RBAC을 이용한 정보유출 방지를 위한 보안성이 강화된 문서 DRM 구현*

최 영 현** · 엄 정 호*** · 정 태 명****

An Implementation Method of Improved Document DRM for Preventing Information Leakage using RBAC Approach

Choi, Young Hyun · Eom, Jung Ho · Chung, Tai Myoung

〈Abstract〉

We implemented the document DRM applying role based access control(RBAC) mechanism for preventing the information leakage of a document which is transmitted in network environment. It must prevent to access document not related to user role and duty, and must allow operation to document for improving security, considering user role and security level according to a document importance. We improved the security of document DRM by adding to the access control module applying RBAC for satisfying security requirements. Though the user access document, our system allows operation authorizations to document by the user's role & security level and the security attribute of RBAC. Our system prevents indiscriminate access to the documents by user who is not associated with the role, and prevents damage the confidentiality and integrity.

Key Words : Document DRM, Access Control, RBAC

Ⅰ. 서론

'2010/2011 CSI Computer Crime and Security Survey'[1]에 따르면 악의적인 내부자에 의해 발생한 보안사고의 피해 경험이 있다고 진술한 경우가 응답자 중에 43.2%라고 밝혔다. 오늘날 악의적인 내부자의 정보유출 사례는 기업이나 공공기관에서 가장 심각한 위협으로 부각되고 있다. 또한, 내부자에 의한 정보나 데이터 유출이 외부자에 의한 침입에 비해 발생하는 횟수는 적지만, 그 피해는 훨씬 심각하다. 특히, 유비쿼터스 컴퓨팅 환경에서는 내부자가 언제 어디서든지 합법적인 권한으로 데이터가 저장된 시스템에 접근할 수 있기 때문에 불법적인 정보유출 탐지는 더 어려워졌다[2-5].

최근에는 경제적 이익이나 이직을 위해서 기업의 비밀기술을 몰래 빼돌려 경쟁 기업에 제공하는 경우도 발

* 본 논문은 지식경제부/산업기술평가관리원에서 지원하는 2011년도 산업원천기술개발사업(KI001810039260, 개인 및 기업 맞춤형 서비스를 위한 개방형 모바일 클라우드 융 통합개발환경 및 이기종 단말-서버 간 협업 기술 개발)의 연구수행으로 인한 결과물임을 밝힙니다.

** 성균관대학교 정보통신공학부 박사과정
*** 대전대학교 군사학과 교수(교신저자)
**** 성균관대학교 정보통신공학부 정교수

생하고 있다. '09년도 한미연합사령부에서 USB를 통해 군사기밀이 유출된 사건과 '10년도 6월에 군 장성의 작계 5027 비밀 유출은 내부자의 비의도 또는 의도적인 정보 유출의 심각성을 보여주는 대표적인 사례이다[6].

지금까지 정보유출 차단 기법은 접근제어 모델, 침입탐지 모델, DRM이 많이 사용되고 있으나, 최근에는 문서 기반 DRM(Document based Digital Rights Management) 기술[8-9]이 각광을 받고 있다. 디지털 콘텐츠의 불법복제 방지와 저작권 보호를 위하여 개발된 DRM 기술은 문서정보의 내부 유출이라든지, 무분별한 문서열람을 방지하는 수단으로 사용되고 있다. 그러나 기업이나 공공기관의 중요한 기밀을 통제하기 위해서는 DRM 기술로는 효과적이지 못하다. 예를 들어 상위 보안등급의 산업기밀을 하위 보안등급의 사용자가 볼 수 있으며, 사용자가 서로 다른 보안등급의 기술정보를 열람하거나 수정할 수 있기 때문에 정보의 기밀성이나 무결성이 훼손될 수 있다. 본 논문은 디지털산업정보학회논문지 제7권제1호(3월호)에 수록된 엄정호의 '국방 정보시스템 환경에서 정보유출 방지를 위한 보안성이 강화된 문서 DRM 설계에 관한 연구'[10]를 기반으로 SiDRM(Security improved DRM)을 구현하였으며 평가를 수행하였다.

