특

기업 정보 유출 방지를 위한 기술

김 종 원[1] 최 종 욱[2]

목 차

1. 서 론

1997년도 우리나라가 국제 금융 위기에 휩싸여서 어려움에 처해있을 때 국내 반도체 회사에 근무하던 회사원들이 회사 기밀문서를 대만의 반도체 회사에 넘기다 검거된 적이 있다. 이 당시 국내 반도체 업체가 입은 손실 추정액은 약 7억 달러에 이르는 것으로 알려졌다. 하나의 정보가 갖는 가격과 피해를 여실히 보여주는 사례라고 할 수 있겠다[1].

네트웍의 발달과 컴퓨터의 성능 향상은 개인용 컴퓨터의 한계를 뛰어넘어서 수많은 정보를 처리하거나 공유할 수 있는 환경을 제공하고 있다. 인터넷은 도입 초기에는 연구자들끼리 이 메일을 통해 정보를 주고 받는 정보였으나, 1990년대 초 CERN에서 개발된 WWW(World Wide Web)의 보급과 모자이크의 개발로 일반인들에게도 인터넷이 사용되기 시작하였다. 90년대 이후 각국에 불어 닥친 초고속 정보망 구축 열풍과 맞물려 모든 비즈니스 환경에 인터넷이 도입되고 그 동안 개별 기업이나 기관에서 LAN(Local Area Network)과 맞물리면서 모든 비즈니스의 중심에 네트워크가 자리잡게 되었다. 인터넷과 인트라넷을 통한 효율적인 정보의 공유와 생산성의 향상이 모든 기업과 기관에 도입되었다. 특히, 컴퓨터의 성능향상으로 대부분의 연구개발, 기획 작업이 디지털화되고 네트워크를 통해 공유되거나 분산되는 결과를 낳았다.

기업들은 많은 정보들이 디지털화 되어가면서 산발적으로 존재하는 정보를 하나로 모아서 기업의 자산으로 관리할 수 있는 KM(Knowledge Management) 시스템이나 EDMS(Electronic Document Management System)를 도입하는 사례가 늘어가고 있다. KM이나 EDMS를 통해서 통합된 정보는 체계적으로 활용되고 관리됨으로써, 기업 내의 지식자산이 되어 기업의 가치를 높이고 업무의 효율성을 극대화 시킬 수 있어 기업의 경쟁력 향상에 큰 기여를 하고 있다.

과거에는 기업 내에서 발생되는 정보는 종이 서류와 같은 물리적인 파일로서 저장되었기 때문에 공간적인 제약으로 인해 많은 사람들이 동시에 접근할 수 없었지만 디지털화된 정보는 손쉽게 공유

1) (주)마크애니 부설연구소장
2) (주)마크애니 대표이사, 상명대 소프트웨어 대학

되거나 네트워크를 통해 손쉽게 복사 배포될 수 있게 되었다. 모든 문서가 디지털화되고 네트워크를 통해 배포되기 이전에는 기업내부의 중요정보들이 오프라인 보안장치에 의해서 보호되고 있었고, 이러한 정보의 탈취를 위해서는 시간과 노력이 많이 필요하였다. 문서의 디지털화 이후에도 오프라인 유출을 막기 위해 출입구에 마그네틱 소거기를 이용하여 출입구를 통해 반출되는 플로피 디스켓의 내용을 자동 삭제하거나 CD등을 반출 통제하는 제한하는 방법을 이용하기도 한다.

오늘날의 디지털화된 기업정보는 네트워크에 연결된 컴퓨터를 통해서 접근이 가능하고 대량 배포가 가능하기 때문에 외부의 침입을 막기 위한 방화벽이나 침입탐지 시스템의 설치, 내부정보에의 접근제어를 이용하여 통제하고 있다. 그러나 이는 외부에서 내부정보로의 접근을 차단하는 방법이며, 전자우편과 같은 시스템을 통해서 내부에서 외부로 전달되는 정보의 유출까지 제어하기에는 많은 어려움이 있다.

디지털로 집중 관리되고 있는 기업내부 정보를 효율적으로 보호하기 위해서는 방화벽이나 침입방지 혹은 침입탐지 시스템으로는 내부자에 의한 정보 유출을 방지할 수 없다. 세계적인 시장 조사 기관인 IDC의 조사에 의하면 전산장애 사고의 25%가 해킹이나 바이러스 등의 불법적인 침입에 의한 것이며 나머지 75%는 인가된 사용자에 의한 것이라고 조사 결과를 발표했으며 기업 내부 정보의 유출이 내부자에 의해서 이루어질 가능성이 현저히 높다는 것을 말해준다[2]. 더우기 평생직장의 개념이 사라지고 직장에서의 이직 현상이 빈번해진 요즘에는 더 더욱 기업의 내부 정보 유출에 대한 보안이 중요시되고 있다.

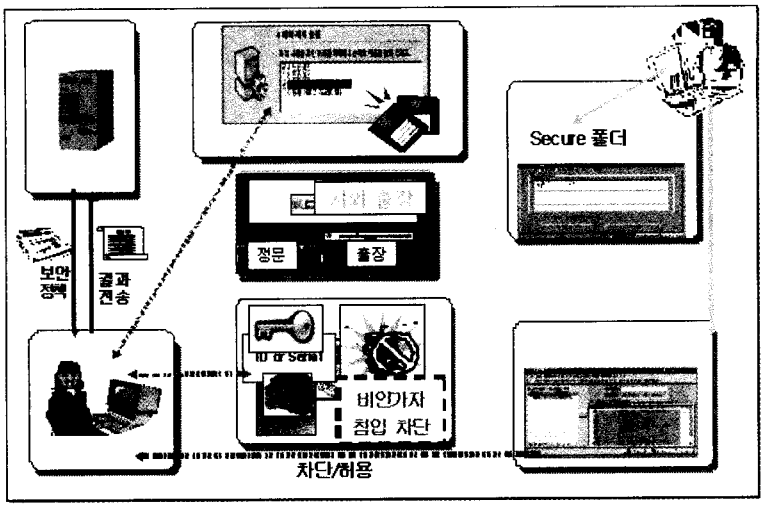
기업 내부 정보의 유출에 의한 사례가 늘어가고, 그 피해의 심각성이 알려지면서 많은 기업들이 자체 보유한 정보에 대한 보안기술 채택을 서두르고 있으며, 국내외적으로 다양한 기술들이 기업 내부 보안기술로서 선을 보이고 있다. 내부 정보의 보안을 위해서 가장 우선적으로 취해지는 기술로서는 접근통제를 위해서 개인별로 ID와 비밀번호를 부여하고 인증을 통해서만 정보에 접근할 수 있도록 하는 방법이 있지만 이것은 내부자에 의한 정보 유출을 방지할 수 있는 방법은 아니다. 기업 내부 정보의 효율적인 보안을 위한 방법으로는 현재 가장 효과적으로 활용되고 있는 기술로서는 DRM(Digital Rights Management) 기술이 있으며, PC보안 기술이나 생체인증 기술이 활용되고 있다.

