인트라넷 보안을 위한 ACM기반 웹 보안 접근 제어 시스템의 설계 및 구현

조 남 덕[†] · 박 현 근[††]

요 약

기업들이 많이 사용하고 있는 인트라넷 시스템은 기본적으로 사용자인증을 거치지만, 인가된 사용자임을 가장한 악의의 사용자들에 의해, 또는 웹 브라우저의 다양한 기능을 통한 사용자들의 실수로 정보가 유출, 편집, 삭제될 수 있다. 따라서 이러한 정보에 대해서 비합법적인 사용, 부분적인 조작을 통한 자료의 변형 또는 도용 등의 불법적 유출을 막기 위한 방법이 필요하다. 본 논문에서는 인트라넷상의 정보를 보안하기 위해 효율적인 보안정책을 세움으로써 유연성 있는 ACM기반 웹 보안 접근제어(Web Security Access Control)시스템을 제안 한다. 웹 보안 접근 제어 시스템은 인트라넷 정보에 대하여 암/복호화를 수행함으로써 보안기능을 강화하였을 뿐만 아니라 기업의 부서 간 민감한 정보의 공유에 대하여 해당 보안 페이지에 권한을 달리 함으로써 효과적이고 유용한 접근 통제를 수행한다. 또한 클라이언트 PC의 여러 가지 기능 제어를 통해 악의적인 혹은 실수로 인한 정보유출을 방지한다.

키워드 : ACM기반 웹 보안 접근 제어 시스템, 인트라넷, 세큐인트라넷

Design and Implementation of ACM-based Web Security Access Control System for Intranet Security

Nam-Deok Cho[†] · Hyun-Gun Park[††]

ABSTRACT

Intranet system for use within an organization, usually a corporation, is to basically pass through user authentication, but information can be leaked, modified, and deleted by malevolent users who disguise an authorized user or due to user's mistakes in using various functions of web browser. Thus, there is a need for measures to protect the information from illegal use, transformation through partial modification, and illegal leakage such as fraudulent use. This paper presents a flexible Web Security Access Control system based ACM which provide efficient security policy to protect information in intranet. This Web Security Access Control system not only enhances security by performing encryption/decryption of information in intranet but also, for sharing confidential information among departments, performs effective and useful access control by assigning different authority to the secured web page. And, by controlling the functions of client PC in various ways, information leakage on malicious purpose or by mistake can be prevented.

Key Words : ACM(Access Control Matrix)Web Based Security Access Control System, Intranet, SecuIntranet

1. 서 론

정보의 바다라 불리는 인터넷이 널리 퍼지면서 현대인들에 있어서 제일의 정보원으로써 자리매김 하고 있다. 이와 동시에 인터넷을 통해서 텍스트, 이미지, 오디오 데이터의 인터넷 전송이 일반화 되었고, 이에 따라 인터넷을 요약하여 하이퍼 멀티미디어 정보검색시스템이라고 할 수 있다. 이러한 인터넷의 발전에 힘입어 현재의 컴퓨팅 환경은 과거보다 복잡해지고, 다양한 환경에서 실행되는 분산 환경으로 발전 되어왔다. 이에 사용자들은 인터넷을 통한 가상공간에서 서로 정보를 공유하고 협력할 수 있는 시스템 개발을 요구하게 되었고, 그 결과로 BSCW(Basic Support Cooperative Work), Domino 등의 많은 협업시스템이 개발되었다[5]. 또한 많은 기업들이 위의 협업시스템을 포함한 인트라넷(Intranet)을 통하여 정보를 공유하고 재사용하고 있다. 그러나 이와 같은 인터넷이 다양한 서비스로 이용되면서 보안성 문제[1, 2, 3]가 제기되었고, 이러한 보안성 문제는 인트라넷으로도 이어졌다. 기본적으로 인트라넷은 사용자인증을 거치지만, 인가된 사용자임을 가장한 악의의 사용자들에 의해, 또는 웹 브라우저의 다양한 기능을 통한 사용자들의 실수로 정보가 유출, 편집, 삭제될 수 있다. 따라서 이러한 정보에 대해서 불법적인 사용, 부분

† 준 회 원 : 소프트캠프(주) 연구원
†† 정 회 원 : 숭실대학교 전산원 교수
논문접수 : 2005년 5월 24일, 심사완료 : 2005년 9월 27일

