DOI: 10.3745/KIPSTC.2010.17C.5.407

다운로드형 수신제한시스템(XCAS)의 평가체계에 관한 연구

황 유 나[†] · 정 한 재[††] · 원 동 호[†††] · 김 승 주[††††]

요 약

CAS란 정당한 사용자만이 방송 콘텐츠에 접근할 수 있도록 하는 하드웨어 기반 시스템이다. CAS의 경우에는, 방송사업자 교체 시 셋탑 박스를 교체해야 한다는 점, 스마트카드에 의한 빈번한 오작동과 같은 문제점이 있었다. 이러한 문제점을 해결하기 위해 2009년에 XCAS가 개발되었다. 그러나 XCAS에 대한 평가체계는 현재까지 정해진 것이 없다. 기존의 평가체계는 XCAS에 그대로 적용하기에는 평가기준, 비용과 효율성 등이 떨어진다. 따라서 XCAS의 안전성 및 적합성을 검증·평가하는 체계가 필요하다. 본 논문에서는 기존에 존재하는 평가체계를 분석하고, XCAS에 적합한 평가체계를 제안한다. 제안하는 평가체계는 평가목적 및 대상, 평가주체, 평가절차, 평가제출물, 평가비용으로 구성되어 있다.

키워드 : XCAS, 다운로드형 수신제한 시스템, 수신제한 시스템, CC, 공통평가기준, CMVP, EMV, PCIDSS, DCAS, Downloadable CAS

A Study on Evaluation Scheme for Exchangeable CAS (XCAS)

Yu-na Hwang[†] · Hanjae Jeong[††] · Dongho Won[†††] · Seungjoo Kim[††††]

ABSTRACT

A condition access system (CAS) refers to a hardware-based system that allows only authenticated users to have access to contents. The CAS has many disadvantages found in that in the replacement of multiple service operator (MSO) a set-top box should be also changed and the smart-card often causes malfunction. To deal with the problems, exchangeable CAS (XCAS) was developed in 2009. However the standards or evaluation schemes for XCAS are absent. Existing evaluation schemes are not appropriate for evaluating XCAS due to the evaluation standard, the evaluation cost and efficiencies. Therefore, a specific scheme that can evaluate the security and suitability of exchangeable conditional access systems has been requested. In this paper, we propose an appropriate evaluation scheme for XCAS. The evaluation scheme includes an evaluation purpose and four components to evaluate the evaluation target, the evaluation process, the evaluation subject, and the evaluation cost involved.

Keywords : XCAS, Exchangeable CAS, Conditional Access System, CC, Common Criteria, CMVP, EMV, PCIDSS, DCAS, Downloadable CAS

1. 서 론

위성 혹은 케이블 방송 시스템에서 유료 채널을 관리하며 불법적인 사용자의 시청을 방지하는 기술은 해당 사업자의 수익성과 직접적으로 연관된다. 이와 관련하여 정당한 사용자만 방송 콘텐츠(contents)에 접근하도록 하는 기술을 하드웨어를 기반으로 구현한 것을 수신제한시스템(CAS, Conditional Access System)이라고 한다. 현재 유료 방송 시스템에서는 CAS가 사용되고 있다. 하지만 CAS는 인증 및 디스크램블 과정을 하드웨어 장치를 기반으로 처리하기 때문에 몇 가지 문제점을 가지고 있다. 이러한 CAS의 문제점을 해결하기 위하여 제안된 시스템이 다운로드형 수신제한시스템(XCAS, Exchangeable CAS)이다. 국외에서는 미국을 중심으로 CAS를 DCAS(Downloadable CAS)로 대체 하려는 움직임이, 국내에서는 XCAS로 대체하려는 움직임이 가속화되고 있다.

그러나 XCAS에 대한 평가체계는 현재까지 정해진 것이 없다. XCAS 시스템은 방송사업자의 유료채널 수익과 깊은 관련이 있으므로, 접근제어와 같은 보안기능을 갖추어야 할 뿐만 아니라 명확하게 동작해야 한다. 기존의 평가체계 중 보안기능을 평가하기 위한 체계는 존재하지만 XCAS에 그대로 적용하기에는 평가기준, 비용과 효율성 등이 떨어진다.

본 논문에서는 기존의 평가체계를 분석하고, XCAS를 평

※ 본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다.(계약번호 UD100002KD)
※ "본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음"
† 준 회 원 : 성균관대학교 전자전기컴퓨터공학과 석사과정
†† 준 회 원 : 성균관대학교 휴대폰학과 박사과정
††† 종신회원 : 성균관대학교 정보통신공학부 교수
†††† 종신회원 : 성균관대학교 정보통신공학부 교수(교신저자)
논문접수 : 2010년 5월 25일
수 정 일 : 1차 2010년 7월 12일
심사완료 : 2010년 7월 20일

가하기 위한 체계를 개발하고자 한다. 본 논문의 이후 구성은 다음과 같다. XCAS에 적합한 평가 체계를 개발하기 위하여 2장에서는 XCAS를 분석하고, 3장에서는 기존의 평가체계를 분석한다. 4장에서는 XCAS를 평가하기 위한 평가체계를 제안한다. 마지막으로 5장에서 결론을 맺는다.

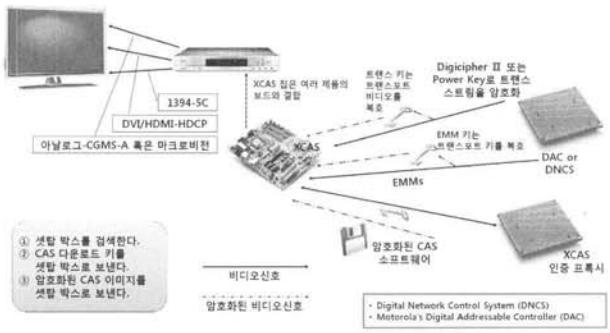
2. 다운로드형 수신제한시스템(XCAS) 분석

CAS는 방송 사업자가 전송하는 방송 콘텐츠를 요금을 지불한 가입자의 단말기에서만 이용할 수 있도록 하는 방송 서비스용 수신제한시스템이다. CAS는 방송 사업자가 비밀번호를 생성하고 생성된 비밀번호를 기반으로 방송 콘텐츠를 스크램블하여 전송한다. 스크램블된 콘텐츠는 비밀번호를 알고 있는 사용자만 스크램블을 제거하여 정상적인 방송을 수신할 수 있다. CAS의 동작과정은 다음과 같다[1, 2].