2. 기업 내부 정보 보호 기술

2.1 PC 보안

PC 보안이란 개인이 사용하고 있는 PC에 저장되는 데이터를 보호하거나 관리하기 위해서 사용할 목적으로 개발된 기술이라 할 수 있다. PC 보안은 정확하게 내부 정보의 보호를 위한 것이라기보다는 종합적인 개인 보안을 위한 기술의 연합체라고 설명할 수 있다. 즉, 개인 PC에 대해서 방화벽, 침입탐지 혹은 침입방지 시스템, 바이러스 방지, 암호화 기술을 이용한 개인용 자료의 보안 등을 포함하는 제품적 개념이다.

PC 보안은 개인의 자료를 보호하기에는 매우 용이하지만 인트라넷을 통해서 KM이나 EDMS와 같이 공유자료로서 활용을 하기 위해서는 다양한 룰과 서버가 지원이 되어야 하며, 공유 자료에 대한 암복호화가 사용규칙에 따라서 이루어져야 하는 등의 추가적인 기술지원이 필요하다. 최근에는 PC 보안제품을 기업내의 공유문서 유출 방지를 위한 시스템으로 사용하기 위해서 서버에서의 관리 툴을 개발하여 제공하는 경우도 있으며, KM이나 EDMS와의 연동을 지원하는 제품이 발표되고 있다.



(그림 1) PC보안 개념도

2.2 생체 인증

기존에 활용되고 있는 ID나 비밀번호는 유출의 위험이 매우 크며, 개인들은 ID나 비밀번호의 관리가 소홀하기 때문에 기업내의 문서 유출을 더욱 손쉽게 만드는 경향이 있다. 따라서 최근에는 개인의 생체적 특징을 이용하여 인증을 시도하는 생체 인증 기술이 확산되고 있다. 생체 인식을 위한 기술로서는 지문을 이용하는 지문인식, 홍채를 이용하는 홍채인식, 손등의 정맥형태를 인식하는 정맥인식, 서명을 인식하는 서명인식, 음성을 인식하는 음성인식, 얼굴을 인식하는 화상인식기술이 활발히 연구되고 있으며, 현재 가장 널리 사용되고 있는 것은 지문인식 기술이다.

이러한 생체 인식기술은 개인마다 차별화되어 있는 생체적 특징을 이용하여 기업 내부의 자료접근을 제한하고 있기 때문에 외부자에 의한 자료접근을 제한할 수 있고, 허용 받지 않은 내부 사용자의 접근도 제한할 수 있는 장점을 가지고 있다. 그러나 앞에서 언급한 것처럼 기업 내부 정보의 유출은 내부자에 의한 소행이 70% 이상을 차지하고 있기 때문에 인가된 사용자에 의해서 정보가 유출되는 것을 방지할 수는 없다.

2.3 DRM 기술

DRM 기술은 기업의 내부 정보를 보호하기 위한 목적이 아니라 멀티미디어 콘텐츠의 유료서비스를 효과적으로 제공하고, 서비스 사업자의 수익원천이 되는 멀티미디어 콘텐츠를 보호하기 위해서 개발된 기술이다. 초창기 콘텐츠 서비스 사업자의 저작권 보호는 회원에게 사용자명과 비밀번호를 부여함으로써 인증된 사용자만이 콘텐츠에 접근하겠다는 정책을 사용하였다. 그러나 웹을 통해 서비스되는 콘텐츠의 특성상 콘텐츠가 존재하는 경로가 노출되면, 사용자명과 비밀번호를 입력하지 않더라도 콘텐츠에 접근할 수 있다는 취약점이 있다. 따라서, 사용자의 콘텐츠 사용권한 제어나 유통, 과금결제, 저작권 사용현황, 사용자의 인증과 콘텐츠의 보호를 종합적으로 다룰 수 있는 기술을 필요로하게 되었다.

DRM 기술은 디지털 콘텐츠의 이용권한을 관장하고 콘텐츠의 전체 라이프 사이클에 걸쳐서 콘텐츠의 이용 결과를 관리하는 하드웨어와 소프트웨어 서비스와 기술이다. 콘텐츠의 가치사슬은 (그림 2)과 같이 나타낼 수 있다[3].

(그림 2) 콘텐츠 가치사슬 (IDC, 2001)

(그림 2)는 콘텐츠 가치사슬에 참여하는 많은 회사들에 의해서 수행되는 중요한 역할을 설명한다. 콘텐츠 유통을 위한 모든 비즈니스 모델이 콘텐츠 가치사슬의 콘텐츠 생산자와 콘텐츠 사용자 사이의 모든 구성이 다 들어가는 것은 아니다. 즉, 하나의 회사가 다중 역할을 수 행할 수도 있다.
일반적으로 기술 업체들은 다음과 같은 두 가지의 기본적 목적을 가지고 DRM을 구현한다[4].

2.3.1 안전한 상거래를 위한 DRM

디지털 콘텐츠를 유료화하기 위해서는 적법한 절차를 거친 사용자만이 이용이 가능하도록 해야 하며, 이와 같은 적법한 사용에 대해서 과금을 하고, 불법적인 사용으로부터 콘텐츠를 보호함으로써 디지털 콘텐츠의 상업적 가치를 보호하기 위하여 DRM을 이용하는 것이다.

2.3.2 통신 기밀성을 위한 DRM

개인 정보보호를 위해서 정보의 기밀성을 유지하는 목적으로 DRM을 이용하는 것이다. 디지털 콘텐츠의 상거래에 있어서 그 거래내역 - 어떤 콘텐츠를 언제 얼마만큼 사용을 했는지 등 - 은 개인의 사생활과 관련된 부분이며, 이러한 정보의 불법적 사용으로부터 보호는 매우 중요한 것이다. 정보의 기밀성을 위한 DRM은 기업의 기밀이나 정책관리에 적용할 수 있다.

