriptions.

보안성의 중요성으로 인해 6가지 품질특성과 대등한 레벨의 특성으로 격상되어 표준화되는 상황이다.

시험모듈은 품질평가를 위한 평가 메트릭에 대해 소프트웨어 품질평가 프로세스를 위한 국제표준인 ISO/IEC 14598[7] - 부분 6의 형식에 의거하여 평가를 위한 제반 사항을 문서로서 정의하는 체계이다. 시험을 위한 모듈에 대해 기본적인 사항을 정리하면 다음과 같다.

5.1 시험모듈의 체계와 개발 내역

5.1.1 시험모듈의 체계

시험모듈은 품질시험에 관한 전반적인 사항을 정리하여 문서화한 것으로 시험의 개요, 기법, 메트릭에 대한 상세 내용, 적용 절차, 결과에 대한 해석 등을 포함하고 있으며 품질평가 프로세스에 관한 국제표준인 ISO/IEC 14598의 <부분 6>인 평가모듈의 형식에 근거하여 작성하였다. 품질시험 모듈의 체계는 <Table 6>과 같다.

〈Table 6〉 System of Quality Testing Module

구성 항목		내용
Outline	Concept of metric	The basic concept of evaluation modules
	Measurement purposes	what you want to get through the measurement of the evaluation module
	Metric category	where the metric belongs
	Term Explanation	explanation of related terms
Coverage	application target	target such as document or software
	Necessary resources	Tools/resources required to apply the metric
	Techniques	Testing techniques that can be applied
	Considerations	Relevant information to be considered when apply evaluation modules
Reference		Related Documents that metrics are derived
Metric	Measurement items	Data items to be measured
	Measurement method	specific measure for the measure item to configure the metric
	Expression	definition of expression using the data items
Application Procedures		Description on specific procedures and method to perform the test
Results interpretation and reporting	Mapping of the measurements	The range of metric results
	Interpretation of the measurement results	Provide guidance about how to interpret the measurement results
	Reporting requirements	items to be reported as a document on the measurement results

5.1.2 메트릭 개발 내역

본 연구를 통해 <Table 7>에 나타낸 DRM 소프트웨어의 보안성에 관해 메트릭을 개발하였다.

〈Table 7〉 The contents of test modules about security of DRM Software

Subcharacteritics	Item	Related Items
Security	Use control	Only one who have duly issued license can use the contents according to the rules
	Temper Resistance	Prevent illegal use by the date change for the contents with the specified period
	License Integrity	To ensure the integrity of license information to prevent unauthorized modification

	Encryption technology	Blocking access for users who are not licensed for use by using encryption technology.
	Setting Permissions	A specified user can use the Contents only within the specified rights
	Symmetric Key Management	Securely manage and distribute symmetric encryption key (CEK) used for encryption of digital content
	Blocking of Function	Whether to block the function which needs blocking
	Prevention of document extracts	prevent arbitrary use or the extraction of decrypted document
	Persistent Protection	Blocking the path for illegal document distribution and use of document by an unauthorized party
	Usage monitoring	Trace of path to contents move through monitoring of content usage
	…	…

5.2 품질검사표

품질검사표는 시험모듈에 정의된 메트릭을 기준으로 실제 품질 시험을 수행하는 과정에서 편리하게 활용할 수 있도록 필요한 핵심적인 사항들을 추출하여 정리한 표로서 메트릭명과 개념, 측정항목, 메트릭의 계산식, 결과의 영역, 결과값, 문제점 기술 부분 등으로 구성되어 있다. 이러한 품질검사표의 예를 <Table 8>에 나타내었다.

