한국항행학회 논문지 제12권 제5호 2008년 10월

소프트웨어 소스코드의 저작권 관리를 위한 보안 컨테이너 크립텍스 모델

Security Container CRYPTEX Model for Copyright Management of Software Source Code

차병래*

Byung-Rae Cha*

요 약

정보화시대의 직접적으로 중요한 인프라의 조립라인에 해당하는 소프트웨어의 소스코드에 대한 관리 및 보안측면은 아직도 초보단계에 머물러있으며, 소프트웨어의 소스코드를 보호하기 위한 지원 기술과 프레임워크는 너무나도 빈약한 상태이다. 현실세계의 문서 보안 장치를 사이버 상의 문서 보안 장치로 크립텍스라는 보안 모듈을 제안한다. 본 연구에서 제안하는 크립텍스는 인증되지 않은 주체로부터 객체인 소프트웨어의 소스코드를 안전하게 보호 및 접근제어를 지원하기 위한 제반 기술들의 집합을 통칭하는 모델이다. 크립텍스를 이용하여 단지 수동적인 문서 상태의 소프트웨어 소스코드에 대해서 능동적이며, 접근제어 및 보안이 가능하며, 이동 및 위임기능을 부여할 수 있는 비즈니스 모델을 제안한다.

Abstract

There are management and security of software source code equivalent to assembly lines of important infrastructure in the early stage of information society directly. A support technology and framework to protect software source code are so poor state.

In this paper, the proposed model that is support protection and access control between software source code as object and subject that is not authenticated safely was named CRYPTEX model. And we propose active business model to provide delegate, mobile, and security/access control function for passive software source code in document state using CRYPTEX.

Key words : CRYPTEX Model, Copyright Management, Security Container

I. 서 론

21세기를 정보지식사회라는 명칭과 더불어 Web 2.0의 시대로 진입하고 있다. Web 2.0 또는 시맨틱 웹(Semantic Web)은 인터넷의 개체들을 단지 수동적인 객체에서 탈피하여 분산된 컴퓨팅 시스템에 의한 자동화 및 능동적인 객체로 전환하는 시대이며, 이를 뒷받침하는 여러가지 기술, 프레임워크 그리고 패러다임들이 시시각각으로 창조 및 출현하고 있다.

그러나 정보화시대의 직접적으로 중요한 인프라

* 호남대학교 정보통신대학 컴퓨터공학과
· 제1저자 (First Author) : 차병래
· 투고일자 : 2008년 10월 6일
· 심사(수정)일자 : 2008년 10월 7일 (수정일자 : 2008년 10월 17일)
· 게재일자 : 2008년 10월 30일

의 조립라인에 해당하는 소프트웨어의 소스코드에 대한 관리 및 보안측면은 아직도 초보단계에 머물러 있다. 소프트웨어의 소스코드를 보호하기 위한 제반적인 지원 기술과 프레임워크는 너무나도 빈약한 상태이다.

크립텍스(CRYPTEX)[1]는 '다빈치 코드'라는 소설에 잠깐 언급되는 비밀문서를 보관하는 하나의 보안 장치 이름이며, 여기서 아이디어를 얻어서 동일한 명칭으로 쓴다. 크립텍스는 문자조합에 의한 암호화된 키를 갖으며, 암호를 풀지 못하여 임의적으로 문서를 여는 경우에는 크립텍스 안의 초산이 파피루스로 만들어진 비밀문서를 녹여버리는 보안 장치이다. 이러한 현실세계의 문서 보안 장치를 사이버 상의 문서 보안 장치로 크립텍스라는 보안 모듈을 제안하고자 한다.

본 연구에서 제안하는 크립텍스는 인증 및 인증되지 않은 주체로부터 객체인 소프트웨어의 소스코드를 안전하게 보호 및 접근제어를 지원하기 위한 제반 기술들의 집합을 통칭하는 모델이다. 크립텍스를 이용하여 단지 수동적인 문서 상태의 소프트웨어 소스코드에 대해서 능동적이며, 접근제어 및 보안이 가능하며, 이동 및 위임기능을 부여할 수 있는 비즈니스 모델 또한 제안한다. 본 논문의 구성은 PKI와 접근제어 기법 및 모델, DRM기술과 국내 DRM 기술 현황을 관련연구에서 기술하며, 3장에서는 크립텍스의 비즈니스 모델을 제안한다. 4장에서는 크립텍스의 물리적 접근제어에 대해서 언급하며, 마지막으로 5장에서는 향후 연구와 결론을 서술한다.

Ⅱ. 관련 연구

2-1 PKI(Public Key Infrastructure)[2]

PKI는 기본적으로 인터넷과 같이 안전이 보장되지 않은 공중망 사용자들이, 신뢰할 수 있는 기관에서 부여된 한 쌍의 공개키와 개인키를 사용함으로써, 안전하고 은밀하게 데이터나 자금을 교환할 수 있게 해준다. PKI는 한 개인이나 기관을 식별할 수 있는 디지털 인증서와, 인증서를 저장했다가 필요할 때 불러다 쓸 수 있는 디렉토리 서비스를 제공한다. 비록 PKI의 구성 요소들이 일반적으로 알려져 있지만, 공급자 별로 많은 수의 서로 다른 접근방식이나 서비스들이 생겨나고 있으며, 그동안에도 PKI를 위한 인터넷 표준은 계속하여 작업이 진행되었다.

PKI는 인터넷 상에서 메시지 송신자를 인증하거나 메시지를 암호화하는데 있어 가장 보편적인 방법인 공개키 암호문을 사용한다. 전통적인 암호문은 대개 메시지의 암호화하고 해독하는데 사용되는 비밀키를 만들고, 또 공유하는 일들이 관여된다. 이러한 비밀키나 개인키 시스템은, 만약 그 키를 다른 사람들이 알게 되거나 도중에 가로채어질 경우, 메시지가 쉽게 해독될 수 있다는 치명적인 약점을 가지고 있다. 이러한 이유 때문에, 인터넷 상에서는 공개키 암호화와 PKI 방식이 선호되고 있는 것이다.

PKI는 디지털 인증서를 발급하고 검증하는 인증기관, 공개키 또는 공개키에 관한 정보를 포함하고 있는 인증서, 디지털 인증서가 신청자에게 발급되기 전에 인증기관의 입증을 대행하는 등록기관, 공개키를 가진 인증서들이 보관되고 있는 하나 이상의 디렉토리, 그리고 인증서 관리 시스템으로 구성된다.

2-2 접근제어 기법(Access Control Techniques) 및 모델[3]

(1) 접근제어 기법

주체가 식별되고 인증되고 책임추궁성이 학립되고 나면, 주체는 리소스를 접근하거나 실행을 수행하기 위해 권한이 부여되어야 한다. 권한부여는 인증을 통하여 주체의 신원이 검증된 후에만 발생할 수 있다. 시스템은 접근 통제의 사용을 통하여 권한부여를 제공한다. 접근제어는 주체가 객체에 대하여 가지는 접근의 유형과 범위를 관리한다. 세 가지 접근제어 기법이 존재한다: 임의적(Discretionary) 접근제어, 강제적(Mandatory) 접근제어, 그리고 비임의적(Nondiscretionary) 접근제어.