상거래를 위한 DRM 이든, 기밀성을 위한 DRM이든 디지털 저작권 관리기술을 구성하는 시스템 요소는 다음과 같이 고려할 수 있다. 그러나 DRM은 콘텐츠 서비스 사업자의 사업모델에 따라서 다양한 정책을 가질 수 있으며, 이러한 다양한 정책에 따라서 다양한 시스템으로 구성될 수 있다[5].

2.3.3 콘텐츠의 암호화

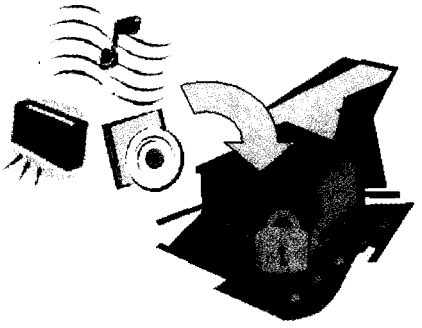
이는 콘텐츠의 포맷에 관계없이 사용자 이외의 파일사용을 방지하는 디지털 콘텐츠의 금고 역할을 수행한다. 암호화는 디지털 콘텐츠를 포장하여 전달하는 것과 같은 의미에서 패키징이라고 불리우기도 한다. 암호화의 형태로는 공개키 방식을 사용하는 것과 비밀키 방식의 알고리즘을 이용하는 방법이 있다. 공개키 방식은 대용량의 콘텐츠를 암호화하기에는 연산량이 너무 많기 때문에 비효율적이고, 콘텐츠 제공 서버의 부담을 가중시키는 문제가 있다. 이에 반해 비밀키 방식은 대용량의 콘텐츠를 암호화하는데 용이하지만 키를 분배하는데 보안상의 어려움이 존재한다. 최근에는 이를 효과적으로 해결하기 위해서 콘텐츠의 암호화는 비밀키 방식으로 하고, 비밀키의 전송에는 공개키를 이용하는 방식이 활용되고 있다.

2.3.4 콘텐츠의 전송

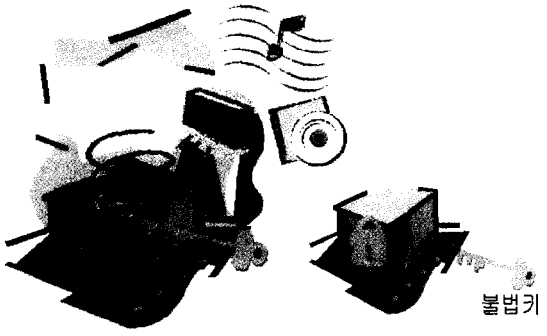
암호화된 콘텐츠는 온라인 상에서 안전하게 사용자에게 전달되어야 한다. 콘텐츠의 전송은 암호화와 연계된 방법을 사용하여 전송하는 것이 일반적이다. 전송방법으로는 원본 콘텐츠를 일괄적으로 서버에서 관리하면서 필요에 따라서 스트리밍으로 전송하는 방법과 개인 사용자에게 콘텐츠를 다운로드시켜서 분산하여 관리하고, 서버에서는 사용규칙이나 암복호화만을 제어하는 방법으로 구분할 수 있다.

2.3.5 콘텐츠의 유통 및 과금

콘텐츠의 유통과 과금은 콘텐츠 서비스 사업자

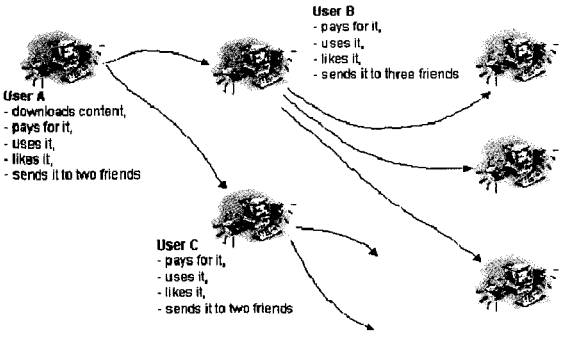


(그림 3) 콘텐츠 암호화의 개념(패키징)



(그림 4) 콘텐츠의 복호화(적법사용자와 불법사용자)

의 비즈니스 모델에 따라서 다양한 형태를 가질 수 있다. 콘텐츠의 유통에서는 사용자의 콘텐츠 사용 이외에도 다른 사용자에 의한 추가적인 전송 여부의 허용 등, 전체적인 콘텐츠의 사용에 관한 규칙을 정의하고, 그에 따른 과금과 결제가 이루어지는 것이다. 콘텐츠의 사용에 있어서는 일회성 사용이나 영구사용, 보관용 등에 따라서 권한이 달라지며, 권한에 따른 비용지불도 달라지게 된다. 과금과 결제에 있어서는 사이버머니를 활용하는 방법에서부터 무선단말기를 통한 결제, 은행이나 카드사를 통한 결제 등 다양한 방법에 의해서 과금과 결제가 이루어질 수 있다. 특히, 콘텐츠의 특성상 B2B(Business to Business)보다는 B2C(Business to Customer) 거래가 많이 이루어지며, 따라서 소액결제가 많이 이루어지기 때문에 소액결제 지원에 대한 부분을 많이 다루게 된다.



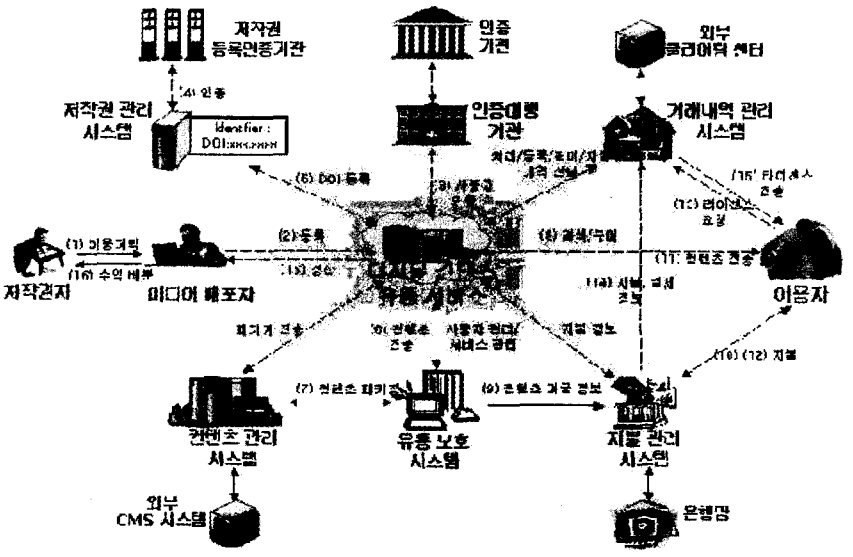
(그림 5) 콘텐츠의 양도(Superdistribution)

2.3.6 콘텐츠의 정보추적

만일 다른 사용자에 의한 콘텐츠의 유통이 발생한 경우 이 콘텐츠를 제어하기 위한 정보의 추적 여부를 고려한다. 정보 추적은 로그분석을 통하여 콘텐츠의 이동 및 복제여부를 확인하는 방법과 이를 이용하여 개별적인 콘텐츠의 사용을 제한하도록 하는 방법 등이 있다.

