협업자료의 원활한 유통을 위한 정보 보안 강화 방안 연구

이영우*, 오승엽
충남대학교 공과대학 전자공학과

Study on the methods of Information security strengthening for the online data sharing

Young-Woo Lee*, Seung-Hyueb Oh
Dept. of Electronic Engineering, ChungNam Univ.

Abstract - 오늘날에는 국가 간의 기술경쟁이 더욱 치열해 지면서, 국가 경쟁력 확보를 위하여 최단기간 내에 최고의 성과를 얻을 수 있도록 협업 정보를 가상공간상에서 지원하기 위한 국가차원의 "소프트 인프라"에 대한 필요성이 강조되고 있다. 기업들은 저렴한 인터넷 망을 사용하지 못하고 상당한 비용의 전용회선을 협업자료의 유통을 위하여 지출하고 있는 것이다. 또한, 기업 내부에는 외부 웹 하드 ASP 사업자들을 통한 웹 하드 서비스를 제공받기 위하여 년간 특정 금액을 지속적으로 자료 유통을 위해서 그 대가를 지불하고 있다. 본 논문에서는 기업 내 협업자료를 업무 환경 속에서 효율적으로 유통시키기 위한 정보 보안 강화 방안을 제시하고자 한다.

1. 서 론

오늘날에는 국가 간의 기술경쟁이 더욱 치열해 지면서, 국가 경쟁력 확보를 위하여 최단기간 내에 최고의 성과를 얻을 수 있도록 협업 정보를 가상공간상에서 지원하기 위한 국가차원의 "소프트 인프라"에 대한 필요성이 강조되고 있다.[1]

또한, 기업 내 작업의 대부분이 조직 및 개인 간 협업을 통하여 이루어짐에 따라 협업에 활용되는 자료의 유통이 많아지고 있다. 이러한 협업자료는 기업 내에서 특별히 정해지지 않은 룰에 따라 파일서버 또는 외부 및 공유의 폭이 큰 웹 하드 ASP 서비스를 통하여 자료 유통 및 저장을 하고 있는 실정이다. 따라서 업무 특성에 맞는 파일관리가 불가능할 뿐 아니라 보안적인 부분에서는 특히 취약한 약점을 가지고 있다.

사내 협업 자료에 대한 리스크 부분은 크게 순수 보안적인 측면과 보안적 측면을 보완하기위한 경제적인 측면으로 분할이 가능하다. 보안적인 측면은 기존 파일서버 및 외부 ASP 서비스를 이용하여 자료 유통 시 암호화, 위변조 관리 등에 대한 보안대책이 전혀 고려되지 않는다. 이러한 보안관련 취약성은 최근 들어 급증하고 있어 이에 대한 대책이 시급한 상황이다. 경제적인 측면은 앞에서 언급한 보안적인 측면을 해소하기 위하여 투입되는 비용이다.

기업 대 기업으로 협업을 위하여 빈번히 자료 교환이 이루어지고 유통되는 데이터가 고도의 보안 관리를 요구하는 경우 대부분의 업체는 이를 위하여 업체 대 업체 간 전용회선을 구축하고 이를 통하여 자료를 주고받는다. 기업들은 저렴한 인터넷 망을 사용하지 못하고 상당한 비용의 전용회선을 협업자료의 유통을 위하여 지출하고 있는 것이다. 또한, 기업 내부에는 외부 웹 하드 ASP 사업자들을 통한 웹 하드 서비스를 제공받기 위하여 년간 특정 금액을 지속적으로 자료 유통을 위해서 그 대가를 지불하고 있다.

본 논문에서는 기업 내 협업자료를 업무 환경 속에서 효율적으로 유통시키기 위한 정보보안 강화 방안을 제시하고자 한다.

2. 자료 유통 보안 필요성

2.1 자료 유통 보안사고 사례

각 기업에서는 내부정보 보안에 대한 임직원 교육은 철저히 하고 있으나, 임직원이 사용하는 시스템 상에서는 이를 지원해주지 못하고 보안시스템이 취약한 상황이다 보니 대규모 고객개인정보 유출 사태, 기업의 중요 기밀문서의 유출 사건 발생 등으로 경제적인 손실뿐만 아니라 기업 이미지에 큰 타격을 입고 있다. 또한 이런 사건들이 대부분이 사내직원을 통해 이루어지고 있어 보안에 대한 경각심을 크게 일깨워 주고 있다.