임의적 접근제어(Discretionary access controls)를 채용하는 시스템은 객체의 소유자(Owner) 또는 생성자 객체에 대한 주체 접근을 통제하고 정의하도록 허용한다. 다시 말하면, 접근제어는 소유자의 재량에 기반한다. 임의적 접근제어는 객체에 대한 접근 통제

목록(access control list, ACL)을 사용하여 자주 구현된다. 각 ACL은 개인 또는 그룹으로 구성된 주체에 대하여 허가되거나 제한된 접근 유형을 정의한다. 임의적 접근 통제는 소유자들이 그들의 객체에 대한 ACL을 변경할 수 있기 때문에 중앙에서 통제되는 관리 시스템을 제공하지 않는다. 따라서, 접근은 강제적 접근 통제에서보다는 동적이다.

강제적 접근제어(Mandatory access controls)는 레이블(labels) 사용에 의존한다. 주체는 그들의 허가(clearances) 수준에 의해서 레이블된다. 객체는 그들의 분류(classification) 또는 민감성 수준에 의해서 레이블된다. 강제 접근 통제 시스템에서, 주체는 동일하거나 보다 낮은 레이블 또는 분류를 가지는 객체를 접근할 수 있다. 이러한 접근 통제 방식의 확장을 NEED-TO-KNOW라고 한다. 보다 상위 허가 수준을 가지는 주체에 있어서, 이들은 그들의 직무가 그러한 접근을 요구하는 경우에만 매우 민감한 리소스에 대한 접근이 허가된다. 만약 그들이 NEED-TO-KNOW를 가지지 않는다면, 비록 그들이 충분한 허가를 가지더라도, 그들의 접근은 거부된다.

강제적 접근제어에서의 보안 레이블(security label)의 사용은 여러 흥미로운 문제를 제시한다. 먼저, 강제적 접근 통제 시스템이 기능하기 위해서, 모든 주체 및 객체는 보안 레이블을 가져야 한다. 보안 분류는 민감성의 계층을 지시하며, 각 수준은 개별적이다. 실제로, 이러한 수준의 개별성은 객체를 한 수준에서 다른 수준으로 이동하려는 시도하는 경우에 문제가 발생한다.

비임의적 접근제어(Nondiscretionary access controls)는 또한 역할 기반 접근 통제(role-based access controls)라고 부른다. 비임의적 접근 통제를 채용하는 시스템은 객체를 접근하는 주체의 능력을 주체의 역할 또는 작업의 사용을 통하여 정의한다. 역할 기반 접근 통제는 접근 주체의 신원보다는 직무 설명(job description)(즉, 역할 혹은 작업)에 기반하기 때문에 자주 변경되는 환경에서 유용하다.

역할과 그룹은 유사한 목적을 가지지만, 도입과 사용에 있어서는 차이가 있다. 이 둘은 사용자들을 관리 가능한 단위로 수집하는 컨테이너(container)로써 기능하는 점에 있어서는 유사하다. 하지만, 사용자는 하나 이상의 그룹의 구성원이 될 수 있다. 각 그룹으로 권리(rights)와 허가(permissions)를 부여하는 것 이외에, 개별 사용자 계정은 또한 권리와 허가가 직접적으로 부여될 수 있다.

래티스 기반 접근 통제(Lattice-based access control)는 비임의적 접근 통제의 변형이다. 래티스 기반 접근 통제는 주체와 객체 사이의 모든 관계에 대하여 상위 및 하위 접근 한계(bounds)를 정의한다. 이러한 한계는 임의적일 수 있지만, 이들은 일반적으로 군사 및 기업 보안 레이블 수준을 따른다. 래티스 기반 접근 통제 하의 주체는 그들의 부여된 래티스 위치에 기반하여 레이블된 객체에 대한 최소 상위 한계와 최대 하위 접근 한계를 가진다.

규칙기반 접근 통제(Rule-based access controls)는 강제적 접근 통제의 변형이다. 규칙 기반 시스템은 주체 접근 허가, 객체에 대한 실행 수행, 또는 리소스 접근과 같이 시스템에서 발생할 수 있는 그리고 발생할 수 없는 것을 결정하는 규칙, 제한, 필터 모음을 사용한다. 방화벽, 프록시 그리고 라우터는 규칙기반 접근 통제 시스템의 보편적인 예이다. 규칙 기반 접근 통제는 시스템 관리자에 의해서 수립되고 유지되며 사용자에 의해서 수정될 수 없다.

(2) 접근제어 모델

접근제어 모델은 보안 정책의 상징적 묘사이다. 많은 경우에, 접근제어 모델은 어떤 컴퓨터 시스템이 접근을 제어해야 하는지를 규칙으로 정의함으로써 복잡한 보안 정책을 이해가능하게 만든다. 다음과 같은 다양한 접근 통제 모델이 존재한다: 상태머산 모델, 벨-라파듈라, 비바, 클락-윌슨, 정보 흐름 모델, 비간섭 모델, Take-Grant 모델, 접근 통제 매트릭스.

벨-라파듈라 모델(Bell-LaPadula Model)은 미국방부의 다수준 보안 정책(multilevel security policy)으로부터 개발되었다. 미국방부의 정책은 민감성의 수준에 따라서 네 가지 수준의 분류를 포함한다: top secret, secret, confidential, 그리고 unclassified. 정책은 어떠한 허가 수준을 가지는 주체는 그들의 허가 수준과 동일하거나 낮은 수준에 있는 리소스를 접근할 수 있다고 규정한다. 하지만, confidential, secret, 그리고 top sevret의 허가 내에서, 접근은 단지 neet-to-know

기반에서 허가된다. 다시 말하면, 특정 객체에 대한 접근은 특정 직무가 드러한 접근을 요구하는 경우에만 분류된 수준에 대하여 허가된다. 이러한 제한을 가지고, 벨-라파듈라 모델은 객체의 기밀성(confidentiality)을 유지하는 데 중점을 둔다. 벨-라파듈라는 객체에 대한 무결성(integrity) 또는 가용성(availability)의 측면을 대처하지 않는다.

벨-라파듈라 모델은 분류된 정보가 보다 덜 안전한 허가 수준으로 새거나 전송되는 것을 방지한다. 이것은 보다 하위로 분류된 주체가 보다 상위로 분류된 객체를 접근하는 것을 차단함으로써 이루어진다.

벨-라파듈라 모델은 상태 머신 모델에 기반한다. 이것은 또한 강제적 접근통제와 래티스 모델을 채용한다. 래티스 계층은 조직의 보안 정책에 의해 사용되는 분류수준이다. 이 모델에서, 안전한 상태는 두 가지 규칙 또는 특성 내에서 제한된다:

단순 보안 특성(Simple Security Property, SS property)은 특정 분류 수준에 있는 주체는 그 보다 상위 분류 수준을 가지는 데이터를 읽을 수 없다고 규정한다. 이것을 때로는 “상향 읽기 불가(no read up)" 라고 간략하게 표현한다.

보안 특성(Security Property)은 특정 분류 수준에 있는 주체는 하위분류 수준으로 데이터를 기록할 수 없다고 규정한다. 이것을 때로는 “하향 쓰기 불가(no write down)"라고 간략하게 표현한다.