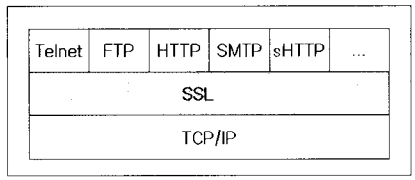
적인 조작을 통한 자료의 변형 또는 도용 등의 불법적 유출을 막기 위한 방법이 필요하다. 본 논문에서는 인트라넷상의 정보를 보안하기 위해 효율적인 보안정책을 세움으로써 유연성 있는 접근 권한 관계를 하나의 테이블로 나타낸 ACM 기반 웹 보안 접근제어시스템인 SecuIntranet을 제안한다. 본 논문의 구성으로 2장에서는 기반연구로 웹 보안 방식과 접근 제어 방법에 대해서 알아보고, 3장에서는 SecuIntranet의 설계, 4장에서는 결과 및 평가에 대해서 논하고 5장에서는 결론과 향후 연구 과제를 제시한다.

2. 기반 연구

2.1 웹 보안 방식

2.1.1 채널 기반 웹 보안 방식

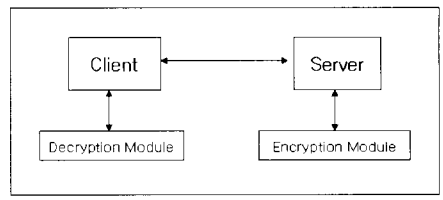
HTTP 계층과 TCP계층 사이에 존재하여 HTTP 메시지가 전달될 TCP 연결에 대하여 암호화 기술을 적용하는 방식이 있다. 이 경우 동일 TCP 연결상의 모든 HTTP 메시지에 대해 동일한 암호화 서비스를 제공하게 되는데 이를 채널 기반(Channel-based)방식이라 하며 SSL(Secure Socket Layer)이 대표적인 프로토콜이다. 넷스케이프사에서 개발된 채널 기반 방식인 SSL은 넷스케이프의 보급에 힘 입어 사실상의 웹 보안 표준으로 정착되었다[6]. IETF에서는 SSL3.0을 기반으로 TLS(Transport Layer Security) Protocol 1.0을 개발하였다[7]. SSL은 (그림 1)에서처럼, 인터넷 응용과 TCP/IP 통신 프로토콜 계층 사이에 존재하는 프로토콜이므로 웹을 위한 HTTP뿐만 아니라 Telnet, FTP등 다른 응용들에도 적용될 수 있다. 이와 같은 측면이 사실상의 웹 보안 표준으로 자리잡게 했지만, 새롭게 부각되고 있는 인터넷 전자상거래에서 필수적으로 요구되어 있는 전송 문서별 디지털 서명과 같은 기능을 제공하지 못하고 있는 약점은 보완해야 할 과제이다.



(그림 1) SSL과 타 프로토콜과의 관계

2.1.2 내용 기반 웹 보안 방식

Kerberos나 PGP와 같은 안정성이 인정되고 있는 기존 암호화 시스템과 연계하여 HTTP의 상위계층에서 보안 기능을 구현해 주는 것이 내용 기반 웹 보안 방식(Content-based)이다. 이 방식은 서버나 브라우저와 별도로 암/복호화를 수행해 주는 프로그램을 별도로 설치한다. 이 방법은 기존의 웹 시스템에 전혀 수정을 요구하지 않으면서 웹 보안 기능을 구현해 준다. sHTTP가 기존의 HTTP와 서버, 브라우저 프로그램을 수정해야 주어야 한다는 부담 때문에 실패한 것과 비교해 보면, 이 특징은 큰 장점으로 생각 할 수 있다. (그림 2)와 같이 독립적으로 암호 기능을 수행하는 외부 프로그램이 서버와 클라이언트에 연결 되어 있으며, 이 외부 프로그램은 HTTP 요청 및 응답 메시지의 암/복호화에 이용된다. 메시지가 서버와 브라우저를 떠나 전송되기 직전에 각 외부 프로그램에 보내지고, 암호화된 메시지들은 다시 서버와 브라우저로 보내져서 인터넷을 통해 전송된다. 이 방법의 가장 큰 장점은 기존의 웹 시스템에 아무런 수정을 요구하지 않는다는 것이다. 또한 전자우편 프로토콜인PGP 등 암호모듈은 웹 이외에도 여러 응용 프로그램들에게 보안 기능지원을 위해 이용될 수 있으므로, 한 시스템에 여러 가지 암호 프로그램을 설치하지 않아도 되는 장점이 있다. 그렇지만, 결국 웹 응용 외부에 위치하기 때문에 불필요한 처리 절차를 수행하게 됨으로써 수행시간이 길어진다는 단점이 있다[10].