<표 1> 자료 유통 중 보안사고 사례

업체명	내용	발생년도
국민은행	·인터넷 복권 구매 홍보메일을 발송하는 과정에서 신상정보를 실수로 첨부하여 고객 3만2천여명의 정보 유출 ·1,026명의 피해자로부터 30억7400만원에 달하는 손해배상 청구소송	2006
인터넷 사업자	·개인KT, 하나로텔레콤, 두루넷, 온세통신 등 국내 4대 인터넷 서비스 업체의 770만 가입자 정보 유출 ·이름, 주소, 주민등록번호, 전화번호, ID, 고객가족관계 등이 유출됨 ·1,026명의 피해자로부터 30억7400만원에 달하는 손해배상 청구소송	2007
금융감독원	·금융감독원 직원이 업무 관련 내부 자료들을 인터넷 웹하드에 올려 보관하던 중 자료가 외부로 유출되는 사고 발생	2007

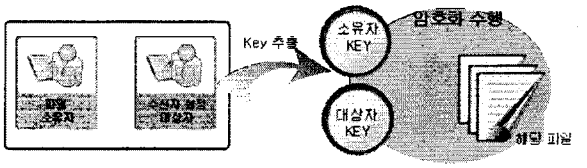
2.2 기업 내 보안사고 발생으로 인한 피해

기업 내 보안사고 발생 시 기업은 그에 따른 막대한 피해를 초래하게 되고 이는 직접적 피해와 간접적 피해로 구분해 볼 수 있다. 직접적 피해는 기업 내 관리되는 핵심 기술 및 기밀 문서가 유출되어 타 기업 및 외국 기업에 해당 정보가 전달 됨에 따른 사업적 피해이다. 이는 기업에 매출 하락 뿐 아니라 국가 내 핵심기술의 유출로 인한 국가 경쟁력 약화를 초래한다. 간접적 피해는 기업 내 정보유출 사고로 인한 대외 이미지 손상에 따른 피해이다. 이는 소비자에 대한 기업의 불신으로 이어져 그 손실 여파에 대한 복구가 어려우며 복구 기한 또한 장기화 되어 사실상 그 회복이 어렵다.

3. 정보 유통과정의 정보 보안 강화 방법

3.1 파일 암호화

파일 별로 패스워드를 각각 지정 및 파일 암호화 기법을 사용하여 파일 유통 시 파일이 암호화된 형태로 주고 받을 수 있다. AES, RSA, MD5등의 강력한 암호화 방식으로 암호화된 파일은 현실적인 시간 내에 풀어낼 수 없음으로 서버의 해킹 또는 디스크 도난 등의 비상상황에서도 완벽한 보안성을 확보한다.

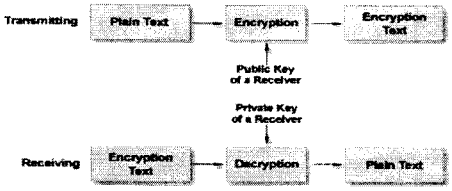


<그림 1> 파일 암호화 처리 모식도

1998년을 기점으로 표준 기한이 만료된 DES(Data Encryption Standard)를 대체할 블록 암호의 필요성에 따라, NIST에서는 향후 정부와 상업계에서 사용할 수 있는 강한 암호화 알고리즘 표준으로 AES(Advanced Encryption Standard)의 개발을 추진하였다. NIST는 3DES보다 더 효율적이고 안전하며 로얄티가 없어야 하는 등을 만족하는 알고리즘을 공모하고, 3년여에 걸쳐 15개의 후보 알고리즘을 공개적으로 평가하여, 2000년 10월 2일 최종 AES알고리즘을 선정, 발표하였다. AES에 채택된 블록암호는 Daemem과 Rijmen에 의해 개발되고 RIJNDAEL로 명명된 알고리즘으로 DES와 3DES를 대신하여 새로운 업계 표준으로 자리잡고 있다. AES는 2001년 12월, 정식으로 표준화가 완료되었다.[2] AES는 키의 크기(블록의 크기)로 128, 160, 190, 224, 256비트를 사용할 수 있으며, 미국 표준으로 인정받은 것은 128비트이다.

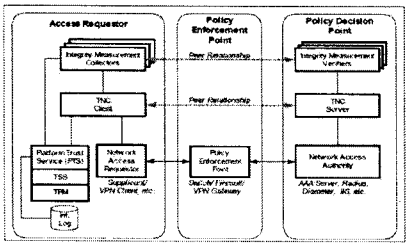
또한, RSA(Rivest Shamir Adleman)는 공개키 암호화 알고리즘의 하나로 현재 전자 상거래 등에 광범위하게 사용되고 있다. 1997년 론 리베스트(Ron Rivest), 아디 셰미르(Adi Shamir), 레오나르드 아델만(Leonard Adleman)등 3명의 수학자에 의해 개발된 알고리즘으로 인터넷 암호화 및 인증시스템을 말하며, RSA라는 이름은 이 3명의 이름 글자를 딴 것이다. 이 세 발명자는 이 공로로 2002년 튜링상을 수상했다. RSA 암호체계의 안정성은 큰 숫자를 소인수분해하는 것이 어렵다는 것에 기반을 두고 있다.