이러한 두 가지 규칙은 시스템이 이행될 수 있는 상태를 정의한다. 다른 어떠한 이행도 허용되지 않는다. 이러한 두 가지 규칙을 통하여 접근 가능한 모든 상태는 안전한 상태이다. 따라서, 벨-라파듈라 모델 시스템은 상태 머신 모델 보안을 제공한다.

2-3 DRM의 개요[4]

디지털콘텐츠는 특성상 무한히 반복하여 사용해도 품질의 저하가 발생하지 않고, 수정과 복사가 편리하며, 그리고 통신망을 통해 대용량의 콘텐츠를 짧은 시간에 전송과 배포가 가능하다. 이러한 특성은 디지털콘텐츠의 배표용이 및 손쉬운 접근 환경을 제공함으로써 누구든지 쉽게 콘텐츠를 이용할 수 있도록 순기능을 제공하기도 하지만, 불법복제로 인한 지적재산권들의 권익이 심각하게 위협하는 등 사회적인 역기능의 주요 원인이 되기도 한다.

이러한 디지털콘텐츠의 불법복제방지와 저작권을 보호하기 위하여 다양한 방식의 기술적 대안들이 제시되었는데 그 중에서 DRM이 최적의 기술로 평가되고 있으며, 이미 다양한 분야에서 DRM 솔루션들이 사용되고 있다.

DRM에 대한 정의는 현재까지 국내외적으로 논란의 여지가 많지만 크게 협의의 의미의 DRM과 광의의 의미의 DRM으로 구분할 수 있다. 협의의 의미의 D끄은 불법복제로부터 디지털콘텐츠에 대한 지적재산권을 지속적으로 보호해 주는 사용권한 제어기술로, 디지털콘텐츠의 암호화를 수행하는 패키징 기술과 허가된 사용자만 허가된 권한으로 콘텐츠를 이용할 수 있도록 권리를 부여하는 라이센스 기술, 그리고 이렇게 부여된 권한이 지속적으로 보호되는 환경에서 콘텐츠의 이용이 이루어질 수 있도록 하는 권한통제 기술 등이 이 범주에 해당된다. 광의의 의미의 DRM은 협의의 DRM 기술요소들이 디지털콘텐츠 유통체계에 통합되어 콘텐츠의 생산, 분배, 거래규칙, 이용규칙, 과금, 거래내역의 관리 및 보고, 정산 등 디지털콘텐츠의 전체 라이프사이클에 걸쳐 투명성과 신뢰성을 보장하는 신뢰기반의 유통체계 전반을 통칭하는 의미로, 디지털콘텐츠 식별체계, 메타데이터 관리체계, 거래내역 관리체계, 그리고 거래 쌍방 간의 신뢰를 보장해 주는 인증관리체계 등 디지털콘텐츠의 유통에 참여하는 모든 참여주체들에게 투명성과 신뢰성을 제공해주는 기반 서비스를 일컫는다. 이외에도 광의의 의미의 DRM은 워터마킹, 핑거프린팅, 수신권한제어기술(CAS), 복제방지기술 등 디지털콘텐츠의 보호를 위해 사용되는 모든 기술을 포함하는 개념으로 사용된다.

디지털콘텐츠에 대한 불법적인 사용이나 복제를 방지하기 위한 기술적인 접근방식은 크게 소극적인 보호기술과 적극적인 보호기술로 구분할 수 있다. 소극적인 보호 기술(Passive Protection Technology)은 일종의 스피드 범퍼와 갖은 역할을 제공하는 기술로, 허가되지 않은 사용자에게 비록 디지털 콘텐츠의 사용은 허가하되 법적인 자각심을 유도하여 스스로 불법적인 행동을 자제하게 만드는 효과를 기대하는 방식이다. 적극적인 보호 기술(Active Protection

Technology)은 암호화 기술을 이용하여 사용이 허가되지 않는 사용자에게는 디지털 콘텐츠의 접근을 차단시키는 강력한 불법복제방지 기술을 사용하는 방식이다.

(1) 소극적 보호 기술

소극적인 보호 기술로는 저작권 정보 표시(Copyrights Information), 디지털 워터마킹(Digital Watermarking), 디지털 핑거프린팅(Digital Fingerprinting) 등이 있다. 저작권 정보의 표시방식은 디지털콘텐츠를 사용하기 전에 사용자가 저작권에 대한 정보를 볼 수 있도록 함으로써, 사용자로 하여금 무단 도용 혹은 복제 및 배포에 대한 행위를 자제하게 하는 역할을 한다. 디지털 워터마킹 방식은 저작권 정보를 담고 있는 워터마크를 원본의 내용을 왜곡하지 않는 범위에서 혹은 사용자가 전혀 인식하지 못하도록 디지털 콘텐츠에 삽입하는 기술이다. 이렇게 삽입된 워터마킹 정보는 저작권에 대한 침해 사례가 발생하였을 경우, 복제된 디지털 콘텐츠의 내부에서 저작권 정보를 추출하여 저작권 소유에 대한 증거자료로 활용될 수 있다. 디지털 핑거프린팅 방식은 디지털 워터마킹과 비슷한 기술이지만 저작권자나 판매자의 정보가 아닌 사용자의 디지털 콘텐츠의 사용내역 정보를 삽입함으로써 사후에 발생하게 될 콘텐츠의 불법복제자를 추적하는데 사용하는 기술이다. 디지털 핑거프린팅 방식은 디지털 콘텐츠를 사용하는 사용자 고유의 정보를 담고 있는 핑거프린팅이 삽입되므로, 정상적인 사용자인 경우 서로 다른 핑거프린팅을 가진 콘텐츠를 사용한다는 것이 워터마킹 기술과의 차이점이다. 또한 디지털 워터마킹은 불법사용 여부를 확인할 수 있는 정보만을 제공하지만, 디지털 핑거프린팅은 사용자가 디지털 콘텐츠를 사용할 때 사용내역이 삽입되기 때문에 디지털 콘텐츠의 불법복제 경로 추적을 위해 사용될 수 있다.

(2) 적극적인 보호 기술

저작권 정보를 표시하는 방법이나 디지털 워터마킹을 사용하는 등의 소극적인 보호기술은 비록 허가되지 않은 사용자라고 하더라도 디지털콘텐츠의 접근을 허용하는 것에 비해 적극적인 보호기술은 허가되지 않은 사용자로부터 접근을 원천적으로 차단함으로써 콘텐츠를 적극적으로 보호하는 기술이다. 적극적인 보호기술은 기술적인 특성에 따라 접근제어 방식과 사용제어 방식, 그리고 복제방지(Copy Protection) 방식으로 크게 구분할 수 있다.

