IPTV 환경에서의 교환 가능한 DRM 적용 방안 연구

The Study to Interchangeable DRM in IPTV Environment

정병옥*, 서상호*, 오성흔*

Bynung-Ok Jung*, Sang-Ho Seo*, and Sung-Heun Oh*

요 약

IPTV 환경에서 복수개의 제한 수신 시스템 CAS(Condition Access System)를 안전하게 다운로드 하여 실행 하도록 하고, IPTV 사업자간에 단말의 호환성 및 이동성을 제공하기 위한 국내 표준화 규격인 iCAS(Interchangeable CAS)는 Real-Time Streaming 방송 보호를 위한 CAS 교환에 대해서만 정의하고 있다. 하지만, IPTV 양방향 통신 환경의 장점을 활용한 다양한 방송 서비스의 콘텐츠 보호 요구사항을 충족시키기에 CAS는 한계가 있으며, CAS가 가지는 한계를 보완하기 위해서 DRM 보호기술이 요구된다. 실시간 방송 서비스 또는 실시간 VOD 서비스의 콘텐츠는 CAS 기술로 보호가 가능하게 하고, PVR 또는 다운로드 VOD 서비스, 다운로드 콘텐츠의 공유 등과 같은 서비스는 DRM 기술로 보호가 가능하므로 CAS와 DRM 상호 보완을 통해 다양한 서비스에 대응하여 유연한 IPTV 단말 서비스 환경을 구축할 수 있다. 따라서, 본 논문에서는 iCAS 표준화 규격에 준하는 DRM 확장 적용 방안을 연구하고, 상용화에서 iCAS/DRM이 적용된 시스템 구성을 제안한다.

Abstract

Multiple CAS (Conditional Access System) could be safely downloaded and implemented in IPTV environment. Domestic standard of iCAS (Interchangeable CAS) which is providing device compatibility and mobility, can only defines CAS replacement for protecting Real-Time Streaming broadcast. CAS, however has limitations in IPTV's two-way communication environment where it needs to fulfill contents protection requirements of various broadcasting service. In order to supplement the limit of CAS, DRM protection technology should be required. Contents for real time broadcasting service or real time VOD service could be protected by CAS technology whereas services such as PVR, download VOD service or downloaded contents sharing could be protected by DRM technology. Therefore, a flexible IPTV device service environment could be constructed by mutual protection of CAS and DRM. This essay is going to research on the method of applying DRM based on iCAS standard, as well as proposing a system configuration applied with iCAS/DRM in commercialization.

Key words : IPTV, ICAS, CAS, DRM

I. 서 론

iCAS 표준은 인터넷 멀티미디어 방송사업의 전기통신설비에 관한 기술기준 중 '가입자 제한수신 모듈

* (주)디지캡(DigiCAP. co. Ltd.)
· 제1저자 (First Author) : 정병옥
· 투고일자 : 2012년 4월 26일
· 심사(수정)일자 : 2012년 4월 27일 (수정일자 : 2012년 6월 25일)
· 게재일자 : 2012년 6월 30일

은 단발장치에서의 분리 또는 교환과 상호호환이 가능해야 한다'는 조항에 따른 것이다. TTA가 여러 관련업체들의 참여로 개발한 표준으로 외국에서는 'DCAS (Downloadable CAS)'로 알려진 기술로서 국내 IPTV 서비스에 적용돼 IPTV 단말기의 호환성과 이동성을 갖게 한다.

하지만, IPTV 사업자가 기존의 DRM 보호 기술 영역의 서비스들은 iCAS 표준에 따라 서비스가 가능하지 않은 문제가 있다. 단말 장치에서 CAS는 분리 또는 교환 상호호환이 가능하지만 DRM 보호 기술의 분리 또는 교환 상호호환에 대해서는 iCAS 표준에 제정되어 있지 않기 때문에 IPTV 서비스 사업자에게는 iCAS 단말에서 할 수 있는 서비스가 제한될 수 있고 CAS와 DRM이 상호 보완하여 단말이 선택적으로 운용 가능하도록 서비스가 가능해야 하는 요구사항이 있다.