2.3.7 저작권 등록 및 관리

디지털 콘텐츠에는 저작권이 있고, 디지털 콘텐츠 생성자가 저작권을 보호받기 위해서 최초의 생성시점을 등록하고, 해당 콘텐츠에 대한 저작권자를 등록함으로써, 향후 발생할 수 있는 저작권 분쟁에 대비할 수 있는 부분이다. 특히, 해당 콘텐츠에 대한 저작권자가 등록되면 콘텐츠의 사용량에 따른 수익분배에 있어서 저작권자의 지분율에 따른 분배가 가능하며, 콘텐츠의 이용현황에 대한 로그분석 등이 가능하다. 콘텐츠의 이용현황에 대한 자료의 축적이나 통계분석 등은 콘텐츠 유통 부분에서 다루는 것이 일반적이며, 클리어링 시스템으로 분리하여 구축하기도 한다. 저작권 등록은 향후 저작권 분쟁에서 보호받기 위해서는 제도적으로 공공성을 띠고 있는 기관에서 관리운영하는 것이 적절하기 때문에 일반 콘텐츠 서비스 사업자는 저작권 등록 시스템을 운영하지 않는 경우도 많이 있다.



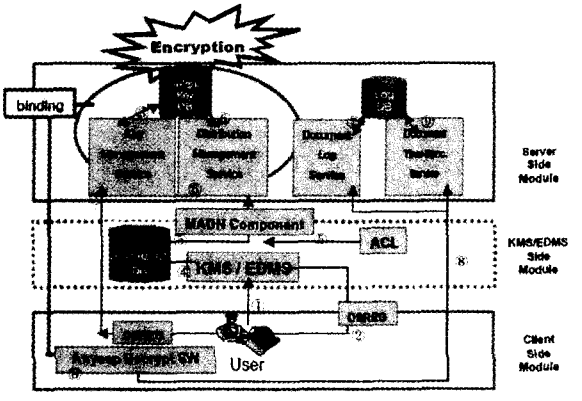
(그림 6) DRM 시스템의 구성 예

이러한 요소들에 의해서 구성된 DRM 시스템의 예를 (그림 6)에 나타내었다.

3. 기업 정보 유출 방지를 위한 기능

DRM 기술은 콘텐츠의 전자상거래를 위한 시스템 기술이었기 때문에 매우 다양한 기술들이 접목되어 있다는 것을 알 수 있다. 이에 반해서 기업 내부의 정보 유출을 방지하기 위한 DRM 기술에서는 과금결제와 같은 부분이 필요하지 않으며, 오히려 복잡한 사용규칙을 다룰 수 있는 효과적인 방법이 필요하다. (그림 7)은 DRM을 활용하여 기업의 KM이나 EDMS에 저장된 내부문서의 유출을 방지하기 위한 시스템 구성 예를 나타내고 있다[6].

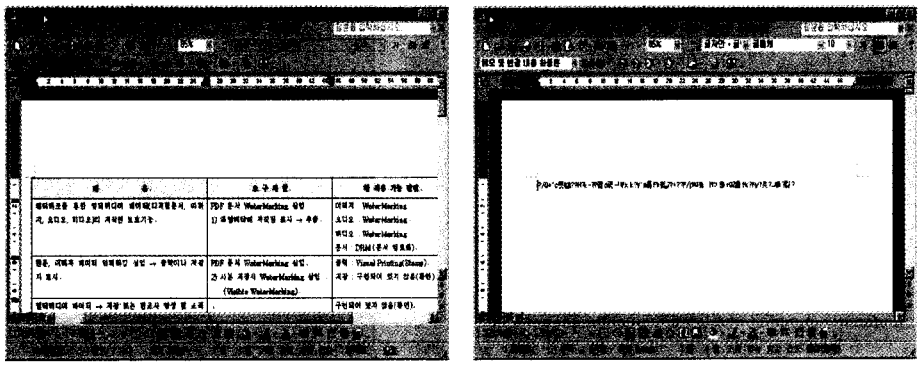
기업의 내부 정보 유출을 방지하기 위해서는 멀티미디어 콘텐츠의 서비스에서 사용되었던 것보다는 다양한 기능들을 지원할 수 있어야 하는데 본 고에서는 대표적으로 지원되어야 할 기능들에 대해서 알아보도록 하겠다.



(그림 7) DRM을 이용한 기업 정보 유출 방지 시스템 예

3.1 내부 문서 열람

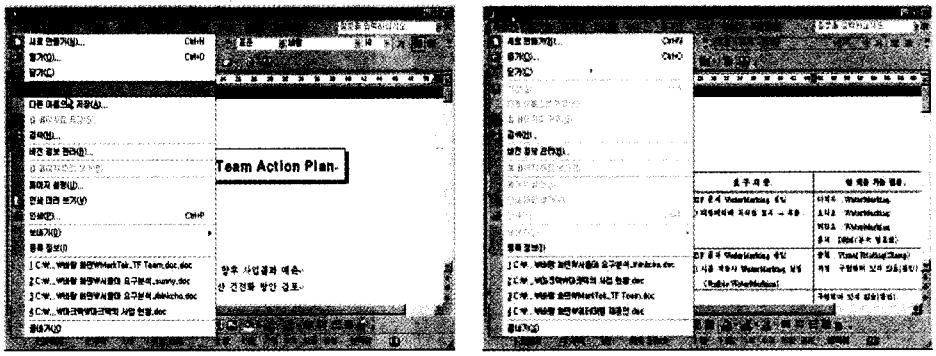
인가된 사용자만이 정상적으로 내부 문서를 열람할 수 있도록 하는 것이다. (그림 8)에서와 같이 인가된 사용자는 문서의 내용을 정상적으로 열람할 수 있지만 비인가된 사용자는 의미 없는 문자열을 열람하게 되는 것이다. 인가된 사용자라도 해당파일을 제 3 자에게 전자우편을 이용하거나 기타의 방법으로 발송하였을 때도 제 3 자는 해당 파일을