(그림 2) 외부 프로그램을 이용한 방법 예

2.1.3 메시지 기반 방식

HTTP와는 독립적으로 존재하여 HTTP메시지의 바디(Body) 영역만을 암호화하는 방식을 메시지 기반 (Message-based) 방식이라고 한다. 이러한 방식에 따라 전송되는 트랜잭션 메시지별로 보안 기능을 제공하는 기술로 제안된 것이 SHTTP (Secure-HTTP)이다[11]. SHTTP는 전자상거래 응용 등에 사용하기에 적합하고 다른 방식에 비해 우수한 기능을 제공하여 제안 당시 주목을 받았으나 SSL에 밀려 확산에는 실패했다.

2.1.4 IP 주소기반 인증 방식

IP 주소기반의 인증은 클라이언트의 TCP 연결요청에 대해서 수행되어지는데, 서버는 연결 요청을 하는 클라이언트의 원격주소를 지명서버에게 질의하고 그 확인으로 원격 호스트의 도메인 이름을 응답받는다.그러나IP주소인증은 원격호스트에 대해서만 인증을 수행할 수 있고 서비스요청을 하는 클라이언트에 대한 인증이 불가능하다. 그리고 원격호스트에 대한 인증이 실패한 경우에도 서버는 클라이언트의 요구를 수행하게 되므로 보안상에 문제점을 내포한다[13, 14].

2.2 Access Control Matrix 모델

ACM(Access Control Matrix) 보안 모델은 주체(Subject)와 객체(Object)간에 허가된 접근 권한에서 주체를 행(row)으로 객체를 열(Column)로 하여 테이블로 나타낸 보안 모델이다. (그림 3)은 접근 권한 관계를 하나의 테이블로 나타낸 것이다. (그림 3)에서 하나의 예를 들어서 접근제어의 흐름을 살펴보면 Subject1은 Object1에 대해서 아무런 권한이 없으나 Object2에 대해서는 execute(실행) 권한을 그리고 Object3에 대해서는 execute(실행), read(읽기) 권한을 갖고 제어 됨을 알 수 있다[4, 8, 9].

	Object1	Object2	Object3
Subject1	-	(execute)	(execute, read)
Subject2	(read, write)	(execute)	-

(그림 3) ACM 테이블

2.3 관련 연구

2.3.1 Apache 서버

Apache 웹 서버는 웹 서비스를 제공하고 있는 웹 서버 중 가장 많이 이용하고 있는 웹 서버중 하나이다[12]. 이러한 웹 서버는 보안을 위해 사용자 인증이나 아이피(IP) 대역을 통해 인증을 하는 등의 방법을 취하지만 이러한 웹 서버로만의 방법은 인증을 통과하고 이미 클라이언트의 브라우저에 나타내어진 정보의 보안에는 취약하다. 즉, 브라우저의 다양한 기능이나 캡쳐 툴 같은 다른 프로그램에 의해서 웹 페이지 정보를 유출할 수 있다.