CAS는 실시간 방송과 관련된 과금 처리가 가능한 서비스에 적합하고, DRM은 콘텐츠를 단일 파일 형태로 다운로드 받아 사용해야 하는 서비스에 적합하다. CAS와 DRM중에 하나를 선택하여 콘텐츠 보호를 위한 체계로 사용하게 되면 각 단일 기술로는 상황에 따라 보안 취약점을 가지고 있다. CAS는 다운로드 받은 콘텐트에 대한 저적권 보호가 취약하고, DRM의 경우에는 실시간 방송의 결제에 대한 취약점을 가지는 특징이 있다. 실시간 방송 콘텐츠를 내려받을 때에는 CAS로 인증하고 이 콘텐츠를 사용자의 단말에 저장하거나 다른 단말로 2차 배포할 때 DRM 기술을 적용하는 이원화된 인증보호체계를 만드는 것이 필요하다.

본 논문에서는 iCAS의 교환 가능한 CAS 시스템을 확장하고, 표준에 준하는 범위 내에서 교환 가능한 DRM을 지원하는 방안을 연구하고, 상용화에서 CAS와 DRM이 상호 보완하여 운용 적용되는 iCAS/DRM 시스템을 제안한다.

Ⅱ. iCAS 표준 규격

iCAS는 IPTV 서비스를 위해서 콘텐츠 보호기술인 CAS를 안전하게 제공하고 사용하기 위한 목적으로 IPTV 수신 단말이 CAS 모듈을 안전하게 다운로드 받아 실행할 수 있도록 정의하는 기술 규격으로서 표준화된 기술 규격을 제공하여 IPTV 수신 단말의 호환성과 이동성을 보장한다.

iCAS 표준에서 세부 적으로 기술하고 있는 범위로는 IPTV 서비스 및 콘텐츠 보호 기술(CAS) 모듈을 안전하게 다운로드 받기 위한 서버 기술과 IPTV 수신 단말과의 프로토콜들을 정의하며, 다운로드 받은 서비스 및 콘텐츠 보호 기술을 단말에서 안전하게 관리하고 실행시키기 위한 IPTV 수신단말 컴포넌트들을 정의한다.[1]

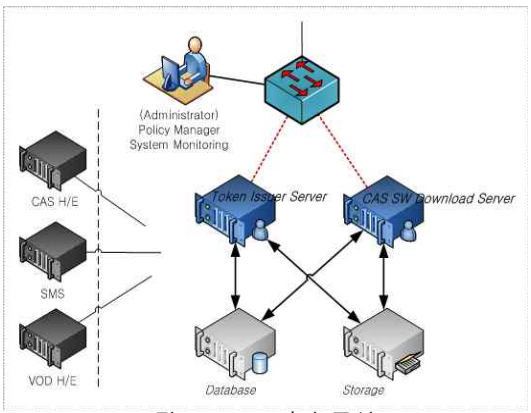

그림 1 iCAS 서버 구성도
Fig 1. iCAS server diagram

iCAS에서 정의하는 서버는 서비스 가입 확인 또는 콘텐츠 구매 시 콘텐츠 시청 권한을 증명하기 위한 CA Token을 발급하는 SMS 또는 CAToken 발급 서버와 CAS S/W를 저장 관리하며 단말의 요청에 따라 CAS S/W를 전송하는 SW Download 서버로 구성된다.[1]

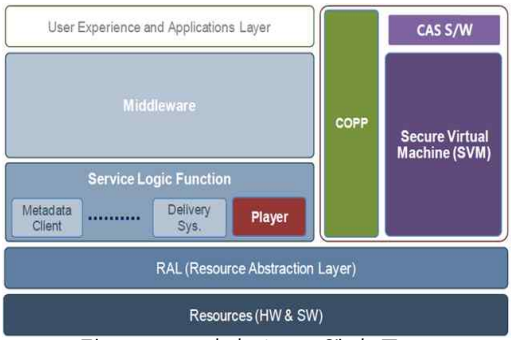

그림 2 iCAS 단말 소프트웨어 구조
Fig 2 iCAS device software structure

iCAS에서 정의하는 단말은 CAS(Conditional Access System) S/W , 다운로드 받은 CAS S/W를 검증하고 실행 시키기 위한 SVM(Secure Virtual Machine), 그리고

정당한 권한을 가진 사용자만이 CAS S/W를 다운로드 받을 수 있도록 관리하는 COPP(Content Protection Platform) 기술로 구성된다.[1]

- Player
  User Input, GUI 처리
  콘텐츠 검색 및 콘텐츠 버퍼 관리, 컨텐츠 재생 입출력 제어, audio/video 입출력, network 입출력, SVM에 Event 전송 (Channel/Content 변경 등), 컨텐츠 Descramble 재생