접근제어 방식은 사용자 혹은 디바이스가 특정 디지털콘텐츠에 대한 접근권한이 있는 경우에만 해당 디지털콘텐츠의 사용을 허가하는 기술이다. 이 방식은 디지털콘텐츠에 대한 정당한 권한을 가지고 있는 사용자만이 콘텐츠에 대한 접근 및 이용을 할 수 있도록 하는 것이다. 그러나, 접근 제어 방식은 비록 암호화 기술을 이용하여 콘텐츠를 암호화한다고 하도라도 허가된 사용자에겐 암호화된 콘텐츠를 복호화하여 원본 콘텐츠를 제공하기 때문에 콘텐츠의 지속적인 보호가 불가능하다는 한계점을 지니고 있다, 사용 제어 방식은 사용권한이 있는 사용자라 하더라도 부여된 권한에 따라서 디지털콘텐츠의 사용권한을 지속적으로 통제하는 방식이다. 이 방식은 원본 콘텐츠에 대한 추출이 디지털콘텐츠의 생명주기 전반에 걸쳐서 보장되기 때문에 현재 많은 디지털콘텐츠들이 이 기술을 이용하고 있다. 복제방지 방식은 디지털콘텐츠를 저장매체나 또는 디바이스에 유일하게 부여된 정보를 키로 사용하여 암호화함으로써, 다른 매체나 디바이스로 복제가 되어도 의미없는 데이터가 되게 하는 기술이다. 소프트웨어 소스코드에 대한 소극적인 보호기술인 저작권 정보 표시 기술은 소프트웨어의 소스코드에 대한 디지털 라이센스를 발행 및 검색하는 기술이 개발되었다[5,6]. 본 논문에서는 소프트웨어 소스코드의 적극적인 보호기술을 개발하기 위한 CRYPTEX 모델을 제안하며, 그림 1과 같이 크립텍스 모델의 기능과 역할을 예측해 본다.

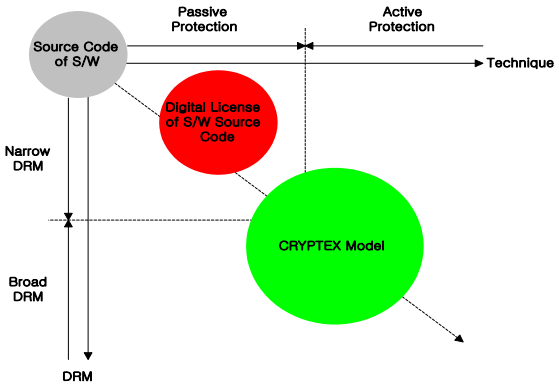

그림 1. 크립텍스 모델의 기능과 역할
Fig 1. Role and function of CRYPTEX model

2-4 국내 DRM의 문제점

2000대 초부터 시작된 국내 DRM 기술은 많은 DRM 벤처 기업들에 의해 다양한 분야의 제품을 개발해 옴으로써 국제 수준과 뒤떨어지지 않는 수준에 도달하였다고 할 수 있다. 특히, 국내 기업의 문서보안용 DRM기술은 국제적인 경쟁력을 갖추고 있을 정도로 주목할 만한 기술적 성과를 이끌어 내고 있다. 그러나 이러한 노력과 성과에도 불구하고 국내의 DRM 기술은 국제무대에서 크게 주목을 받지 못하고 있는 실정이다. 이러한 상황은 여러 가지 요인에 의해서 발생된 것이긴 하겠지만 대표적인 원인은 크게 DRM 원천 기술의 부족과 국내 DRM 표준화 추진체계 미비이다.

(1) DRM 원천 기술 부족

국내 DRM 기술은 문서 보안 분야 및 인터넷 기반의 디지털콘텐츠 유통 분야 등 틈새시장 분야의 응용기술면에서 해외 기술에 비해 다소 우위이거나 대등한 수준의 기술력을 보유하고 있음에 비해, 선진 국가는 디지털 방송, 동영상, 오디오, 미디어 등 분야에서 대중시장을 겨냥한 다양한 종류의 DRM 원천 기술 개발 및 국제적 영향력을 발휘하고 있다. 그러나 국내에서는 오직 협의의 DRM 분야에 대한 기술 개발에만 치중함으로써 디지털 방송 및 멀티미디어 등 대중 미디어 시장분야에선 디지털콘텐츠 보호기술의 기반이 취약한 것으로 분석되고 있다. 또한 서진국가에서는 원천기술 확보와 표준화에 주력하고 있음에 비해, 국내 DRM 기술은 응용 레벨의 기술개발에 치중하여 원천기술에 대한 지적재산권 확보 미흡 및 표준화 활동이 저조한 것으로 파악되고 있다.

(2) 국내 DRM 표준화 추진체계 미비

국내의 DRM 기술은 다양한 분야에서 국제적 수준의 기술 경쟁력을 보유하고 있으나 국내 DRM의 표준화는 매우 초보적인 단계에 머무르고 있는 실정이다. 이것은 국내 DRM 업체들이 매우 적극적인 기술개발과 치열한 시장경쟁 구도 속에서 자발적인 표준화 논의를 할 필요성을 느끼지 못한 점도 있었겠지만, 국제 표준 기술의 우선 수용 정책으로 인해 국내 표준을 유도하기 위한 국내 DRM 표준화 추진체계의 구조적, 정책적 인식 부족도 큰 요인으로 꼽을 수 있다. 또한 이미 다양한 종류의 DRM 제품이 상용화되어 시장 전반에 걸쳐 사용되고 있는 상황에서 하나의 기술규격을 통한 DRM 표준화를 추진하는 것은 기존 DRM 업체들의 이해관계를 고려해 볼 때 쉽지 않을 것으로 판단된다. 특히 2000년대 초에 진행되었던 많은 국제적 DRM 표준화 활동의 실패와 현재까지 진행되고 있는 다양한 국제표준화단체의 더딘 표준화 진행으로 아직까지 시장에서 지배적 위치의 DRM 표준이 등장하지 못하고 있는 점도 국내 표준화가 난항을 겪게 되는 주요 요인으로 작용하였다. 국내 DRM 표준화 미비는 곧 제품의 기능 및 기술규격에 대한 일관성을 떨어뜨림으로서 고객의 요구에 따라 용역형태의 DRM 공급과 수요 중심으로 시장을 형성하였을 뿐만 아니라 DRM 제품간 호환성을 크게 악화시키는 요인으로 작용하게 되었다. 이로 인해 국내 DRM 기술은 기술개발의 응집력이 결여됨으로 인해서 DRM 솔루션 개발업체, 콘텐츠 사업자, 제조업체들 간의 통일된 비전을 도출하지 못하는 결과를 초래하였으며, 이는 곧 DRM 업체의 수익구조 악화와 국제 경쟁력 확보를 할 수 있었던 좋은 기회를 놓치게 됨으로써 국가적 기회상실의 요인으로 작용하고 있다.

