「정보시스템연구」 제11권 제1호
한국정보시스템학회
2002년 6월, pp. 175-198

다중등급 보안 정책을 적용한 전자결재 모듈의 개발

김 진 성 경상대학교 경영정보학과 dosa8080@hanmail.net
안 병 혁 경상대학교 경영학부 bahn@nongae.gsnu.ac.kr

<목 차>

I. 서 론

전자결재 시스템은 문서의 생성 및 결재가 컴퓨터를 통해서 이루어지는 것을 말한다. 즉, 문서 편집기를 이용하여 문서를 작성하여 결재자에게 컴퓨터 통신망을 이용하여 결재를 상신 하면 결재자는 전자적인 방법을 이용하여 문서에 결재를 한다(이명재, 1997). 전자결재 시스템은 많은 이점을 주지만 동시에 보안상의 위협을 가지고 있다. 보안상의 위협에는 시스템에 저장되어 있는 문서의 무단 유출, 파괴, 변조 등의 위협과 네트워크를 통한 문서의 전송 중 도청, 변조, 부인 등의 위협이 존재한다(S. Boran, 2002; Yasinsac, Ale, 2002). 이러한 보안상의 위협에 대응하기 위해 접근제어(Access Control), 인증(Authentication), 기밀성(Confidentiality), 무결성(Integrity), 부인방지(Non-repudiation)등의 보안 서비스를 제공해야 한다.

본 연구는 전자문서를 작성하여 전송하고 보관할 때 발생할 수 있는 보안상의 위협으로부터 문서의 안전성을 보장할 수 있도록 보안 서비스를 제공하는 모듈의 개발에 관한 것이다.

II. 전자결재 시스템의 보안요구사항 분석

2.1 전자결재 시스템의 기본 구조

현재 우리나라 행정기관에서 규정하는 전자문서 관리시스템은 조직도 관리, 전자우편, 전자게시판, 전자결재, 전자문서 수발 등의 구조를 갖는다(www.metro.busan.kr; law.haman.kyongnam.kr). 지역별 혹은 부서별로 전자결재 시스템이 다소 차이는 있지만 주요 제공 기능 및 정의는 다음 <표 1>과 같다.

<표 1> 우리나라 행정기관의 전자문서 관리 시스템의 구조

구 조	정 의
조직도 관리	전자문서 관리 시스템을 이용하는 사용자 및 기구·조직 체계를 전자적으로 관리하는 기능
전자우편	전자문서 관리 시스템 사용자간에 편지·문서·파일 등을 전산망을 이용하여 주고받는 기능
전자게시판	전자문서 관리 시스템 내에 전자적으로 구현한 게시판
전자결재	전자문서를 전자서명에 의해 결재하는 것
전자문서 수발	각 부서에서 생성한 각종 공문서에 대한 등록, 발송, 접수 등의 처리를 할 수 있는 전자적인 기능

2.2 전자결재 시스템에서 보안의 필요성

전자결재 시스템의 경우 전자문서가 네트워크를 통하여 전송되므로 신분 위장, 문서의 도청, 문서의 변조, 부인 등의 보안상 위험이 존재한다. 또한 문서가 네트워크에 연결된 컴퓨터의 데이터베이스에 저장되므로 문서의 도난이나 불법적인 유출의 위험이 존재한다. 이러한 보안상의 위협에 대하여 인증, 데이터 비밀성, 데이터 무결성, 부인 방지, 접근제어 서비스를 제공하여 문서의 안정성을 보장하려는 연구가 이루어져 왔다.

황의주(1999)는 인터넷 환경에서의 전자결재와 보안에 대한 연구를 하였다. 사용자 인증은 사용자ID와 패스워드를 이용하여 이미 등록되어 있는 사용자 정보와 비교하는 방법을 사용한다. 기안자가 결재자를 선택하여 문서를 전송할 때 문서를 해쉬하여 전자 서명을 생성하고 문서를 암호화하여 전송한다. 결재자는 결재 문서를 복호화하여 인증을 수행하고 결재처리를 수행하는 과정을 거친다. 서버는 문서를 데이터베이스에 저장할 때 기안자와 교환한 세션 키를 사용하여 암호화된 문서를 복호화한 후 저장하며 평문으로 저장한다.

황의주의 경우 문서의 전송 과정에서 발생할 수 있는 보안상의 위협에 중점을 두었으며, 문서가 데이터베이스에 저장될 때 평문으로 저장된다. 평문으로 저장된 문서는 데이터베이스의 침입자에 대하여 문서의 내용이 누출될 수 있는 위험이 존재하며 사용자 인증시 replay back 공격에 대한 언급이 미흡하다.

장용철(1997)등은 전자결재 시스템의 암호화 및 복호화를 통한 네트워크 보안뿐만 아니

라 시스템 보안에 대해서도 다루고 있다. 전자결재 시스템 접속시 시스템은 사용자에게 로그인 ID와 패스워드를 입력받아 이를 서버가 체크하는 방법으로 사용자의 신분을 확인한다. 문서작성자가 문서를 작성하면 작성된 문서를 다른 부서원이 볼 수 없게 부서원 고유의 ID를 이용하여 부서ID를 구분한 후 암호화하여 저장한다. 이와 같은 방법을 이용하여 결재권자만이 문서를 복호화 하여 내용을 볼 수 있게 하였다. 결재 처리가 완료된 문서는 암호화하여 저장하는 방법을 사용하여 문서의 안전성을 고려하였다. 사용자의 ID를 이용하여 문서에 접근을 제어하는 방법은 다중등급 보안에서 사용자의 취급인가 등급과 유사한 방법이지만, 다중등급 보안에 대한 언급이 미흡하여 다양한 보안수준의 사용자에게 문서를 공유시키는데 어려움이 있다.

김경식(1997)은 공동작업을 지원하는 형태의 멀티미디어 전자결재 시스템에서 발생할 수 있는 문서에 대한 보안 관리 문제를 사용자와 문서에 부여된 보안 등급과 문서의 상태를 조합하여 사용자의 접근 권한을 통제하는 방법을 제시한다. 멀티미디어를 이용한 결재처리에 대한 연구와 더불어 사용자와 문서에 대하여 보안 등급을 부여하여 접근을 제어하는 방법에 비중을 두는 반면, 문서의 암호화와 복호화와 관련된 제반 사항이나, 문서의 저장시 등급별로 암호화하고 복호화 하는 문제에 대한 언급이 미흡하다.

김종언(1992)은 기안된 문서를 서명하는 방법과 서명인의 신원 검증 방법에 대한 프로토타입을 제시하면서, 서명 검증과 신원 증명 및 공개키 관리 문제에 대한 연구 과제를 제시하였다.

전자결재 시스템의 보안 문제에 관한 기존의 연구에서 결재처리 과정을 보면 첫째, 사용자가 입력한 사용자ID와 패스워드를 서버에 전송하여 데이터베이스에 저장된 사용자 정보와 비교하여 인증을 수행한다. 둘째, 기안자가 작성한 문서를 암호화하여 서버 혹은 결재자에게 전송한다. 셋째, 결재자는 결재 요청 문서를 복호화 하여 결재처리를 한다. 이러한 결재 처리 절차에는 다음과 같은 문제점이 있다.

첫째, 기안자와 결재자와의 통신에서 발생할 수 있는 보안 문제에 중점을 두어 온 반면 결재 처리 후 저장된 문서에 대한 보안 문제에 관한 연구는 미흡하며, 또한 전자결재 전반의 보안 문제, 즉 사용자 인증에서 기안문의 전송 및 결재 처리 결과의 전송에 관한 보안 문제와 결재 처리 된 문서의 보안 문제에 대한 통합적인 보안 문제에 관한 연구는 미흡하며, 방화벽 내부의 사용자에게 모든 문서가 검색될 수 있다. 방화벽 내부의 사용자란 응용 프로그램을 사용할 수 있는 권한을 가진 사용자를 말한다. 즉, 방화벽 외부에서 시스템에 불법적인 접근을 시도하면 방화벽이 응용 프로그램과 IP를 여과하여(filtering) 막아주지만(Nick Hutton, 2002; Lance Spitzner, 2000; 3Com Technical Paper,1996) 방화벽 내부인은 동일한 응용 프로그램을 이용하여 방화벽을 통과할 수 있고, 방화벽 내부에서 다른 응용 프로그램을 이용하여 문서를 검색할 수 있다.

둘째, 사용자ID와 패스워드를 입력받아 이를 확인하는 과정에서 replay back공격에 노출될 수 있다. replay back 공격이란 사용자가 입력한 패스워드를 중간에서 가로채어 재사용하는 방법을 말한다. 문서의 경우는 암호화하여 전송하면 제 3자가 문서를 도청해도 문서의 내용은 공개되지 않지만, 패스워드의 경우 암호화하여 전송해도 제3자는 내용을 해독 할 필요 없이 전송되는 패킷을 복사하여 재 사용할 수 있다.