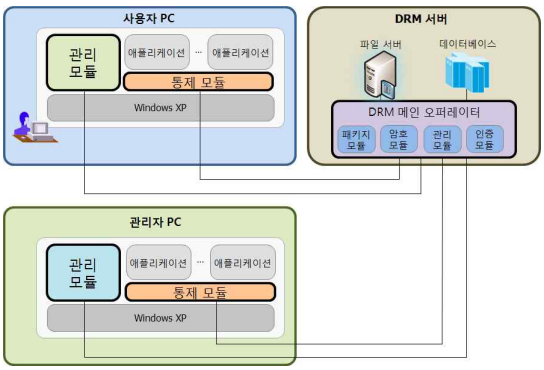
논문의 구성은 2장에서 관련연구를 기술하고 3장에서 우리가 제안한 문서 DRM 구현을 설명하며, 4장에서 평가를 수행한다. 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 관련연구

2.1 DRM

DRM(Digital Rights Management)[8-12]은 인터넷에서 디지털 콘텐츠가 불법적으로 복제·사용되는 것을 방지하고 허가받은 사용자만 콘텐츠를 활용하도록 저작권자 권리 및 이익을 보호하는 메커니즘이다. DRM 메커니즘은 콘텐츠에 대해 합법적인 권한을 보유한 사용자에게 안전하게 전송하고 허가된 권한범위 내에서 작업할 수 있게 하고 불법적으로 콘텐츠가 복제되어 유포되었을 때 해당 콘텐츠의 원 저작권자를 증명하는 등 불법 복제방법과 유통경로를 추적하는 기능이 있다. 본 논문에서는 다양한 디지털 콘텐츠 중에 문서기반 정보를 다루고 있는 전자문서에 한정한다. 즉, 전자문서 암호화와 작업권한 통제를 통해 합법적인 사용자들만 허가한 권한범위 내에서 작업하도록 전자문서의 불법사용을 방지하는 기능에 한정한다.

일반적인 문서 DRM 시스템은 <그림 1>과 같이 DRM 서버, DRM 매니저, 사용자 PC로 구성된다. DRM 서버는 콘텐츠 사용자가 해당 콘텐츠를 이용할 수 있는 라이선스(License)를 발급해 준다. 또한, 매니저 모듈을 통하여 관리 시스템의 사용자 및 문서를 관리한다. DRM 매니저는 별도의 관리 애플리케이션을 통하여 사용자 추가 및 문서 등을 관리한다. 사용자 PC는 문서를 요청하거나 권한 설정 및 업로드를 지원하고 문서를 다운로드 받아 권한에 맞는 문서를 열람할 수 있게 한다.



<그림 1> 문서 DRM 구성

문서 DRM 구성 요소의 세부기능은 다음과 같다. DRM 서버는 패키지 모듈, 암호모듈, 관리모듈, DRM 데이터베이스로 구성된다.

- 패키지 모듈: 문서의 기밀성을 위한 암호화 수행 후

문서관리 수행을 위해 부가정보가 포함된 패키징 헤더를 생성하여 DRM 매니저나 사용자 PC에 전송되는 문서 패키징 파일을 만든다.

- 암호 모듈: 문서 암호화 및 서버와 DRM 매니저나 사용자 PC간 통신메시지를 암/복호화한다.

- 관리 모듈: DRM 매니저 및 사용자 PC 요청에 따라 서비스를 제공하도록 각 모듈과 연결시켜 주고 DRM 서버내의 모듈들을 관리한다.

- 인증 모듈: 사용자가 입력한 로그인 정보를 이용하여 합법적인 사용자임을 인증한다.

- DRM 데이터베이스: 사용자의 정보, 권한그룹 정보, 문서정보, 라이선스 정보 등을 저장한다.

DRM 매니저는 관리모듈과 통제모듈로 구성된다.

- 관리모듈: 사용자 인증 후 문서 업/다운로드 기능과 사용자 추가 및 권한그룹을 관리한다.

- 통제모듈: 사용자 인증시 문서 기능을 권한정보에 따라 통제한다.

사용자 PC 내에는 관리모듈과 통제모듈로 구성된다.

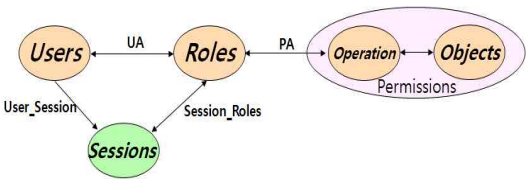
- 관리모듈: 사용자 인증 후 사용자가 작성한 문서를 서버에 전송하거나 서버로부터 문서를 수신한다.

- 통제모듈: 라이선스 패키징 키를 이용하여 문서를 복호화하고 라이선스 권한정보에 따라 문서열람을 통제한다.

2.2 RBAC

RBAC(Role Based Access Control) 모델[7]은 사용자에게 객체에 대한 접근권한을 할당할 때 역할에 따라서 할당하는 모델이다. 즉, 권한을 역할과 연관시켜 사용자들에게 적절한 역할을 할당한 후 역할에 따라서 권한을 부여함으로써 객체에 대한 접근을 허가한다. 역할은 조직에서 다양한 작업 기능들을 바탕으로 정의되며, 사용자들은 직무에 따른 직책과 직능에 따라서 역할을 할당받을 수 있다. 역할이 기존의 접근제어의 사용자 그룹 개념과 다른 큰 차이점은 그룹은 전형적으로 사용자들의 집합이나 권한의 집합은 아니며, 역할은 사용자들의 집합이면서 권한들의 집합이라는 것이다. 역할은 사용자 집합과 권한 집합의 매개체 역할을 수행한다.