(3) 국내 DRM 표준화를 위한 제언

국내 DRM 표준화를 위한 제언으로는 상이한 DRM간 디지털콘텐츠 연동 기술 개발, 국내 자체 원천 기술 개발 필요, 국내 표준화 대책 마련 그리고 국제 표준화 추진전략 등이다. 상이한 DRM간 디지털

콘텐츠 연동 기술 개발측면에서 현재까지 DRM 기술 간 상호호환성을 보장하기 위하여 각 표준단체나 산업체에서 접근한 방식은 하나의 기술규격을 통한 DRM 시스템의 호환성을 보장하는 방식이었다. 그러나 다양한 종류의 보호 기술과 다양한 공급업체의 이해관계 대립으로 상호호환성을 보장하기란 매우 어려운 상황에 처해있는 실정이다. 따라서 디지털콘텐츠가 다양한 보호 시스템 환경에서 투명하고 호환성 있게 사용되기 위해서는 각 보호 시스템이 서로의 기술규격이나 특성을 유지하면서 연동될 수 있는 표준기술의 개발 및 보급 확산 정책이 필요하다. 디지털콘텐츠의 보호에 대한 주요 원천기술들은 이미 유수한 선진국가의 기업들에 의해 특허가 등록된 상태이다. 이들 업체는 이러한 특허를 기반으로 국제 표준화 활동을 적극적으로 펼치고 있는 상태지만 국내의 DRM 솔루션 업체들은 이에 대한 자생적인 지적재산권 대항력을 갖지 못하고 있는 상태이다. 또한 국내 DRM 솔루션 업체들이 보유하고 있는 기술 경쟁력에 비해 국제시장에서의 인지도는 매우 낮은 상태에 있기 때문에 해외 진출 시에도 많은 어려움을 겪고 있는 실정이다. 특히 향후 본격적인 디지털콘텐츠 보호 시장이 펼쳐질 경우 해외 선진업체들의 막대한 기술 로열티 요구로 인하여 막대한 비용의 로열티 지출이 불가피함은 물론 국내 디지털콘텐츠 산업의 위축도 예상될 수 있다. 따라서 국내 DRM 기술이 세계적인 기술 경쟁력을 확보하기 위해서는 연구개발 방향을 다시 점검해 보고 국제적인 기술 경쟁력이 있는 분야를 선정해서 국제적인 인정을 받을 수 있도록 전폭적인 지지와 투자를 해야 할 것이다. 정부는 연구소나 산업체가 충분할 기술개발을 할 수 있도록 디지털콘텐츠 산업의 시장 활성화를 위한 정책의 개발 및 각종 기술 지원책을 마련해야 할 것이며, 산업체와 학계, 연구소는 세계적인 경쟁력을 가질 수 있는 기술 및 제품의 연구 개발과 적극적인 국제 표준화 활동으로 국내 콘텐츠 보호 기술의 국제 인지도 향상과 영향력을 증진하도록 노력해야 할 것이다. 국내 표준화 측면에서 DRM 기술은 인터넷 기반의 디지털콘텐츠 유통뿐만 아니라 디지털 방송과 디지털 홈 엔터테인먼트 등 다양한 응용 도메인에서 공통적으로 사용될 수 있는 기술이다. 그러나 현재의 DRM 기술 개발은 uIT-839 전략의 각 분문별 또는 응용 도메인별 자체적인 DRM 기술 개발을 진행하는 등 상호연관성을 갖지 못한 채 개발이 진행되고 있는 실정이다. 따라서 디지털 컨버전스 시대에서 반드시 요구되는 투명성(transparency)과 상호호환성(interoperability) 측면에서 향후 적지 않은 문제점이 야기됨은 자명한 일이다. 이를 개선하기 위해서는 국내 DRM 관련 표준화 단체를 재정비하고, 범국가적인 체계적 표준화 방안을 준비하여 실질적인 국내 표준화 작업이 진행될 수 있도록 여러 가지의 지원방안을 마련해야 할 것이다. 또한 국내의 DRM 기술 표준화 진행 정도와 병행해서 이를 인증하고 관리할 수 있는 국내 조직체계의 구축과 향후 해외 인증기관과의 협력관계 정립 등을 통해 인증기관 간 국제 상호 이증체계의 구축을 해나갈 수 있도록 해야 할 것이다. 국제 표준화 추진 전략 측면에서는 이미 앞에 언급된 바와 같이 국내의 DRM 기술은 원천기술이 미약한 상태이기 때문에 현 상태에서 국제 표준화를 추진하는 것은 많은 어려움을 가질 수 밖에 없다. 또한 다양한 DRM 표준화 단체 중에서 아직까지 지배적 위치를 차지한 DRM 표준기술이 없다는 점도 선택과 집중을 할 수 밖에 없는 우리의 상황에서 매우 어려운 결정을 요구한다고 할 수 있다. 그러나 현재 활발한 활동을 벌이고 있는 단체를 전략적 표준화 대상으로 삼아서 지속적인 참여와 기여의 폭을 넓혀 나가야 할 것이다. 특히, 국제적으로 선도적인 위치에서 진행되고 있는 DRM 분야에서 국내 DRM 표준을 적극적으로 만들고, 이를 기반으로 해외 대형 IT 업체들의 참여를 유도하는 동시에 국제적인 산업표준으로 끌고나가는 전략적 국가정책이 절실히 요구된다.

Ⅲ. 크립텍스의 비지니스 모델

본 연구의 선행 연구로 소프트웨어의 저작권을 보호하기 위한 소극적인 보호 기술로 소프트웨어의 소스코드에 대한 디지털라이센스 발행, 검색, 분류 그리고 성능에 대한 연구를 수행하였다[5-8]. 소프트웨어 소스코드의 디지털라이센스는 저작권과 소프트웨어의 아키텍처, 색인정보, 노드 정보를 이용하여 저

작권 정보를 표시하는 방법이었다. 디지털라이센스는 소프트웨어의 소스코드와 같이 수동적인 개체이며, 능동적인 수행능력을 갖지 않는다.

이를 지원하기 위한 적극적인 보호 기술은 소프트웨어의 소스코드를 보호하기 위한 제반 기술의 지원과 프레임워크는 너무나도 빈약한 상태이다. 이를 해결하기 위한 하나의 방법으로서는 먼저, 크립텍스의 비즈니스 모델이 수립되어야 한다.

크립텍스(Cryptex)는 인증 및 인증되지 않은 주체로부터 객체인 소프트웨어의 소스코드를 안전하게 보호 및 접근제어를 지원하기 위한 제반 기술들의 집합을 통칭하는 모델이다. 크립텍스 비즈니스 모델의 시스템 구성은 주체인 개발자, 객체는 크립텍스 그리고 인증기관이 된다. 크립텍스의 비즈니스 모델은 크게 인증 단계와 접근제어 단계로 나눌 수 있다. 인증 단계는 인증기관, 지적재산권의 소유자, 크립텍스의 세 가지로 구성된다. 접근제어 단계의 구성은 인증서, 지적재산권의 소유자, 그리고 크립텍스이다. 크립텍스는 소프트웨어의 소스코드와 이를 접근제어하는 알고리즘으로 구성된다.

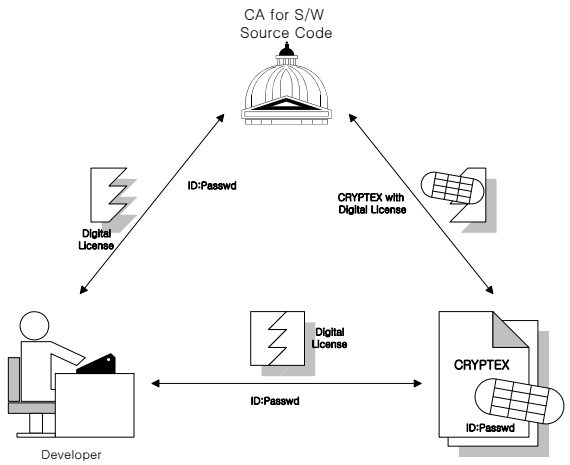

그림 2. 크립텍스의 비즈니스 모델
Fig 2. Business model of CRYPTEX

3-1 크립텍스 : 소스코드 관리 및 보안 기능

크립텍스의 핵심 기능은 소프트웨어 소스코드의 관리와 이를 접근제어하기 위한 알고리즘으로 구현된 이동에이전트(Mobile Agent) 소프트웨어이다. 소프트웨어의 소스코드는 코드 자체가 아스키코드 또는 유니코드로 이루어졌으며, 프로그래밍 언어로 소프트웨어가 수행할 작업들이 기술되어 있는 수동적인 문서 상태이다. 능동적인 일을 수행할 수 있는 프로세스 상태가 아니기 때문에 이를 보완하기 위한 기능을 갖는 크립텍스에 포함시켜서 이동, 관리 및 접근제어를 수행하게 된다.