① 서버는 제어단어생성기(CWG, Control Word Generator)에서 생성한 제어단어(CW, Control Word)를 이용하여 스크램블된 방송 콘텐츠를 수신자에게 전송
② CW는 서버의 인증키(Service Key)를 이용하여 자격제어메시지(ECM, Entitlement Control Message)로 변환되어 전송
③ 인증키는 가입자관리시스템(SMS, Subscriber Management System)에 의해 관리 및 배포되는 가입자 비밀키(Secret Key, 스마트카드에 탑재)를 통해 자격관리메시지(EMM, Entitlement Management Message)로 변환되어 전송
④ 수신자는 자신의 비밀키를 이용하여 서버의 인증키를 복호화
⑤ 수신자는 복호화된 서버의 인증키를 이용하여 CW를 복호화한 뒤 수신된 데이터를 디스크램블링

이와 같은 방법을 사용하기 위해 셋탑 박스에 비밀번호를 저장한 칩을 내장하거나, 스마트카드를 셋탑 박스에 삽입하는 방법을 이용한다. 그러나 이와 같은 방법은 사용자가 방송 사업자를 옮기게 될 경우, 셋탑 박스 자체를 바꾸거나 스마트카드를 교체해야 한다는 문제점이 있다. 스마트카드의 경우, 셋탑 박스를 변경하는 방법보다 진보한 방법이지만 스마트카드에서 발생하는 열에 의하여 셋탑 박스가 오동작하는 문제점이 발생하였다[1, 2]. 따라서, 이러한 문제점을 해결하고자 새로운 개념의 수신제한시스템으로 다운로드형 수신제한시스템(Exchangeable CAS, XCAS)이 등장하였다. XCAS의 일반적인 시스템 구조는 (그림 1)과 같다.

기존 시스템이 하드웨어 칩이나 스마트카드를 이용한 하드웨어 기반의 사용자 인증 방식을 사용하는데 반해, XCAS는 적절한 소프트웨어를 다운로드 및 설치하여 이를 활용한다. 소프트웨어를 다운로드 받기 위해서는 방송사업자(MSO, Multiple Service Operator)와 통신을 해야 하며, 이 때 발생하는 통신에 대한 보안 및 안전한 소프트웨어의 다운로드를



(그림 1) XCAS 구조[2]

위하여 기존 CAS에 비해 훨씬 높은 강도의 보안성을 필요로 한다[1, 2].

XCAS와 유사한 아이디어를 가지고 등장한 제품은 미국 케이블통신협회(NCTA, The National Cable & Telecommunications Association)에서 차세대 네트워크 아키텍처(NGNA, Next Generation Network Architecture)의 일환으로 개발한 DCAS(Downloadable CAS)가 있다. NGNA는 미국 3대 MSO인 컴캐스트, 콕스 커뮤니케이션, 타임워너 케이블이 주축이 되어있으며 현재 케이블 TV망인 광동축 혼합망(HFC) 인프라에 추가적인 비용 투자 없이 제품혁신과 가격절감을 유도하는 통합 멀티미디어 구조의 구현을 목표로 하고 있다. NGNA에서는 소프트웨어 다운로딩 방식을 도입한 NGNA 보안 모델이 있는데, 기존 디지털 방송의 보안 모델과 뚜렷한 차이점은 하드웨어 기반 시스템을 원격으로 재구성할 수 있고, 소프트웨어 기반 시스템도 다운로드에 의해 접근제어시스템의 일부를 업데이트 할 수 있다는 점이다. NGNA의 보안 모델은 크게 3가지 서브 시스템으로 구성된다[1, 2].

- 하드웨어 기반이나 원격으로 재구성 가능한 콘텐트와 키 암호화/복호화 시스템
- 소프트웨어 기반 접근제어 모듈의 다운로딩으로 재정의 할 수 있는 키 관리 시스템
- 부분적인 소프트웨어 기반 접근제어 모듈 다운로딩으로 업데이트 가능한 인증 시스템

미국의 MSO들은 연방통신위원회가 규정하고 있는 분리의무화를 케이블카드를 교체하는 셋탑 박스 뿐만 아니라 소프트웨어 다운로딩 방식의 XCAS까지 포함하도록 요구하고 있다. 이와 같이 XCAS는 점차 기존의 CAS를 대체하여 케이블 및 위성방송 시스템과 같은 유료시스템의 대표적인 수신제한시스템으로 자리를 잡아가고 있다[1, 2].

3. 기존 평가체계 분석

본 장에서는 기존에 존재하고 있는 CC (Common criteria), CMVP (Cryptographic module verification program), PCIDSS (Payment card industry data security standard), EMV (Europay, MasterCard, VISA) 등 총 4가지 평가체계를 분

석한다.

CC는 보안기능이 구현된 IT 제품이나 시스템의 보안성을 평가하기 위한 공통의 요구사항을 제시한 국제적인 기준이다. 보안기능과 보증요구사항의 표준분류를 제공한다. 2010년 현재 공통평가기준 v3.1 R3가 공식문서로 등재되어 있다. 국가 간 상이한 평가기준 적용으로 평가결과가 상호인정되지 않는 문제점 보완 및 평가시간·비용 절감에 따른 제품 가격인하, 그에 따른 신제품 개발 가속화 등을 목적으로, 미국, 영국, 프랑스 등 선진국을 중심으로 각국의 보안성 평가기준을 하나로 통합 및 일원화하여 개발하였다. 공통평가기준 인증서를 획득한 정보보호제품은 CCRA (Common Criteria Recognition Arrangement, 국제공통평가기준 상호인정협정) 회원국에서 모두 인정된다. 우리나라는 2004년 9월 인증서발행국으로 가입신청을 하여 2006년 5월 11번째로 CCRA 인증서발행국으로 가입되었다.