셋째, 문서가 데이터베이스 혹은 파일로 서버에 저장되어 보관될 때 서버관리자나 혹은 데이터베이스 관리자에게 의도하지 않은 문서의 노출이 가능하다.

따라서 본 연구에서는 기안자와 결재자 사이의 문서의 안전성을 보장할 뿐만 아니라 위와 같은 문제를 해결하기 위하여 다음과 같은 방법을 제시한다.

첫째, 결재 처리후의 문서를 평문으로 저장하여 발생할 수 있는 보안 문제를 해결하기 위한 다중등급 보안 정책을 제시하고자 한다. 즉 사용자와 문서에 보안 등급을 부여하여 보안 등급별로 암호화하여 서버에 저장한다. 이와 같이 다중등급 보안을 적용하여 하위 보안 그룹의 사용자에게 문서가 노출되는 것을 막고, 방화벽내부에서 다른 응용 프로그램을 이용하여 데이터베이스에 접근하는 사용자에게 문서가 노출되는 것을 방지한다. 또한 서버관리자와 데이터베이스 관리자에게 의도하지 않은 문서의 노출을 방지한다. 뿐만 아니라 외부 침입자가 방화벽을 불법적으로 통과하여 데이터베이스에 접근하는 경우에도 문서가 등급별로 암호화되어 있어 그 내용의 노출을 막을 수 있다.

둘째, 일회용 패스워드 기법을 사용하여 전송되는 패스워드를 도청하여 재 사용하는 것을 방지한다.

셋째, 전송되는 모든 문서는 암호화하여 전송하며, 특히 기안자가 작성하여 결재를 요청하는 문서는 결재자를 제외하고는 어느 누구도 그 내용을 열람할 수 없게 하여 결재 요청문서의 노출을 방지한다.

본 논문은 인트라넷(intranet) 환경의 어플리케이션(application) 수준에서 다중등급 보안 기법(Multi-Level Security)을 적용한 정책을 제시하고, 전자문서 관리 모듈 개발의 적용에 관한 것이다. 주체인 사용자에 보안등급을 부여하고 객체인 전자문서에 대해서도 보안등급을 부여하여 사용자의 보안등급이 문서의 보안등급 이상일 경우만 접근을 허용한다. 문서의 암호화와 복호화는 대칭키 암호화 알고리즘인 DES(Data Encryption Standard)를 이용하고 키 교환 알고리즘으로는 공개키 암호화 알고리즘인 RSA(Rivest-Shamir-Adelman)를 이용하여 문서의 안전성을 보장하고자 한다(RSA Laboratories, 2001; FIPS P PUB 46-3,1999; Burton S, Kaliski Jr,1993).

행정기관 및 일반적인 전자문서 관리 시스템은 조직도 관리, 전자결재 관리, 전자문서 수발관리, 게시판 관리, 전자 우편관리 5가지 기능을 제공한다. 본 연구에서는 조직도 관리, 전자결재 관리, 전자문서 수발관리에 대한 다중등급 보안 문제에 중점을 두며, 게시판 관리의 경우 게시판에 등록되는 정보는 모든 사람에게 공개되는 정보이므로 다중등급 보안의 적용이 의미 없으므로 제외하며, 본 연구는 인트라넷 환경이므로 웹 환경하의 전자우편관리의 기능도 제외한다.

본 연구에서는 마이크로소프트 CryptoAPI를 Visual Basic개발자에게 사용하기 편하도록 암호 모듈을 제공하는 Richard Bondi의 WCCO를 이용한다(Richard Bondi, 2000).

본 연구에서 이용하는 전자문서는 2001년 1월 행정자치부의 행정기관 간 전자문서유통 표준에서 제시하는 8종의 문서를 참조하였으며, 전자문서 관리 시스템의 제공 기능은 행정기관의 시스템을 참고하였다(행정자치부, 2001, 2000).

III. 전자결재 모듈의 다중등급 보안정책

3.1 다중등급 보안

다중등급 보안은 1960년 후반 미 국방성이 컴퓨터에 저장된 기밀 정보를 보호하기 위하여 개발하였다. 미 국방성의 군사보안정책을 보면 모든 정보는 기밀등급(classification)을 가지며 모든 사람은 취급인가(clearance)를 가진다. 만일 어떤 사람이 문서를 읽고자 한다면 그 사람의 기밀 취급인가와 문서의 기밀등급과 비교하여 권한의 부여 여부를 결정한다.

보안 등급은 UNCLASSIFIED < CONFIDENTIAL < SECRET < TOP SECRET 와 같은 선형적인 순서를 갖는다. 사용자가 정보를 얻기 위해서는 접근하고자 하는 정보의 접근 등급보다 사용자의 접근 등급이 같거나 더 높아야 한다. 대표적인 다중등급 보안으로 BLP(Bell-La Padular)모델이 있다(홍승필, 고제욱, 1998).

BLP모델은 ACM(Access Control Matrix)과 보안 수준(security level)을 통해서 주체가 객체에 접근하는 것을 통제함으로써 데이터의 비밀성(confidentiality)을 보장한다. 즉, 대상 주체와 객체에 상응하는 적절한 보안 수준을 부여하고 이를 ACM을 통해서 관리하여 주체가 객체에 접근하는 것을 통제하여 시스템의 비밀성을 보장한다. BLP모델은 NRU (No-Read-Up) 보안정책, NWD (No-Write-Down) 보안정책이 있다. NRU는 보안 수준이 낮은 주체는 보안 수준이 높은 객체에 대하여 읽기 권한이 없음을 뜻하며. NWD는 보안 수준이 높은 주체는 보안 수준이 낮은 객체에 쓰기(write) 권한이 없음을 뜻한다.

BLP모델에서는 NRU와 NWD 정책은 있지만 no read-down과 no write-up을 명시하지 않아 blind write 문제가 존재한다. blind write 문제는 보안 등급이 낮은 주체가 자신보다 높은 보안등급의 객체에 쓰기(write) 행위가 가능함을 말하는데 BLP의 경우 이에 대한 규제가 명시되어 있지 않다. 이를 보완하기 위해서 주체의 취급인가와 객체의 기밀등급이 같은 경우에만 쓰기를 허락하고 그 외는 쓰기를 금지하는 정책을 사용한다(홍승필,고제욱,1998).

3.2 전자결재 모듈의 다중등급 보안 정책

본 연구에서는 적용하는 다중등급 보안 정책은 기안자 혹은 결재자와 같이 서비스를 받고자 시스템에 접근하는 모든 주체는 접근 권한과 취급인가 등급을 가지며, 생성되는 모든 문서들, 즉 객체는 기밀등급을 갖는다. 취급인가와 기밀등급을 보안 등급이라 한다. 접근 권한과 보안 등급의 우선 순위는 다음과 같다.

- 접근 권한 : 읽기(read), 쓰기(write)
- 주체(사용자)의 취급인가 등급 : 1급 > 2급 > 3급 > 4급
- 객체(전자문서)의 기밀 등급 : 1급 > 2급 > 3급 > 4급
- 주체와 객체는 각각의 '부서'라는 속성을 가진다.

주체가 가지는 취급인가 등급과 부서를 주체의 보안 속성이라 하고, 객체가 가지는 기밀 등급과 부서의 속성을 객체의 보안 속성이라 칭하며, 주체의 보안 속성은 조직의 정책

에 따라 부여되며, 객체의 보안 속성은 문서 기안자가 문서를 기안하는 경우에 최초로 부여되며 이때 문서는 기안자와 동일한 보안 속성을 가지게 된다. 기안자의 속성을 그대로 가지는 문서의 최종적인 보안 속성은 결재자에 의해서 변경될 수 있다. 주체와 객체의 보안 속성을 다음과 같이 표현하기로 한다.

- 주체의 보안 속성 : S{취급인가 등급 : 부서1, 부서2,…}
- 객체의 보안 속성 : O{기밀 등급 : 부서1, 부서2,…}

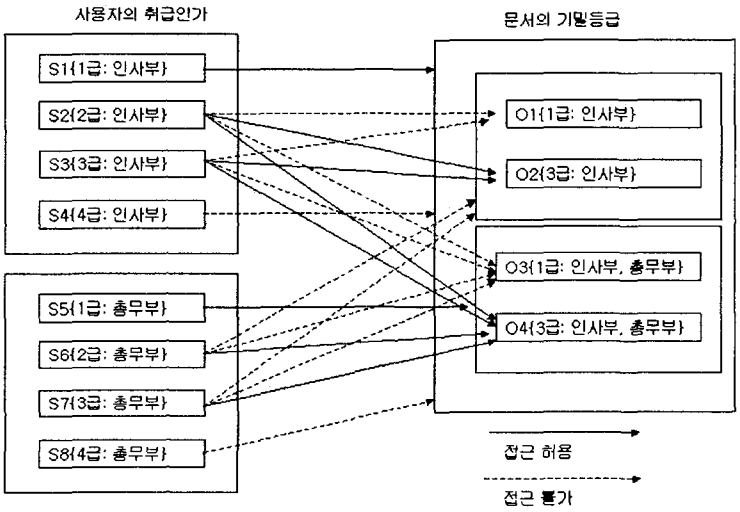
주체와 객체에 대하여 부여된 보안 속성이 다음을 만족하면 접근 권한이 주어진다.