- COPP (Content Protection Platform)
  CAS S/W의 다운로드 및 로딩, CA Token을 이용한 Single-Sign-On 인증 및 CAS S/W 다운로드, CAS S/W 및 Policy 검증 및 SVM에 적재, SVM에 Event 전송 (시작/종료)

- SVM (Secure Virtual Machine)
  암호화된 CAS S/W 실행, CAS Key 관리 알고리즘 실행 (EMM/ECM 등), Renewability 지원

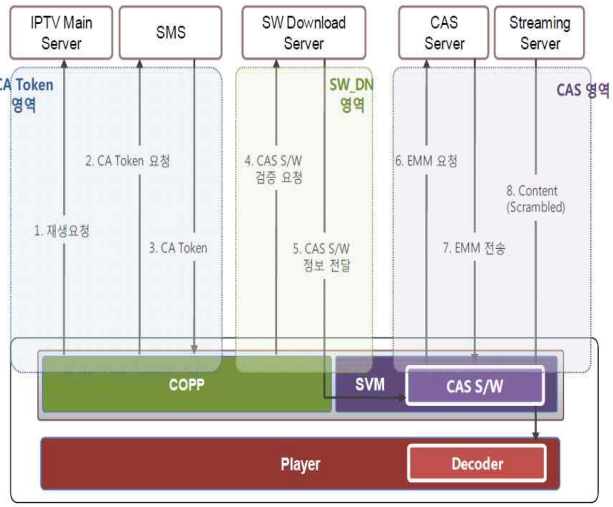

그림 3 iCAS 시스템 구조
Fig 3 Structure of iCAS System

Player는 IPTV Main Server 에 접속해서 사용하고자 하는 콘텐츠를 선택하고, CA Token 발급을 위하여 COPP Client 에게 구매 관련 정보를 전달한다. 이때 COPP Client는 SMS(Token Issuer Server) 에게 CA Token 발급을 요청하고. SMS는 정당한 콘텐츠 시청 권한 획득(서비스 가입 또는 콘텐츠 구매)이 확인된 경우 CA Token을 생성하고, 해당 CA Token을 암호화 하여 COPP Client 에게 전송한다.[1]

COPP는 발급 받은 CAToken 콘텐츠 자격증명을 S/W Download Server로 SW Download 요청할 때 전송하여 해당 콘텐츠 사용권한이 있는 단말인지 확인 후에 CAS S/W를 단말의 COPP로 다운로드 해주게 된다. COPP는 다운로드 받은 CAS S/W를 Secure Virtual Machine(SVM)상에서 동작하도록 실행한다. SVM 상에서 동작하는 CAS S/W는 CAS 규격에 따라 동작하며 해당 콘텐츠를 복호화 하기 위한 키를 발급받아 Player로 전달하고 암호화 콘텐츠를 복호화하여 재생하게 된다.

SVM은 CAS S/W를 실행하기 위한 가상의 실행환경을 제공함으로써, CAS SW를 플랫폼 독립적으로 구현 가능하도록 하고 있기 때문에 iCAS 규격을 만족하는 CAS S/W라면 어떠한 벤더의 CAS도 단말에서 운용이 가능하게 한다. 또한 서버와 단말간에 CAS S/W를 교환하기 위한 인터페이스를 표준에 기술하고 있기 때문에 IPTV 사업자간에 단말의 이동성을 보장하게 될 수 있게 한다.

Ⅲ. IPTV 환경에서 CAS와 DRM 보호 기술

CAS는 기본적으로 Broadcasting 전송 방식에 적용되어 왔다. 일반적인 IT 기술이 Interactive network을 기본적으로 고려하는 것과는 달리 CAS는 Non-interactive network 환경을 기본적으로 고려해야 한다. 그리고 CAS를 적용함에 있어서 Network 환경뿐만 아니라 방송(Mass Media Broadcasting)은 동시에 많은 시청자가 몰린다는 특징도 함께 고려해야 한다. 이러한 점이 DRM과 가장 큰 차이를 발생시키는 것이다.