크립텍스 = 모빌 에이전트 기능 + 캡슐 기능
캡슐 기능 = 인증 + 인증서(디지털라이센스) + 접근제어 + 암호 및 압축 기능

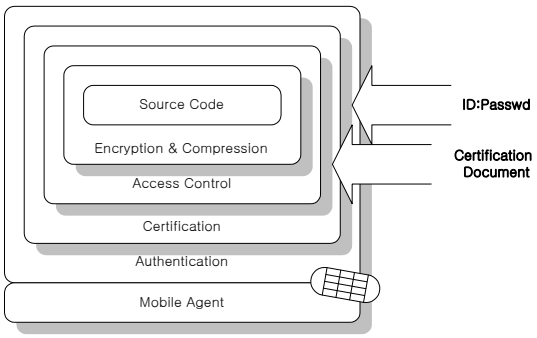

그림 3. 크립텍스 모델
Fig 3. CRYPTEX model

(1) 소스 코드의 이동 및 관리 기능

소스코드는 아스키 코드 또는 유니코드로 구성된 수동적인 파일 개체이다. 크립텍스 자체는 의미가 없으며, 소스코드를 관리하기 위해서 능동적인 관리시스템의 역할 기능의 수행과 네트워크를 통한 이동 기능을 갖는다. 관리 기능으로는 소스코드의 관리 기능, 인증서 관리 기능, 압축 기능, 디지털라이센스 기능, 인증 기능, 접근제어의 매칭 및 권한부여 기능, 그리고 네트워크를 통한 이동 기능을 갖는다.

(2) 소스 코드의 보안 기능

인증 단계의 완료후의 사용자와 소스코드에 대한 접근제어, 접근 레벨에 의한 소스코드의 접근 제어 기능을 수행하게 된다. 접근제어 기능으로는 접근 정책과 레벨, 위임, 인증서의 시한 기능, 암호 기능 등을 수행한다.

3-2 주체/객체의 인증서

(1) 소스코드의 디지털라이센스

주체/객체의 인증서는 소스코드에 대한 디지털 라이센스를 포함한다. 디지털 라이센스는 소스 코드에 하드 카피보다 더 많은 정보를 제공할 수 있다. 디지털 라이센스는 소스코드에 대한 노드와 트리로 구성된 아키텍처 정보와 개발자의 정보로 구성되어 있다. 디지털 라이센스에 의해서 크립텍스와 개발자 또는 구매자가 서로 일치하는 지를 결정할 수 있는 패턴 정보를 제공한다. 또한 디지털라이센스는 직접 소스코드를 열어보지 않더라도 소스코드에 동등한 정보를 제공하는 기능을 제공한다. 디지털라이센스에 의해서 소스코드를 분류 및 검색, 매칭이 가능하고, 효과적인 정보제공으로 지능적인 응용프로그램 개발 및 지원이 가능하다[5,6].

(2) 접근제어 레벨 및 모델

인증서에는 접근제어 레벨과 시한이 기록되어 있다. 사용자 또는 구매자와 크립텍스는 각각의 접근제어 레벨과 시한을 갖는다. 주체와 객체 인증서의 결합에 의해서 접근제어 레벨과 모델 그리고 접근할 수 있는 시한이 결정된다.

(3) 인증서의 보안

인증서에는 인증서 자체의 무결성을 보장하기 위한 보안 코드가 삽입되어 있으며, 인증서는 객체와 주체 인증서로 구분된다. 객체 인증서를 소프트웨어 소스코드에 대한 인증서이며, 주체 인증서는 개발자, 판매자 또는 구매자에 대한 인증서이다. 인증서에는 주체와 객체에 대한 정보를 포함하고 있으며, 두 인증서의 결합에 의해서 완벽한 인증서를 만들게 된다. 인증서에 기술된 보안 정책에 의해서 크립텍스와 크립텍스 사용자에 대한 접근 제어가 이루어진다. 2차적인 보안 정책으로는 ID:Passwd에 의해서 한번 더 보안정책을 검증하게 된다.

(4) 주체 및 객체 인증서의 결합

주체의 인증서에 포함된 디지털라이센스와 객체의 인증서에 포함된 디지털라이센스의 내용에 의한 매칭이 이루어져야 주체/객체의 인증서의 결합이 완료된다. 주체/객체의 인증서의 접근레벨과 모델이 정의에 의해서 결정되며, 이를 위배할 시에는 모든 기능이 정지되거나, 파기된다.

Ⅳ. 크립텍스의 물리적 접근제어 모델

과거의 소프트웨어 소스코드를 대변하는 디지털 라이센스의 수동적 인증에서 진보하여, 소프트웨어 소스코드의 능동적인 접근제어가 필요하다. 소프트웨어 소스코드는 아스키코드(ASCII code)나 유니코드(Unicode)로 구성되어 있어서, 능동적인 접근제어가 불가능하다. 주체의 ID:Passwd와 주체/객체의 인증서에 의해서 객체인 크립텍스는 접근제어를 수행하게 된다. 먼저, 주체의 ID:Passwd는 주체의 신원을 식별하고, 책임추궁성이 시작되는 과정이다. 주체와 객체의 인증서에는 소프트웨어 소스코드에 대한 디지털 라이센스와 크립텍스의 접근제어 정보로 구성된다[9-11].

4-1 인증 단계

인증 단계는 소프트웨어 소스코드의 접근에 따른 책임추궁을 위한 신원 확인단계이다. 신원 확인은 인증기관에서 발급된 ID와 Passwd에 의해서 주체의 신원과 접근제어를 위한 레벨이 결정된다.

4-2 접근제어 단계

인증 단계의 완료에 의해서 주체의 신원이 확인되면, 이어서 발급된 주체와 객체의 인증서에 의해서 접근제어 단계가 수행된다.

(1) 접근제어의 정책 및 레벨

크립텍스에 포함된 소스코드에 접근하기 위해서는 CA에 초기 등록자에 의해서 정책 수립, 레벨 부여, 위임 부여 그리고 판매전략과의 매핑이 설정되어야 한다.

■ 정책 수립 단계 ■ 레벨 부여 단계
■ 위임 부여 단계
■ 정책수립과 판매 전략과의 매핑

크립텍스를 이용하여 소프트웨어의 소스코드를 전자상거래로 판매할 수 있게 된다. 과거에는 소스코드는 개발자와 구입자간에 1:1 간의 거래에만 가능하였고, 구입자에 의한 2차 거래에는 제한할 수가 없었다. 그렇지만, 크립텍스를 이용하면 좀더 진보적인 전자상거래가 가능하게 되며, 모든 거래에 대한 저작권 관리가 어느 정도 이루어진다.