S{취급인가 등급} ≥ O{기밀 등급} 이고, --- (1)

S{부서1, 부서2,…} ∩ O{부서1, 부서2,…} ≠ {} --- (2)

(1)의 조건은 기본적으로 주체가 객체에 접근 권한을 획득하기 위해서는 주체의 취급인가 등급이 객체의 기밀 등급보다 높거나 같아야 함을 뜻한다. 즉, 주체의 취급인가 등급이 객체의 기밀 등급보다 낮을 경우 부서와 상관없이 객체에 접근 권한이 없다. 사용자가 문서의 열람을 위하여 문서를 검색하는 경우 문서의 기밀 등급보다 같거나 높아야 하므로 NRU(No read-up) 정책을 만족시킨다. (2)의 조건은 주체와 객체에 공통적인 부서가 존재하면 접근 권한을 획득할 수 있음을 뜻한다. 즉, 주체와 객체 사이의 부서의 속성이 S{부서1, …} ⊃ O{부서1, 부서2,…}와 같이 포함 관계일 필요는 없음을 뜻한다.

위의 정책을 인사부와 총무부의 경우에 예를 들면 다음 <그림 1>과 같다.

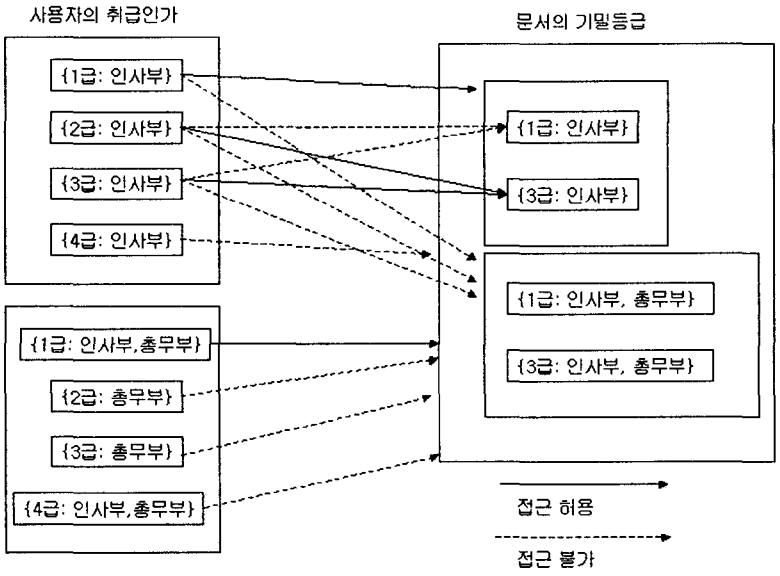


<그림 1> 다중등급 보안의 예

<그림 1>에서 사용자 S1이 접근할 수 있는 문서는 조건 (1)에 의하여 객체의 기밀 등

급이 1급 이상인 O1, O2, O3, O4이다. 또한 사용자 S1의 부서의 속성인 '인사부'와 교집합이 공집합이 아닌 객체는 O1, O2, O3, O4이다. 따라서 S1은 모든 문서에 접근이 가능하다. S3의 경우 조건 (1)을 만족하는 객체는 O2와 O4이며, 이들 객체는 조건 (2)또한 만족하므로 객체에 접근 권한을 갖는다. S5의 경우 조건 (1)을 만족하는 객체는 O1, O2, O3, O4이며, 이들 중 조건 (2)를 동시에 만족하는 객체는 O3과 O4이다. 따라서 S5는 O3과 O4에 접근 권한을 갖는다.

이와 같이 주체와 객체에 보안 등급을 적용하여 접근을 통제하는 방법은 미 국방성이 사용한 군사보안정책과 유사하다. 본 연구에서 제시하는 다중등급 보안 정책과 미 국방성의 경우를 비교하기 위하여 동일한 예제를 미 국방성의 경우를 적용하여 나타내면 <그림 2>와 같다.



<그림 2> 군사보안정책 적용 예

미 국방성의 다중등급 보안의 표현은 {보안등급, 분류1,분류2,}이다. 위의 예는 미 국방성이 사용한 보안등급인 TOPSECRET, SECRET, CONFIDENTIAL, UNCLASSIFIED 대신 1급, 2급, 3급, 4급을 사용하였으며, 분류1, 분류2 대신 인사부, 총무부를 사용하였다. 인사부 사용자 1급은 문서의 기밀등급이 1급이고 부서가 인사부인 문서에 대해서만 접근이 가능하고, 문서의 기밀등급에 총무부가 포함된 문서는 접근이 불가능하다. {1급:인사부, 총무부}의 사용자만 예제의 모든 문서에 접근 가능하다. 인사부의 2급과 3급 사용자는 {3급:인사부}문서만 접근 가능하다.

미 국방성의 다중등급 보안은 사용자가 문서에 접근 권한을 가지기 위해서는 사용자의 보안등급이 문서의 보안 등급 보다 높거나 같아야 하며, 사용자의 취급인가에 명시되는 분류(부서)는 문서의 기밀등급에 명시되는 부서를 포함해야(사용자의 부서 ⊃ 문서의 부서) 한다. 즉, 사용자{보안등급, 분류1,분류2,…} ⊃ 객체{보안등급, 분류1,분류2,…}와 같이 포함 관계의 조건이 적용되지만 본 연구의 경우 포함 관계를 적용하지 않는다. 이는 문서의 안전성뿐만 아니라 부서별 정보의 공유를 고려하기 때문이다. <그림 1>과 <그림 2>에서 주체와 객체가 동일한 조건이지만 본 연구에서 제시하는 다중등급 보안 정책이 더 많은 문서에 접근함을 볼 수 있다.

(1), (2)와 같은 접근 권한 정책을 기본으로 문서의 안전성을 높이기 위하여 다음과 같은 보안 정책을 추가적으로 적용한다.

- NWD(No write-down) 정책 : 이 정책은 결재자가 결재를 위하여 문서를 열람한 경우 결재자가 기안자 보다는 보안등급이 높지만 결재 상신 된 문서에 대하여 그 내용을 수정 할 수 없음을 뜻한다. 또한 결재 처리가 완료된 문서에 대해서는 보안 속성을 변경할 권한이 없음을 뜻한다.
- NWU(No write-up)정책 : 주체의 보안등급보다 높은 객체에 쓰기 행위를 하는 문제(blind write problem)가 발생하는 것을 방지하기 위한 정책이다. 기안자가 문서를 기안하는 경우 문서의 쓰기 행위가 발생하는데 이때 기안자가 자신의 보안 등급보다 높은 보안등급의 문서를 생성할 수 없다.
- 결재처리 후 문서의 쓰기 금지 정책 : 결재처리가 완료된 문서에 대해서는 모든 사용자에게 문서의 수정 및 삭제를 허용하지 않는다. 문서의 삭제는 관리자가 조직의 문서 삭제 절차를 거쳐서 로컬에서 직접 삭제만 가능하다.

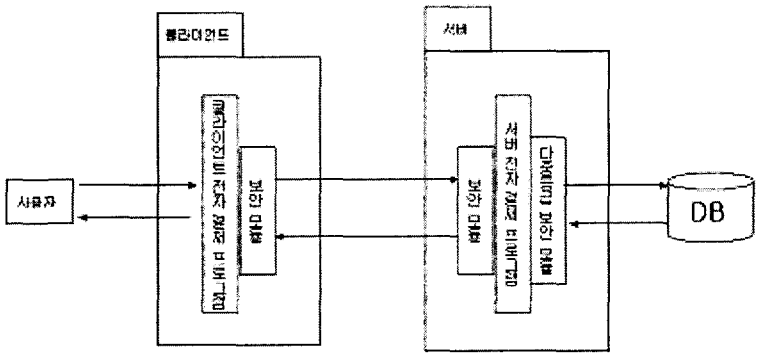
다중등급 보안 정책을 적용하기 위한 사용자의 보안 수준은 조직의 관리자에 의해서 결정되고, 관리자가 로컬로 사용자 정보를 등록 할 때 함께 등록된다. 사용자의 보안 등급의 수정은 관리자만 수정 할 수 있다. 문서의 보안 등급은 문서의 결재자가 결재 처리 시 보안 등급을 지정하여 문서의 보안 등급을 결정한다. 일반 사용자의 경우 문서의 등급은 비록 문서의 보안 등급이 자신의 보안 등급보다 낮다고 해도 결재가 처리된 문서에 대해서는 보안 등급을 변경 할 수 없으며, 문서의 보안 등급의 변경은 조직의 행정 절차에 따라서 관리자만 수정이 가능하다.