〈Table 8〉 An example of quality inspection table

Measure name		Diversification of the packaging approach		
		Is it possible to choose packaging method depending on the need?		
Measurement items	A	The number of packaging approach		
		- Pre-Packaging - On-the-fly packaging		
	B	The number of Packaging method to support in the software		
		A measure of the number of packaging approach supported by the DRM software to be tested.		
expression		Diversification of the packaging approach = B/A		
The range of results		0 ≤ Diversification of the packaging approach ≤ 1	result value	
problem				

품질검사표에는 기본적으로 메트릭명과 메트릭이 측정하고자 하는 내용에 대한 문장이 포함되어 있다. 측정항목은 계산식을 통해 메트릭을 구성하는 요소로 1개 이상의 요소로 구성되며 항목 개요와 측정 방법에 대한 기술을 포함한다. 결과 영역은 계산식에 의해 산출되는 값이 나타날 수 있는 영역으로 메트릭들은 전체적으로 0과 1사이의 값으로 사상될 수 있도록 정의하였다.

5.3 점검표

점검표는 품질검사표를 이용하여 측정항목에 대한 측정을 수행하기 위해 작성된 테스트 케이스의 시험 목록이다. <Table 9>는 DRM에 의해 제공되어야 할 기능차단이 적절히 이루어지고 있는가를 점검하는 점검표의 예를 보여주고 있다.

점검표의 도출은 DRM 소프트웨어의 보안성에 관한 요구사항으로부터 출발한다. DRM 소프트웨어의 보안성 전반에 관한 요구사항(품질특성)이나 도메인별로 도출된 요구사항에서 특정 메트릭의 개념과 부합되는 내용을 도출하여 점검표의 항목을 구성하게 된다.

〈Table 9〉 Checklist of Blocking of Function

No	Item name	Test result
1	Copy / paste in the document security is limited?	Y
2	Is it limited to save the original in the document security?	N/A
3	Is it limited to capture screens in the document security?	Y
4	Is Copy & Paste function being blocked in the Important documents?	Y
5	Is the use of printer controlled-in a specific User, group/p and PC?	Y
6	Is the insertion of print marking controlled-in a specific User, group/p and PC?	Y
7	Is voice capture being blocked in online music?	Y
8	Is the download through URL link being blocked in online music?	N
9	Is the copy method being blocked that intercept network transmission data in online music?	Y
10	Is the copy using a camcorder being blocked in case of a video?	Y
11	Is the copy using a capture program being blocked in case of a video?	Y
…	…	…
The number of Y		
The number of N		
Result		

6. 결론

컴퓨터의 용도에 따라 다양한 소프트웨어가 개발되어 활용되고 있다. 이제 사용자는 다양한 유형의 소프트웨어들 중에서 자신이 컴퓨터를 사용하는 목적과 용도에 알맞은 소프트웨어를 적절히 선택할 필요성이 제기되었다. 선택의 기준은 결국 소프트웨어의 품질이며 특정 유형의 소프트웨어에 대한 선택 기준이 될 수 있는 품질에 대해 정의하고 품질을 측정하기 위한 방법의 구축에 따른 품질시험 및 인증 방법에 대한 연구가 지속적으로 추진되고 있다.

지금까지 국내 소프트웨어 제품 인증에 대한 관련 기반 연구는 패키지 소프트웨어, 산업용 소프트웨어, 임베디드 소프트웨어, 의료용 소프트웨어, 생체인식 소프트웨어 등 다양한 분야에서 연구되어 왔으며 시험 인증 현장에서 활용되고 있다.

그러나 최근 급격히 발전하고 있는 DRM 소프트웨어 분야의 품질평가 모델에 대한 연구는 아직까지 미흡한 부분이 있는 실정이다.

DRM 소프트웨어에 대한 제품 인증 체계가 구축되기 위해서는 먼저 품질 시험을 위한 측정 방법과 기준에 대한 연구가 선행되어야 한다. 국내에서 패키지 소프트웨어 분야를 필두로 소프트웨어 품질시험 방법에 대한 연구에 많은 진전이 있었으며 초기단계의 품질인증 서비스가 진행되고 있지만 다양한 소프트웨어 분야를 전반적으로 커버할 수 있는 수준에 이르기 위해서는 향후 지속적인 연구 개발이 이루어져야 할 것이다. 현재, 세계적으로 DRM 소프트웨어 시장은 빠른 성장세를 보이고 있으며 다양한 콘텐츠 분야에서 DRM 소프트웨어 시장의 급속한 확산이 진행되고 있다.