(2) 접근제어의 규칙

10 여 년 전에는 보안의 기본정책은 특별한 사유가 없으면 허가되었으나, 해커와 바이러스 등으로 인트라넷 보호를 위한 방화벽(FireWall) 시스템의 활성화로 허가되지 않으면 허가하지 않는다는게 묵시적인 기본원칙이 되었다. 크립텍스의 접근제어의 규칙 역시 시대적 흐름에 따라, 주체와 객체의 두 인증서에 의해서 주체의 레벨과 객체의 레벨이 동일한 경우에는 해당 레벨에 해당하는 접근 제어가 수행된다. 주체와 객체의 레벨이 다른 경우에는 규칙에 의한 접근 제어가 수행된다.

정의 1) 능동 주체인 크립텍스의 접근제어를 위해서는 크게 문서 객체와 접근제어 리스트로 이루어진다.

- 문서 객체 = { 소스코드, 인증서 }
- 접근제어 리스트 = { C_cal, U_cal, CM_cal }
  - C_acl : 크립텍스의 접근제어 리스트
  - U_acl : 사용자의 접근제어 리스트
  - CM_acl : 인증서의 접근제어 리스트
- 접근제어 행위
  - act = { Open, Read, Write, Close, Destroy, Access_time }
  - Read = { Read_part, Read_full, Capture }
  - Write = { Write_part, Write_full, CaptureWrite }
  - Access_time = { Publication_time, Limit_time }

정의 1-1) 크립텍스, 사용자, 인증서의 접근제어 리스트

- C_acl = {Open, Read, Write, Close, Destroy}
- U_acl = {Open, Read, Write, Close, Destroy}
- CM_acl = {Open, Read, Write, Close, Destroy}

정의 1-2) 크립텍스, 사용자, 인증서의 접근제어 연산

- ∧ : 피연산자의 Min 연산
- ∨ : 피연산자의 Max 연산

정의 1-3) 모든 접근제어는 소스코드의 합법적인 접근에 최소 오픈을 전제로 수행된다.

정의 1-4) 소스코드의 구매자 위임에 의한 접근 제어는 정의 1-3)과 판매에 의한 보안 정책에 따라 결정된다. 구매자에 대한 최소의 권한이 보장되며, 개발자와 CA에 대해서 동등한 권한을 제공하지는 않는다.

(3) 접근제어 레벨의 충돌

- 객체의 레벨이 높은 경우

  -> 주체의 레벨이 따른 접근제어 수행

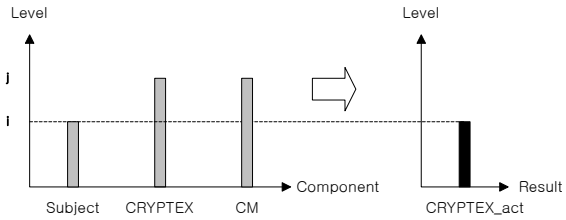

그림 4. 접근제어의 충돌 예제1의 해결

Fig 4. Solution of conflict example 1 for access control

- 주체의 레벨이 높은 경우

-> 객체의 레벨이 따른 접근제어 수행 (a)

-> 인증기관으로부터 주체의 레벨에 해당하는 객체인 크립텍스를 새로 생성하여 다운로드하여 접근제어를 수행 (b)

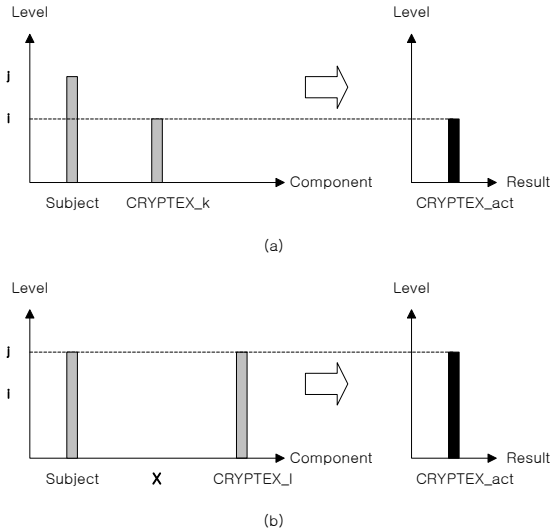

그림 5. 접근제어의 충돌 예제2의 해결
Fig. 5. Solution of conflict example 2 for access control

(4) 접근시한 충돌

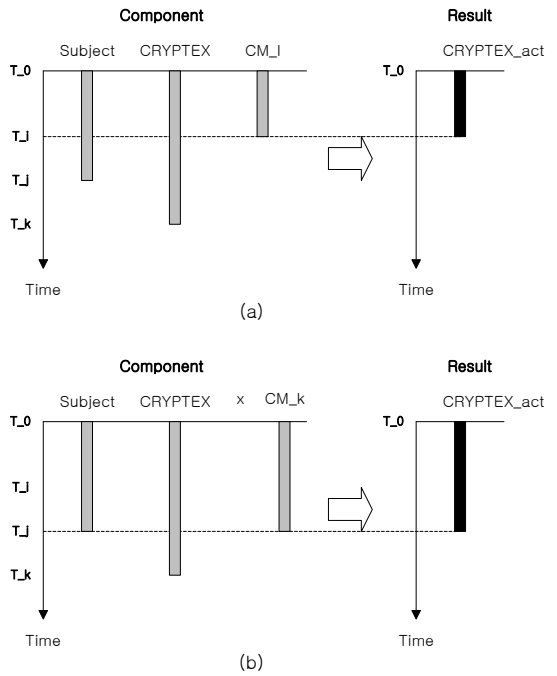

그림 6. 접근시한의 충돌 예제3의 해결
Fig. 6. Solution of conflict example 3 for access time limit

■ 주체 접근시한이 객체 접근시한 초과

-> 객체 인증서에 의한 시한에 따라 접근 제어 수행

-> 인증기관으로부터 객체의 접근시한을 재발급 받아서 접근제어를 수행

■ 객체 접근시한이 주체 접근시한 초과

-> 객체 접근시한과 무관하게 주체 접근시한까지만 접근제어 가능하며, 그 이후에는 접근제어 금지(파기)

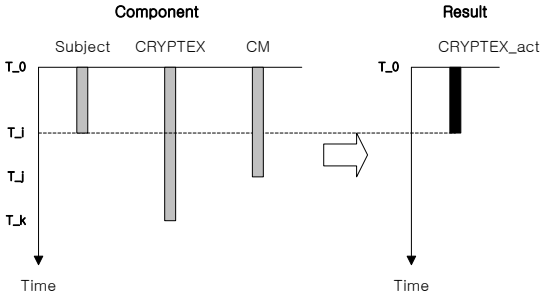

그림 7. 접근시한의 충돌 예제4의 해결
Fig 7. Solution of conflict example 4 for access time limit

(5) 제 3자에 의한 소프트웨어 소소코드의 판매 및 구매

개발된 소프트웨어는 일반적으로는 컴파일된 바이너리 파일 형태로도 팔리지만, 기술이전 및 원천기술 구매에 의한 소프트웨어의 소스코드 자체로도 판매가 된다. 제 3자로부터 소프트웨어의 소스코드를 구매하거나 판매한 경우에는 물리적인 물질이 아니므로, 지적재산권에 해당하는 권리와 소스코드 문서의 접근권한을 얻게 된다. 이를 위해서는 판매자는 주체에 대한 권한을 구매자에게 위임을 하며, 구매자는 판매자에게 주체에 대한 권한을 위임 받게 된다. 구매자의 위임 레벨은 판매전략과 접근 정책에 의해서 접근권한이 결정된다.