CMVP는 2001년 새롭게 제정된 FIPS 140-2에 근간을 두고 있다. FIPS 140-2는 암호모듈의 안전성 평가를 위한 보안요구사항을 4가지 평가등급에 따라 11개 영역으로 분류하고 있으며, 암호모듈의 핵심기능인 암호알고리즘 등을 포함하여 물리적인 보안까지 광범위하게 다루고 있다. 미국의 NIST (National Institute of Standards and Technology)는 민간 기업이 개발한 암호제품을 미연방 정부기관의 안전한 사용을 위해 FIPS 표준을 제정하였다. FIPS 표준은 암호알고리즘에서부터 컴퓨터 보안에 이르기까지 광범위한 영역에 대해서 다루고 있으며, NIST는 현재 FIPS 140-2를 발표 및 적용하고 있다. 또한 NIST는 FIPS 140-2의 원활한 평가를 위해 암호모듈의 개발자 및 평가자를 위한 문서도 제공한다. 암호모듈의 실제 평가는 NIST의 NVLAP (National Voluntary Laboratory Accreditation Program)에 의해 인정된 신뢰할 수 있는 제 3의 기관인 CMT (Cryptographic Module Testing) 실험실에 의해 수행된다. CMT 실험실에서 작성된 결과보고서를 바탕으로 NIST는 평가받은 암호모듈에 대한 인증서를 발행하고, 인증된 제품은 암호모듈 검증리스트(Validation List)에 공개한다. 암호모듈의 분석 수준을 잘 다루기 위해 4가지 평가등급이 있으며, 전체 요구사항을 11개의 영역으로 구분하여 4가지 평가등급에 따른 요구사항을 분류하여 정의하고 있다.

PCIDSS는 가맹점이나 결재대행업자가 취급하는 회원의 신용카드 정보나 거래 정보를 안전하게 보호하기 위해 PCI (Payment Card Industry)에 의해 만들어진 보안 표준이다. PCI는 아메리칸 익스프레스(American Express), Discover, 마스터카드(MasterCard), 비자(VISA), JCB사가 모여 만든 보안 표준 협의회 단체를 말한다. PCIDSS는 PCI가 공동으로 책정한 신용카드 업계 글로벌 보안 기준으로, 2008년 3월 현재 약 430개사 이상이 가입되어 있다. PCIDSS에는 웹 서비스 보호와 애플리케이션 및 프로토콜의 안전한 사용 강화, 사용자와 프로세스 인증 등이 모두 포함되며, 안전한 네트워크 수립 및 유지, 고객 데이터 보호, 취약부분 관리 프로그램 유지, 강력한 액세스 관리, 정기적인 모니터링 및 네트워크 테스트, 정보 보안 정책 운영 등 6가지 항목의 12가지 조건으로 이루어져 있다.

EMV 인증은 EMV 표준과 제품이 부합되는지를 검증하는 것이다. 타입인증은 EMV 표준명세가 복잡하고 많은 카드와 터미널 공급자가 존재하며 구별되는 핵심 비즈니스가 포함되어 있기 때문에 완전한 지불시스템의 모든 구성요소 간에 상호호환성을 보증하는데 목적이 있다. EMV 인증을 위하여 1999년 2월 EMVCo, LLC가 설립되었다. EMVCo, LLC는 EMV 표준의 보급, 갱신 등의 제반관리 담당하고 있으며, 업체에서 생산된 EMV 제품이 표준에서 정한 규격대로 준수하고 있는지 여부를 테스트하기 위한 승인절차를 제정한다. 이에 대한 실제 인증은 EMVCo가 인가한 인증센터에서 수행한다.

CC, CMVP, PCIDSS, EMV의 평가요소를 비교한 결과는 <표 1>과 같다.

〈표 1〉 기존 평가체계 분석결과 비교[3-9]

구분		CC	CMVP	PCIDSS	EMV
발표년도		1999	2001	2004	1995
평가대상		보안기능이 구현된 IT 제품	암호모듈	신용카드거래정보	IC 카드
평가등급		존재	존재	존재하지 않음	존재하지 않음
평가주체	신청기관	보안기능이 구현된 IT 제품의 개발업체	암호모듈 개발업체	카드결제를 지원하는 상점, 인터넷 쇼핑몰 등의 가맹점	IFM 제공자
	평가기관	KISA, KOSYAS, KTL, KSEL, TTA 등	CMT 실험실	PCIDSS 보안감사를 수행할 수 있는 평가기관	ICT Korea Co., Ltd. 등 지정된 인증센터
	인증기관	IT보안인증사무국 등	미국의 NIST, 캐나다의 CSE	VISA와 같은 글로벌 카드 브랜드	EMVCo.
평가절차		준비단계→평가·인증단계→종료단계	예비검증단계→검증시험단계→검증유지단계	신청단계→감사단계→종료단계	인증준비 및 등록단계→테스트단계→인증단계
특징		각국마다 존재하던 평가기준을 통합한 국제 표준	제품에 사용되는 암호모듈의 평가를 위해 제정	특정 업계(신용카드)의 글로벌 보안 기준	ISO의 IC카드 표준인 ISO 7816 기반의 IC카드 규격
장점		CCRA 가입국들 간 평가 결과를 인정	암호 모듈의 알고리즘 및 물리적 보안까지 평가	신용카드 결제시스템의 보안성을 평가하는 기준	· 국가간 / 벤더간 상이한 표준 적용에 의한 상호호환성 문제 해결 · 다양한 멀티 어플리케이션 수행을 지원
단점		· 암호모듈에 대한 세부적인 평가 방법이 존재하지 않음 · 제출물 종류가 많고 작성이 어려움	전체시스템에 대한 평가는 하지 않음	만족해야 하는 요구사항의 의미가 아직까지 명확하지 않음	규격을 준수하기 위한 구현내용이 매우 어렵고 복잡

4. 제안하는 평가체계

본 장에서는 이전 장에서 분석한 기존 평가체계를 바탕으로 XCAS에 적합한 평가체계를 제안한다. 제안하는 평가체계는 평가목적 및 대상, 평가절차, 평가주체, 평가제출물, 평가비용으로 구성된다.