만약 큰 수의 소인수분해를 획기적으로 빠르게 할 수 있는 알고리즘이 발견된다면 이 암호 체계는 가치가 떨어질 것이다. 1993년 피터 쇼어는 쇼어 알고리즘을 발표하여 양자 컴퓨터를 이용하여 임의의 정수를 다항 시간 안에 소인수분해 하는 방법을 보였다. RSA암호화 알고리즘은 1983년 발명자들이 소속되어 있던 매사추세츠 공과대학교에 의해 미국에 특허로 등록되었고, 2000년 9월 21에 그 특허가 만료되었다.



<그림 2> 공개키 암호화 블록 다이어그램

RSA는 두 개의 키를 사용한다. 여기서 키는 메시지를 열고 잠그는 상수(constant)를 의미한다. 이 중 공개키(public key)는 모두에게 알려져 있으며, 메시지를 암호화(encrypt)하는데 쓰여진다. 이렇게 암호화된 메시지는 개인(비밀)키(private key)를 가진 자만이 해독(decrypt)하여 열어볼 수 있다. 다시 말하면, 누구나 어떤 메시지를 암호화할 수 있지만, 그것을 해독하여 열람할 수 있는 사람은 개인키를 지닌 단 한 사람 뿐인 것이다. RSA는 소인수분해의 난해함에 기반하여, 공개키만을 가지고는 개인키를 쉽게 유추할 수 없도록 디자인 되어 있다. 보다 이해하기 쉬운 예를 들자면, A라는 사람에게 B라는 사람이 메시지를 전달하고자 할 때, B는 A의 열린 자물쇠를 갖고 그의 메시지를 봉인하고, 그런 다음 A에게 전해주면, 그 자물쇠의 열쇠를 가지고 있는 A만 그 메시지를 열어보는 식이 된다. 중간에 그 메시지를 가로채는 사람은 그 열쇠를 가지고 있지 않으므로 메시지를 열람할 수 없다.[3]

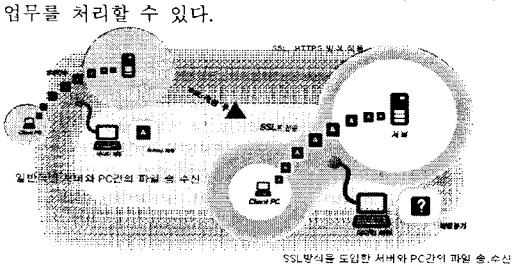


<그림 3> RSA 운영 흐름도

마지막으로, MD5(Message-Digest algorithm 5)는 128비트 해쉬를 제공하는 암호화 해쉬 함수이다. RFC 1321로 지정되어 있으며 수많은 프로그램과 파일의 무 결성 검사에 사용된다.[4]

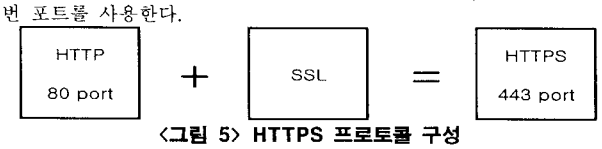
3.2 네트워크 구간 암호화

파일 암호화와 별개로 네트워크에 대한 추가적인 암호화를 위하여 SSL과 HTTPS를 적용하여 파일 송수신 뿐만 아니라 웹 컨텐츠도 모두 암호화 하여 처리하여 보안성이 취약한 인터넷 망에서도 안전하게 업무를 처리할 수 있다.



<그림 4> 네트워크 구간 암호화

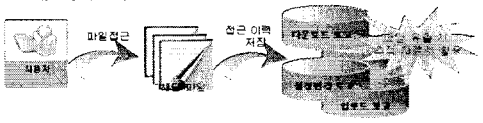
HTTPS는 넷스케이프에 의해 개발된 웹 프로토콜로서, 사용자의 페이지 요청들과 웹서버에 의해 반환되는 페이지들을 암호화하고 해석하는데 사용된다. HTTP는 실제로 SSL을 정규 HTTP 응용계층 하에서 서브 계층으로서 사용한다. HTTP가 하부계층인 TCP/IP와의 상호작용을 위해 80번 포트를 사용하는데 비해, HTTPS는 443번 포트를 사용한다.