CAS(Conditional Access System: 수신제한시스템)는 방송시스템에 가입자(subscriber) 개념을 도입하여 수신자격(entitlement)이 있는 시청자만 특정 프로그램을 수신할 수 있도록 하는 시스템으로, 송신기에서 스크램블링된 신호를 수신 측의 수신 인가를 받은 가입자만이 디스크램블링 하여 프로그램을 시청할 수 있도록 한다.[2]

DRM(Digital Rights Management) 기술은 디지털 콘텐츠의 생성에서 이용까지 유통 전 과정에 걸쳐 디지털 콘텐츠를 안전하게 관리/보호하고, 부여된 권한정보에 따라 디지털 콘텐츠의 이용을 제어/통제하는 기술이다. DRM은 세부적으로 디지털 콘텐츠의 지적 재산권 보호를 위해 사용되는 보호기술(Protection Technology)과 디지털 콘텐츠의 관리 효율화를 위해 사용되는 관리기술(Management Technology), 그리고 디지털 콘텐츠의 신뢰성 있는 전자상거래 환경을 위해 사용되는 유통기술(Distribution Technology)로 크게 구분할 수 있다.[2]

CAS는 실시간 방송과 관련된 스트리밍 콘텐츠의 보호와 실시간 과금 처리가 가능한 서비스에 적합하기 때문에 CAS 단일 기술로는 IPTV 사업자의 다양한 부가 서비스에 대응하여 콘텐츠의 보호 기능을 제공하기에는 취약한 부분이 있다. 따라서 CAS로 보호가능한 서비스는 다음과 같다.

- PPV(Pay per View) 유료 가입 채널 서비스
- Streaming VoD(Video on Demand) 서비스

IPTV 환경에서 DRM은 콘텐츠를 단일 파일 형태로 다운로드 받아 사용해야 하는 서비스에 적합하고 DRM 기술은 실시간 방송 결제에 대한 취약점을 가지고 있으며, 다음과 같은 부가서비스가 가능하게 하는 특징이 있다.

- 실시간 채널 방송의 PVR 저장된 콘텐츠의 보호
- PVR 저장된 콘텐츠를 2차 디바이스로 전송
- Download VoD 콘텐츠의 보호
- 로컬에 저장된 콘텐츠의 사용 시간/횟수 제한

IPTV 양방향 통신 환경의 장점을 활용한 다양한 방송 서비스의 콘텐츠 보호 요구사항을 충족시키기에 CAS 단일 보호기술 만으로는 한계가 있으며, CAS 보호기술이 가지고 있는 한계점을 보완하기 위해서 DRM 보호기술이 요구된다. 따라서 실시간 방송 콘텐츠를 내려받을 때에는 CAS로 인증하고 이 콘텐츠를 사용자의 단말에 저장하거나 다른 단말로 2차 배포할 때 DRM 기술을 적용하는 이원화된 인증보호체계를 만드는 것이 필요하게 된다.

Ⅳ. 연구 내용

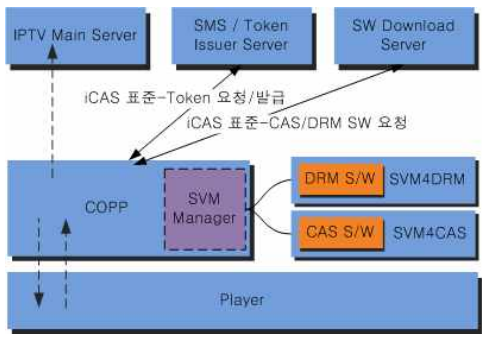

그림 4 iCAS 표준으로 DRM S/W 다운로드
Fig4. DRM S/W Download using iCAS standard

iCAS의 표준 범위내에서 CAS S/W처럼 DRM S/W를 다운로드하고, SVM에서 DRM S/W를 운용하기 위해서는 다음의 조건은 지켜져야 한다. Token 발급 서버와 SW 다운로드 서버와 단말COPP간의 인터페이스는 반드시 지켜져야 하고, S/W를 실행하는 SVM 규격과 SVM에서 구동되는 S/W Packaged 포맷 규격은 준수해야 한다.

단말에서 콘텐츠에 따라서 CAS S/W를 다운로드 받기 위한 서버와의 인터페이스를 변경 없이 DRM S/W를 다운로드 받기 위해서는 Token을 발급 받고, 발급 받은 Token을 사용하여 S/W 다운로드 서버로 S/W 다운로드를 요청하게 되면 서버는 S/W 다운로드 응답으로 CAS S/W 대신에 DRM S/W를 응답하게 되면 된다. 하지만, 단말은 다운로드 받은 S/W가 CAS인지 DRM인지 구분하기 위해서 다음과 같이 CAS S/W Response Message의 파라미터 중에서 Response Type(1byte)을 추가로 정의함으로서 단말이 다운로드 하는 S/W의 타입을 구분할 수 있게 된다.