<그림 2>는 RBAC의 구성과 접근제어 메커니즘을 보여준다. RBAC은 User(U), Roles(R), Permissions(P), Session(S) 등의 기본적인 개체들과 사용자와 역할의 관계를 나타내는 User Assignment(UA), 역할과 권한의 할당 관계인 Permission Assignment(PA) 등을 포함한다.



<그림 2> RBAC 모델

- 사용자(U: User): 조직의 구성원이나 프로세스 등 조직의 자원에 대한 접근을 요청하는 모든 개체

- 역할(R: Role): 조직의 직무, 직책 및 책임 등을 반영하여 추상화한 개체

- 권한(P: Permission): 조직의 자원이나 객체에 대한 오퍼레이션의 관계를 추상화시킨 개체

- 세션(S: Session): 역할의 활성화 개념의 요소. 사용자와 역할간의 할당은 해당 조직 내에서 이루어질 수 있는 모든 할당 관계를 나타낸다. 실제 동작에서는 할당 관계뿐만 아니라 역할 활성화를 통해 활성화된 역할에 사용자가 자신이 원하는 권한을 할당받아 사용할 수 있다.

- 사용자-역할 관계(UA: User Assignment): 사용자에게 역할을 할당

- 역할-권한 관계(PA: Permission Assignment): 역할에 권한을 할당

Ⅲ. 제안한 문서 DRM

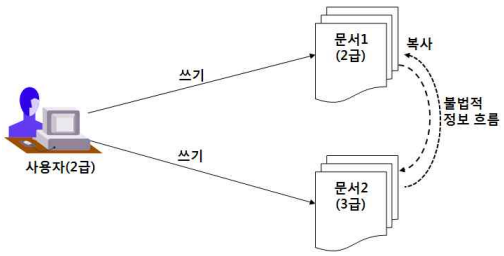
3.1 요구사항

기존의 문서 DRM 메커니즘으로 네트워크에서 소통되는 문서기반의 중요정보의 무분별한 접근과 작업기능을 제한하기에는 한계가 있다. 기업이나 공공기관에서 사내 망을 이용하는 사용자는 본인 역할에 따라 정보접근 또는 작업모드를 수행한다. 아울러 중요한 정보가 포함되어 있는 문서일 경우에는 사용자 역할과 직위를 고려한 보안등급에 따라 접근하도록 권한을 부여해야 한다. 즉, 문서와 사용자 역할의 보안등급에 따라 문서접근과 작업모드를 통제해야 한다[13]. 이와 같은 환경에 기존의 문서 DRM 메커니즘을 적용할 경우, 발생할 수 있는 문제점을 제시하고 그에 따른 요구사항을 도출한다.

첫째, 사용자는 본인의 역할과 관련된 문서에만 접근해야 한다. 문서 DRM 메커니즘은 인증모듈이 시스템 내에서 사용자가 합법한 사용자임을 확인하면 모든 문서에 접근을 허가한다. 만약, 기존의 문서 DRM 메커니즘을 적용한다면 사용자들은 모든 문서에 접근하여 열람함으로써 필요 이상의 무분별한 문서접근이 발생하고 정보유출 가능성이 높아진다. 사용자는 자신의 역할과 관련된 문서에만 접근해야 한다.

둘째, 사용자에게 본인 역할, 직책과 직위 수준보다 높은 보안등급의 문서에 접근하거나 작업권한을 할당해서는 안 된다. 예를 들어, '사용자는 보안등급이 2급 이상의 문서에 접근할 수 없다.' 그러나 보안등급이 2급인 문서에 대한 접근권한을 허가한다고 가정해 보자. 기존의 문서 DRM 메커니즘은 보안등급을 고려하지 않기 때문에 사용자가 접근할 수 없는 상위 보안등급의 문서에 대해 Read, Write 등의 작업기능 등을 수행함으로써 정보가 유출되어 비밀성이 훼손될 수 있다. 즉, 사용자가 본인의 보안등급보다 높은 상위 보안등급 문서에 접근하여 작업모드를 수행하는 것을 근본적으로 차단해야 한다.

