情報保護學會論文誌
第17卷 第1號, 2007. 2

재생 공격에 안전한 Domain DRM 시스템을 위한 License 공유 방식*

최 동 현,[1†] 이 윤 호,[1] 강 호 갑,[2] 김 승 주,[1] 원 동 호[1‡]
[1]성균관대학교 정보통신공학부 정보보호연구소, [2]DRM inside

A Secure License Sharing Scheme for Domain DRM System Against Replay Attack

Donghyun Choi,[1] Yunho Lee,[1] Hogab Kang,[2] Seungjoo Kim,[1] Dongho Won[1†]
[1]Information Security Group, Sungkyunkwan University, [2]DRM inside

요 약

현재의 DRM 시스템은 콘텐츠의 불법적인 사용을 방지하기 위해 제한에 지나치게 초점을 맞추고 있어 사용자의 정당한 권리를 침해하는 측면이 있다. 이러한 문제를 해결하기 위해 AD (Authorized Domain) DRM 방식이 제안되었다. AD DRM은 인가된 도메인 내에서 기존의 DRM 시스템보다 자유로운 콘텐츠 사용을 보장하고 있지만, 도메인에 속한 모듈의 탈퇴 과정에 필요한 자원 소모가 많은 인증서 폐기 메커니즘의 유지와 인가된 도메인을 벗어나더라도 기존의 콘텐츠를 사용할 수 있는 문제점이 있다.

본 논문에서는 가환암호를 이용하여 AD DRM이 가지고 있는 이러한 문제점을 해결하고, 보다 안전한 라이선스 공유를 위해 타임스탬프를 활용한다. 제안하는 시스템은 자원 활용 측면에서 보다 효율적이고, 재생 공격에 안전하다.

ABSTRACT

The purpose of DRM is to protect the copyrights of content providers and to enable only designated users to access digital contents. From the consumers' point of view, they have a tendency to go against complex and confusing limitations. Moreover, consumers' rights of use of the content obtained legally were frequently harmed by arbitrary limitations. The concept of Authorized Domain (AD) was presented to remove such problems. However, the previous work on authorized domain has two problems. The first is that it requires a rather expensive revocation mechanism for withdraw process. The second is that the modules still can play contents which are previously obtained even though they are currently out of the authorized domain. On the contrary, our scheme presents the content from being played by modules which are out of the domain for better security. Furthermore our scheme does not need to maintain a revocation list and prevent replay attack.

Keywords : *DRM, Home Networks*

접수일: 2007년 1월 16일; 채택일: 2007년 1월 27일
* 본 연구는 정보통신부 및 정보통신진흥원의 대학 IT연구센터 육성·지원사업의 연구결과로 수행되었음.
† 주저자, dhchoi@security.re.kr
‡ 교신저자, dhwon@security.re.kr

Ⅰ. 서 론

현재의 DRM 기술은 콘텐츠의 불법 사용 제한에 지나치게 초점을 맞추고 있다. 다시 말하면 최초 콘텐츠를 구매한 DRM 모듈에서만 콘텐츠를 사용할 수 있도록 설계되어 있다. 이는 사용자의 정당한 권리를 제한하는 것으로 볼 수 있다. 따라서 사용자로 하여금 자신이 구매한 콘텐츠를 사적 복제의 범위 내에서 자유롭게 사용하도록 하는 것이 바람직할 것이다. 이러한 사용자 권리의 제한 문제를 해결하기 위해 제안된 것이 AD DRM이다[1, 8]. AD DRM은 인가된 도메인 내에서 기존의 DRM 시스템보다 자유로운 콘텐츠 사용을 보장하고 있지만, 도메인에 속한 모듈의 탈퇴 과정에 필요한 자원 소모가 많은 인증서 폐기 메커니즘의 유지와 인가된 도메인을 벗어나더라도 기존의 콘텐츠를 사용할 수 있는 문제점이 있다.

본 논문에서는 디지털 콘텐츠를 사용자가 속한 도메인 안에서 자유롭게 사용할 수 있는 라이선스 공유 방식을 제안한다. 즉, 가환 암호(commutative encryption)를 사용하여 라이선스를 두 번 암호화함으로써 인가된 도메인 내에서 콘텐츠를 자유롭게 사용할 수 있게 하고, DRM 모듈이 도메인을 벗어날 경우 콘텐츠 사용을 제한하여 콘텐츠 저작자의 권리도 함께 보호한다. 또한 안전한 라이선스 공유를 위해서 타임스탬프를 이용하여 재생 공격으로부터 안전한 라이선스 공유 방식을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 Domain DRM시스템에 대해 설명하고, 3장에서는 제안하는 DRM 시스템에 대하여 기술하고, 기존의 DRM 시스템과 비교한다. 마지막으로 4장에서 결론을 맺는다.