XCAS와 관련되어 제안되어있는 표준 및 평가체계는 아직 존재하지 않는다. 하지만 디지털시네마와 관련해서는 DCI(Digital Cinema Initiatives)에서 발행한 Digital Cinema System Specification라는 표준이 존재한다. DCI는 영화 환경이 디지털시네마로 변화하게 됨에 따라 디지털시네마 환경 및 장비에 대한 표준이 요구됨에 따라 미국 헐리우드의 메이저 회사들을 중심으로 결성된 단체이다. DCI는 디지털 시네마와 관련된 표준을 주도하고 있다[17-19]. XCAS에서도 디지털 영상 콘텐츠를 다루고 있으므로 디지털 시네마를 다루는 DCI의 요구사항을 적용하는 것이 가능하다. 또한 DCI의 요구사항을 참고하여 평가체계를 제안할 경우, 평가된 제품이 국내뿐만 아니라 국외에서까지 보안성을 검증 받은 제품으로 인정받을 수 있다는 장점이 있다.

DCI에서 직접적으로 요구하는 평가체계는 없으나, 암호장비의 경우 CMVP Level 3를 준수해야한다는 요구사항을 제시하고 있다. Digital Cinema System Specification에 기재된 해당 내용은 (그림 2)와 같다.

CMVP에는 각 Level에 맞게 운영되어야 할 환경이 명시되어 있다. CMVP Level 3의 암호모듈은 안전한 경로(FTP_TRP.1)와 비정형화된 TOE 보안정책모델(ADV_SPM.1)이 추가된 EAL3이상의 평가를 받은 환경에서 운영하도록 명시되어 있다. 즉, XCAS에 필요한 암호모듈은 CMVP Level 3을 만족해야 하며, 운영되는 환경은 EAL3를 만족해야 한다[3-11]. FIPS 140-2에 기재된 해당 내용은 (그림 3)과 같다.

제안하는 평가체계는 이전까지 존재하지 않았으며, 엄격한 제출물을 요구하여, XCAS 개발업체에서 평가·인증에 부담을 느낄 수도 있다. 따라서 평가체계의 적용을 2단계로 나누어서 초기에는 일부 평가제출물에 대한 요구사항을 완화하여 시행하고, 추후 국제적인 수준의 엄격한 평가제출물을 요구하도록 시행하는 것이 바람직하다.

9.5.2.5. FIPS 140-2 Requirements for Type 1 Secure Processing Blocks

Robustness requirements for Digital Cinema Secure Processing Blocks (SPBs) shall follow the guidelines of the Federal Information Processing Standards [FIPS PUB 140-2][25]. A summary of these requirements is shown in the table below.

FIPS 140-2 specifies eleven areas for evaluation against a rating, which shall be performed by US government recognized independent laboratories.

All SPB type 1 shall meet and be certified for the requirements of FIPS 140-2 Level 3 in all areas except those subject to the following exceptions or additional notes (the Nr indicators refer to the table items by row):

(그림 2) 평가체계 제안 근거(1)

Security Level 3 allows the software and firmware components of a cryptographic module to be executed on a general purpose computing system using an operating system that

- meets the functional requirements specified in the PPs listed in Annex B with the additional functional requirement of a Trusted Path (FTP_TRP.1) and
- is evaluated at the CC evaluation assurance level EAL3 (or higher) with the additional assurance requirement of an Informal Target of Evaluation (TOE) Security Policy Model (ADV_SPM.1).

An equivalent evaluated trusted operating system may be used. The implementation of a trusted path protects plaintext CSPs and the software and firmware components of the cryptographic module from other untrusted software or firmware that may be executing on the system.

(그림 3) 평가체계 제안 근거(2)

4.1 평가목적 및 대상

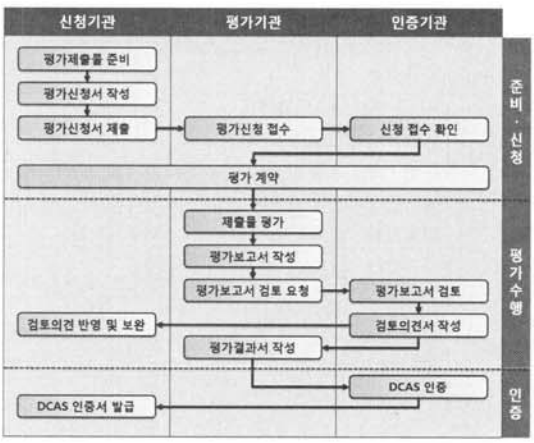
제안한 평가체계의 목적은 다양한 업체에서 개발한 XCAS의 적합성여부를 인증하는 것이다. 현재까지 XCAS에 대한 국제 표준 뿐만 아니라 국내 표준이 정립되지 않아서, 다양한 사업자들에 의하여 XCAS가 독자적으로 개발되고 있으며, 향후 개발될 수 있다. 그러나 아직까지 XCAS에 대한 보안성이나 안전성 등 적합성 여부를 평가할 수 있는 기준 및 체계가 정립되어 있지 않은 실정이다. 따라서 본 연구에서는 XCAS에 적합한 평가체계를 제안하였으며, 개발된 XCAS의 적합성 여부를 평가하여, 정당한 사용자가 안전하게 XCAS를 이용할 수 있도록 하는 것이 목표이다.

그러므로 제안한 평가 체계에서의 평가대상은 업체에서 개발한 XCAS이며, 이 후 기술된 절차에 따라 평가를 수행하게 된다.

4.2 평가절차

제안하는 평가절차는 (그림 4)와 같다.
평가단계의 절차별 설명은 다음과 같다.