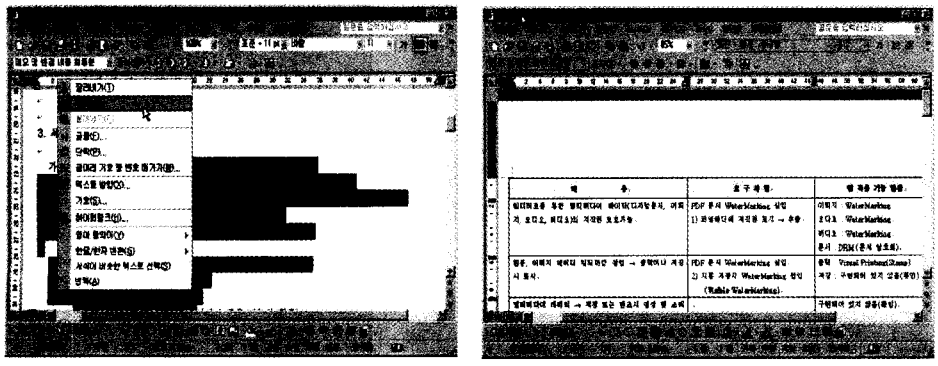
(그림 8) 인가된 사용자와 비인가 사용자의 화면 예시

열람할 수 없게 되는 것이다.

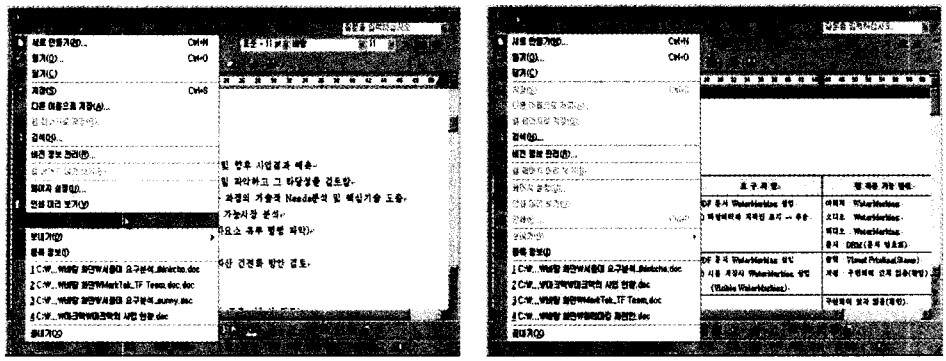
기능은 암호화된 문서를 평문으로 저장할 수 있는 기능과 편집을 허용하는 기능, 출력을 허용하는 기능에 대한 것이다. 단순히 디지털화된 문서만을 보호하는 것이 아니라 오프라인으로 출력하지 못하게 함으로써 오프라인으로의 내부 정보 유출까지 방지할 수 있는 것이다.



(그림 9) 저장권한의 통제



(그림 10) 편집권한의 통제



(그림 11) 출력권한의 통제

3.2 직급, 직무, 개인별 데이터의 접근 통제

직급이나 직무, 개인에 따라 데이터의 접근 권한 적용이 다르게 이루어져야 한다. 즉 직급에 따라 문서 혹은 데이터를 출력할 수 있는 권한, 복사하여 저장할 수 있는 권한, 타인에게 전자우편이나 공유폴더를 통해 보낼 수 있는 권한, 편집할 수 있는 권한이 다르게 적용되어야 한다. 출력권한을 가진 사용자가 문서를 출력할 때는 해당 사용자에 대한 정보가 출력물에 함께 인쇄되도록 처리함으로써, 향후 출력된 문서가 유출되었을 때에도 유출자를 추적함으로써 책임을 물을 수 있는 워터마킹(핑거프린팅) 기술도 함께 사용이 된다.

3.3 문서의 복사와 전송 시 사용 불가

자신의 컴퓨터에 내려 받은 문서/데이터를 CD, Floppy Diskette, USB Key등의 저장 정치에 복제(copy)하거나 인터넷/인트라넷을 통해 타인에게 전송한 경우, 문서의 사용이 불가능 하여야 한다. 이는 문서 유출을 원천적으로 차단하기 위한 가장 기본적인 기능으로서 국내에서 개발된 대부분의 문서 보안 시스템에서 구현되어 있다. 한편 내부적으로 허용된 직원(상사 혹은 부하직원)이나 외부의 협력 업체, 해외에 근무하고 있는 동일 기관 근무자들과의 문서 교환은 전혀 문제없이 이루어 질 수 있어야 한다.

3.4 문서 생성시 자동 암호화 가능

문서의 생성시 모든 문서가 암호화 되는 경우 어떤 문서라도 허가 받지 않고 불법적으로 유출되는 경우 외부 불법 사용자 혹은 문서 생성자 역시 이를 열어볼 수 없도록 하여야 한다. 모든 문서에 대해 유출하지 않는 경우 KM, EDM, Groupware 등에 upload시키는 중요한 문서의 경우에만 문서 유출 방지 기술을 적용할 수도 있어야 한다. 일반적으로 문서 생성시 암호화 하는 경우 이를 서버로 자동 전송하고 생성 당사자 컴퓨터에는 문서가 남지 않도록 하고 있다.

3.5 문서의 생성부터 폐기까지 전체 사이클 제어

기본적으로 문서 유출 방지시스템에서는 문서의 열람, 출력, 복제, 전송, 출력 등의 기능을 통제할 수 있어야 하며 문서의 폐기에 대한 통제도 가능하여야 한다. 이는 문서를 e-mail을 통해 타인에게 전송하거나 Task Force Team에서 작성하여 공동으로 사용하는 문서를 upload할 때 적용한다. E-mail을 통해 전송 받은 문서에 기한이 설정되어 있는 경우 기간이 지나면 자동으로 문서가 폐기되며 하드 디스크에서 자동으로 삭제되어야 한다. 전송 받은 문서는 출력 횟수, 조회 횟수가 제한되며 제3자에게 전송할 수 있는 권한도 제한된다.

3.6 화면 캡처와 캡처 도구에 의한 저장 방지

각 사용자별로 문서의 열람이나 복제 저장 등의 권한이 다르게 설정되어 있다. 문서의 조회권한만을 가진 사용자가 화면에 문서를 띄워 놓고 이를 화면 캡처 기능을 이용하거나 캡처 도구를 이용하여 문서를 재편집하려는 의도를 막을 수 있어야 한다.