IV. 전자결재 모듈의 개발(사례)

4.1 EDMM-MLS의 구조

본 연구에서 구현하는 전자결재 모듈을 EDMM-MLS(Electronic Document Management Module Multi Level Security)라 칭하며 클라이언트/서버 환경으로 <그림 3>과 같은 구조를 갖는다.

사용자가 클라이언트용 전자결재 프로그램을 이용하여 문서를 기안, 결재를 요청, 결재자의 결재 처리, 문서 검색 등의 작업을 행하고 보안 모듈을 거쳐 암호화하여 서버와 통신을 한다. 서버는 클라이언트의 암호문을 보안 모듈을 이용하여 복호화하고, 다중등급 보안을 적용하여 데이터베이스에 저장하거나 읽어 온다. 서버가 클라이언트와 통신을 하는 경우는 서버 보안 모듈이 암호화하고 클라이언트 보안 모듈이 복호화하게 된다.



<그림 3> 다중등급 보안 전자결재 모듈의 구조

4.2 EDMM-MLS의 제공 기능 및 운용 환경

EDMM-MLS는 기본적으로 3개의 모듈로 구성된다. 기안자가 문서를 기안하거나 혹은 결재자가 결재를 하기 위한 클라이언트 모듈과 클라이언트의 서비스 요청을 처리하는 서버 모듈과 부서와 직원 신상 등 데이터베이스에 직접 접근을 할 수 있는 관리 모듈로 구성되며, 여기에 클라이언트가 서버에 서비스를 요청하는 경우와 서버가 요청된 서비스를 응답하는 경우 암호화와 복호화를 수행하는 모듈이 추가되며, 또한 데이터베이스에 저장 및 검색과정에 적용하는 다중등급 보안을 수행하는 모듈로 구성된다. 서버의 경우 접근 제어의 보안 기능을 제공하는 Windows 2000을 사용하였으며(K. Hanner, R. Hormanseder), 기타 상세 운용 및 개발 환경은 <표 2>와 같다.

<표 2> 운용 및 개발 환경

구 분	환 경
서버 환경	OS(Operating System) : Windows 2000 DBMS : SQL Server7.0
클라이언트 환경	Windows 98 , Windows 2000
개발 환경	Visual basic6.0 CryptoAPI(WCCO:Wiley CryptoAPI COM Objects)

4.3 EDMM-MLS의 보안

4.3.1 키 생성 및 키 관리

EDMM-MLS에서 문서를 암호화하기 위하여 CryptoAPI에서 지원하는 세션키(session key), 교환용 키(exchange key), 서명용 키(signature key)와 다중등급보안 key 4가지 종류의 키를 사용한다. 그 용도와 표기는 <표 3>과 같다.

<표 3> key의 종류 및 용도

암호 알고리즘	key		용 도	표 기	
				server	client
대칭키	session key		문서의 암호화 및 복호화	SessKey	
비대칭키	교환용 키 (exchange key)	개인키 (private key)	session key 복호화	SvrExPrv	UserExPrv
		공개키 (public key)	session key 암호화	SvrExPub	UserExPub
비대칭키	서명용 키 (signature key)	개인키 (private key)	hash code 암호화	SvrSigPrv	UserExPrv
		공개키 (public key)	hash code 복호화	SvrSigPub	UserExPub
대칭키	다중등급 보안 키		다중등급 보안 적용	-	

교환용 키와 서명용 키는 사용자가 최초로 로그인하는 시점에 생성한다. 사용자 및 부서의 정보는 서버 응용프로그램이 실행되는 컴퓨터에서 관리자에 의하여 데이터베이스에 사용자의 최초 접속 이전에 등록된다. 즉, 사용자의 이용ID와 패스워드는 사용자가 최초 접속 이전에 등록되어 있으며, 사용자가 등록된 아이디와 패스워드를 이용하여 접속에 성공하면, 클라이언트 응용 프로그램은 사용자의 교환용 키와 서명용 키를 생성하고, 이들 각각의 공개키(public key)를 서버에 전송하여 데이터베이스에 저장한다.

암호화와 복호화에 사용하기 위한 서버의 교환용 키와 서명용 키를 서버가 설치되면서 생성한다. 이때 다중 보안 등급을 위한 다중등급 보안키를 1급에서 4급까지 4개를 생성한다.

4.3.2 사용자 인증 및 키 전송

로그인 과정에서 접근 제어 및 사용자 인증을 위하여 사용자ID와 패스워드를 이용하며, replay back 공격을 방지하기 위하여 일회용 패스워드 기법을 이용하며 이때 서버의 교환용 공개키를 클라이언트에게 전송한다.

① 사용자가 클라이언트 응용 프로그램을 실행하여 사용자ID와 패스워드를 입력한다. 3번 이상의 입력 오류 혹은 인증 실패일 경우 프로그램 종료

② 패스워드는 클라이언트에 저장하고, 사용자ID만 서버에 전송한다.

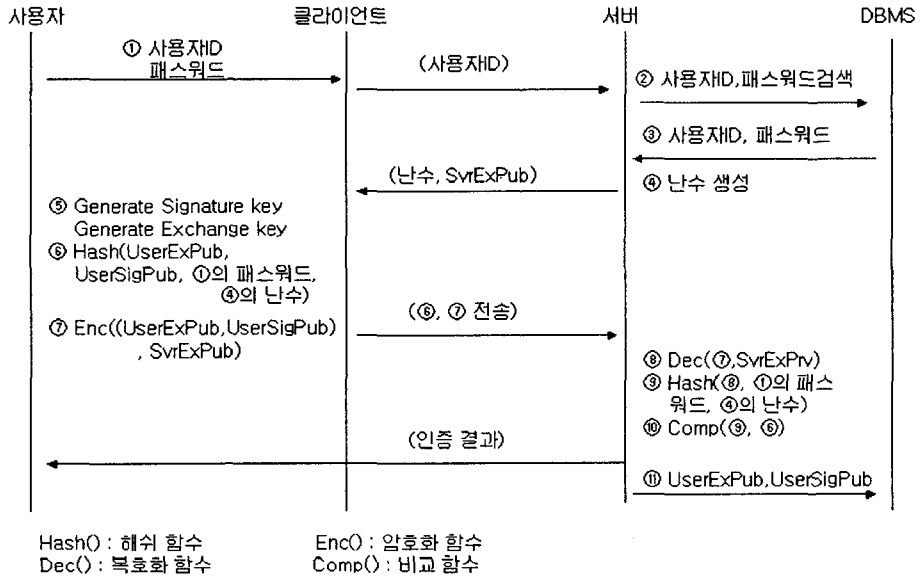
③ 서버는 사용자ID를 이용하여 데이터베이스에서 해당 사용자의 패스워드를 검색한다. 이 때 해당 사용자가 검색되지 않으면 로그인을 거부하는 메시지를 전송한다. 등록된 사용자이면 사용자ID와 패스워드를 저장한다.

④ 등록된 사용자라면, 즉 데이터베이스에서 해당 사용자ID가 검색되면 서버는 난수를 생성한다. 난수와 서버의 교환용 공개키를 클라이언트에 전송한다.

⑤ 클라이언트는 서버가 전송한 난수와 서버의 교환용 공개키를 저장하고 사용자ID를 이용하여 교환용 키와 서명용 키를 생성한다.

⑥ 클라이언트는 교환용 공개키, 서명용 공개키, 서버가 전송한 난수, 사용자가 입력한 패스워드를 hash 함수로 압축하여 hash code를 생성한다.

⑦ 서버에서 전송 받은 서버의 교환용 공개키(SvrExPub - key 표기는 <표 2>를 참조 >)를 이용하여 암호화하고 ⑥의 hash code와 함께 서버에 전송한다.



<그림 4> 사용자 인증 및 키 전송 과정

⑧ 서버는 먼저 클라이언트로부터 전송 받은 ⑦을 복호화 하여 클라이언트의 교환용 공개키와 서명용 공개키를 구한다.

⑨ 서버는 ⑧의 과정에서 구한 사용자의 교환용 공개키, 서명용 공개키, 데이터베이스에서 구한 사용자의 패스워드, 클라이언트에 전송한 난수를 클라이언트가 사용한 hash 함수와 동일한 함수를 사용하여 hash code를 생성한다.

⑩ 클라이언트에서 전송 받은 hash code와 ⑨에서 구한 hash code를 비교하여 사용자 인증을 수행한다. 즉, 일치하면 로그인을 허가하고 일치하지 않으면 로그인을 거부한다.

⑪ 인증이 성공하면 사용자의 교환용 공개키와 서명용 공개키를 데이터베이스에 저장한다.