Ⅱ. 관련연구

AD DRM은 인가된 도메인에 있는 장치들 사이에 디지털 콘텐츠의 자유로운 공유를 가능하게 한다[9,10]. 여기서 도메인이란 홈 네트워크처럼 콘텐츠를 재생할 수 있는 PC, PDA, DVD 플레이어 등으로 구성되어 있는 네트워크를 말한다[7]. AD DRM은 최초 홈 네트워크에서 콘텐츠를 보호하기위해 개발되었다. 초기에 제안된 메커니즘들은 소비자의 올바른 사용과 편리성의 문제를 정확히 해결하지 못했다. 그 후에 Digital Video Broadcasting (DVB)[3]에 의해 AD라고 불리게 되었다[4].

2.1 xCP

IBM에 의해서 제안된 xCP[5]는 AD DRM 시스템이다. 이 방식은 안전한 콘텐츠 분배를 위해 broadcast encryption을 사용한다. 또한 이 시스템은 공개키 암호 방식이 아닌 대칭키 암호 방식을 사용하기 때문에 경제적인 측면에서 장점이 있다. 하지만 broadcast encryption을 사용하기 때문에 xCP는 도메인에 속한 하나의 멤버가 탈퇴 할 때 자원이 많이 소모되는 단점이 있다.

2.2 SmartRight

Thompson에서 제안한 SmartRight[6] 시스템은 CE 장치 안의 스마트카드 모듈에 의존한다. 일단 장치가 도메인에 가입을 하면, 도메인에 속한 장치들은 대칭 도메인 키를 공유 한다. 이러한 접근 방법은 도메인에 속한 장치가 탈퇴할 경우 도메인 키의 취소와 재설정을 필요로 한다.

2.3 A DRM security architecture for home networks[1]

[1]은 소비자가 소유하고 있는 장치들로 이루어진 홈 네트워크의 보안 구조를 다루고 있다. 그들이 제안하는 방법은 AD라 불리는 장치들로 이루어진 그룹을 생성하고 그 그룹 내에서는 라이선스에 따라 그룹안의 장치들 간 자유로운 콘텐츠 공유를 가능하게 하는 것이다. 이 방식의 핵심은 혼합 승인 체크와 그룹 생성 프로토콜이다. 이것은 미리 분배된 대칭키를 기반으로 설계되어 공개키 암호화 방식의 사용을 최소로 줄인다. 이 방식의 구조는 키의 취소와 효과적인 업데이트를 가능하게 한다. 하지만 이 구조는 인증서 취소 리스트가 사용자에 의해서 만들어지기 때문에 사용자들에 의해서 오용될 소지를 가지고 있다. 게다가 AD 시스템은 장치가 도메인으로부터 벗어날 경우 새로운 콘텐츠의 사용은 불가능하게 설계되어 있지만, 기존에 가지고 있던 콘텐츠의 사용은 도메인을 벗어나도 가능하다는 문제점을 가지고 있다.

Ⅲ. 제안하는 DRM 시스템

이 장에서는 도메인 DRM 시스템을 위한 라이선스

공유 방법에 관해 설명한다. 또한 라이선스 공유시 타임 스탬프를 사용하여 재생 공격에 안전한 공유 방법을 제안한다. 제안하는 시스템의 운영 환경에 제한이 있는 것은 아니지만 편의상 제안하는 시스템은 홈 네트워크 환경 하에서 사용된다고 가정한다.

3.1 용어

본 논문에서 사용할 몇 가지 용어에 대해서 설명한다. 그중 가환암호는 암호화 순서에 상관없이 복호화 할 수 있는 방식을 말하며 식 (1)을 만족한다.