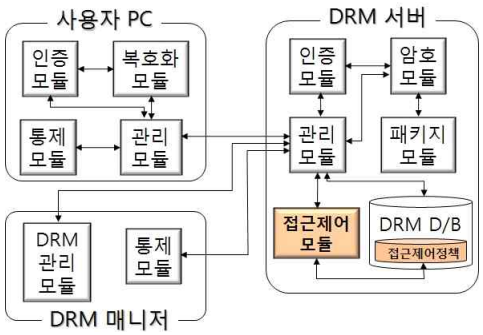
마지막으로, 사용자가 서로 다른 보안등급의 문서를 동시에 요청하여 작업모드를 수행하는 것을 차단해야 한다. 예를 들어, <그림 2>와 같이 사용자가 3급인 문서와 2급인 문서를 동시에 활성화시켜서 쓰기 권한을 허가하면, 3급 문서정보가 2급 문서로 복사되어 정보의 무결성이 훼손되거나 2급 문서정보가 3급 문서로 복사되어 정보의 기밀성이 훼손될 수 있다. 그래서 서로 다른 보안등급의 문서에 대한 작업요청이 있을 경우에는 사용자 보안등급을 확인한 후, 작업권한을 Read로 제한해야 한다.



<그림 3> 불법적 정보 유출

3.2 SiDRM 설계

본 논문에서는 DRM 서버에 RBAC을 기반으로 한 접근제어 모듈[14]을 추가하여 사용자의 역할 및 보안등급에 따라 문서에 대한 접근 및 작업권한을 허가하도록 하였다. <그림 3>은 보안성을 강화시킨 문서 DRM(SiDRM: Security improved DRM) 구성을 보여준다.



<그림 4> 제안한 문서 DRM 설계

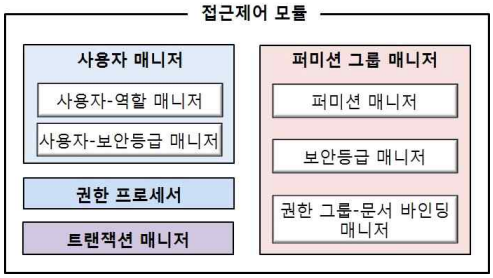
SiDRM의 구성요소 중에서 기존의 DRM의 요소들은 동일한 기능을 수행하기 때문에 설명을 생략한다. 추가된 접근제어 모듈은 RBAC 메커니즘 기반으로 DRM 데이터베이스에 추가된 접근제어 정책에 따라 사용자와 문서간의 작업모드를 통제한다. 사용자 인증 후 관리모듈로부터 접근제어 수행에 필요한 정보인 사용자 식별자, 문서 등에 대한 정보와 접근제어 정책 데이터베이스로부터 접근제어 정책 규칙정보를 받아 작업모드 권한을 할당한다. 접근제어 정책 데이터베이스는 사용자-역할간의 관계, 역할-문서간의 관계, 사용자-역할-문서간의 작업권한 할당 관계 등 접근제어 정책 구성을 저장한다. 접근제어 모듈의 세부 구성요소는 사용자-역할 매니저, 퍼미션 매니저, 보안등급 매니저, 트랜잭션 매니저, 권한 프로세서로 구성된다.

- 사용자-역할 매니저: DRM 서버로부터 사용자 식별자 정보를 전송받아 사용자-역할을 활성화한다.
- 퍼미션 매니저: 문서정보와 작업기능 정보를 이용하여 트랜잭션 구성에 필요한 작업권한 정보를 생성한다. 작업권한은 읽기, 저장, 쓰기, 수정, 프린트 등이 있다.
- 보안등급 매니저: 역할과 문서의 중요도에 따라 보안등급을 부여하고 관리한다.
- 트랜잭션 매니저: 사용자-역할, 보안등급, 권한 등의 정보를 이용하여 보안 트랜잭션을 구성한다.
- 권한 프로세서(Authorization Processor): 트랜잭션 매니저에서 생성한 보안 트랜잭션과 접근제어 정책 규칙정보에 따라서 문서에 대한 작업 기능 권한을 부여한다.

접근제어모듈의 세부 구성요소는 <그림 4>와 같이 사용자 매니저, 퍼미션 그룹 매니저, 권한 매니저, 트랜잭션 매니저, 권한 프로세서로 구성된다.

사용자 매니저는 사용자-역할 매니저와 사용자-보안등급으로 구성된다.

- 사용자-역할 매니저: DRM 서버로부터 사용자 식별자 정보를 전송받아 사용자-역할을 활성화한다.
- 사용자-보안등급 매니저: 사용자의 신분, 역할에 따라 사용자 단위의 보안등급을 관리한다.



<그림 5> 접근제어 모듈

퍼미션 그룹 매니저는 퍼미션 매니저, 보안등급 매니저와 권한 그룹-문서 바인딩 매니저로 구성된다.