① XCAS를 개발한 업체에서 인증기관으로부터 인증을 받기 위해서 평가제출물을 준비한다.
② 평가제출물이 준비되면, 신청업체는 평가기관이 요구하는 평가 신청서를 작성한다.
③ 작성한 평가 신청서를 평가 제출물과 함께 제출한다.
④ 신청기관이 평가기관에 평가를 신청하면, 평가기관은 평가신청을 접수하고 해당 내용을 인증기관에 보고한다.
⑤ 인증기관은 평가기관의 보고 내용을 확인하고 평가신청 접수를 확인한다.
⑥ 평가 기간 및 범위, 비용 등의 평가계약에 관한 내용은 신청기관, 평가기관, 인증기관이 모두 동일하게 알아야 하므로 세 기관이 평가계약 체결에 참여하도록 한다. 원활한 평가 진행을 위해 신청기관은 평가기관에 평가제출물의 설명을 제공한다.



(그림 4) 평가 절차[12-13]

⑦ XCAS에 대한 시험이 이루어지기 전에 평가 신청 시에 제출된 평가제출물에 대한 평가를 우선 수행해야 한다.
⑧ 평가기관에 의해 작성된 평가보고서는 평가의 공정성 및 평가결과에 대한 검토를 받기 위하여 인증기관의 검토를 거쳐야한다.
⑨ 인증기관은 평가기관이 수행한 평가결과 및 평가보고서를 검토한다.
⑩ 인증기관은 평가보고서 검토 후에 평가에 대한 인증기관의 의견을 검토의견서에 작성한다.
⑪ 인증기관이 작성한 검토의견서에 따라 신청기관 및 평가기관의 다음 절차가 달라진다. 수정의견이 나왔을 경우에는 신청기관은 인증기관의 의견에 따라 수정 후 다시 평가를 받아야 한다. 수정의견이 없을 경우, XCAS에 대한 평가가 제대로 이루어졌으며, XCAS 자체에 문제가 없는 것으로 간주하고 평가기관은 시험결과보고서를 작성한다.
⑫ 평가기관이 수행한 평가에 대해 인증기관의 검토가 완료되었을 경우 인증기관은 해당 XCAS의 인증서를 정상적으로 신청기관에 발급한다.

4.3 평가주체 정의 및 선정

제안하는 평가체계에서 평가주체는 <표 2, 3>과 같이 정의할 수 있다.

제안한 XCAS 평가체계의 평가기관 선정의 근간이 되는 CC와 CMVP의 경우, CC는 KISA, KTL과 같은 국가기관 및 민간 기관인 KOSYAS에서 평가를 수행하고 있고, CMVP의 국내버전인 KCMVP는 KISA와 한국전자통신연구원 부설연구소, 2개의 CMT 실험실에서 평가를 수행하고 있다. 제안하는 XCAS의 평가체계의 1단계 평가는 XCAS 평가에 대한 인식이나 중요성을 알리는 초기 도입단계로 2단계 평가에 비해 비교적 간소화하여 평가를 수행한다. 따라서 1단계 평가는 인증기관이 XCAS에 대한 연구경험이나 XCAS 평가에 관심을 가지고 있는 기관을 선정하여 평가기관으로서 역할을 수행하게 할 수 있다.

2단계 평가는 국제적으로 인정받을 수 있는 수준의 평가제출물을 요구한다. 따라서 1단계 평가체계에 평가기관으로 참여하여 XCAS 평가에 대한 경험을 쌓고, 평가능력 및 환경을 갖춘 기관만이 2단계 평가체계에서의 평가기관으로 선정될 수 있다.

〈표 2〉 제안하는 평가체계에서의 평가주체의 정의[3-5][12-13]

구분	설 명
신청 기관	· XCAS를 개발한 주체이며, 개발한 XCAS를 검증받기 위하여 평가제출물을 준비하여 평가신청을 함
평가 기관	· 인증기관을 대신하여 평가 신청 접수 및 XCAS의 평가를 수행하는 기관 · XCAS 평가 능력을 갖춘 국가기관 또는 인증기관 지정 민간업체일 수 있음
인증 기관	· 평가기관을 지정하는 역할 수행 및 평가기관에서 수행한 XCAS에 대한 평가를 검증함 · 평가기관이 제출한 XCAS 평가보고서를 검토 후 검토 의견서를 작성하며, XCAS의 인증을 수행함

CC와 CMVP의 인증기관은 IT보안인증사무국, NIST, CSE 등의 국가기관에서 인증기관의 역할을 담당하고 있다. 인증기관은 평가기관을 지정하는 역할 및 평가기관에서 수행한 XCAS평가에 대한 검증해야 한다. 따라서 국내의 방송통신 업무를 총괄하며 공신력을 지니고 있는 방송통신위원회가 인증기관의 역할을 수행하는 것이 바람직하다.

4.4 평가제출물

제안하는 평가체계는 CC EAL3와 CMVP Level3를 기반으로 하고 있다. 이에 해당하는 평가제출물은 <표 4>와 같다.

〈표 4〉 CMVP Level 3에 준하는 기존 평가체계의 평가 제출물 비교[3-5][13]

CC	CMVP
보안목표명세서	암호모듈명세, 암호모듈 포트와 인터페이스
준비절차서	N/A
기능명세서	역할, 서비스와 인증, 암호키 관리
사용자운영설명서	N/A
형상관리문서	N/A
보안구조서	설계 보증
TOE설계서	유한상태모델
배포문서	운영환경
시험서	EMI/EMC, 자가 시험
생명주기정의문서	N/A
개발보안문서	N/A
N/A	기타 공격대응의 완화
N/A	물리적인 보안

〈표 3〉 제안하는 평가체계에서의 평가주체 선정 및 선정근거[3-5][12-13]