만일 제3의 도청자가 인증 과정에서 도청하려고 할 때 알 수 있는 정보는 사용자의 ID, 서버의 교환용 공개키, 서버가 전송하는 난수, 클라이언트가 생성한 hash code, 서버의 교환용 공개키로 암호화된 암호문이다. 도청자가 송신자를 위장하려 한다면 송신자의 패스워드를 알아야만 한다. 하지만 송신자의 패스워드는 전송 도중 도청이 불가능하다. 왜냐하면 클라이언트는 hash 함수를 이용한 hash code를 전송하기 때문에 원문인 패스워드를 역으로 계산할 수 없다(FIPS PUB 180-2, 2001; A. Menezes, 1997; M.J.B. Robshaw, 1996). 또한 replay back 공격을 시도하는 경우에도 서버로부터 매번 다른 난수를 전송 받기 때문에 불가능하다. 또한 도청자가 송신자의 공개키 전송을 가로채어 자신의 공개키로 바꾸고자 하는 경우 방지하기 위하여 hash code를 생성할 때 이들도 함께 사용한다.

4.3.3 전자결재 모듈의 다중등급 보안 정책 적용

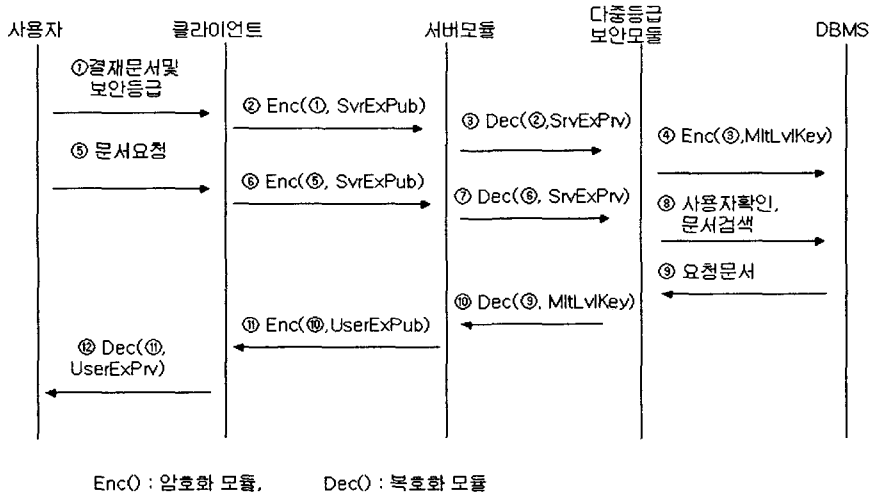
다중등급 정책을 적용하기 위하여 서버는 1급부터 4급까지의 4개의 키를 생성하여 암호화와 복호화에 적용한다. 이때 암호화와 복호화에 사용되는 암호 알고리즘은 대칭키 암호 알고리즘인 DES(Data Encryption Standard)를 사용한다. 키의 길이는 등급과 무관하다. 즉, 암호의 강도가 1급이 4급 보다 높지 않고 4개 모두 동일하다. 4개의 키는 서버가 설치 될 때 서버 프로그램이 생성한다. 최초 문서가 기안 될 때 기안자와 동일한 보안 등급을 가지며, 결재자가 결재 처리를 하면서 문서의 보안 등급 속성을 다시 지정할 수 있으며, 결재자가 보안 속성을 서버에 전송하면 서버는 문서의 보안 등급에 맞는 키를 선택하여 문서를 암호화한다. 보안 등급 키를 이용하여 암호화하는 과정은 <그림 5>와 같다.

① 의 과정에서 결재자는 결재 처리를 하면서 기안문의 보안 등급에 관한 속성을 지정한다.

② 클라이언트는 서버의 공개키를 이용하여 결재 처리가 완료된 문서를 암호화하여 서버에 전송한다. 결재자가 결재 처리 후의 문서를 서버에 전송하는 경우 문서의 내용은 DES를 이용하여 암호화하며, 암호화에 사용된 DES key를 공개키 암호 알고리즘인 RSA 방식을 이용하여 암호화한다. hash code를 이용한 전자 서명을 생성하여 암호문과 함께 전송한다. Enc(①, SrvExPub)의 의미는 서버의 교환용 공개키를 이용하여 암호화함을 나타낸다.

③ Dec(②, SrvExPrv)는 클라이언트에서 전송 받은 ②를 서버의 교환용 개인키를 이용하여 복호화 함을 나타낸다.

④ 복호화 한 문서를 다중등급 보안 모듈을 이용하여 등급에 맞는 key를 이용하여 암호



<그림 5> 보안 등급을 적용한 문서의 암호화 과정

화하여 저장한다. 다중등급 보안 모듈은 복호화한 문서에 일치하는 키를 이용하여 DES 방식으로 문서를 암호화하여 저장한다.

⑤ 사용자가 문서의 열람을 위하여 문서 검색을 요청하면

⑥ 사용자의 문서 요청 내역을 ②와 동일한 방법으로 암호화하여 서버에 전송한다.

⑦ 서버는 암호화된 문서 요청내역을 서버의 비밀키를 이용하여 복호화한다.

⑧ 데이터베이스에서 해당 문서를 검색한다. 이 때 사용자ID를 이용하여 사용자의 보안 등급을 데이터베이스에서 검색하여 사용자의 보안등급과 문서의 보안 등급을 비교한다. 즉, S{취급인가 등급} ≥ O{기밀 등급}와 S{부서1, 부서2,…} ∩ O{부서1, 부서2,…} ≠ {}의 조건을 검사하여 문서의 열람 여부를 결정한다.

⑨ 검색된 문서가 ⑧의 조건을 만족하면 문서의 내용을 서버가 읽는다. 이때 문서는 다중등급 보안 key에 의해 암호화된 상태이다.

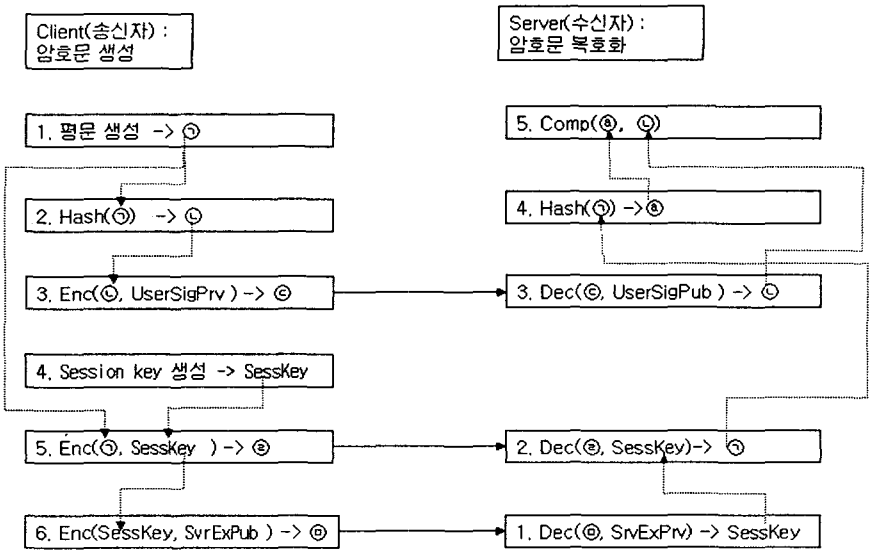
⑩ 문서의 보안 등급에 맞는 키를 이용하여 복호화 하여 서버 모듈에 전달한다. 즉, ④의 과정에서 암호화를 위해서 사용한 것과 동일한 key를 이용하여 복호화 하게 된다.

⑪ 서버는 문서 검색자의 교환용 공개키를 이용하여 암호화하여 전송한다.

⑫ 클라이언트는 자신의 교환용 개인키를 이용하여 문서를 복호화 하여 문서의 내용을 보여준다.

4.3.4 전자 서명된 메시지의 암호화와 복호화

본 연구에서는 마이크로소프트 CryptoAPI를 Visual Basic개발자에게 사용하기 쉬운 모듈로 제공하는 Richard Bondi의 WCCO를 이용하여 문서를 암호화하고 복호화 한다. 기본적으로 문서의 암호화는 대칭키 알고리즘인 DES를 이용한다. 이때 사용되는 DES key는 일회성 키이며 세션 키라 한다. 문서의 암호화에 사용한 세션 키를 공개키 암호 알고리즘을 이용하여 전송한다(msdn.microsoft.com). 문서를 암호화하여 전송하는 경우 문서의 무결성과 부인 방지를 위하여 전자 서명을 생성하여 암호문과 함께 전송한다.