■ 구매자는 소프트웨어 소스코드 판매자로부터 위임된 새로운 ID:Passwd를 승계 받음

■ 구매자는 승계된 ID:Passwd에 의한 크립텍스 객체를 새로 생성 및 다운받아 사용

■ 구매자는 개발자와 CA로부터 모든 권한을 위임받을 수 있으나, 위임된 권한은 계약된 상황과 보안정책에 의해서 100% 승계되지 않으며, 일부분 제약을 받는다.

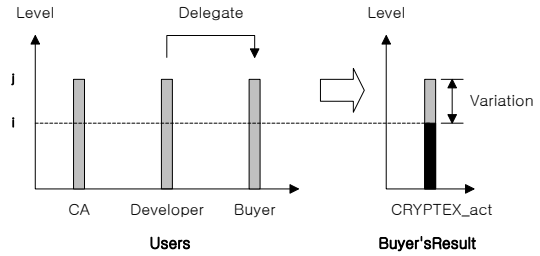

그림 8. 위임에 의한 충돌 예제5의 해결
Fig 8. Solution of conflict example 5 for delegation

4-3 소스코드 핸들링

크립텍스의 소스코드에 대한 접근은 일반적인 파일처리에 유사하다. 먼저 소스 코드 파일을 Open-Read-Write-Close의 절차를 따르게 된다.

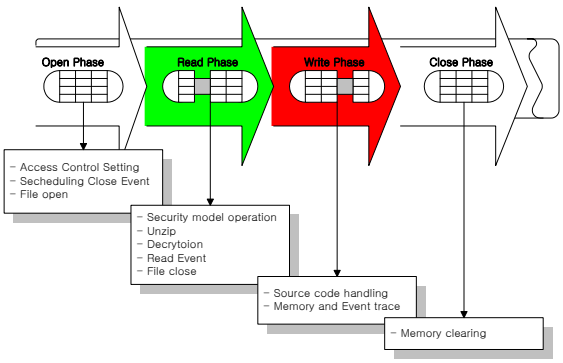

그림 9. 크립텍스의 소스코드 핸들링 과정
Fig 9. Source code handling process of CRYPTEX

(1) Open 보안 : 크립텍스의 소스코드를 접근하기 위해서는 소스코드를 Open하여야 한다. 크립텍스는 Open핸들링이 이루어지면, 자동적으로 Close 핸들링이 스케쥴링이 계획된다.

(2) Read 보안 : 크립텍스에 의해서 Open 핸들링이 수행된 소스코드는 Read 핸들링이 이루어지는데, 이때 암호화와 압축의 해제가 이루어진다. 또한 접근제어 정책에 의한 접근 레벨이 결정되어 진행된다.

(3) Write 보안 : 크립텍스의 Write 핸들링은 소스코드를 외부로 유출시키는 동작이다. 이 또한 접근제어 정책에 의해서 접근 레벨이 결정되며, 소스코드의 블록복사 또는 화면 캡쳐도 이 단계에서 수행되거나 거부된다.

(4) Close 보안 : 크립텍스에 의해서 이루어진 모든 동작에 사용된 메모리와 기타 정보들을 모두 초기화 시키는 단계이다. Open 핸들링이 진행되면 수행된 동작의 스케줄링에 의해서 메모리의 사용을 추적하면서 초기화 작업을 계획 및 수행된다.

4-4 소스코드 파기

은행의 ATM기기에서 3번의 인증이 실패한 경우, 인증 및 인출이 불가능하며, 그 계정에 대한 보안을 재설정이 되어야 한다. 크립텍스 모델 또한 3번의 인증 실패 경우, 크립텍스는 자체 파기 또는 불능이 되도록 설계된다. 크립텍스를 다시 사용하기 위해서는 소스코드 다운로드 사이트에서 크립텍스를 다시 다운로드를 받아야 한다.

Ⅴ. 결 론

본 논문에서는 크립텍스라는 인증 및 인증되지 않은 주체로부터 객체인 소프트웨어의 소스코드를 안전하게 보호 및 접근제어를 지원하기 위한 제반 기술들의 집합을 통칭하는 모델을 제안하였다. 그리고 크립텍스를 이용하여 단지 수동적인 문서 상태의 소프트웨어 소스코드에 대해서 능동적이며, 접근제어 및 보안이 가능하며, 이동 및 위임기능을 부여할 수 있는 비즈니스 모델을 제안하였다.

감사의 글

이 논문은 2007년도 정부재원(교육인적자원부 학술연구조성사업비)으로 한국학술진흥재단의 지원을 받아 연구되었음(KRF-20078-313-D00763).

참 고 문 헌

[1] Dan Brown, "The Da Vinci Code", 베텔스만, p.306-312, 2004.

[2] Andrew Nash, William Duane, Celia Joseph, and Derek Brink, "PKI Implementing and Managing E-Security", *McGraw-Hill,* 2001.

[3] Ed Tittel, Mike Chapple and James Michael Stewart, "CISSP:Certified Information Systems Security Prof

essional Study Guide", *Sybex,* 2003.

[4] Hogap Kang, "Opposition strategy and Trend analysis of Domestic DRM Standardization", *Communications of The Korea Information Science Society*, Vol. 23, No. 8, p.15-24, August, 2005.

[5] Byungrae Cha, "Comparison of S/W Source Code vs. Digital License for IPR", *JCIT,* Dec, 2006.

[6] Byungrae Cha, "Business Model and Comparasion of S/W Source Code vs. Digital License for IPRs", *KES-AMSTA 2007, LNAI 4496*, p.825-832, May, 2007.

[7] Byungrae Cha, Kyungjun Kim, and Dongseob Lee, "Study of Digital License Search for Intellectual Property Rights of S/W Source Code", *ICCSA 2007,* LNCS 4707 Part 3, p.201-212, August, 2007.

[8] 차병래, 정영기, “소프트웨어 소스 코드의 저작권 관리를 위한 디지털 라이센스의 비교와 분류 그리고 크립텍스 모델", *한국콘텐츠학회 논문지,* January 2008.

[9] Byungrae, "CRYPTEX Model for Software Source Code", *ISA 2008,* April 2008.

[10] Byungrae Cha, , , "Access Control of Software Source Code by CRYPTEX Model", *ICCSA 2008*, July 2008.

[11] Byungrae Cha, Sun Park, "Copyrights Expression and Secure Container of Software Source Code", *NCM 2008*, September 2008.

차 병 래(車洪炳)

1995년 2월 : 호남대학교 수학과(이학사)

1997년 2월 : 호남대학교 컴퓨터공학과(공학석사)

2004년 2월 : 국립목포대학교 컴퓨터공학과(공학박사)

2005년 2월~현재 : 호남대학교 컴퓨터공학과 전임강사

관심분야 : 신경망, 컴퓨터 보안, 디지털저작권 관리 등