구분	평가주체		선정 근거
신청 기관	XCAS 개발 업체		개발한 XCAS를 검증받기 위한 주체는 개발업체가 된다.
평가 기관	1단계	· XCAS에 대한 연구경험이나 XCAS 평가에 관심을 가지고 있는 기관 · 기존의 평가체계에서 인증, 평가 경험이 있는 정부기관 및 민간기관	1단계 평가는 XCAS 평가체계의 초기 도입단계이므로 2단계 평가체계에 비해 간소화한 평가를 수행한다. 따라서 1단계 평가체계에서는 XCAS에 대한 연구경험이나 XCAS 평가에 관심을 가지고 있는 업체 중 인증기관이 지정한 정부기관이나 민간기관이 수행가능하다.
	2단계	· 1단계 평가체계에서 평가 업무를 수행했던 기관 중 XCAS를 평가하기 위한 전문 인력 및 환경을 갖춘 기관 · 1단계 평가체계에 평가기관으로 참여하지 않았어도, 평가능력과 XCAS에 대한 전문지식을 보유하고 있는 기관	2단계 평가체계는 국제적으로 인정받을 수 있는 수준의 평가제출물을 요구하므로 평가기관의 평가 수행 능력이 중시된다. 따라서 1단계 평가체계에 참여하여 XCAS평가에 대한 경험을 쌓고, 평가를 수행할 수 있는 전문인력 및 환경을 갖춘 기관이 평가기관의 업무를 수행해야 한다. 단, 1단계 평가체계에서 평가기관의 역할을 수행하지 않은 기관도 XCAS를 평가하기 위한 전문적인 지식 및 인력을 보유하고 있는 기관의 경우 인증기관의 승인 하에 평가기관의 업무를 수행할 수 있다.
인증 기관	방송통신위원회		국내의 방송·통신과 관련된 업무를 총괄하는 방송통신위원회에서 평가기관의 선정 및 평가업무의 관리·감독을 수행해야 한다.

각 평가체계에서 FIPS 140-2 Level 3에 준하는 평가등급의 평가제출물을 정리한 위 표를 바탕으로 공통적인 평가제출물은 '보안목표명세서', '기능명세서', '보안구조서', '상세설계서(TOE설계서)', '배포문서', '시험서'가 있었다. 그리고 각 평가체계마다 공통적인 제출물은 아니지만, XCAS 평가에 적합하다고 고려되는 평가제출물인 '형상관리문서', '사용자운영설명서', '생명주기정의문서', '개발보안문서', '취약성 분석서(기타 공격대응의 완화)', '물리적인 보안'을 추가로 선정할 수 있다. 추가로 선정한 평가 제출물의 선정 근거는 다음과 같다.

- 형상관리문서 : 초기 설계 단계에서부터 이후 유지 및 관리 단계까지의 모든 단계에서 무결성을 보장하기 위해 필요함
- 사용자운영설명서 : 시스템을 올바르게 사용하기 위해 일반 사용자 관점의 설명서가 필요함
- 생명주기정의문서 : 개발 과정에서의 물리적, 절차적, 인적 보안대책을 식별함으로써 개발과정에 대한 보안을 보장하기 위해 필요함
- 개발보안문서 : 개발 환경에서 사용될 수 있는 물리적, 절차적, 인적, 기타 보안대책에 관한 내용을 보장하기 위해 필요함
- 취약성분석서 : 개발 및 운영과정 상에서 악용 가능한 취약성이 발생할 가능성과 대책을 식별하기 위하여 필요함
- 물리적인 보안 : 운영과정 상에서 물리적 공격에 대한 가능성 및 대책을 제시하기 위하여 필요함

제안하는 XCAS 평가체계는 신청기관의 편의를 위하여 2단계로 나누어 시행하게 된다. 1단계 평가체계에서는 XCAS를 평가하기 위한 기본 제출물인 '보안목표명세서', '기능명세서', '보안구조서', '상세설계서', '배포문서', '시험서', '물리적인 보안'만 제출하여 평가를 수행하게 된다. 물리적인 보안의 경우 기존 평가체계에서 공통적으로 요구하는 항목은 아니지만, XCAS 특성상 물리적인 공격에 노출되어 있다는 점을 고려하여 1단계 평가시행부터 제출물로 요구되어야 한다. 향후 XCAS 평가체계가 활성화되어, 엄격한 평가제출물을 요구하는 2단계 평가체계가 시행될 경우, 추가로 '형상관리문서', '사용자운영설명서', '생명주기정의문서", '개발보안문서', '취약성분석서'를 요구하게 된다. 이와 같은 제출물을 요구함으로써, 평가를 신청한 XCAS에 대하여 엄격한 수준의 평가를 수행할 수 있게 된다.

제안하는 평가 단계별 평가 제출물을 정리하면 <표 5>와 같다.

위의 평가 제출물을 정보시스템 생명주기 단계에 따라 분류하면 다음과 같다.

- 설계 : 보안목표명세서, 물리적인 보안
- 개발 : 기능명세서, 보안구조서, 상세설계서, 개발보안문서, 형상관리문서, 배포문서(1)

〈표 5〉 평가단계 평가제출물

평가단계	제출물
1단계 평가체계	보안목표명세서, 기능명세서, 보안구조서, 상세설계서, 배포문서, 시험서, 물리적인 보안
2단계 평가체계	보안목표명세서, 기능명세서, 보안구조서, 상세설계서, 배포문서, 시험서, 물리적인 보안, 형상관리문서, 사용자운영설명서, 생명주기지원서, 개발보안문서, 취약성 분석서

- 검증 : 시험서, 취약성 분석서(1)
- 확인 : 사용자운영설명서, 배포문서(2)
- 운영 및 유지보수 : 생명주기정의문서, 취약성 분석서(2)

각각의 평가 제출물에 대한 정의와 기술내용은 다음과 같다.