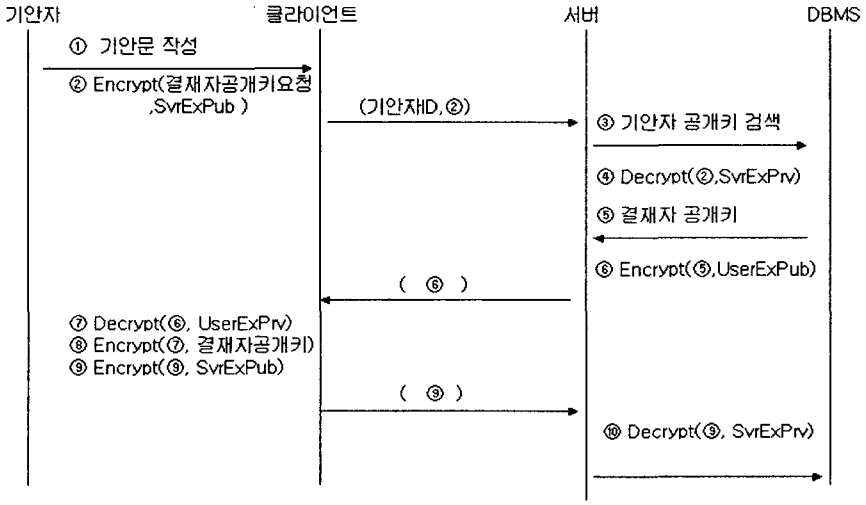
<그림 6>암호화와 복호화

송신자가 먼저 송신하고자 하는 평문을 생성하고 hash 함수를 이용하여 메시지를 고정 길이 비트열로 압축한다. hash 함수의 결과 값인 ㉡을 hash code라 한다. 수신자도 동일한 hash 함수를 이용하여 hash code를 생성하고 비교함으로서 문서의 전송 중 변경이나 훼손 여부를 확인할 수 있다. Hash code를 이용하여 송신자 3의 과정과 같이 전자 서명을 생성한다. 전자 서명은 압축한 메시지(hash code)를 자신의 서명용 개인키를 이용하여 암호화하는데 이는 송신자의 송신 사실 부인을 방지할 수 있게 한다. 즉, 송신자의 신분 확인 기능을 하게 된다. 송신자 4의 과정에서 문서의 암호화에 사용할 세션 키를 생성한다. 세션 키는 대칭키 암호 알고리즘인 DES를 사용하며 문서를 전송할 때 매번 다른 키를 생성하여 문서를 암호화한다. 문서의 암호화에 사용한 세션 키를 수신자의 교환용 공개키

를 이용하여 암호화한다. 송신자는 전자 서명 코드인 ㉢, 문서의 암호문 ㉣ 그리고 세션 키를 암호화한 ㉤을 수신자에게 전송한다. 수신자는 그림과 같이 암호화의 역순으로 복호화 한다. 수신자는 1의 과정에서 자신의 교환용 개인키를 이용하여 전송 받은 ㉤을 복호화 하여 암호화에 사용한 세션 키를 구한다. 이렇게 구해진 세션 키를 이용하여 암호문 ㉣을 복호화 하여 평문 ㉠을 구한다. 송신자 4의 과정에서 전자 서명 코드인 ㉢을 송신자의 서명용 공개키를 이용하여 복호화 하여 hash code를 구하고 자신이 복호화 하여 얻은 평문을 송신자가 사용한 hash 함수와 동일한 함수를 이용하여 hash code를 생성하여 서로 비교하여 인증을 수행한다.

4.3.5 문서 작성 및 전송

기안자가 기안문을 작성하여 결재를 요청하는 경우에 결재자의 공개키를 이용하여 문서를 암호화한다. 결재자의 공개키를 서버에 요청하여 전송 받고, 이를 이용하여 기안문을 암호화하는 과정은 <그림 7>과 같다.



<그림 7> 기안문의 전송

① 기안자가 문서를 생성한다.

② 생성한 문서를 암호화하여 전송하기 위하여 서버에 결재자의 교환용 공개키를 요청한다. 서버에 결재자의 공개키를 요청하는 메시지는 서버의 교환용 공개키를 이용하여 암호화하여 전송한다. 서버와 기안자간의 통신은 <그림 6> 암호화와 복호화의 단계를 거친

다. 즉, <그림 7>의 'Encrypt()' 함수와 'Decrypt()' 함수는 <그림 6>의 암호화와 복호화 단계를 나타낸다.

③ 서버는 전송 받은 기안자ID를 이용하여 기안자의 교환용 공개키와 서명용 공개키를 데이터베이스에서 검색한다.

④ ③을 이용하여 복호화 및 인증을 수행한다. 만일 도청자가 기안자를 위장하려는 경우 전자 서명 과정에 필요한 기안자의 서명용 개인키를 알지 못하므로 위장이 불가능하다.

⑤ 서버는 ④에서 복호화해서 구한 결재자의 ID를 이용하여 결재자의 교환용 공개키를 데이터베이스에서 검색한다.

⑥ ⑤를 기안자의 교환용 공개키를 이용하여 암호화하여 클라이언트에 전송한다.

⑦ 클라이언트는 ⑥을 복호화 하여 결재자의 교환용 공개키를 구한다.

⑧ ⑦에서 구한 결재자의 교환용 공개키를 이용하여 기안문을 암호화한다. 이 단계를 거치면 결재요청 중인 문서는 결재자만 내용을 볼 수 있다.

⑨ 결재자의 교환용 공개키를 이용하여 암호화한 기안문을 다시 서버의 교환용 공개키를 이용하여 암호화하는데 이는 기안자와 서버와의 무결성을 보장하기 위함이다.

⑩ 서버는 자신의 교환용 개인키를 이용하여 복호화하고 결재자의 공개키로 암호화 된 기안문을 데이터베이스에 저장한다.

4.3.6 문서의 결재

결재자가 시스템에 로그인하여 결재 문서를 요청하면, 서버는 해당 결재자를 확인하여 DB에서 해당 결재자가 처리해야 할 문서를 검색하여 전송한다. 결재자가 요청하는 결재 문서는 기안자의 전자 서명과 결재자의 교환용 공개키에 의해서 암호화된 암호문으로 되어 있어 결재자만 복호화 할 수 있다. 결재자의 결재 처리가 완료되어 서버에 전송되면 다중등급 보안 정책에 따라 등급에 맞는 키에 의해서 암호화되어 저장된다. 결재 처리 과정은 <그림 8>과 같다.

① 결재자가 결재 문서가 존재하는지 확인하기 위하여 서버에 결재문서의 요약 정보를 암호문으로 요청한다. 결재자의 요청에 대하여 서버는 해당 문서의 요약 정보를 전송한다. 이 때 클라이언트와 서버는 <그림 6>의 단계를 거치면서 암호 통신을 한다. 클라이언트가 서버에서 전송 받은 문서 목록을 출력하면 결재가 특정 문서를 선택하여 결재할 문서의 전송을 요청한다.

② ①을 서버의 교환용 공개키를 이용하여 암호화하여 전송한다.

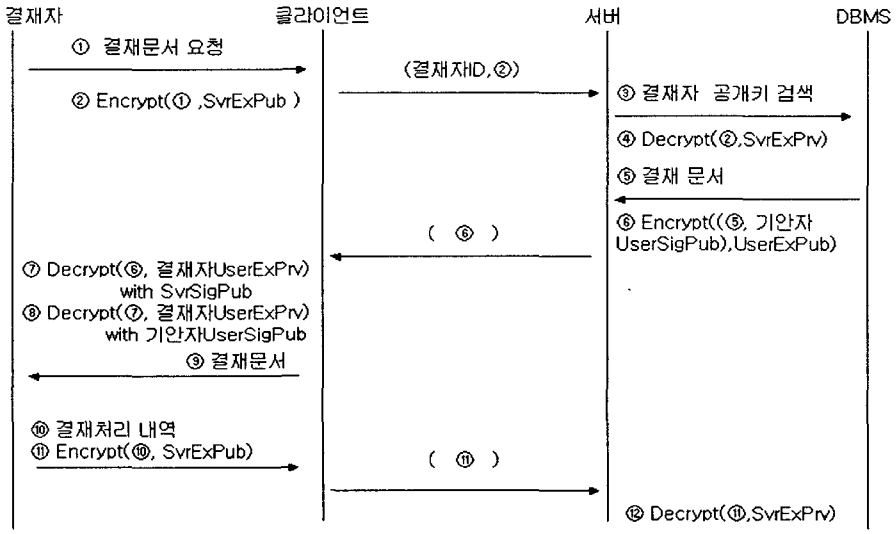
③ 결재자ID를 이용하여 결재자를 확인하고, 결재자의 공개키를 검색한다.

④ ②를 서버의 교환용 개인키를 이용하여 복호화한다.

⑤ 결재 문서와 기안자의 서명용 공개키를 검색한다.

⑥ ④에서 검색한 문서와 기안자의 서명용 공개키를 암호화하고 전송한다.

⑦ 결재자는 자신의 교환용 개인키를 이용하여 복호화 하여 기안자의 서명용 공개키를 구한다. 이때 서버와 결재자 사이의 무결성을 확인과 인증을 위하여 서버의 서명용 공개키를 이용한다.



<그림 8> 결재 처리 과정

⑧ ⑦을 다시 자신의 교환용 개인키를 이용하여 복호화하며, 이때 ⑦에서 복호화한 기안자의 서명용 공개키를 이용하여 인증을 수행한다. 인증이 완료되면 기안에서 결재까지 문서의 안전성이 보장된다.