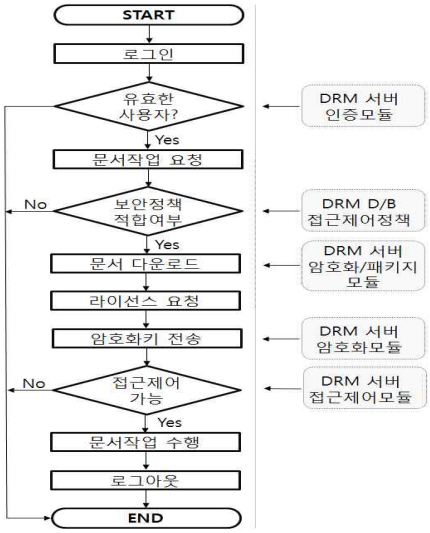
- 퍼미션 매니저: 문서정보와 오퍼레이션 정보를 이용하여 트랜잭션 구성에 필요한 오퍼레이션 권한 정보를 생성한다. 오퍼레이션 권한은 읽기(Read), 쓰기(Write), 저장(Save), 수정(Modify), 프린트(Print) 등이 있다.
- 보안등급 매니저: 그룹 단위의 역할과 문서 등에 대한 보안등급을 관리한다.
- 권한 그룹 - 문서 바인딩 매니저: 각 권한 그룹과 문서들의 상관관계 바인딩 구성을 관리한다.

트랜잭션 매니저는 사용자-역할, 보안등급, 권한 등의 정보를 이용하여 보안 트랜잭션을 구성한다. 권한 프로세서는 트랜잭션 매니저에서 생성한 보안 트랜잭션과 접근제어 정책 규칙정보에 따라서 문서에 대한 오퍼레이션 권한을 부여한다.

Ⅳ. SiDRM 구현 및 평가

SiDRM의 동작과정은 <그림 6>과 같다. 사용자가 DRM 서버로 인증을 요청하면 인증모듈이 인증 메커니즘을 통해서 사용자 인증을 수행한다. 사용자가 인증이 성공한 후 문서를 요청하면 관리모듈은 DRM 서버에 저장되어 있는 DRM 보안정책에 요청문서의 접근권한이 있는지 확인한다. 그리고 암호화모듈을 통해 요청문서를 암호화하고 패키지모듈에서 패키징 헤더를 부착하여 사

용자에게 전송한다. 문서를 수신한 사용자는 문서에 대한 오퍼레이션을 얻기 위해서 암호화모듈과 접근제어모듈에게 라이선스를 요청한다. 그러면 암호화모듈은 암호화키를, 접근제어모듈은 접근제어 정책을 확인한 후에 오퍼레이션 권한을 전송한다.



<그림 6> 제안한 문서 DRM의 동작 과정

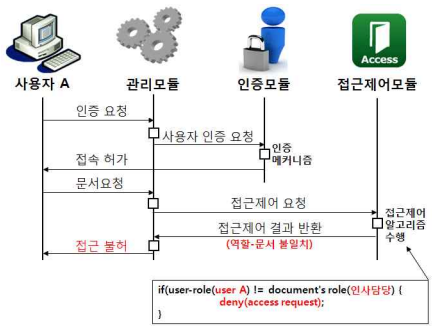
다음으로는 구현된 SiDRM 시스템을 이용하여 표 2와 같은 임의의 컴퓨팅 환경을 바탕으로 정보유출 방지를 위한 강화된 보안성을 보여주는 실행의 예를 보여준다.

<표 1> SIDRM 컴퓨팅 환경의 예

사용자 현황				
소속	사용자 (User)	계급 (Rank)	역할 (Role)	보안등급 (SL)
○○ 회사	A	사원	영업담당	일반
	B	대리	인사담당	3급
	C	부장	재무담당	2급
문서/역할/보안등급(File/Role/SL)				
인사이동보고서/인사/일반, 인사이동계획서/인사/3급 영업실적보고서/영업/3급, 분기재무계획서/재무/3급 연간재무계획서/재무/2급				

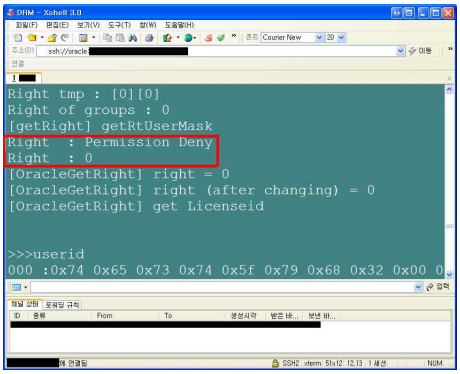
SiDRM에서는 기존의 문서 DRM 메커니즘으로 문서 기반 정보에 대한 무분별한 접근과 작업모드 수행을 제한하기 위해서 3가지 요구사항을 도출하여 해결하였다.