3.7 문서의 출력시 추적 기능

문서의 출력권한을 가진 사용자가 문서를 출력하여 반출한 뒤 이를 스캐닝하여 재편집하려는 경우, 혹은 복사하여 배포하는 것을 막기 위해서 문서를 출력하는 경우 문서의 출력자, 부서, 시간을 출력시 문서에 인쇄하여 유출자를 추적할 수 있어야 한다.

3.8 로그 관리

사용자의 모든 접근 활동은 서버에 로그로서 남아 차후에 분석자료로서 활용되어야 한다.

3.9 저장 매체 제어

CD, Floppy Diskette, USB Key등에 저장하여 이를 제3장에게 전달하는 경우에도 지정된 사용자는 쓸 수 있어야 하지만 지정되지 않은 불법적인 사용자는 사용할 수 없도록 할 수 있어야 한다.

3.10 다중창 활용

보안을 요하는 암호화된 비밀 문서들과 일반문서를 여러 개 동시에 열어 놓고 이를 편집하거나 상호 사용이 가능하여야 한다. 만약 비밀문서와 일반문서를 열어 비밀 문서의 일부를 복사(copy)하여 일반문서로 paste할 수 없어야 하지만, 일반문서의 일부를 복사하여 비밀문서에 paste할 수는 있어야 한다.

이처럼 내부자에 의한 문서와 자료 유출을 막기 위해서는 다양한 기능이 필요하다. 그러나 가장 중요한 기능은 사용자들이 불편 없이 전자 금융시스템을 사용할 수 있도록 시스템에 설계되고 운영되어야 한다는 점이다. 사용자 컴퓨터에 복잡하고 어려운 절차 없이 접근이 가능하지만 확실한 보안장치로 문서의 복사 외부 유출 시 사용이 불가능하여야 한다. 또한 출장 시 노트북 컴퓨터를 분실하는 경우 컴퓨터에 저장된 모든 파일과 데이터를 무력화 시킬 수 있는 기능이 있어야 하면서도 출장 시 번거로운 등록을 여러 번 거치지 않도록 하여야 한다.

이외에도 일정시간동안만 해당 사용자들이 내부문서를 열람할 수 있도록 함으로써 정보유출을 방지할 수 있다. 이런 경우에는 사용자들이 자신의 PC에 대한 시간 정보를 수정함으로써 문서를 열람하려는 시도를 무력화 시키기 위해서 시간설정이 된 문서에 대해서는 서버에 있는 시간동기 시스템과의 연계를 통해서만 문서를 열람할 수 있도록 처리한다. 이렇게 권한관리가 되고 암호화된 문서는 전자우편을 통해서나 다른 기록매체를 통해서 외부로 유출되더라도 인가 없이는 열람을 할 수 없기 때문에 무용지물이 될 수 밖에 없다.

4. 요소 기술

DRM 기술을 이용하여 기업 정보 유출을 방지하기 위한 요소기술로서는 가장 기본적으로는 암호화 기술과 사용자 인증을 위한 인증기술이 필요하며, 인가된 사용자에 의한 출력물 등의 유출을 추적하기 위한 워터마킹(핑거프린팅) 기술이 사용되고 있다. DRM 기술의 특성상 하나의 기술로 구성되는 것이 아닌 다양한 기술들에 의해서 하나의 시스템을 구성하는 것이기 때문에 각 요소기술 간의 연계나 크래킹에 대비한 시스템의 설계와 구현도 매우 중요하며, 이에 대비한 요소기술로서

obfuscation이나 tamper-proofing 기술을 들 수 있다[7].

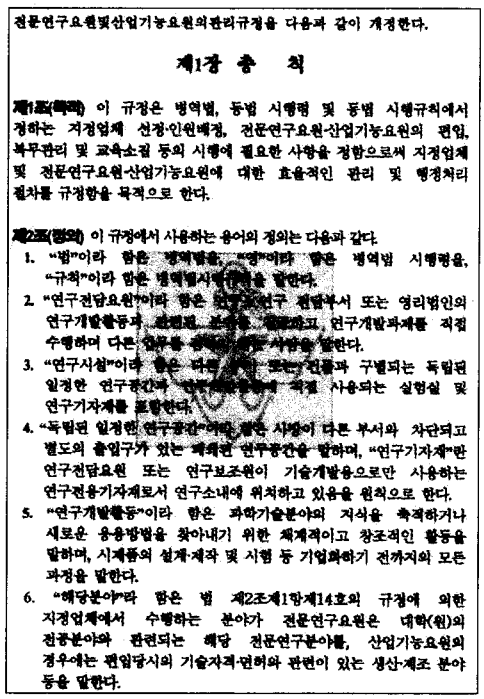
암호화 기술에 대해서는 2장의 DRM 기술소개에서 간단히 언급한 것처럼 대칭키 암호화 방식과 비대칭키 암호화 방식이 혼합적으로 사용되며, 대칭키 암호화 방식에서는 적어도 128비트 이상의 키 길이를 사용하는 것이 일반적이다. 또한 사용자 인증에 있어서는 단순히 ID와 비밀번호에 의한 것에서부터 생체인증이나 스마트카드를 이용하는 방법들이 병행되어 사용될 수 있는 기술이 된다.

본 고에서는 유출자의 추적을 위한 워터마킹(핑거프린팅) 기술과 크래킹을 방지하기 위한 두 가지 기술에 대해서 간략히 소개하도록 하겠다.

4.1 Watermarking(Fingerprinting)

워터마킹 기술이란 콘텐츠의 저작권 보호를 위해서 개발되기 시작한 기술로서 콘텐츠에 저작권 정보를 은닉하여 향후에 저작권 분쟁이 일어났을 때, 저작권 확인 등을 위해서 사용될 수 있는 기술이다. 이러한 워터마킹 기술은 가시적으로 확인이 가능한 워터마킹과 확인이 불가능한 워터마킹 기술로 나눌 수 있으며, 워터마킹 정보를 추출하기 위해서 원본이 필요한 경우와 그렇지 않은 경우로 나눌 수 도 있다[8].