⑨ ⑧에서 복호화한 결재 문서의 내용을 결재자에게 보여준다.

⑩ 결재자는 결재처리를 수행한다. 이때 문서의 다중등급 보안 등급을 지정할 수 있다.

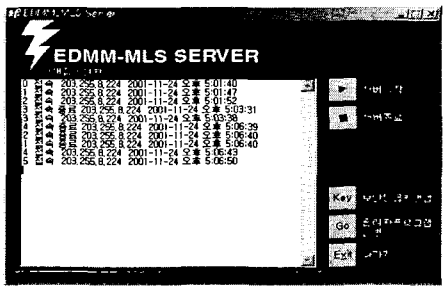
⑪ ⑩의 결과를 서버의 교환용 공개키를 이용하여 암호화고 서버에 전송한다.

⑫ ⑪을 복호화하고 문서의 등급에 맞는 다중등급 키를 선택하여 다중등급 보안을 수행한다.

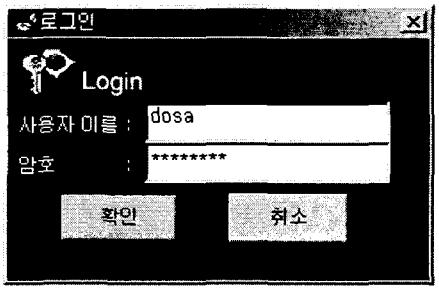
4.4 EDMM-MLS의 사용자 인터페이스

EDMM-MLS는 서버 프로그램, 클라이언트 프로그램, 관리자 프로그램으로 구성된다. 기안자 및 결재자는 클라이언트 프로그램을 이용하여 문서 작성 및 결재처리를 하게 된다. 사용자가 클라이언트 프로그램을 이용하여 서비스를 요청하면 서버 프로그램이 요청한 서비스를 처리한다. 관리자 프로그램은 ODBC를 이용하여 직접 데이터베이스에 접근하며 사용자의 신상정보 및 부서 정보를 관리한다. 이는 EDMS-MLS서버와 동일한 컴퓨터에 인스톨되며 로컬 로그인만 허용한다.

클라이언트는 본 모듈의 사용자인 기안자 및 결재가 문서를 기안하고 결재하는 제반 기능을 제공한다. 다음은 클라이언트의 로그인 화면으로 사용자가 응용 프로그램을 사용하기 위하여 프로그램을 실행하면 사용자의 ID와 패스워드를 입력받아 사용자의 인증을 서버에 요청한다.

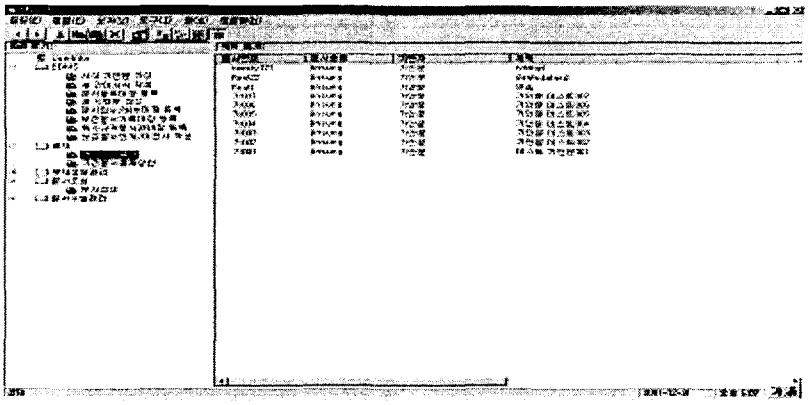


<그림 9> 서버의 메인 화면



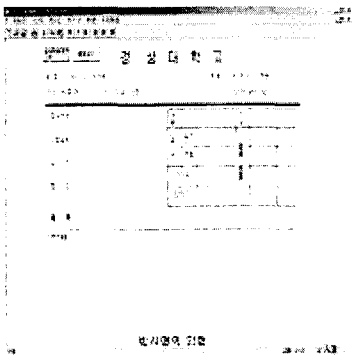
<그림 10> 사용자 로그인 화면

클라이언트 메인 화면의 메뉴는 사용자의 정보를 게시하는 메뉴, 문서를 기안하는 메뉴, 결재를 위한 메뉴, 문서 검색을 위한 메뉴로 구성된다.

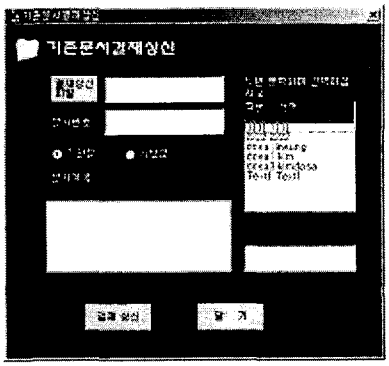


<그림 11> 클라이언트 메인 화면

기안자가 기안문을 작성하기 위하여 새 서식에서 기안문 작성 메뉴를 선택하면 <그림 12>와 같은 기안문 작성화면이 실행되며 기안문 작성에서 결재자를 선택할 수 있는 화면을 제공하며 결재자의 공개키를 서버에 요청하는 모듈과 결재 요청을 수행하는 모듈로 구성된다. 결재 공람을 클릭하면 결재자를 선택할 수 있는 화면이 실행되며 결재가 완료되면 결재 완료 메시지를 보여준다.

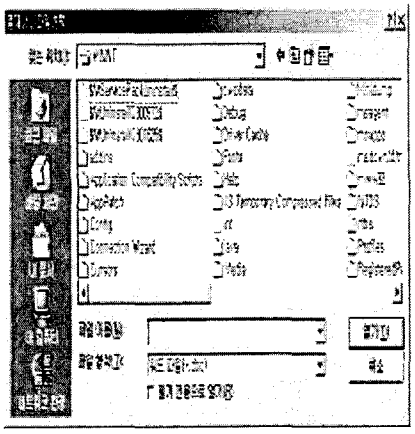


<그림 12> 기안문 작성 화면

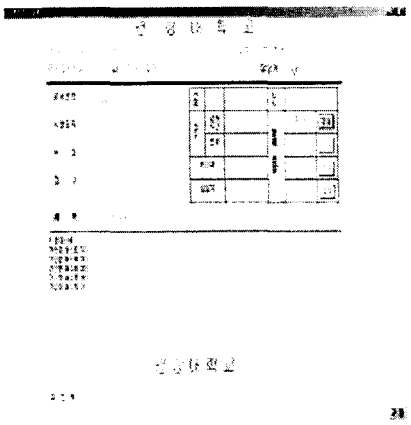


<그림 13> 결재파일 상신 화면

<그림 13> 결재파일 상신 화면은 기안자가 기안문을 MS-Word를 이용하여 작성하고 결재를 상신 하는 기능을 제공하는 화면이다. 결재 상신 파일을 클릭하면 기존의 작성된 문서를 찾을 수 있는 화면을 <그림 14>와 같이 제공한다. 결재파일을 선택한 후 부서의 종류를 선택하고, 문서 제목을 입력한다. 결재자를 선택하면 결재자의 공개키를 서버에 요청하여 전송 받는다. 전송 받은 결재자의 공개키를 이용하여 선택한 파일을 암호화하여 서버에 전송한다.

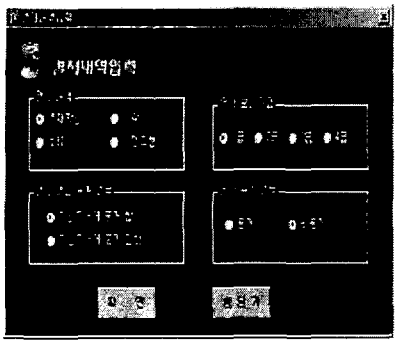


<그림 14> 결재파일 선택화면

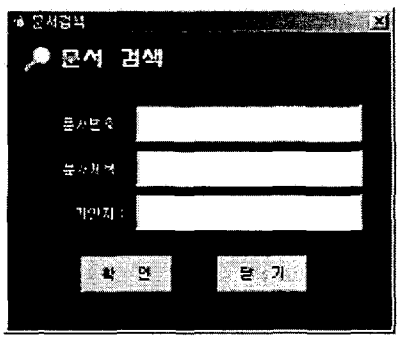


<그림15> 결재문서 상세보기

결재자가 결재를 위하여 메인 화면의 결재문서목록을 선택하면, 문서의 요약 정보인 제목, 작성자, 문서 종류 등의 목록을 출력하며, 결재자가 이를 선택하면 <그림 15>와 같이 기안자가 작성한 문서의 내용이 출력된다. 결재란에 나타난 자신의 이름에 있는 '결재'를 클릭하면 결재처리에 필요한 내용을 입력하는 폼이 <그림 16>과 같이 출력된다



<그림 16> 결재 내역 입력 화면



<그림 17> 문서 검색

메인 화면에서 사용자가 문서조회 메뉴를 선택하면 <그림 17>과 같이 문서의 검색 화면이 실행된다. 사용자가 입력하는 문서 검색의 조건은 암호화되어 서버에 전송되며 서버는 이를 복호화 하여 문서를 데이터베이스에서 다중등급 보안 정책을 적용하여 검색한다. 검색한 문서를 암호화하여 사용자에게 전송한다. 클라이언트는 문서의 목록을 출력한다.