첫째는 역할에 따른 문서 접근통제 방법이다. 사용자는 본인의 역할과 관련된 문서에만 접근할 수 있어야 한다. SiDRM에서는 사용자 A가 인사이동보고서에 대한 접근을 요청하면, 클라이언트에서는 사용자 인증 후 서버에 라이선스 요청을 한다. 이때 접근제어 모듈에 접근제어 요청을 하면 접근제어 모듈에서는 DRM DB의 접근제어정책에 접근제어규칙 정보를 요청하고 역할별 접근제어 알고리즘을 통해 요청이 역할에 맞는 지 확인한다. 그리고 관리 모듈에 접근제어 결과를 반환하고 관리 모듈에서는 클라이언트로 접근제어 결과를 바탕으로 라이선스를 전송한다. 하지만 사용자 A의 역할은 영업담당으로 인사이동보고서의 역할인 인사와 다르다. 이 상황에서는 역할별 접근제어 알고리즘에 의하여 접근 요청이 거부되어 권한(접근 불허)의 결과를 받기 때문에 사용자 A는 인사이동보고서에 접근할 수 없다.

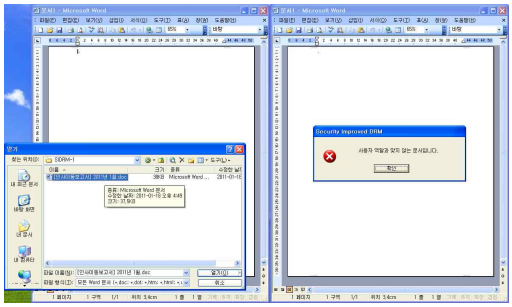


<그림 7> 사용자 역할에 따른 문서 접근제어

둘째는 정보의 비밀성 훼손을 차단해야 한다. 비밀성을 유지하기 위해서는 보안등급이 낮은 사용자가 보안등급이 높은 문서 접근을 금지해야 한다. SiDRM에서는 사용자 A가 영업실적보고서에 접근을 요청하면, 클라이언트에서는 사용자 인증 후 서버에 라이선스 요청을 한다. 이때 접근제어 모듈에서는 접근제어 요청을 받아 DRM

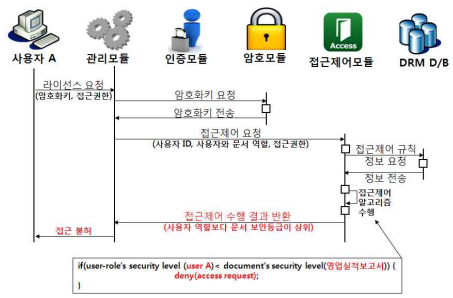


<그림 8> 역할별 접근제어 알고리즘 결과 로그



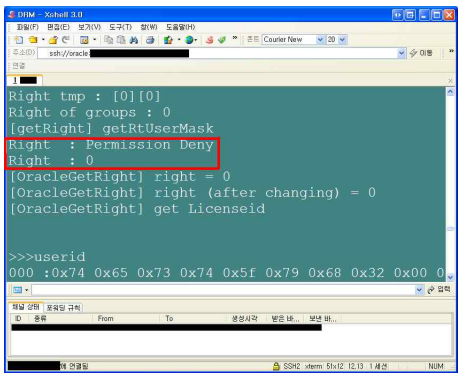
<그림 9> 역할에 따른 문서 접근통제 결과

DB의 접근제어 정책에 접근제어 규칙정보에 따라 비밀성 유지 알고리즘을 통해 요청 문서와 요청자의 보안등급이 적합한지 확인한다. 그리고 관리모듈에 접근제어 결과를 반환하고 관리모듈에서는 클라이언트로 접근제어 결과를 바탕으로 라이선스를 전송한다.

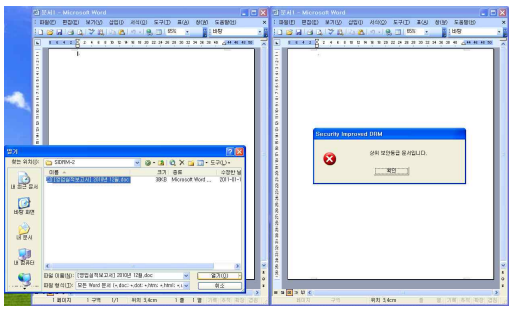


<그림 10> 역할과 문서 보안등급에 따른 문서 접근제어

하지만 이때 보안등급이 일반인 영업담당 역할의 사용자 A는 영업실적보고서가 영업담당과 관련된 문서라도 보안등급이 높기 때문에 비밀성 유지 알고리즘에 의하여 접근요청이 거부되어 접근 불허 결과를 받는다. 이렇게 해서 사용자 A는 영업실적보고서 문서에 접근할 수 없다.