이러한 워터마킹 기술은 그 응용분야가 매우 다양하며, 은닉되는 정보가 저작권자에 대한 정보인 경우에는 워터마킹으로 사용자에 대한 정보이면 핑거프린팅으로 구분된다. 즉, 핑거프린팅 기술은 출력문서의 어느 한 부분에 사용자에 대한 정보를 함께 출력함으로써 향후 내부 문서가 유출되었을 때, 유출자를 추적하는데 활용할 수 있는 것이다. 가장 손쉬운 방법은 출력문서의 하단에 가시적으로 출력시간과 출력자에 대한 정보를 인쇄함으로써 사용자에게 유출에 대한 경각심을 심어주는 것이 되겠다. 그러나 이렇게 가시적인 정보는 사용자에 의해서 제거될 가능성이 매우 높기 때문에 사용자는 가시적으로 볼 수 없지만 문서 내부에 정보를 은닉함으로써 추적에 활용하는 기법이 더욱 적절한 방법이 될 수 있다. (그림 12)는 출력된 문서에 대해서 핑거프린팅 정보가 은닉된 문서 예를 나타내고 있다. 문서의 중앙에 있는 로고 속에는 본 문서에 대한 사용자 정보가 은닉되어 있기 때문에 유출된 문서에 대한 추적이 가능하다.



전문연구요원및산업기능요원의관리규정을 다음과 같이 개정한다.

제1장 총 칙

제1조(목적) 이 규정은 병역법, 동법 시행령 및 동법 시행규칙에서 정하는 지정업체 선정·인원배정, 전문연구요원·산업기능요원의 편입, 복무관리 및 교육소집 등의 시행에 필요한 사항을 정함으로써 지정업체 및 전문연구요원·산업기능요원에 대한 효율적인 관리 및 행정처리 절차를 규정함을 목적으로 한다.

제2조(정의) 이 규정에서 사용하는 용어의 정의는 다음과 같다.

1. "법"이라 함은 병역법을, "영"이라 함은 병역법 시행령을, "규칙"이라 함은 병역법시행규칙을 말한다.
2. "연구전담요원"이라 함은 연구소(연구 전담부서) 또는 영리법인의 연구개발활동과 관련된 업무를 전담하고, 연구개발과제를 직접 수행하며 다른 업무를 겸직하지 않는 사람을 말한다.
3. "연구시설"이라 함은 다른 시설 또는 건물과 구별되는 독립된 일정한 연구공간과 연구활동에 직접 사용되는 실험실 및 연구기자재를 포함한다.
4. "독립된 일정한 연구공간"이라 함은 사람이 다른 부서와 차단되고 별도의 출입구가 있는 폐쇄된 연구공간을 말하며, "연구기자재"란 연구전담요원 또는 연구보조원이 기술개발용으로만 사용하는 연구전용기자재로서 연구소내에 위치하고 있음을 원칙으로 한다.
5. "연구개발활동"이라 함은 과학기술분야의 지식을 축적하거나 새로운 응용방법을 찾아내기 위한 체계적이고 창조적인 활동을 말하며, 시제품의 설계·제작 및 시험 등 기업화하기 전까지의 모든 과정을 말한다.
6. "해당분야"라 함은 법 제2조제1항제14호의 규정에 의한 지정업체에서 수행하는 분야가 전문연구요원은 대학(원)의 전공분야와 관련되는 해당 전문연구분야를, 산업기능요원의 경우에는 편입당시의 기술자격·면허와 관련이 있는 생산·제조 분야 등을 말한다.

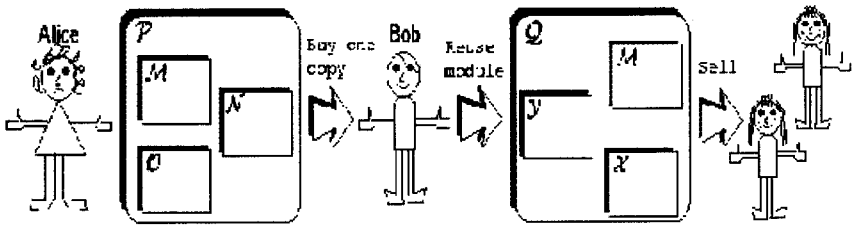
(그림 12) 핑거프린팅 된 출력문서

4.2 Obfuscation

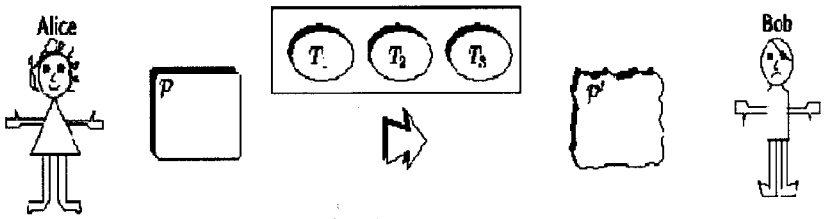
Obfuscation은 역공학분석에 의한 공격을 방어하는 기술이다. 역공학이란 공격자가 다른 사람의 프로그램에서 어떠한 모듈을 가져와서 자기 자신의 프로그램에 그 모듈을 다시 사용하는 것을 말한다. (그림 13)에서는 Bob이 Alice의 프로그램 P에서 모듈 M을 추출하여 자신의 프로그램 Q에 모듈 M을 다시 사용하고 있다.

이러한 공격을 막기 위해 obfuscating 변환을

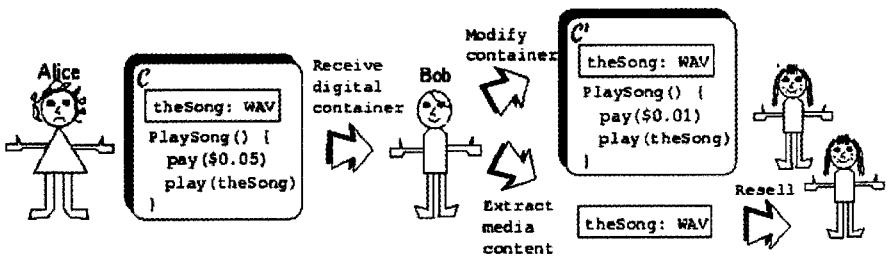
통하여 프로그램은 동일하게 작동하지만, 외부 공격자에게는 훨씬 프로그램을 이해하기 어렵게 만드는 기술이 obfuscation이다. (그림 14)에서는 Bob이 Alice의 프로그램 P에서 모듈을 사용하려고 하지만, 소스코드가 obfuscating 변환 T1, T2, T3에 의해 변환되어 있기 때문에 사용할 수가 없게 된다.