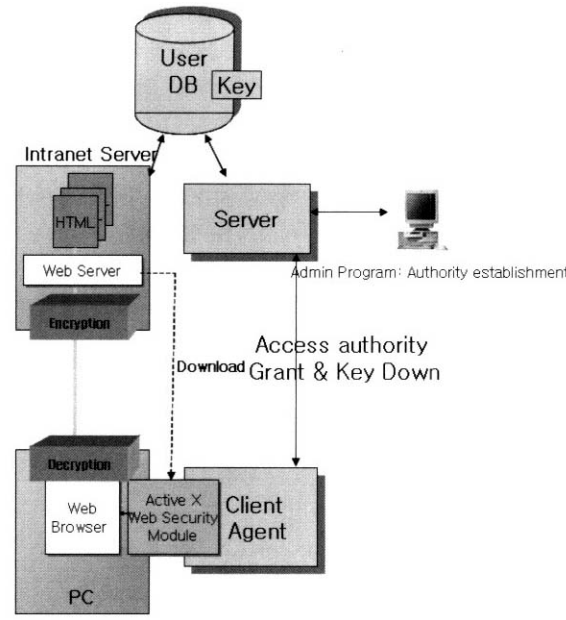
2.3.2 협업 시스템

협업 시스템은 인터넷을 통한 가상공간에서 서로 정보를 공유하고 협력할 수 있는 시스템이며[5], 주로 기업에서 많이 이용하고 있다. 이러한 협업시스템에도 보안문제가 대두되어 버전 업그레이드가 되면서 사용자별 접근제어가 강화되고 있다. 그러나 협업시스템은 정보 공유 우선시에 개발된 소프트웨어 이므로 사용자별 접근 제어 기능 자체가 제약이 있어, 이미 브라우저 상에 나타내어진 정보에 대해 프린트 스크린 키나 캡쳐 툴에 역시 취약하며, 또한 정말 중요하다 할 수 있을지도 모르는 첨부 파일에 대해서의 보안 및 접근 제어는 매우 취약하다.

3. 시스템 설계

본 논문에서 제안하는 웹보안 접근제어시스템인 SecuIntranet은 기업의 인트라넷 시스템에서의 정보 유출 방지와 각 부서간의 민감한 정보가 될 수 있는 사안에 대해서 사용자 별 접근 제어를 제공하기 위한 시스템이다. 본 시스템은 기본적으로 C/S(Client/Server)환경이며, 기존 인트라넷 시스템과 연동한다. 인가된 사용자에 대해서 웹 페이지를 보여줄 때에 서버에서는 암호화 모듈을 통해서 해당 웹 페이지를 내려주고, 클라이언트 프로그램이 이를 복호화 해준다. 복호화된 웹 페이지는 사용자에 따라 접근 권한을 달리 부여한다. 전체 시스템 구조는 (그림 4)와 같다.

(그림 4)에서의 UserDB는 사용자 데이터 베이스로써 사용자 아이디, 암/복호화 키, 사용자 이름등의 각종 사용자 정보를 포함하고 있다. 그리고 그 데이터베이스를 인트라넷 서버와 SecuIntranet의 서버가 공유한다. 그리하여 사용자가 클라이언트 에이전트 프로그램으로 인트라넷에 로그인 하였을 때 그 인트라넷의 권한을 SecuIntranet의 서버에서 할당받는다. 또한 관리자 프로그램도 SecuIntranet서버와의 통신을 통하여 사용자들의 권한을 설정한다.



(그림 4) 시스템 구조

3.1 클라이언트 에이전트

본 시스템의 클라이언트 에이전트는 백그라운드 프로그램으로, 윈도우가 부팅 시에 실행되며 로그 오프 시에 종료되는 프로그램이다. 이는 브라우저의 각종 기능을 제한하는 Active X를 포함하며 첨부파일에 대해 접근 제어를 웹 페이지에 대한 것과 똑같이 부여하기 위해 항상 실행되어져 있는 것이다. 즉 서버에서 설정한 모든 접근 권한 제어는 실제로 클라이언트에서 그 기능을 수행한다.

3.2 서버

서버 프로그램은 사용자 데이터베이스(DB)를 인트라넷 서버와 공유하면서 통신을 통하여 클라이언트에 권한을 부여하고, 관리자에 의한 권한설정을 반영한다. 클라이언트로의 권한 부여는 사용자 로그인이 성공하였을 경우 이미 설정되어 있는 그 사용자의 권한을 부여하며, 관리자는 관리자 프로그램에 의해서 각 사용자의 권한을 설정/변경하여 그 사항을 서버에 전달한다.

3.3 사용자 인증

사용자 인증은 기존 인트라넷 로그인을 그대로 이용한다. 사용자는 브라우저를 통해서 로그인을 하고 인증된 아이디로 서버로부터 해당 인트라넷 시스템의 접근 권한을 부여 받는다. 이때 로그인을 통과했다고 하더라도 해당 시스템에 읽기 권한 조차 없다면 그 사용자는 시스템에 접근 할 수 없다. 사용자 인증은 다음과 같은 사항이 요구된다.

- 사용자 데이타베이스(DB)는 인트라넷서버와 SecuIntranet 서버가 같은 것을 사용한다.
- 권한 서버에는 사용자에 대한 인트라넷 시스템에 대한 접근 권한이 설정되어 있다.
- 암/복호화 키는 사용자데이타베이스(DB)에 같이 저장되

어 있으며 로그인 성공시 부여받는다.
- Active X 컨트롤을 다운로드 하고 설치한다.