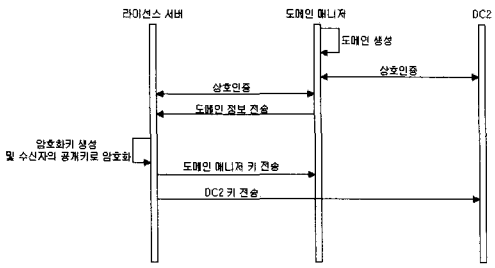
$$CE_{K1}(CE_{K2}(M)) = CE_{K2}(CE_{K1}(M)) \quad (1)$$

- $CE_K(\cdot)/CE_K^{-1}(\cdot)$: 키 K와 가환 암호계를 이용한 암호화 및 복호화
- $E_{PUB\_A}(\cdot)$: A의 공개키를 이용한 암호화
- $D_{PRI\_A}(\cdot)$: A의 개인키를 이용한 복호화
- $DS_A(\cdot)$: A의 서명 생성정보를 이용한 전자서명
- $H(\cdot)$: 해쉬함수
- K_C : 콘텐츠 암호화 키
- DC : DRM 사용자 모듈
- DM : 도메인 관리자

3.2 도메인 생성

Step 1 : 도메인 매니저 생성. 하나의 도메인에는 하나의 도메인 매니저가 필요하다. 도메인이 생성될 때 도메인 매니저가 동시에 생성되고, 도메인 매니저는 도메인 ID를 생성하게 된다. 홈 네트워크 환경의 경우 도메인 매니저는 게이트웨이가 그 기능을 담당한다.

Step 2 : DRM 사용자 모듈 등록. 새로운 DRM 사용자 모듈 하나를 도메인에 추가 하려면 그 모듈의 도메인 매니저에게 등록하는 과정이 필요하다. 그 모듈은 도메인 매니저에게 자신의 ID, 미리 할당되어 있는 공개키와 해당 인증서를 도메인 매니저에게 전송한다. 인증서 교환을 통해 도메인 매니저와 사용자 모듈은 서로를 인증할 수 있다[11].



〔그림 1〕 도메인 생성과 등록

2.3 도메인 등록

도메인을 생성한 후에 도메인 매니저는 라이선스 서버에 등록할 필요가 있다. 등록하는 과정은 도메인 인증과 키 분배 두 단계로 이루어진다.

Step 1 : 도메인 인증. 도메인 매니저와 라이선스 서버는 서로간의 인증서 교환을 통해서 인증을 한다. 인증을 완료하면 도메인 매니저는 자신이 가지고 있는 도메인 정보(도메인 ID, 모듈 리스트, 각 모듈들의 공개키)를 라이선스 서버로 전송한다.

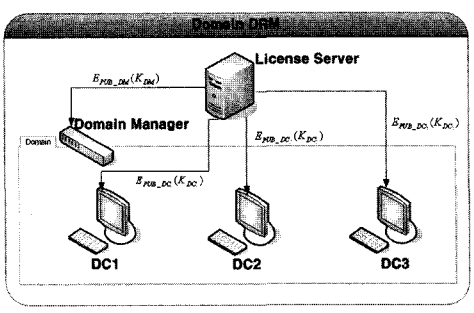
Step 2 : 키 분배. 라이선스 서버는 도메인 매니저와 사용자 모듈들에게 할당할 각각의 비밀키를 생성한다. (그림 2)에서 보이는 바와 같이 생성된 비밀키는 사용자 모듈이나 도메인 매니저의 공개키로 RSA 암호화 방식을 이용하여 암호화되어 전송된다.

$$E_{PUB\_DM}(K_{DM}) \quad (2)$$

$$E_{PUB\_DC\,i}(K_{DC\,i}) \quad (3)$$

3.4 콘텐츠 사용

장치가 콘텐츠를 재생하려면 라이선스 서버로 부터 라이선스를 발급 받고, 받은 라이선스를 도메인 매니저로



〔그림 2〕 라이선스 서버에 의한 키분배

부터 복호화 과정을 거쳐야만 한다. 단계는 다음과 같다.

Step 1 : 라이선스 발급. 도메인에 속한 장치가 디지털 콘텐츠를 구매하면 해당 콘텐츠를 암호화한 콘텐츠 암호화 키 K_C를 패키징 서버가 라이선스 서버로 전송한다. 라이선스 서버는 이를 콘텐츠 구매자에게 전송한다. 제안하는 시스템에서 라이선스 서버는 K_C를 도메인 초기 등록과정에서 할당된 구매자의 키로 암호화한 후 암호화된 값을 다시 한 번 도메인 매니저에게 할당한 키로 암호화 한다. 이때 사용하는 암호방식은 가환암호 방식을 사용한다. 가환암호계의 예로는 [2]와 함께 스트림 암호를 들 수 있다.