- CAS S/W Response Message 기능 확장
  Response Type(1byte)
  -0x00:CAS S/W ID
  -0x01:CAS S/W ID and CAS S/W Package
  -0x10:DRM S/W ID
  -0x11:DRM S/W ID and DRM S/W Package

다운로드 받은 DRM S/W를 SVM에서 정상적으로 동작하기 위해서는 S/W Package Format 규격을 지켜서 만들어져 있어야 하는데, 해당 S/W Package가 CAS인지 DRM인지 구분할 수 있는 정보가 없기 때문에 헤더의 Type 정보를 추가로 확장하여 정의되어야 한다. 아래는 S/W Package의 헤더 구조이며 다음과 같은 정의로 CAS와 DRM을 구분한다.

표 1 S/W Package의 헤더 구조
Table 1. Header structure of SW Package

Prefix (8bytes)
Version (2bytes)
Type (2bytes)
CAS S/W ID (4bytes)
Super CAS ID (4bytes)

- S/W Package 헤더 기능 확장
  Type (2bytes)
  -0x00:압축되지 않은 CAS S/W
  -0x01:압축된 Code와 Policy 포함된 CAS S/W

-0x10:압축되지 않은 DRM S/W
-0x11:압축된 Code와 Policy 포함된 DRM S/W

CAS S/W와 DRM S/W를 다운로드 받은 단말의 COPP는 Player의 요청에 의해서 상황에 맞는 적절한 S/W를 SVM에 로드시켜 CAS 및 DRM 보안 서비스가 동작 하도록 하는 역할을 해야 한다. 하나의 SVM에서 두 가지의 다른 CAS가 동시에 실행되면 안 되므로 SVM은 한번에 하나의 S/W만 구동할 수 있도록 규정하고 있다. 따라서, SVM에서는 동시에 CAS와 DRM이 동시에 운용될 수 없는 구조이다. CAS와 DRM은 상호 보완적인 보안 기술이기 때문에 동시에 구동이 되어야 하므로 SVM은 변경하지 않고 COPP의 SVM 관리 기능을 정의하여 CAS와 DRM이 동시 운용이 가능하게 해야 한다.

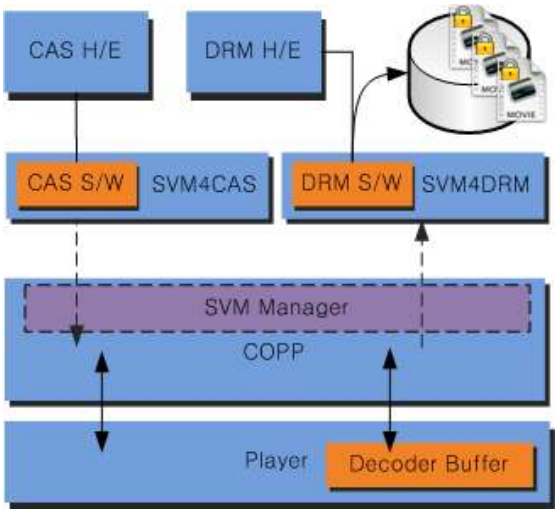

그림 5 COPP의 CAS와 DRM 관리
Fig 5 Management of the CAS and DRM in the COPP

COPP는 CAS S/W를 구동하기 위한 SVM과 DRM S/W를 구동하기 위한 SVM을 스레드로 실행하고, 각각의 SVM을 구분하여 관리할 수 있게 하고, Player에서의 실시간 방송 채널에 대한 CAS 로드 요청과 Downloadable VOD에 대한 DRM 로드 요청을 처리해 주게 되면 단말에서 CAS와 DRM을 동시에 운용이 가능하다.

단말이 초기 IPTV 사업자 서비스에 접속하게 되면, iCAS 표준에 의거하여 해당 사업자가 제공하는 CAS S/W와 DRM S/W를 단말의 COPP는 다운로드 받게 되고, COPP가 관리하는 SVM4CAS와 SVM4DRM에 각각의 S/W를 로드하게 되고 IPTV 사업자가 제공하는 서비스를 제공 받을 수 있다.

사용자가 시청 중인 방송을 정당한 서비스 범위에서 PVR 기능을 사용할 경우에 단말의 Player는 COPP를 통해 DRM S/W에게 DRM Packaging 요청을 하게 되고, DRM S/W는 해당 DRM 벤더의 비즈니스 시나리오에 의한 DRM H/E와의 PVR 준비후에 Player는 CAS S/W를 통해 Descramble되어 Decoder Buffer에 있는 암호화되지 않은 방송 스트림을 DRM S/W로 전송하여 해당 단말에서만 접근이 가능하도록 DRM으로 Packaging하여 단말의 Local Storage에 저장하게 된다.