3.4 암/복호화

인증이 통과되면 인트라넷 서버는 클라이언트가 요구하는 웹 페이지를 내려 보낸다. 이 때 본 시스템에서 제공된 암호화API를 호출해줘서 해당 웹 페이지를 암호화한다. (그림 5)는 암호화API의 프로토타입이다. 암호화해 줄 데이터(웹 페이지 내용 중 암호화 할 문자열)를 source_string에 입력값으로 넣어주고 그 결과를 dest_string에 반환한다. 해당 페이지 전체를 암호화 하기를 원할 경우 해당 파일 경로를 source_string에 입력값으로 주면 된다.

```
function FileEncrypt().
{
        var vRe = DSSLATL.RequestFileEncrypt( source_string, Authrity, dest_string);
}
// [in] source_string : 암호화할 데이터.
// [in] Authority : 로그인한 사용자의 권한정보.
// [out] dest_string : 암호화 성공시 결과 데이터.
```

(그림 5) 암호화 API 프로토타입

클라이언트 PC에 다운받을 때까지 암호화 되어 있으므로 해당 웹 페이지는 안전하다.

다운 받은 웹 페이지는 클라이언트 PC에 설치된 Active X 컨트롤을 이용하여 복호화를 한다. 그 후 복호화 된 웹 페이지가 브라우저를 통해서 보여 진다. 또한 웹 페이지 전체를 암호화를 하면 성능상의 문제가 생길 수 있으므로 암호화 하기를 원하는 부분만 암호화 할 수 있는 부분 암호화 기능을 제공한다.

3.5 권한 제어

인증된 사용자는 권한 서버로부터 해당 시스템에 대한 권한을 부여 또는 제한 받는다. 제어 목록은 (그림 6)과 같다.

읽기 제어	해당 웹페이지 보기	0) 보기권한 없음 1) 보기권한 있음
프린트 제어	인쇄 차단을 통한 정보유출 방지	0) 인쇄권한 없음 1) 인쇄권한 있음
소스보기 제어	소스 보기 차단을 통한 정보유출 방지	0) 소스보기 불가능 2)소스 보기 가능
편집 기능 제어	편집을 통한 데이터 무결성 예침	0) 편집 불가능 1) 편집 가능
화면캡쳐 방지	각종 화면캡쳐툴을 이용한 멀티미디어 유출 방지	0) 화면캡쳐 불가능 1) 화면 캡쳐 가능
브라우저 기능 제어	브라우저 자체의 핫키, 메뉴 등의 제어를 통한 멀티미디어 유출 방지	

(그림 6) 접근 제어 목록

이와 같은 제어방식은 인트라넷 시스템을 사용하는데 있어서 기업 내의 부서 간에 권한을 달리 관리하는데 편리하며 사용이 쉽다. 또한 위 제어 목록에서의 기능들은 실제로 웹 브라우저에서 쉽게 정보를 유출할 수 있게 해주는 기능이므로 그 기능들을 제어한다는 것은 정보유출을 원천적으로 봉쇄하는 것이다.

3.6 첨부 파일 보안 및 접근 제어

사용자가 첨부 파일 요청시, 서버는 다운로드 시킬 때에 웹페이지를 암호화하는 동일한 방법으로 암호화를 해서 내려 보낸다. 암호화 헤더 정보에는 해당 웹페이지에 적용된 접근 제어를 포함한다. 이렇게 다운로드 된 파일은 제안된 웹 보안 접근 제어 시스템인 SecuIn tranet에 로그인 한 사용자만 열람 할 수 있으며, 인증이 통과 되었다고 하더라도 해당 권한으로만 그 파일을 사용할 수 있다. 또한 클라이언트 에이전트가 항상 실행되어 있기 때문에 인트라넷 시스템을 로그오프하고 브라우저를 종료한다고 하더라도 사용 가능하다.

3.7 관리자 프로그램

본 시스템에서는 사용자의 권한을 관리하는 관리자 프로그램을 제공한다. 관리자 프로그램으로 보안 관리자는 인트라넷 시스템에 대한 사용자 권한을 변경할 수가 있다.