도메인에 속한 장치 DC_2가 콘텐츠를 구매하면 라이선스 서버는 식(4) 처럼 도메인 매니저 키와 DC_2키를 이용 가환암호 방식을 이용해서 콘텐츠 암호화키를 두 번 암호화하여 DL_2를 생성한다.

$$License\ Server: DL_2 = CE_{K_{DM}}(CE_{K_{DC2}}(K_C)) \quad (4)$$

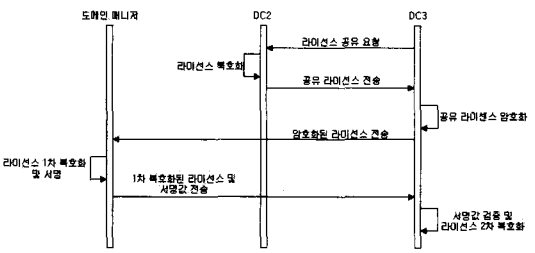
이렇게 생성된 값 DL_2을 라이선스 서버는 콘텐츠의 구매자에게 전송한다.

Step 2 : 도메인 매니저에 의한 라이선스 복호화. 콘텐츠 구매자 DC_2는 라이선스 서버로부터 받은 DL_2를 도메인 매니저에게 전송한다. 도메인 매니저는 받은 정보를 자신이 라이선스 서버로부터 받은 키로 복호화 한 후 그 값에 현재 시간 값의 타임스탬프 T_n을 연접하여 CL_2를 생성한다. 도메인 매니저는 식 (6)에서 처럼 CL_2를 해쉬한 값에 전자 서명을 한다.

$$Domain\ Manager: CL_2 = CE^{-1}_{K_{DM}}(DL_2) \parallel T_n \quad (5)$$

$$Domain\ Manager: S_2 = DS_{DM}(H(CL_2)) \quad (6)$$

이렇게 생성된 정보 CL_2와 서명값 S_2는 DC_2에게 전



[그림 3] 라이선스 공유와 콘텐츠 사용 과정

송된다. DC_2는 받은 S_2를 도메인 매니저의 검증 정보로 검증하여 이 값이 CL_2를 해쉬한 값과 같고, T_n값과 DC_2의 현재시간과의 차가 임계값 이하로 나타나면 이 값의 정당성을 인정한다. 정당성이 인정되면 DC_2는 CL_2값에서 T_n을 제거한 값을 초기 등록과정에서 라이선스 서버로부터 할당 받은 키로 복호화 하여, K_C를 얻는다. DRM 사용자 모듈은 이렇게 얻은 K_C를 이용 콘텐츠를 재생한다.

$$DC_2: K_C = CE^{-1}_{K_{DC2}}(CE_{K_{DC2}}(K_C)) \quad (7)$$

3.5. 라이선스 공유

같은 도메인 내에서 라이선스를 공유하기 위해서 DC_2는 라이선스 서버로부터 받았던 DL_2를 자신의 키로 복호화 한다. 복호화된 SL은 DC_3에게 전송한다.

$$DC_2: SL = CE^{-1}_{K_{DC2}}(CE_{K_{DM}}(CE_{K_{DC2}}(K_C))) \quad (8)$$

SL을 받은 DC_3는 수신한 정보를 다시 초기 도메인 등록 단계에서 라이선스 서버로부터 받은 키로 암호화하여 도메인 매니저에게 전송한다.

$$DC_3: DL_3 = CE_{K_{DC3}}(CE_{K_{DM}}(K_C)) \quad (9)$$

도메인 매니저는 DC_3로부터 받은 DL_3을 자신이 가지고 있는 키로 복호화 한 후 그 값에 현재 시간 값의 타임스탬프 T_n을 연접하여 CL_3를 생성한다. 도메인 매니저는 식 (11)에서 처럼 CL_3를 해쉬한 값에 전자 서명을 한다.

$$Domain\ Manager: CL_3 = CE^{-1}_{K_{DM}}(DL_3) \parallel T_n \quad (10)$$

$$Domain\ Manager: S_3 = DS_{DM}(H(CL_3)) \quad (11)$$

이렇게 생성된 정보 CL_3와 서명값 S_3는 DC_3에게 전송된다. DC_3는 받은 S_3를 도메인 매니저의 검증 정보로 검증하여 이 값이 CL_3를 해쉬한 값과 같고, T_n값과 DC_3의 현재시간과의 차가 임계값 이하로 나타나면 이 값의 정당성을 인정한다. 정당성이 인정되면 DC_3는 CL_3값에서 T_n을 제거한 값을 초기 등록과정에서 라이선스 서버로부터 할당 받은 키로 복호화 하여, K_C를 얻는다. DRM 사용자 모듈은 이렇게 얻은 K_C를 이용 콘텐츠를 재생한다.