- 보안목표명세서 : XCAS의 보안문제 및 보안요구사항을 정의하고, 보안요구사항을 만족시키기 위해 XCAS가 제공하는 보안기능 명세
- 기능명세서 : XCAS의 보안기능 및 인터페이스의 사용목적 및 방법 명세
- 보안구조서 : XCAS 보안기능 영역분리, 자체보호, 우회불가성에 대한 구조적 관점에서의 특성 서술
- 상세설계서 : XCAS 보안기능이 보안기능요구사항을 어떻게 구현하는지에 대한 설계정보 제공
- 배포문서 : XCAS가 생산되어 사용자에게 배포 시 무결성을 유지하기 위해서 진행되는 과정 서술
- 시험서 : 평가대상인 XCAS에 대한 시험계획, 절차, 결과 서술
- 물리적인 보안 : XCAS의 물리적인 운영 환경 및 범위를 식별하기 위해 접근 가능한 경로 및 인터페이스를 정의하고, 물리적 보안 대책을 서술
- 형상관리문서 : XCAS에 대한 형상관리 관련 규칙, 절차 등 서술
- 사용자운영설명서 : 평가받은 구성에서의 XCAS 운영과 관련된 요구사항 서술
- 생명주기정의문서 : XCAS 개발과정의 전반적인 품질을 강화하기 위해, XCAS 개발 및 유지에 사용되는 생명주기 모델 정의
- 개발보안문서 : XCAS 개발 환경에서 사용될 수 있는 물리적, 절차적, 인적, 기타 보안대책에 관한 내용 서술
- 취약성분석서 : XCAS 개발자가 직접 평가대상 제품에 대해서 취약성 분석을 수행하고, 각각의 취약성 분석과정 및 결과를 서술

4.5 평가비용

제안한 XCAS 평가체계의 평가비용은 국내의 여러 가지 법적 근거를 고려하여 평가비용이 산정된 공통평가기준의 산정 근거를 수용하였다. 제안하는 XCAS 평가체계는 국내에서 시행할 수 있는 제도이므로, 기존에 제정된 법적 근거를 준수해야 하므로 공통평가기준의 평가비용을 산출방법을

〈표 6〉 평가수수료 산정 기준 및 고려사항[14]

구분	기준
투입인력 일 노임 단가	(고급기술자+중급기술자)의 평균값 적용 ※ 소프트웨어산업진흥법 시행령 제16조에 의한 「소프트웨어기술자 등급별 노임단가」 준용 ※ 이후 평가기관내의 정책에 따라 변경가능
투입인력(명)	2명
평가기간	1단계 : 48일, 2단계 : 82일
복잡도	평가 제품의 경우에 따라 다름
평가장비 취득원가	실비
기타 직접경비	실비

적용하는 것이 적절하다고 할 수 있다.(<표 6>)

제안한 XCAS 평가 체계는 평가대상이 XCAS에 한정되어 있으므로, 평가장비 취득원가는 어떤 제품을 평가 하느냐에 관계없이 동일하다.

평가기간은 단계별로 차이가 생긴다. 제안한 XCAS 평가 체계는 평가기관과 인증기관에서 작성해야 하는 문서의 수가 적다는 면이 공통평가기준의 국내용 평가와 유사하다. 그리고 제안한 XCAS 평가 체계에서 2단계는 공통평가기준으로 생각하면 EAL3에 해당하는 것이기 때문에, EAL3의 국내용 평가기간 산출 방법으로 계산하면 제안한 XCAS 평가 체계의 2단계 평가기간은 82일이 적합하다는 것을 알 수 있다. 이를 기반으로 1단계의 평가기간을 산출 할 수 있는데 2단계 평가시 제출해야 하는 제출물이 12종인 것에 비하여 1단계의 제출물은 7종이기 때문에 이 비율을 적용 하여 계산하면 제안한 XCAS 평가 체계의 1단계 평가기간은 48일이 적합하다는 것을 알 수 있다.

위에서 도출한 단계별 평가기간을 이용하고, 평가기관 내에서 투입인력 일 노임 단가를 확정 한다면, 인건비, 제경비, 기술료 뿐만 아니라 직접경비의 평가도구비에 해당하는 비용까지 각 단계별로 상수로서 결정할 수 있다.

결정한 상수비용에 단계별 평가기간을 고정하면서 고려되지 못한 복잡도를 곱하고 기타 직접경비를 추가하는 방법으로 총 비용을 계산할 수 있다. 원래 평가기간을 계산할 때 반영되던 복잡도를 이후에 반영하더라도, 인건비, 제경비, 기술료, 직접경비의 평가도구비 모두가 평가기간에 비례하기 때문에 같은 결과를 얻을 수 있다.

해당 평가비용 계산 방법은 공통평가기준 국내 평가비용 산정방법에 비해 신청자가 이해하기 평이하고 그 당위성에 있어서 부족한 점이 없기 때문에 XCAS 평가비용으로 합당하다.

〈표 7〉 평가수수료 산정 시 상수비용 계산[14]

구 분	산정 방법
인건비	∑평가기간*(일)×투입인력별 일 노임단가 ※ 1단계 : 48일, 2단계 : 82일
직접경비 (평가도구비)	평가장비취득원가×(평가기간(일)/내용연수)
제경비	인건비 × 110%
기술료	(인건비+제경비)×20%
합계	인건비+직접경비(평가도구비)+제경비+기술료
총 비용	(상수비용합계×복잡도)+기타직접경비

해당제품에 대한 최초평가/재평가 구분과 대기업/중소기업 등의 구분, 복잡도 구분은 공통평가기준 국내 평가비용 산정방법을 따르도록 한다. 결론적으로 평가비용 산정방법을 정리하면 <표 7>과 같다.

4.6 제안하는 평가체계의 특징 및 장점

기존에 존재하는 평가 체계 중 XCAS를 평가할 수 있는 평가체계는 CC가 있다. 하지만 CC는 보안기능을 가진 모든 IT 제품을 대상으로 하기 때문에 평가 및 인증 절차가 복잡하고, 평가기관에서 다양한 IT 제품을 평가해야 하기 때문에 특정 제품군에 대한 전문적인 평가인력을 확보 할 수 없어 평가기간이 길다. 평가기간에 따라서 평가비용도 늘어난다.

제안하는 평가체계는 CC에 비해 평가 제출물을 강화하였다. 또한 평가기간과 평가비용을 줄여 XCAS 업체의 부담을 줄이고, 제품에 대한 보안성 평가가 제품 개발 속도를 늦추는 부작용을 줄이고자 하였다. CC EAL3 평가와 제안하는 평가체계의 비교는 <표 8>과 같다.