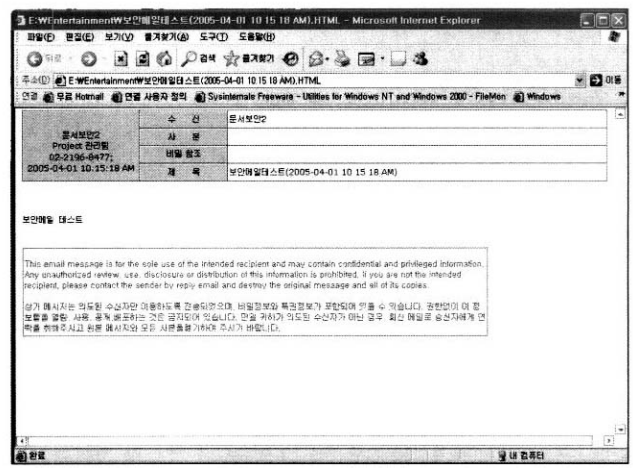
또한 접근 제어를 수행하려면 접근 제어 관리자가 필요하다. 이에 따른 별도의 프로그램이 요구되며 (그림 11)은 관리자 프로그램의 권한 설정 창을 보여준다.

4. 결과 및 평가

4.1 결과

앞장에서 인트라넷 시스템에서의 웹 보안 접근 제어 시스템에 대한 설계에 대해서 살펴보았다. 본 장에서는 본 시스템의 구현과 그 결과에 대해서 살펴본다.

(그림 7)은 본 시스템의 예제 웹 페이지 이다. 본 그림은 이 페이지에 읽기 권한이 있는 사람이 보았을 때 보여 지는 화면이다.

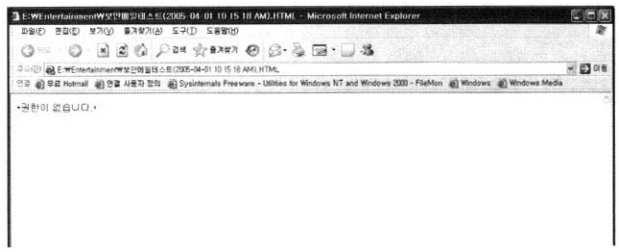


(그림 7) 읽기 권한이 있는 사람이 본 보안 웹 페이지

이 페이지를 소스 보기를 통해 실제 웹 페이지 내부를 살펴 보면 (그림 8)과 같다. (그림 8)은 위의 페이지가 암호화 되어 있음을 보여준다. $swsmanstart$은 암호화 시작점을 $swsmanend$은 암호화 끝나는 점을 나타낸다. 웹 페이지 전체를 암호화할 필요가 없을 경우 이러한 구분자를 두어 필요한 부분마다 시작점과 끝점을 표시하여 암호화 모듈을 호출하게 되면 부분만 암호화를 할 수 있다.

(그림 9)은 (그림 7)과 같은 페이지이나 읽기 권한이 없는 사람이 보았을 때 보여지는 화면이다.

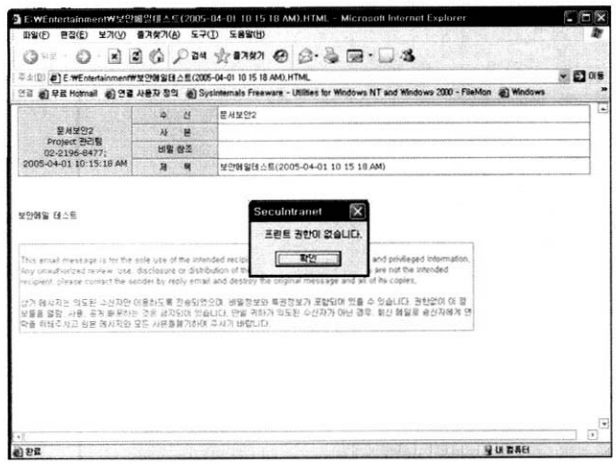
(그림 8) 암호화 된 보안 웹 페이지



(그림 9) 권한 없는 사람이 본 보안 웹 페이지

위와같은 절차에 따라 본 시스템은 암/복호화와 접근 제어로 인트라넷 시스템에 대한 보안과 접근 제어를 수행한다.

읽기 권한이 있는 사용자라도 프린트 권한이나 소스보기 권한, 편집권한이 없으면 해당 기능을 사용할 수 없게 된다. 즉, 예를 들어 프린트 권한이 없는 사용자가 웹 브라우저 메뉴의 인쇄를 통하여 해당 웹 페이지를 프린트 하려고 해도 "프린트 권한이 없습니다."란 메시지를 보여주고 인쇄를 할 수 없게 한다. (그림 10)은 읽기권한은 있어서 웹페이지를 열람한 사용자가 프린트권한이 없는 상태에서 인쇄를 하려고 했을때의 화면이다.