<그림 5> HTTPS 프로토콜 구성

3.3 파일 접근이력 관리

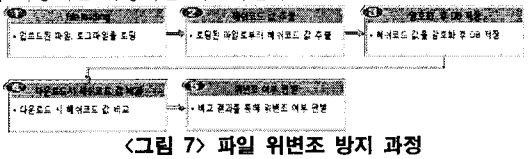
유통되는 파일에 대한 업로드, 다운로드, 설정 변경 등 사용 내역 기록 조회기능을 제공하고 이력 내에는 사용자명과 파일 송수신 시 사용된 PC의 IP 정보까지 기록됨에 따라 추후 악의에 의한 파일 유출이 시도 될 경우 파일 유출 경로의 추적이 가능하도록 한다.



<그림 6> 파일 이력관리

3.4 파일 위변조 방지

유통자료 체크섬 값을 자료 저장 시 체크하여 시스템적으로 보관하고 자료가 유통되는 시기에 이를 비교하여 파일이 원본과 차이가 있을 경우 사용자에게 알려줌으로써 보안상 중요한 파일이 위,변조되어 사용되는 불상사를 최소화한다.



<그림 7> 파일 위변조 방지 과정

위변조 검사를 위한 체크섬으로는 해시 알고리즘(hash algorithm)이 적합하며, 이는 임의의 데이터로부터 일종의 짧은 "전자지문"을 만들어 내는 방법이다. 해시 함수는 데이터를 자르고 치환하거나 위치를 바꾸는 등의 방법을 사용해 결과를 만들어내며, 이 결과를 흔히 해시값(hash value)이라 한다.

3.5 사용자별 파일 사용횟수 제한

유통자료에 대한 유효기간을 설정할 수 있으며, 파일의 유효기간을 할당 받은 파일은 해당 유효기간이 만료되면 자동 삭제 된다. 또한, 파일의 다운로드 횟수를 제한할 수 있어 필요이상으로 공유되는 것을 방지하여 자료의 보안성을 강화한다.

3.6 접속 제한

접속하는 사용자에 대한 통제기능으로 허가된 IP 및 MAC Address에서만 접속이 가능하게 한다. 이를 통해 인증되지 않은 사용자 및 인증된 사용자라도 인증된 PC에서만 접속을 하도록 제한한다.

<그림 8> 접속제한 인증 과정

4. 결 론

기업 내 업무 환경이 더욱더 분업화 되고 기업 간에도 분업화 되어감에 따라 자료 공유를 통한 협업은 필수적인 요소이며 더욱더 그 양 또한 증가 할 것이다. 이러한 빈번한 자료 공유 환경 속에서 기업 내 자료 유통에 대한 보안 사고가 속출 하고 보안에 대한 관심은 증폭 되고 있으나 이에 대한 해결책을 구성한 기업은 현재까지 미비한 상태이다. 이러한 자료 보안에 대한 중요성은 기업 내 경쟁력뿐만 아니라 국가 경쟁력과 직결되는 문제임에 따라 기업은 협업에 대한 효율성과 보안성 강화라는 두 가지 요건을 모두 충족 시켜야 한다.

본 논문에서 제시한 정보보안 강화 방안은 자료 유통 시 발생할 수 있는 보안적 문제점을 최대한 해결할 수 있는 요소이다. 파일 자체에 대한 보안성으로 파일 암호화와 파일 위변조 방지를 통하여 각각의 파일에 대한 보안성을 확보하고 해당 파일이 송수신되는 네트워크 구간 암호화 및 사용자별 파일 사용횟수 제한을 통하여 파일이 유통되는 시기의 보안성을 강화 할 수 있다. 아울러, 파일 유통에 대한 모든 이력 정보는 추후 유출 경로 추적으로 유통되는 자료들에 대한 강력한 보안성이 확보될 것이다.

[참 고 문 헌]

[1] 성원경, 정한민, 박동인, "협업 연구 지원을 위한 시멘틱 웹 기반 지식 정보 공유·유통 플랫폼", 한국정보과학회지, 제24호, pp65-74, 2006.5

[2] Joan Daemen and Vincent Rijmen, "The Design of Rijndael: AES - The Advanced Encryption Standard", ISBN 3-540-42580-2, 1992

[3] R. Rivest, A. Shamir, L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems Communications of the ACM", Vol. 21 (2), 1998.

[4] Berson. Thomas A, "Differential Cryptanalysis Mod 232 with Applications to MD5". EUROCRYPT: 71-80. ISBN 3-540-56413-6, 1992