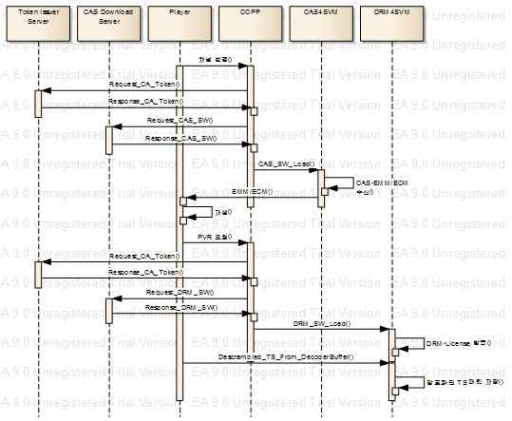

그림 6 CAS와 DRM의 실행위한 시나리오
Fig 6 Scenarios for Execution of CAS and DRM

V. 결 론

iCAS 표준 규격을 준수하면서 DRM S/W도 교환할 수 있는 구조를 위해서 iCAS 단말과 서버와의 S/W 다운로드 인터페이스의 메시지 포맷은 유지하고 CAS와 DRM을 구분할 수 있는 Type의 확장을 통해 CAS S/W와 DRM S/W를 COPP 단말에서 다운로드가 가능하며, SVM 규격에서 동작하는 S/W Package규격으로 만들어진 CAS S/W와 DRM S/W를 동시에 운용하기 위해 COPP에서 각각의 S/W를 동시에 구동할 수 있는 SVM을 관리하도록 기능을 확장하면 IPTV 사업자가 제공하는 CAS로 보호되는 콘텐

츠와 DRM으로 보호되는 콘텐츠를 사용할 수 있게 할 수 있다.

표 2 XCAS, iCAS와 제안방안의 비교
Table 2 Comparison of proposed protocol with XCAS and iCAS

표준기술 / 항목	XCAS	iCAS	제안방안
CAS 지원	O	O	O
DRM 지원	X	X	O
표준 분야	CableTV	IPTV	IPTV

iCAS를 도입하는 IPTV 사업자는 기존에 운용중인 CAS시스템과 DRM 시스템의 변경없이 iCAS 단말에 다운로드 시켜줄 S/W만 관리하면 iCAS 표준 단말일 경우에 기존의 제공하던 서비스 그대로 사용자에게 서비스를 제공할 수 있다.

감사의 글

본 연구는 지식경제 기술혁신사업의 다양한 방송·통신 서비스와 콘텐츠를 통합 제공하는 셋톱박스 오픈 플랫폼 개발(10040158)로 지원된 연구임.

참 고 문 헌

[1] IPTV 용 교환 가능한 CAS, (iCAS) TTAK.KO-08.0023/R1, 2010. 12.
[2] 윤기송, CAS-DRM 연동기술, *TTA 저널 NO.117*, 2010. 5.
[3] 김태현, [DRM] 표준화 이슈가 되고 있는 IPTV 보호기술 상호연동, *TTA 기술 표준 이슈*, 2007. 9.
[4] 백종호, 개방형 IPTV 환경조성을 위한 기술 표준화 방향 및 업계 동향, *KT 디지에코*, 2010, 4.

정 병 옥 (鄭昺玉)

2005년 3월 : 대전대학교 컴퓨터공학과(학사)
2007년 3월 : 대전대학교 컴퓨터공학과(공학석사)
2006년 10월 ~현재 : (주)디지캡
관심분야 : CAS/DRM, Forensic, Multimedia, 응용 보안

서 상 호 (徐祥豪)

2006년 3월 : 대전대학교 컴퓨터공학과(학사)
2008년 3월 : 대전대학교 컴퓨터공학과(공학석사)
2010년 3월 ~현재 : (주)디지캡
관심분야 : Mobile Security, CAS/DRM, 네트워크 보안

오 성 흔 (吳成欣)

1996년 3월 : 인천대학교 정보통신공학(학사)
1998년 3월 : 숭실대학교 컴퓨터학과(석사)
2002년 3월 : 숭실대학교 컴퓨터학과(박사)
2002년 3월 ~현재 : (주)디지캡
관심분야 : CAS/DRM, 암호학, 멀티미디어 시스템, 실시간 시스템