(그림 10) 프린트 권한이 없을 때의 화면

그리고 (그림 11)은 관리자 프로그램의 권한 설정 화면을 나타내고 있으며, 이를 통하여 관리자는 각 사용자의 인트라넷 시스템의 권한을 설정한다.

또한, 제안된 웹 보안 접근 제어 시스템을 적용한 결과 암호화 모듈이 별도의 프로그램이

아니라 API로 제공되므로 암호화 시간이 기존 시스템 보다 짧으며, 각 부서에 맞는 인트라넷 시스템이나 하부 메뉴에 대해 접근 제어를 할 수 있으므로 부서 간 민감한 정보의 보안적용에도 유용하다.

(그림 11) 관리자 프로그램의 권한 설정 창

4.2 평가

4.2.1 보안의 안전성

본 시스템은 사용자의 인증이 성공되어 해당 웹 페이지가 열람 되었다고 하더라도 해당 웹 페이지에 대해 그 이상의 권한이 없다면, 사용자는 고의적이든 실수든 그 정보를 유출 할 수가 없다. 즉 편집권한이나 프린트 불가능, 카피 앤 페이스트, 캡쳐 툴 차단 등이 설정되어 있으면 사용자는 프린트 스크린등의 키조작이나 별도의 프로그램을 이용하더라도 그 정보를 유출할 수 없다. 이러한 기능은 클라이언트에서 이루어지는 것이기 때문에 가능하다. 그리고 실제 인트라넷 환경은 웹 페이지 정보보다 첨부파일에 대한 정보가 더 중요한 경우가 많다. 본 시스템은 이러한 첨부파일을 보안 해줌으로써 정보유출을 막을 수가 있다. 또한 위와 같은 기능으로 사용자의 실수로 인한 정보유출도 막을 수 있으므로 안전하다 하겠다.

4.2.2 보안정책 수립

본 시스템은 웹 서비스 중 인트라넷 보안에 그 제한을 둔다. 기업에서의 인트라넷은 각 기업의 정보를 공유하지만 각 기업 내 부서끼리도 정보 공유에 민감한 부분이 있을 수 있다. 예를 들어 A라는 부서에서 생성한 문서를 B란 부서에서는 열람만 가능하게 하고, C란 부서에서는 A와 공통 작업을 하는 등의 이유로 모든 권한을 주되 변경이나 삭제를 할 수 없도록 하게하는 등의 요구가 있을 수 있다. 본 시스템은 이

를 충족시키며, 각 기업에 맞게 혹은 각 부서 및 업무에 맞게 보안 정책을 수립하게 해준다.

4.2.3 관련 시스템 비교

본 시스템을 기존의 관련된 타 시스템들과 특징을 비교하면 (그림 12)와 같다.

시스템	Apache	협업시스템	SecuIntranet
웹 페이지 암호화	O(SSL)	O	O
사용자 인증	O	O	O
접근제어(클라이언트)	X	△	O
첨부파일 암호화	X	X	O
첨부파일 접근제어	X	X	O
C/S환경과의 호환성	X	O	O

(그림 12) 관련 타 시스템과 비교

기업내의 인트라넷 환경하에서 기능은 실제 클라이언트에서 이루어지는 것이기 때문에 본 연구에서의 제안시스템은 인트라넷 환경하에서 클라이언트 접근제어가 가능하다. 또한 첨부파일에 대한 정보가 더 중요한 경우에 첨부파일을 보안해줌으로써 정보유출을 막을 수가 있다. C/S환경과의 호환성은 정보공유를 웹이 아닌 C/S 환경 하에서 한다고 하더라도 본 시스템은 서버에서 API 하나만 호출해 주면 되므로 호환이 용이하다.

5. 결론 및 향후 연구과제

본연구에서는 기존 인트라넷 시스템에 웹 보안 접근 제어 시스템을 적용하여 그 정보에 대하여 보안을 적용하고, 기업내의 부서 간 민감한 정보에 대해서 효과적이고 유연하게 접근 통제를 수행하게 하였다.