〔표 1〕 다른 DRM 시스템과의 비교

	xCP	[1]	제안하는 방식
도메인 내에서의 콘텐츠 공유	○	○	○
인증서 폐기 리스트 필요 여부	○	○	X
도메인 밖에서의 콘텐츠 사용 제한	X	X	○

$$DC_3 : K_C = CE^{-1}_{K_{DC3}}(CE_{K_{DC3}}(K_C)) \quad (12)$$

3.6 다른 DRM 시스템과의 비교

〔표 1〕에서 보이는 바와 같이 제안하는 DRM 시스템은 기존의 DRM 시스템과 동일한 기능을 수행함과 동시에 라이선스를 구매한 사용자가 자신이 속한 도메인 내의 다른 모듈에서도 사용이 가능하다. 또한 타임스탬프를 사용하여 재생 공격에 안전하다.

Ⅳ. 결론

DRM이 정당한 콘텐츠 사용을 지나치게 제한한다면 이는 사용자의 정당한 권리를 침해 하는 것이다. AD DRM은 기존 오프라인 콘텐츠에서 가능한 사적 복제의 개념을 디지털 콘텐츠에 적용함으로써 콘텐츠 사용자의 권리를 보장하고자 하였다. 하지만, 도메인에서 모듈이 탈퇴 할 때 자원 소모가 많은 인증서 폐기 메커니즘을 필요로 하고, 모듈이 인가된 도메인을 벗어나더라도 기존의 콘텐츠를 사용할 수 있는 문제가 있었다. 제안한 방식은 가환암호를 사용하여 인가된 도메인내의 라이선스 공유를 가능하게 하고, 도메인을 벗어난 모듈의 경우 콘텐츠의 사용을 제한하여 사적 복제의 범위가 지나치게 확대되는 것을 방지하였다. 또한 라이선스 공유시 타임스탬프를 활용하여 재생 공격에 안전한 공유 방식을 제안하였다.

참고문헌

〔1〕 B. Popescu, B. Crispo, A. Tanenbaum, F. Kamperman, "Systems and architectures: A DRM security architecture for home networks," Proceedings of the 4th ACM workshop on Digital rights management, October 2004.

〔2〕 F. Bao, R.H. Deng, and P. Feng, "An efficient and practical scheme for privacy protection in the e-commerce of digital goods," ICICS'00, LNCS 2836,pp.162-170,2001.

〔3〕 DVB-The Digital Video Broadcasting Consortium. http://www.dvb.org/

〔4〕 Call for proposals for content protection & copy management technologies, July 2001.

〔5〕 F. Pestoni, IBM response to DVB-CPT call for proposals for content protection and copy management. http://www.almaden.ibm.com/software/ds/ContentAssurance/papers/xCP_ DVB.pdf

〔6〕 Smartright technical white paper. http://www.smartright.org/images/SMR/c ontent/SmartRight_tech_whitepaper_ jan28.pdf, Jan. 2003.

〔7〕 M. Ripley, C.B.S. Traw, S. Balogh, and M. Reed. Content Protection in the Digital Home. Intel Technology Journal, 6(9):49-56,2002.

〔8〕 A.M. Eskicioglu and E.J. Delp. An overview of multimedia content protection in consumer electronic devices. Signal Processing: Image Communication, 16(5):681-699, April 2001.

〔9〕 S.A.F.A. van den Heuval, W. Jonker, F.L.A. J. Kamperman, and P.J. Lenoir, "Secure Content Management in Authorized Domains," In Proc. IBC 2002, pp. 467-474, Sept. 2002

〔10〕 S. Sovio, N. Asokan, and K. Nyberg, "Defining Authorization Domains Using Cirtual Devices." In SAINT Workshops 2003, pp. 331-336, 2003.

〔11〕 L. Perlman, V. Welch, I. Foster, C. Kesselman and S. Tuecke. "Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile," RFC 2830, 2004.