V. 결 론

본 논문에서는 다중등급 보안(MLS : Multi-Level Security)기법을 적용하여 전자문서 관리 모듈을 개발하였다. 부서별 사용자와 문서에 대하여 보안 등급을 1급 > 2급 > 3급 > 4급으로 분류하고 문서에 대한 접근을 통제하였다. 문서의 보안 속성은 부서의 속성이 결합하여 '문서{보안등급:부서1,부서2,..,..}'와 같이 표현되며, 사용자의 보안 속성은 '사용자{보안등급:부서1,부서2,}'로 표현된다. 기본적으로 주체의 보안 등급이 객체의 보안 등급보다 높거나 같은 경우에만 문서에 접근 가능하며, BLP모델의 필수 보안 정책인 NRU보안 정책과 NWD보안 정책을 적용하며 보완적으로 write-up에 대한 규제를 적용하였다. 결재 처리가 완료되는 시점에 문서의 등급을 결재자가 결정하며, 결재자 보안 등급 이상의 등급으로 문서의 보안 등급을 설정할 수 없다. 결재 처리가 완료된 문서에 대해서는 쓰기 권한이 주어지지 않으며, 문서의 열람은 사용자의 부서 속성이 문서의 부서 속성에 포함되며, 사용자의 보안 등급이 문서의 보안 등급보다 높거나 같은 경우에 가능하다.

본 연구에서는 마이크로소프트 CryptoAPI를 Visual Basic개발자에게 사용하기 편하도록 암호 모듈을 제공하는 Richard Bondi의 WCCO를 이용하였다. 사용자 인증은 패스워드를 이용하는데 replay back 공격을 막기 위하여 일회용 패스워드 기법을 이용하였다. 문서의 암호화와 복호화 및 전자서명 기능을 제공하기 위하여 CryptoAPI에서 지원하는 함수를 이용하였다.

본 연구의 전자문서 관리 모듈은 기안자가 작성한 문서를 결재자의 공개키를 이용하여 암호화하고, 서버의 공개키를 이용하여 다시 암호화하여 전송하는 방법을 사용하였다. 이와 같이 하여 결재 상신 중인 문서에 대해서는 결재자만 그 내용의 열람이 가능하도록 하

였으며, 결재 처리가 완료된 문서에 다중등급 보안 정책을 적용시켜 등급 별 키를 이용하여 문서를 암호화한 후 저장하여 방화벽 내부에서 문서의 노출을 방지하고, 관리자에게 의도하지 않은 문서의 노출을 방지하며, 문서의 도난시 그 내용이 노출되지 않도록 하였다.

본 연구에서는 행정기관 및 일반적인 전자문서 관리 시스템이 제공하는 조직도 관리, 전자결재 관리, 전자문서 수발관리, 게시판 관리, 전자 우편관리 기능 중 조직도 관리, 전자결재 관리, 전자문서 수발관리에 대한 다중등급 보안 문제에 중점을 두어 개발하였으며, 모든 사람에게 공개되는 정보를 게시하는 게시판 관리와 웹 환경하의 전자 우편관리의 기능은 제외하였다.

본 모듈은 클라이언트 프로그램, 서버 프로그램, 관리자 프로그램으로 구성되며 인트라넷 환경의 클라이언트/서버 시스템 환경으로 비주얼 베이직 6.0을 이용하여 개발하였다. DBMS는 SQL서버7.0을 사용하였으며, 서버OS(Operating System)는 Windows 2000이며, 클라이언트 OS는 Windows98 및 2000을 사용한다.

모듈의 개발에 있어 문서의 양식은 2001년 1월 행정자치부의 행정기관 간 전자문서유통 표준에서 제시한 8종의 문서 양식을 기본 문서 양식으로 참조하였다. 본 논문에서 개발한 보안 모듈은 공공 기관뿐만 아니라 일반 기업에서 보안등급을 필요로 하는 전자문서 관리에 적용 가능하며, 웹 환경으로 전환 가능한 다중 보안 모듈의 개발과 SSO(Single Sign-on)에서의 다중등급 보안 정책의 적용 등이 향후 연구 과제라 할 수 있다.

참고문헌

김경식, 보안 통제를 고려한 전자결재 시스템 구현, 고려대학교 경영정보대학원 석사학위, 1997.

김종언, 서명이 추가된 전자결재 시스템에 관한 연구, 동국대학교 교육대학원 석사학위, 1992.

김태훈 역(Joel Scambaray, Stuart MCClure, George Kurtz), Hacking Exposed Second Edition, 사이버출판사, 2001.

부산광역시, 부산광역시전자문서관리시스템운영규정, http://www.metro.busan.kr/open_admin/admindata/LAW/MAST/C/C1160.html

이만영, 김지홍, 류재철, 송유진, 염홍열, 이임영, 전자상거래 보안 기술, 생능출판사, 2001, pp.29-49

이명재, "전자결재 시스템에 관한 연구", 사회과학연구 제10호 ,1997, pp. 213-234.

장용철, 오태석, 오무송, "암호화를 이용한 전자결재 시스템의 설계 및 구현", 한국정보처리학회 논문지 제4권 제8호, 1997, pp. 2060-2069.

함안군, 함안군전자문서관리시스템운영규정, http://law.haman.kyongnam.kr/law/htmls/LAW/law4-5-3.html

황의주, 인터넷환경에서 암호 라이브러리를 이용한 전자결재 시스템의 설계 및 구현, 배재대학교 대학원 석사학위, 1999.

행정자치부, 정부전자서명인증 표준 보안 API 사용지침, 행정자치부 예규 제61호, 총칙 제3조, 2000.10.26.

행정자치부, 행정기관간 전자문서유통 표준, 2001.1.

홍승필, 고제욱, 정보보안 기술과 구현, 파워북, 1998.

A. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, Algorithm 9.53 Secure Hash Algorithm - revised (SHA-1), CRC Press, 1997.

Burton S, Kaliski Jr, An Overview of PKCS Standards, RSA Laboratories, 1993. FIPS PUB 180-2, SECURE HASH STANDARD, 2001.

K. Hanner, R. Hormanseder, "Managing Windows NT®file system permissions -A security tool to master the complexity of Microsoft Windows NT®file system permissions," *Journal of Network and Computer Applications*, Vol. 22, No. 2,1999, pp. 119-131.

Lance Spitzner, FirstVPN, Building your firewall rulebase, 2000.

Microsoft, http://msdn.microsoft.com/library/default.asp.

M.J.B. Robshaw, "On Recent Results for MD2, MD4 and MD5," RSA Laboratories Security Bulletin #4, 1996.

Nick Hutton, Security and the Internet, WorldCom, Inc., Whitepaper, March 1, 2002.

Richard Bondi, Cryptography for visual Basic : a programmer's guide to the Micro soft CryptoAPI, John Wiley & Sons, Inc, 2000.

RSA Laboratories, RSA Cryptography Standard, PKCS#1 v2.1, 2001.

S. Boran, The IT Security Cookbook, Boran.com, 2002.

3Com Technical Paper, Internet Firewalls and Security - A Technology Overview, 3Com, 1996.

William Mehuron, Data Encryption Standard(DES), FIPS P PUB 46-3, 1999.

Yasinsac, Ale, "An environment for security protocol intrusion detection," *Journal of Computer Security*, Vol. 10 Issue 1/2, 2002, p177, 12p.

<Abstract>

Building an Electronic Approval Module Using Multi-Level Security

Kim JinSung Gyeongsang National University dosa8080@hanmail.net
Byung-Hyuk Ahn Gyeongsang National University bahn@nongae.gsnu.ac.kr

This paper is to develop a security module for electronic approval systems. Electronic documents are created, transmitted and saved in the company's intranet computer network. Transmitting electronic documents, however, brings us a security problem. Communications among various computer systems are exposed to many security threats. Those threats are eavesdropping, repudiation, replay back etc.

The main purpose of this paper is to develop a module which provides the security of electronic documents while they are passed from one place to another. This paper applies Multi-Level security to the electronic approval system that guarantees security of electronic documents from many threats.

Multi-Level security controls the access to the documents by granting security level to subject users and object electronic documents. To prevent possible replay back attacks, this paper also uses one time password to the system.

The security module is composed of client program and server one. The module was developed using Microsoft Visual Basic 6.0 and Microsoft SQL Server 7.0. The code uses Richard Bondi's WCCO(Wiley CryptoAPI COM Objects) library functions which enables Visual Basic to access Microsoft CryptoAPI.