기존의 인트라넷 시스템도 이미 사용자 인증을 통하여 그 시스템을 사용하는 것이나, 인증은 통과했으나 악의적인 사용자이거나 혹은 악의적이진 않더라도 클라이언트 PC의 여러 기능으로 인해 실수로 정보를 유출할 수 있었다. 본 연구에서 제안한 인트라넷 보안을 위한 웹보안 접근제어 시스템에서는 그것을 봉쇄하였다. 예를 들어 어떤 부서에서 인트라넷을 통해 공유하는 정보를 어떤 사용자나 모든 권한을 갖고 그 정보를 사용하게 하는 것이 아니라, 즉 사용자마다 권한을 달리하여 신뢰도가 높은 사용자일수록 많은 권한을 주는 방법으로 악의적인 사용자에 의한 정보사용을 제한할 수 있다. 그리고 소스보기나, 프린트 등의 기능이 제한되어 있어서 실수로 인한 정보유출을 방지하며, 첨부파일보안 및 접근제어를 할 수 있다.

또한 암호화를 통해 인트라넷 정보를 보안하였고, 이 암호화가 별도의 프로그램이 수행하는 것이 아니라 인트라넷 시스템 내부에서 수행 해주는 것이므로 기존의 내용기반 웹 보안 방식 시스템보다도 속도가 빠르다.

향후 연구 과제로는 기업내의 부서 간 공유작업 문서가 있을 때에 그 문서 하나 하나에 대하여도 접근 제어를 할 수 있는 방법을 연구가 필요하다.

참 고 문 헌

[1] 강신각, "Web Security and Payments, WWW-KR 워크샵", 자료집, 4-2호, 1996.11.

[2] 박정수, 강신각, 박성열, "월드 와이드 웹 보안 기술 및 동향", 정보과학회지, 한국정보과학회, 1997.4.

[3] 강신각, 박정수, "월드 와이드 웹(WWW)의 보안기술", 정보처리논문지, 제 7권, 제2호, 2000.3.

[4] 김양석, 강주미, 원용관, "웹 기반 협업 시스템의 문서보안", 정보처리 추계학술발표 논문집, 제9권, 제2호, 2002.2.

[5] R.Bently, "Basic Support for Cooperative Work on the World Wide Web", International Journal or Human Computer Studies, 1997.

[6] A. Freier, P.Karlton, and P.Kocher, "The SSL Protocol Version 3.0", http//:www.netscape.com/eng/ssl3/3-spec.ps, 1996.3.

[7] T.Dierks, et, al., "The TLS Protocol 1.0" RFC2246, 1999.1.

[8] 홍승필, 고제욱, "정보보안 기술과 구현", 정보과학회지, 한국정보과학회, 1998.

[9] C.Eckert, "On Security Models", International Conference on Information Security, 1996.

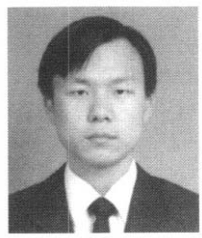
[10] J. Weeks, etc, "CCI-Based WebSecurity : A Design Using PGP", WWW Journal 95, 1995.

[11] B.Rescorla, ef, al, The Secure HyperText Transfer Protocol, RFC 2660, 1999.8.

[12] Ivan Ristic, "Apache Security", O'REILLY, 2005.03.15.

[13] S.M.Bellovin, "Security Problems in the TCP/IP Protocol Suite", Computer Communication Review, Vol. No.2, pp.32~48.

[14] D.Bernstein, "TAP", TAP-std working group, Aug., 1992.



조 남 덕

e-mail : ndcho@softcamp.co.kr

1999년 중앙대학교 컴퓨터공학과(학사)

2001년 중앙대학교 대학원 컴퓨터공학과(석사)

2003년 중앙대학교 대학원 컴퓨터공학과 박사수료(박사과정)

2000년~현재 소프트캠프(주) 연구원

관심분야 : 인공생명, 인공지능, 시맨틱 웹, 인터넷 보안 등

박 현 근

e-mai : gatepark@ssuci.ac.kr

1968년 연세대학교 교육대학원 석사

1995년 서강대학교 정보처리 이학석사

1998년~2005년 중앙대학교 대학원 컴퓨터 공학박사

2002년~현재 중국 연변 과학기술대학 겸임 교수

1989년~현재 숭실대학교 전산원 교수

관심분야 : 인터넷 보안, 시맨틱 웹, 인공지능, 네트워킹, 전자상거래운영, 전산수학