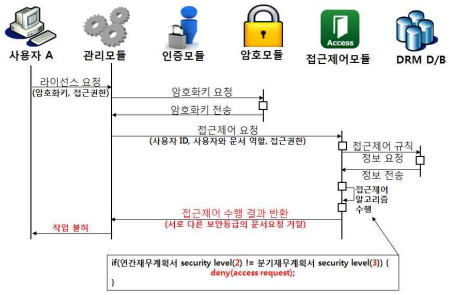
<그림 11> 비밀성 유지 알고리즘 결과 로그



<그림 12> 보안등급에 따른 문서 접근통제 결과

마지막으로 정보의 기밀성 및 무결성 훼손을 차단한다. 기밀성과 무결성을 유지하기 위해서는 사용자가 서로 다른 보안등급의 문서를 동시에 접근하는 것을 차단해야 한다. SiDRM에서는 사용자 C가 연간재무계획서 열람 중 분기재무계획서의 추가 접근을 요청하면, 클라이언트에서는 사용자 인증 후 서버에 라이선스 요청을 한다. 이때 접근제어 모듈에서는 접근제어 요청을 받으면 DRM DB의 접근제어 정책에 접근제어 규칙 정보를

요청하고 이를 이용해 관리모듈에 접근제어 결과를 반환한다. 관리모듈에서는 클라이언트로 라이선스를 전송하면 클라이언트에서는 받은 라이선스에서 얻은 보안등급과 사용자가 열람 중인 문서의 보안 등급을 확인하고 정보의 기밀성 및 무결성 유지 알고리즘을 통해 최종 작업 권한을 확인한다.

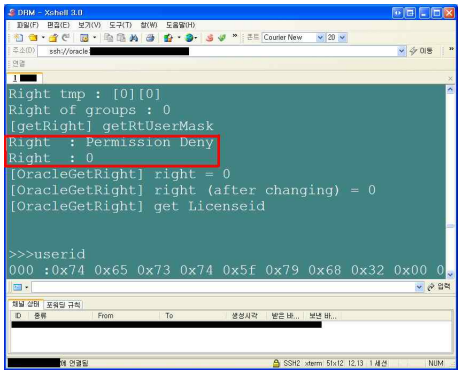


<그림 13> 역할과 문서 보안등급에 따른 문서 접근제어

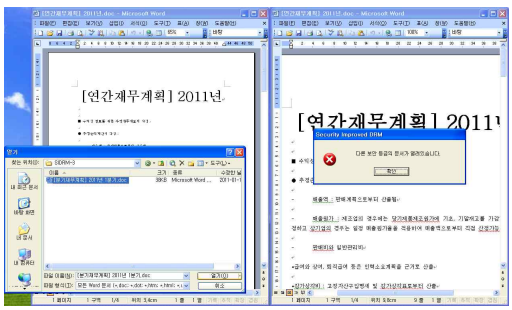
이때, 분기재무계획서는 3급, 연간재무계획서는 2급으로 다른 보안등급 문서를 동시에 요청하게 된다. 이 상황에서는 정보의 기밀성 및 무결성 유지 알고리즘에 의하여 클라이언트 내부에서 접근요청이 거부되어 사용자 C는 분기재무계획서에 접근권한을 받지 못하게 된다.

Ⅳ. 결론

본 논문에서는 기업이나 공공기관에서 사내 망을 이용하는 정보시스템 환경에서 소통되고 있는 문서기반의 정보유출을 방지하기 위해서 보안성을 강화시킨 문서기반 DRM(SiDRM)을 설계 및 구현하였다. 사내 망 환경에서 소통되는 전자문서들은 내용의 중요도에 따라 보안등급(SL)이 부여된다. 사용자도 역할, 직책, 계급에 따라 보안등급을 할당받는다. 그래서 전자문서에 접근하여 작업 기능을 수행할 때는 문서 내용이 유출되지 않도록 사용자(역할)와 전자문서의 보안등급을 반영하여 접근통제를 수행해야 한다. 우리는 기존의 문서 DRM에 RBAC 모델



<그림 14> 비밀성 유지 알고리즘 결과 로그



<그림 15> 서로 다른 보안등급 문서 접근통제 결과

을 적용한 접근제어모듈을 추가하여 사용자의 역할 및 보안등급과 문서 보안등급을 고려하여 문서 접근 및 작업 기능 권한을 통제함으로써 정보의 기밀성과 무결성을 유지할 수 있게 하였다. 또한, 제안한 DRM 시스템을 설계와 구현을 통해서 문서통제와 접근제어 정책에 따라서 요청한 문서를 효율적으로 통제할 수 있는지 입증하였다. 문서 접근과 통제 요구사항에 대해서는 시나리오를 작성한 후 테스트하여 각각의 요구사항을 만족시키지도 평가하였다.