(그림 13) 역 공학 공격



(그림 14) Obfuscation



(그림 15) Tampering 공격

(그림 16) Tamper-proofing

4.3 Tamper-proofing

Tamper-proofing 기술은 부정조작, 즉 tampering에 대한 방어기술이다. 여러 가지 tampering이 소프트에어에 적용될 수 있겠지만, 이러한 tampering이 가해졌을 때, tampering 검출 시스템을 통하여 tampering을 감지하게 되고, 프로그램이 정상작동이 아닌 오류 동작을 하게끔 만드는 기술이 tamper-proofing 기술이다. (그림 15)에서 Bob은 디지털 콘텐츠 C로부터 wav 파일을 추출해 내거나, 보다 낮은 지불정보로 콘텐츠에 대한 tampering 공격을 하고 있다. 이러한 공격에 대해서 (그림 16)에서 Alice는 콘텐츠 S에 대하여 tamper-proofing 코드 T를 더해 줌으로써, 만일 콘텐츠 S에 대한 tampering이 감지되었을 경우 프로그램이 작동하지 않도록 해 준다.

5. 결 론

기업 내에서 업무의 효율성을 위해서 개별적으로 보존되거나 작성되는 다양한 정보들을 하나의 데이터베이스로 저장하고 공동으로 활용하기 위한 KM이나 EDMS의 도입이 활발히 이루어지고 있다. 그러나 이러한 디지털 문서들은 매우 손쉽게 복제가 가능하며, 초고속 통신망을 통해서 시공간을 초월하여 전달될 수 있다는 약점을 가지고 있다. 따라서 기업 내부 정보의 유출을 방지하면서 업무의 효율성을 높이기 위한 방안이 요구되고 있으며, 이에 부응하는 기업 내부 정보 유출 방지 기술이 등장하였다.

대부분 기업들의 초창기 정보화 과정에서는 네트웍 보안에 치중하여 방화벽이나 침입탐지 시스템 혹은 침입방지 시스템을 설치하여 외부 침입자를 차단하기 위한 노력에 집중하였으나 대다수의 기업 내부 정보 유출 사례가 내부자의 소행이라는 것이 밝혀지면서 업무의 효율성이라는 측면과 기업 내부 정보 보안이라는 두 마리 토끼를 잡을 수 있는 효과적 방법으로 이러한 보안 기술을 채택하고 있는 것이다.

과거에 기업 내의 정보들이 디지털화되기 이전에도 산업스파이에 의한 기업비밀의 유출이 있었지만 이러한 과정은 물리적인 보안시설을 뚫고 들어가야 하는 어려움이 있기 때문에 빈번하게 일어날 수 없는 일이었다. 그러나, 디지털 시대에서는 12세의 소년들 조차도 국가 주요시설의 컴퓨터 시스템에 침입하여 중요자료를 열람하거나 불법적으로 빼돌리는 것이 가능하다. 인터넷이라는 네트웍은 시공간을 초월하여 모든 사람들을 연결해 주기 때문에 물리적인 보안시설은 의미가 없어지고 불법적인 사용자를 기술적으로 어떻게 무력화시킬 것인가가 중요하다. 방화벽이나 사용자 인증과 같은 절차가 기존의 1차적인 기업 내의 디지털 정보를 지키기 위한 수단이었다면 디지털 정보에 대한 권한 관리와 암호화 등을 통해서 불법 사용자의 의지를 무력화시키는 보안기술은 차세대 디지털 정보보호 기술이라 하겠다.

창과 방패와 같이 크래킹을 시도하는 불법 사용자들에 대해서 보다 완벽한 보안 기술을 개발하기 위한 노력이 이제는 종합적인 보안기술의 집적으로 완성되어가고 있다. 그러나, 이러한 기술의 완성 가운데에서는 실질적으로 구현단계에서 보이지 않는 실수에 의해서 틈새를 만들어 줄 수 있기 때문에 섣불리 기술적 구조를 구현하여 시장에 진출하려는 무리한 시도보다는 체계적인 구조설계와 크래킹의 방지책을 고려하여 기술적 구조를 완성하려는 노력이 필요하다. 이러한 기술적 노력과 더불어 신뢰로 이루어진 사회를 구현해나가는데 우리모두 노력한다면 기업의 경쟁력 향상을 위해서 서로의 지식을 공유하는데 걸림돌을 제거해 나갈 수 있을 것이다.

참고문헌

[1] 조선일보 1998. 2. 18일자 기사

[2] 정연서, 류걸우, 남택용, 손승원, "사이버 위협에 대한 보안 솔루션 기술 동향", 한국전자통신연구원 주간기술동향, 제1068호, pp.1-14, Oct., 2002.

[3] J. Dubl and S. Kevorkian, "Understanding of DRM", IDC White Paper, 2001.

[4] "DRM White Paper" - Sonera Plaza Medialab, Feb., 2002.

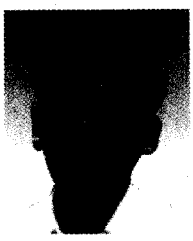
[5] 김종원, "디지털 저작권 관리기술", 정보보호 21, 제35호, pp.100-103, July, 2002.

[6] "Document SAFER", MarkAny White Paper, 2002.

[7] C. S. Collberg and C. Thomberson, "Watermarking, Tamper-Proofing, and Obfuscation - Tools for Software Protection", U. of Arizona, TR, Mar., 2000.

[8] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking Digital Image and Video Data", IEEE SP Mag., Vol.17, no. 5, pp.20-46, Sep. 2000.

저자약력



김 종 원

1989년 서울시립대학교 공과대학 전자공학과(공학사)

1991년 서울시립대학교 대학원 전자공학과(공학석사)

1995년 서울시립대학교 대학원 전자공학과(공학박사)

1995년 ~ 1996년 과학기술정보연구원 선임연구원

1996년 ~ 2000년 주성대학 정보통신학과/음향전자기기학과 조교수

2000년 - 현재 (주)마크애니 부설연구소장

관심분야 : 디지털 워터마킹, 저작권 보호기술, 디지털 신호처리

최 종 욱

1978년 ~ 1982년 아주대학교 공대 산업공학과(학사과정)

1982년 서울대학교 대학원 경영학과(석사과정)

1982년 ~ 1988년 Univerity of South Carolina 유학 (〈MIS/인공지능〉박사)

1985년 ~ 1986년 Institute of Information Management, Technology and Policy at University of South Carolina(Research Assistant-'C' Programmer)

1986년 ~ 1987년 Johnson C. Smith University (Charlotte, NC)

1988년 ~ 1991년 한국과학기술원(KIST)시스템공학 센터 인공 지능 연구부 지식 처리 연구실 실장 (선임연구원)

1991년 - 현재 상명대학교 소프트웨어학부(교수)

2000년 - 현재 주식회사 마크애니(대표이사)