본 연구에서는 DRM 소프트웨어의 보안성에 관한 품질을 평가할 수 있는 모델을 개발하기 위한 연구로서 DRM 소프트웨어 분야 기반 기술과 관련 응용 기술을 분석하고 DRM 소프트웨어 평가모델 개발을 위해 DRM 소프트웨어 제품에 관한 품질 요구사항을 파악하고 DRM 소프트웨어 유형별 품질평가의 주요 요소를 분석하여 품질시험 메트릭을 개발하였다.

향후, DRM 소프트웨어의 보안성에 대한 평가사례의 구축 및 축적을 통해 객관성과 타당성을 갖춘 평가체계로 발전시키기 위한 지속적인 연구를 수행할 필요가 있다.

REFERENCES

[1] Ki-Jung Lee, Tae-Kyoung Kwon, Seong-Woon Hwang, Iki-Song Yoon, A Study on the Secure Storage Device for Protecting Cryptographic Keys in Untrusted DRM Client Systems, Journal of the Korea Institute of Information Security and Cryptology Vol 14 No. 2, p.4, 2004. 4.

[2] Seong-Eun Yang, A Study on document security that use DRM(Digital Rights Management) Solution, Dongguk University, p. 6, 2008. 2.

[3] Tae-Hyun Kim, Ho-Gap Kang, Hee-Don Yoon, Seong-Hwan Cho, A Study of 데UB-based Interoperability Method of Rights Information Supporting Mutual Comparability of eBook DRM, Journal of the Institute of Webcasting, Internet and Telecommunication, Vol.12, No.2, p.206, 2012. 12.

[4] Ho-Gap Kang, et al., Study on technical specification for interoperability between heterogeneous e-Book DRMs, Korea Copyright Commission, 2010.

[5] Ho-Gap Kang, Tae-Hyun Kim, et al., A Study of ePub-based Standard Framework Supporting Mutual Comparability of eBook DRM, Vol. 11, No. 6, The Journal of The Institute of Webcasting, Internet and Telecommunication, pp. 235-245, 2011.

[6] ISO/IEC 9126, "Information Technology - Software Quality Characteristics and metrics

[7] ISO/IEC 14598, "Information Technology - Software product evaluation - Part 1~6.

[8] ISO/IEC 12119, "Information Technology - Software Package - Quality requirement and testing".

이 하 용(Ha-Yong Lee)

- 1993년 2월 : 강원대학교 전자계산학과 졸업(이학사)
- 1995년 2월 : 강원대학교 대학원 전자계산학과 SW공학전공(이학석사)
- 2005년 2월 : 호서대학교 벤처전문대학원 컴퓨터응용기술학과졸업 (공학박사)
- 1996년 3월 ~ 2005년 8월 : 경희대, 경원대, 선문대, 호서대 컴퓨터공학부강사

- 1995년 6월 ~ 2002년 12월 : 한국SW품질연구소 선임연구원
- 2005년 9월 ~ 현재 : 서울벤처대학원대학교 교수
- 관심분야 : 소프트웨어공학(특히, S/W 품질보증과 품질평가, 품질감리, 객체지향 프로그래밍, 객체지향 분석과 설계, 컴포넌트기반 S/W 개발방법론, 품질평가)
- E-Mail : lhyazby@suv.ac.kr

김 중 규(Jung Gyu Kim)

- 1979년 2월 : 한양대학교 전자공학과 졸업(학사)
- 1995년 8월 : 한양대학교 전자공학과 졸업(석사)
- 2010년 2월 : 건국대학교 컴퓨터정보통신학과 졸업(공학박사)
- 1979년 2월 ~ 1998년 12월 : 삼성전자 이사
- 1999년 6월 ~ 2003년 5월 : 현대정보기술 상무 본부장
- 2004년 9월 ~ 2006년 7월 : 동부정보기술 부사장
- 2007년 1월 ~ 2008년 12월 : 디비정보통신 사장
- 2012년 3월 ~ 현재 : 호서대학교 글로벌창업대학원 부교수
- 관심분야 : IT 창업, 컴퓨터정보통신, S/W프로젝트관리
- E-Mail : jgkimjg@yahoo.co.kr