접근제어모듈은 사용자-역할(User-Role), 보안등급(Security Level), 퍼미션(Permission), 트랜잭션(Transaction) 매니저 그리고 권한 프로세서로 구성하였다. 접근제어정책 데이터베이스에 저장되어 있는 정책 규칙에 따라 사용자와 역할을 매칭시키고 역할과 문서의

보안등급을 설정하여 피미션에 따라 접근 및 작업권한을 줄 수 있는 지 트랜잭션을 구성한다. 제안한 DRM 시스템은 사용자들의 역할과 직무에 상관없는 문서에 무분별하게 접근하는 것을 방지할 수 있고 사용자의 보안등급보다 높은 보안등급의 문서에 접근을 차단할 수 있다. 또한, 사용자가 동시에 서로 다른 보안등급의 문서들을 접근하여 작업하는 행위를 금지하여 문서의 비밀성을 유지하고 문서 정보에 대한 기밀성과 무결성을 훼손시키는 것을 방지할 수 있다.

참고문헌

[1] Robert Richardson, "2010/2011 CSI Computer Crime And Security Survey," Computer Security Institute, 2011.

[2] Brian M. Bowen et al, "Designing Host and Network Sensors to Mitigate the Insider Threat," IEEE The Journal of Security & Privacy, Vol7. No6, December, 2009, pp. 22-29.

[3] Felicia A. Duran et al, "Building a System for Insider Security," IEEE The Journal of Security & Privacy, Vol7 No6, December, 2009, pp. 30-38.

[4] Salvatore J. Stolfo et al, Insider Attack and Cyber Security Beyond the Hacker, Springer, 2008.

[5] Frank Stajano, Security for ubiquitous computing, Wiley, 2002.

[6] 엄정호, "사이버전, 제5의 전쟁인가?," 2010년 공군사관학교 전자전산학과 세미나 발표자료, Nov, 2010.

[7] David F. Ferraiolo, D. Richard Kuhn and Ramaswamy Chandramouli, Role-Based Access Control, Artech Haouse, 2003.

[8] 문진규, "내부 정보 유출 방지를 위한 DRM 적용 방법 설계," 한국컴퓨터종합학술대회 논문집, Vol. 34, No. 1(D), Jun, 2007, pp. 7-10.

[9] 최동현 외 3명, "DRM(Digital Rights Management) 기술," 정보과학회지, 제25권, 제5호, May, 2007, pp. 17-21.

[10] 엄정호, "국방 정보시스템 환경에서 정보유출 방지를 위한 보안성이 강화된 문서 DRM 설계에 관한 연구," 디지털산업정보학회 논문지, 제 7권, 제 1호, March, 2011, pp. 41-50.

[11] 김종우 외 2명, "네트워크 상에서 디지털 콘텐츠 보호를 위한 DRM 프레임 설계"," 정보보호학회논문지, 제16권, 제3호, Jun, 2006.

[12] 이선영, "홈네트워크를 위한 DRM 기술," 정보보호학회지, 제16권, 제6호, Dec, 2006.

[13] 김승환 외 3명, "문서 DRM의 보안성 강화를 위한 연구," 한국정보처리학회 추계학술대회 논문집 제17권 2호, Nov, 2010.

[14] 엄정호, "유비쿼터스 전장 컴퓨팅 환경에서 상황 인식과 직무-역할 기반의 접근제어에 관한 연구," 박사학위 논문, 성균관대학교, 2008.

■ 저자소개 ■

최 영 현
Choi, Young Hyun

2010년 3월~현재 성균관대학교 전자전기컴퓨터공학 (박사과정)
2010년 2월 성균관대학교 전자전기컴퓨터공학 (석사)
2008년 2월 성균관대학교 정보통신공학 (학사)

관심분야 : 모바일 네트워크, 경로 최적화, 시스템 보안
E-mail : yhchoi@imtl.skku.ac.kr

엄 정 호
Eom, Jung Ho

2011년 3월~현재
대전대학교 군사학과 교수
2010년 9월 성균관대학교 BK21 연구교수
2008년 성균관대학교 컴퓨터공학과(박사)
2003년 성균관대학교 컴퓨터공학과(석사)
1994년 공군사관학교 항공공학과(학사)
1994년~2010년 8월
대한민국 공군 정보장교

관심분야 : 사이버전, 사이버공격, 접근제어, 위협분석
E-mail : eomhun@gmail.com

정 태 명
Chung, Tai Myoun

1995년~현재
성균관대학교 정보통신공학 교수
1995년 Perdue University W. Lafayette, IN, U.S.A. 컴퓨터공학 (박사)
1987년 University of Illinois Chicago IL, U.S.A. 컴퓨터공학 (석사)
1984년 University of Illinois Chicago IL, U.S.A. 전자계산학 (학사)
1981년 연세대학교 전기공학과 (학사)

관심분야 : 통합보안관리, 네트워크, 무선망
E-mail : tmchung@ece.skku.ac.kr

논문접수일 : 2011년 11월 04일
수 정 일 : 2011년 11월 14일
게재확정일 : 2011년 11월 25일