〈표 8〉 CC EAL3와 제안하는 평가체계 비교

	제안하는 평가체계	CC EAL3
제출물	12종 (2단계)	11종
평가기간	82일 (2단계)	137일 (등급별 표준 평가 일수)
평가비용	[59,593,481*+직접경비(평가도구비)] × 복잡도 + 기타직접경비 * 인건비+제경비+기술료 = 59,593,481 원	[142,558,572* + 직접경비] × 복잡도 * 인건비 + 제경비 + 기술료 = 142,558,572 원

5. 결 론

본 논문에서는 기존의 평가체계를 분석하고, XCAS를 평가하기 위한 체계를 제안하였다. 제안한 평가체계는 2단계로 나누어서 시행하는 것이 특징이다. 새롭게 제안된 평가체계인 만큼 1단계 평가체계에서는 업체의 부담을 줄이고, 평가체계의 활성화를 위하여 XCAS를 평가하기 위한 기본적인 평가제출물을 요구한다. 2단계 평가체계는 국제적인 수준의 평가제출물을 요구하여, 개발한 XCAS의 보안성, 안전성 및 적합성 여부를 검증하고, 인증의 강도를 높이고자 하였다. 그러므로 제안한 평가체계를 상황에 따라 단계별로 시행을 하는 것이 바람직하다.

또한 제안하는 평가체계는 평가절차를 간소화 하고, 평가기관이 제품을 평가한 후에 작성해야 하는 평가 결과 관련 보고서를 최소화 하여 평가기간이 현실화 될 수 있도록 하였다. 평가기간이 짧아짐에 따라서 기존에 시행중인 평가체계에 비해서 평가비용도 현격히 줄일 수 있었다.

본 논문에서 제안된 XCAS에 적합한 평가체계를 통해 다양한 XCAS를 평가할 수 있으며, 이를 통해 XCAS의 보급화 및 활성화에 기여할 수 있을 것으로 기대된다.

참 고 문 헌

[1] OpenCableTM Technical Reports, "DCAS System Overview Technical Report", OC-TR-DCAS-D02-060912, 2006.

[2] NCTA, "Report of the National Cable & Telecommunications Association on Downloadable Security", 2005.

[3] ISO/IEC 15408-1, "Information technology – Security techniques – Evaluation criteria for IT security – Part 1:Introduction and general model"

[4] ISO/IEC 15408-2, "Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements"

[5] ISO/IEC 15408-3, "Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements"

[6] NIST, "FIPS 140-2: SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES," May, 2001.

[7] EMVCo, LLC. "EMVCo Type Approval - Contact Terminal Level 1 - Administrative Process Version 5.0", January 2009

[8] EMVCo, LLC. "EMVCo Type Approval - Contact Terminal Level 2 - Administrative Process Version 2.0," January, 2009.

[9] PCI Security Standard Council, "Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures Version 1.2.1," July, 2009.

[10] Digital Cinema Initiatives, LLC, "Digital Cinema System Specification Compliance Test Plan Version 1.1," May, 2009.

[11] Digital Cinema Initiatives, LLC, "Digital Cinema System Specification Version 1.2," March, 2008.

[12] 국내·외 암호모듈 검증정책, IT보안인증사무국.

[13] 국가정보원 2009. 3. 20 정보보호제품 평가·인증 수행규정.

[14] 한국정보보호진흥원,"신청인을 위한 정보보호시스템 평가수수료 산정가이드", 2008, 7.

[15] 황유나, 정한재, 조성규, 김송이, 원동호, 김승주, "다운로드형 수신제한시스템(XCAS)에 적합한 평가체계 제안", 한국 소프트웨어공학 동계학술대회(KCSE 2010)논문집, pp.192-198, 2010.02.08-10.

[16] Yu-na Hwang, Hanjae Jeong, Sungkyu Cho, Songyi Kim, Dongho Won and Seungjoo Kim, "A proposal of appropriate evaluation scheme for exchangeable CAS (XCAS)," Information Security Practice and Experience Conference (ISPEC 2010), Seoul, Korea, March 12-13, 2010, pp.217-228.

황 유 나

e-mail : ynhwang@security.re.kr

2009년 성균관대학교 자연과학부 수학전공 (학사)

2009년~현 재 성균관대학교 전자전기컴퓨터공학과 석사과정

관심분야 : 정보보호, 보안성평가, PKI 인증, 장치인증, 암호이론, XCAS

정 한 재

e-mail : hjjeong@security.re.kr

2006년 성균관대학교 정보통신공학부(학사)

2008년 성균관대학교 전자전기컴퓨터공학과 (공학석사)

2008년~현 재 성균관대학교 휴대폰학과 박사과정

관심분야 : 정보보호, 보안성평가, 무선네트워크, 리버스 엔지니어링

원 동 호

e-mail : dhwon@security.re.kr

1976년~1988년 성균관대학교 전자공학과 (학사, 석사, 박사)

1978년~1980년 한국전자통신연구원 전임연구원

1985년~1986년 일본 동경공업대 객원연구원

1988년~2003년 성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장

1996년~1998년 국무총리실 정보화추진위원회 자문위원

2002년~2003년 한국정보보호학회장

2002년~현 재 대검찰청 컴퓨터범죄수사 자문위원, 감사원 IT 감사 자문위원

2007년~현 재 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, 정보통신부지정 정보보호인증기술연구센터 센터장, 정보통신대학원장, 성균관대학교 BK21 사업단장

관심분야 : 암호이론, 정보이론, 정보보호

김 승 주

e-mail : skim@security.re.kr

1994년~1999년 성균관대학교 정보공학과 (학사, 석사, 박사)

1998년~2004년 한국정보보호진흥원 (KISA) 팀장

2004년~현 재 성균관대학교 정보통신공학부 교수

2001년~현 재 한국정보보호학회, 한국인터넷정보학회, 한국정보과학회, 한국정보처리학회 논문지 및 학회지 편집위원

2002년~현 재 한국정보통신기술협회(TTA) IT 국제표준화 전문가

2005년~현 재 교육인적자원부 유해정보차단 자문위원, 디지털콘텐츠유통협의체 보호기술워킹그룹 그룹장

2007년~현 재 대검찰청 디지털수사 자문위원, KISA VoIP보안기술 자문위원, 기술보증기금 외부 자문위원, 전자정부서비스보안위원회 사이버침해사고대응 실무위원회 위원

관심분야 : 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET