Journal of Korea Multimedia Society Vol. 7, No. 7, July 2004(pp. 934-943)

쿠키보호기능을 제공하는 안전한 웹 시스템의 설계 및 구현

최은복[†], 최향창[††], 이형옥[†††]

요 약

본 논문에서는 웹에서 사용되는 쿠키를 안전하게 사용할 수 있도록 쿠키보호를 위해 쿠키 보호키 관리 시스템을 두고 사용자별로 다른 쿠키 보호키를 유지하게 함으로써, 쿠키 사용에 따른 사용자 정보의 무결성, 비밀성, 사용자 인증 서비스를 제공한다. 또한 웹 기술을 이용할 경우 노출된 URL을 이용해 내부 문서의 위치를 추측하고 접근하는 것을 방지하기 위해 URL을 노출시키지 않는 방법을 제시하였다. 본 시스템은 기업의 인트라넷에 적용함으로써 공격자에게 쉽게 정보 노출이 발생하는 취약한 쿠키의 안전함을 제공하고 내부사용자에 대한 내부문서 유출 문제를 최소화할 수 있을 것이다.

Design and Implementation of Secure Web System with Cookies Protection Function

Eun-Bok, Choi[†], HyangChang, Choi[††], HyeongOk, Lee[†††]

ABSTRACT

In this paper, we propose cookie protection-key management system for cookie protection and maintain separate cookie protection-key of each user. We provide integrity, confidentiality, and user authentication of cookie by using registered cookie protection-key and applying encryption techniques. And, we use the technique for hiding the URL of an internal document to a user to minimize the problem of its exposure. When this system is applied to the intranet of an enterprise, it will be able to provide a security to cookie and minimize the problem of internal document exposure by an internal user.

Key words: Cookies(쿠키), Web System(웹시스템), Secrecy(비밀성), Integrity(무결성)

1. 서 론

기업 내에 속해있는 사설네트워크인 인트라넷을 이용하는 기업이나 특정조직에서는 웹 기술을 이용하여 자동문서 생성과 전자결재, 전자회의 등의 내부 정보 시스템을 구축한다. 이러한 내부정보 시스템은 웹 브라우저를 기반으로 사용하고 있어서 거의 모든 플랫폼에서 사용이 가능하며 웹 도구들이 인트라넷과 기존의 데이터베이스 응용프로그램 상호간에 연결해주는 강력한 메커니즘을 가지고 있어 기존 시스템과의 연계가 쉬울 뿐 아니라 같은 프로그램을 여러 기종의 하드웨어에서 사용할 수 있으므로 필요한 소프트웨어 개발이나 유지 보수비용의 많은 절감 효과가 있다.

사용자가 이전에 제공했던 정보를 또다시 입력해야 하는 불편함을 해결하기 위해 웹 환경에서는 사용자가 제출한 정보를 클라이언트 영역에 임시로 저장

※ 교신저자(Corresponding Author) : 이형옥, 주소 : 전남 순천시 매곡동 315번지(540-742),전화 : 061)750-3345, FAX : 061)750-3308, E-mail : oklee@sunchon.ac.kr
접수일 : 2003년 10월 8일, 완료일 : 2003년 12월 23일
[†] 정회원, 전주대학교 정보기술공학부
(E-mail : ebchoi@jj.ac.kr)
[††] 전남대학교 정보보호협동과정
(E-mail : hcchoi@athena.chonnam.ac.kr)
[†††] 순천대학교 컴퓨터교육과

하는데 사용되는 개념이 쿠키이다[6,9]. 사용자의 편의를 위해 사용되는 쿠키는 클라이언트 영역에 평문인 일반 텍스트로 저장되어지므로 공격자가 쿠키의 정보를 가져오는 코드를 삽입하게 되면 이 쿠키에 삽입된 정보는 쉽게 노출되고 이용될 수 있다. 또한, 쿠키정보는 평문으로 전송되므로 도청에 의한 공격에 매우 취약하므로 네트워크를 통해 전송중인 정보가 물건을 구매하기 위한 신용카드 정보나 개인의 비밀번호일 때 매우 위험한 단점을 갖고 있다[3]. 따라서 언급한 기업의 인트라넷에서 내부사용자로부터 발생할 수 있는 보안사고와 웹 사용자인 외부 이용자에 대한 보안 취약점이 인트라넷 보호의 중요한 보안 문제이며 웹 기술에 주로 사용되고 있는 쿠키를 안전하게 이용할 수 있는 방법이 필요하다.

2. 쿠 키

2.1 쿠키 형식

쿠키 설정 헤더는 다음과 같은 형식으로 클라이언트 영역에 저장한다.

Set-cookie:Name=Value;expires=DATE; path=PATH; domain=DOMAIN_NAME; secure

각 요소의 세부적인 사항은 다음과 같다.

▣ NAME=VALUE : NAME 항목은 쿠키의 유일한 이름이다.

▣ expires : 쿠키의 만료일시를 의미한다. 서버가 클라이언트 영역의 쿠키에 접근할 때, 만료일시에 의해서 만료일시가 초과되었으면 해당 쿠키를 삭제한다.

▣ domain : 서버의 주소를 가지고 있다. 클라이언트가 어떤 서버에 쿠키정보를 제공하고 클라이언트 영역에 저장했는지 알 수 있는 항목이다. 이것은 어떤 클라이언트가 특정 웹 사이트에 접속할 때, 그 웹 사이트에 해당하는 쿠키 값을 서버에게 보낸다.

▣ path : 웹 사이트를 방문할 때의 경로 값을 가지고 있다. 클라이언트가 웹사이트에 방문할 때, 그 서버의 주소와 일치하는 쿠키 값 중에 이 경로에 해당하는 쿠키 값을 서버에 전송한다.

▣ secure : 쿠키 안전함을 표현하는 항목이다. 이 항목이 추가되면 안전한 전송 방법에 의한 SSL 프로토콜을 사용하는 경우에만 쿠키 값을 서버에 전송한다. 즉 쿠키가 웹 서버로 안전한 방법으로 전송된다.

2.2 쿠키 보호 서비스

쿠키를 안전하게 사용하기 위해서는 세 가지의 보호 서비스가 제공하여야한다[15].

첫 번째 서비스는 웹 서버에 사용자가 쿠키 정보를 보내올 때 쿠키를 보내는 사용자가 맞는지 확인하기 위한 사용자 인증과정이다. 사용자 인증(User Authentication)은 주소기반, 패스워드 기반, 전자서명 기반의 인증방법이 있는데, 주소기반 인증은 쿠키정보에 인터넷 주소를 저장하는 주소쿠키를 두어 인증하게 하는 방법으로 쿠키정보에 대한 사용 이전에 주소쿠키를 통하여 상대방을 인증하고 인증되면 통신한다[7,8]. 패스워드기반 인증방법은 웹 서버에서 사용자를 인증할 수 있는 키 값을 생성해서 쿠키 값으로 저장하는 방법이다[12,14,15]. 마지막은 전자서명기반 인증에 의한 사용자 인증이 있다. 전자서명 방식에 의해 인증하는 방법은 웹 서버가 사용자의 공개키를 알고 있을 때 사용자가 자신의 개인키를 이용해서 RSA와 유사하게 전자서명하여 보내게 되면 웹 서버가 사용자의 공개키를 이용해서 복호화 한 후에 사용자를 인증하는 방법이다[10,11].

두 번째 서비스는 쿠키의 무결성을 보장하는 서비스이다. 공격자에 의해 위조된 쿠키가 웹 서버로 보내질 때 쿠키 값에 바이러스나 이상행위를 수행하게 하는 스크립트 소스를 삽입하거나 쿠키의 기한 속성 값을 늘려 사용이 되도록 하는 등 공격자에 의해 이용될 수 있다. 따라서 쿠키가 이전에 제공한 정보가 맞는지 확인이 필요하다. 쿠키 무결성 확인 방법에는 공개키 기반 방법이나 비밀 키를 이용하는 방법이 있다. 공개키 기반 무결성 제공방법은 개인키를 가지고 무결성을 유지할 쿠키 정보를 암호화해 놓는다. 이 값을 공개키로 복호화 함으로써 무결성을 확인할 수 있다[10].

다른 하나는 비밀키 기반 무결성 확인 방법이 있다. 웹 서버와 개인사용자간에 비밀키를 이용해 무결성을 확인하는 방법이다. 쿠키의 무결성을 위해서 비밀키를 이용해 쿠키들을 해싱 함수를 사용해서 해싱하여 값을 생성하여 사용자 클라이언트 영역에 쿠키 값으로 저장해 둔다. 사용자가 웹 서버에 요청될 때 비밀키를 이용해서 쿠키들을 해싱 함수를 사용해 해

싱 해보고 이미 해싱 된 쿠키데이터와 비교해 봄으로서 무결성을 확인한다[2].

세 번째 서비스는 중요한 쿠키 정보의 비밀성을 보장하는 서비스이다. 이 방법은 사용자가 제공한 쿠키정보가 저장되기 전에 암호화되어 쿠키 값으로 저장된다. 따라서 해커가 사용자의 쿠키 값을 얻어낸다 하더라도 암호화 되어있어 암호화키를 알지 못하면 무용지물이 되므로 안전하다.

3. 안전한 웹 시스템

인트라넷의 구성 요소 중 일부분이 기업의 웹 페이지이며 기업은 자사의 기술과 물품에 대한 홍보를 위해 웹 페이지를 운용하고 있다. 이러한 웹 페이지는 많은 취약점을 내포하고 있는데 이러한 취약점 중 전자상거래나 사용자 인증에 밀접한 관련을 갖고 있는 쿠키에 대한 보안과 웹을 이용한 조직 내부문서의 노출에 대한 안전함을 제공하는 시스템에 대해 제안하고자 한다.

3.1 쿠키보호 시스템

정보검색을 위한 사이트나 무료로 공개되어 있는 보통의 사이트에는 쿠키의 보호성이 필요하지 않다. 쿠키 보호가 필요한 사이트는 일반적으로 공용정보를 제공하는 사이트가 아니고 전자상거래나 전문적인 서비스를 제공하는 사이트로 볼 수 있다. 따라서 위와 같은 전문적인 서비스를 하기 위해서는 사용자의 등록과정이 필요하다. 쿠키는 웹 서비스를 사용하고자 하는 사용자의 정보를 각각의 클라이언트 영역에 저장하므로 쿠키를 암호화시키는 키를 사용자별로 다르게 유지해도 문제가 없다. 따라서, 사용자가 제공하는 쿠키를 암호화 및 복호화 하는데 사용되는 쿠키 비밀키를 관리하기 위한 서버를 만들고 이 서버에서 사용자의 인증 쿠키를 생성한다. 인증 쿠키를 기반으로 웹 서비스를 제공하는 시스템이 서비스를 요청한 사용자를 인증하고 사용자별 쿠키 보호키를 얻어낸다. 이 쿠키 보호키에 의해 쿠키 정보는 암호화 및 복호화 되어 웹 서비스 시스템과 웹 사용자간에 안전한 서비스를 제공한다.

3.1.1 쿠키 보호키 관리 시스템

쿠키 보호키 관리 시스템(Cookie Security Key Management System : CSMS)은 웹 사용자의 가입을 받고 웹 사용자가 제공하는 정보를 저장하며 웹 서비스 시스템(Web Service System)에 사용자 정보를 전송한다. 또한 웹 사용자에 대해 인증서를 발급하고 웹 사용자 시스템에 쿠키 값으로 인증서를 저장시킨다. 쿠키 보호키 관리 시스템 모듈의 구성요소는 그림 2와 같다.

쿠키 보호키 관리시스템의 키 DB를 이용한 관리자 인증(CSMS Administrator Authentication)모듈(①), 공개키 분배 모듈(Public key Distribution)(ⓔ), 웹 서비스 시스템 관리 DB에 정보를 등록 및 수정 모듈(ⓑ, ⓕ), 사용자 등록(Insert Web User)모듈(ⓖ), 웹 사용자 정보 복사 및 수정(Web User Information Copy and Update) 모듈(ⓘ), 웹 서비스 시스템 관리자 인증(WSS Administrator Authentication)모듈(ⓗ), 웹 사용자 인증 모듈(ⓙ), 사용자

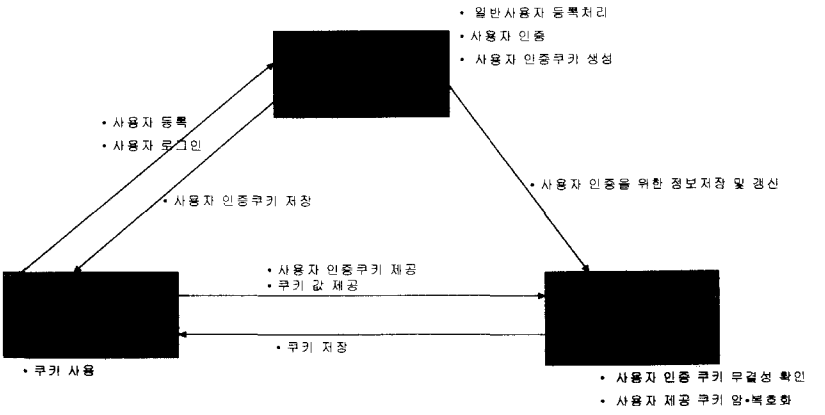


그림 1. 쿠키 보호 시스템 기능

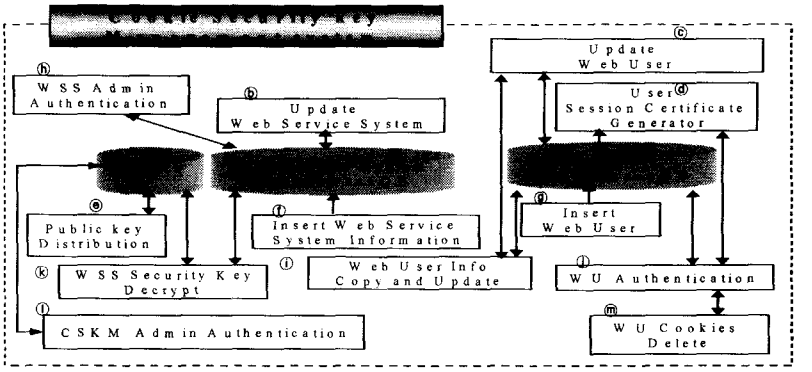


그림 2. 쿠키 보호키 시스템 구성 모듈

세션 인증서 생성(User Session Certificate Generator)모듈(ⓓ)로 구성된다. 또한, 웹 서비스 시스템 비밀키 복호화(WSS Security key Decrypt)모듈(ⓚ)은 쿠키 보호키 관리시스템의 공개키로부터 암호화되어진 웹 서비스 시스템의 비밀키를 키 데이터베이스(Key DB)에 저장되어 있는 쿠키 보호키 관리 시스템의 개인키로 복호화 하여 원래의 키를 얻어내는 모듈이다.

사용자 등록 과정과 사용자 인증과정에서는 SSL 프로토콜을 사용하여 사용자가 쿠키 보호키 관리 시스템에 정보를 제공하는데 있어서의 안전함을 제공하는데, 이 시스템에서 유지하는 데이터베이스 정보는 그림 3과 같다.

3.1.2 웹 서비스 시스템

웹 서비스 시스템(Web Service Systems : WSS)은 웹 사용자의 접속 요구를 받아들이고 사용자를 인증하고 사용자별 쿠키 비밀키를 이용 쿠키 정보를 암호화 및 복호화 하여 사용자가 안전하게 쿠키를 사용할 수 있도록 해주는 시스템이다. 이러한 웹 서비스 시스템 모듈의 구성 요소는 그림 4와 같다.

웹 서비스 시스템 관리자 인증 모듈은 쿠키 보호

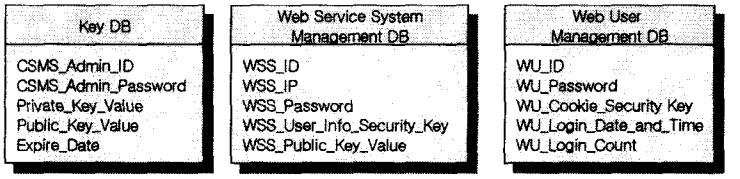


그림 3. CSMS에서 유지하는 정보

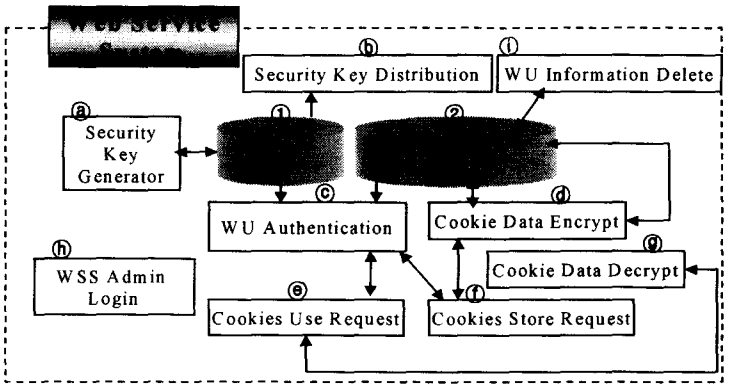


그림 4. 웹 서비스 시스템 구성 모듈

키 관리시스템의 웹 서비스 시스템 관리 데이터베이스를 통해 웹 서비스 시스템 관리자 인증을 제공하는 모듈이다.

웹 서비스 시스템의 비밀키를 생성하고 분배하는 비밀키 생성기(Security key Generator) 모듈(ⓐ)과 분배기(Security key Distribution)모듈(ⓑ), 웹 사용자 인증(authentication)모듈(ⓒ), 그리고 웹 사용자 인증모듈을 통해 사용자를 인증하고 사용자로부터 얻어낸 쿠키 정보를 사용자의 쿠키 보호키로 복호화하여 원래의 데이터를 얻어내어 사용하는 모듈인 쿠키 사용 요구(Cookies Use Request)모듈(ⓔ) 등으로 구성된다.

웹 서비스 시스템에서 유지하는 데이터베이스 정보는 그림 5와 같다.

3.1.3 웹 사용자 시스템

웹 사용자 시스템(Web User Systems : WUS)은 일반사용자의 시스템을 의미한다. 일반 사용자들은 어떤 웹 사이트에서 물품을 구매하거나 필요정보를 얻어내기 위해서 사용자 로그인후 웹 서핑을 하는데 이때 쿠키 보호를 제공하기 위해 쿠키 보호 시스템에 로그인 해야 한다. 이러한 웹 사용자 시스템의 구성 모듈은 그림 6과 같다.

웹 사용자 로그인 ⓐ를 통해 사용자는 로그인 하게 되고 사용자의 서비스 요구를 받아들인다. 웹 브라우저는 그림 6의 (1)은 무결성 확인을 위한 쿠키이며, (2)는 쿠키 보호키로부터 받은 사용자 인증 세션키를 의미하며, (3)은 웹 사용자가 필요로 하는 쿠키 값 리스트 이다.

사용자 로그인과정에 쿠키 보호키 관리 시스템으로부터 생성된 인증 쿠키 정보는 안전을 위해서 웹 사용자의 로그아웃으로부터 쿠키보호시스템과 웹 서비스 시스템에 접속하여 웹 사용자가 제공한 쿠키 값과 웹 서비스 시스템의 사용자 정보 사본 데이터베이스에 저장되어 있는 사용자 정보를 삭제한다. 따라

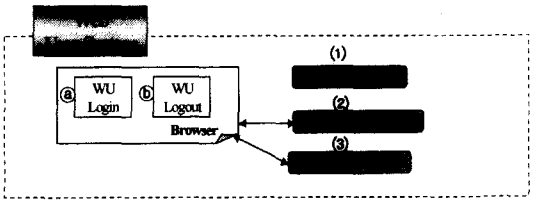


그림 6. 웹 사용자 시스템 구성모듈

서 로그아웃 후에 다시 사용하기 위해서는 로그인 과정을 거치면서 쿠키보호 시스템에서 새로운 인증 쿠키 값을 서버로부터 부여받아야 한다.

3.1.4 동작 시나리오

먼저 사용자 가입의 안전성을 위해 SSL을 이용하여 사용자 가입을 시작하게 된다. 일반 사용자가 가입요구를 하게 되면 가입 입력화면이 화면상에 보이는데 이때 사용자 가입 정보와 쿠키를 위한 쿠키 암호화 키를 입력하게 된다. 표 1과 표 2는 사용자의 가입요구 후의 CSMS와 WSS의 사용자 정보이다.

등록된 사용자가 로그인할 때 ID와 비밀번호를 제공한다. 이때의 비밀번호는 MD5를 이용해서 해싱하여 사용자의 ID와 일치하는 사용자 정보를 표 1의 (2)와 비교해서 일치하면 사용자는 정상적인 사용자로 인증한 후 표 2의 (3), (4)번을 갱신시킨다. 다음으로 쿠키 보호키 관리 시스템은 사용자의 인증 쿠키를 생성하는데 인증쿠키 생성방식은 사용자의 ID와 사용자의 접속 IP를 표 1에 저장되는 (4)와 (5)와 함께 MD5를 이용해서 해싱한 후에 생성하고 이 데이터를 사용자의 클라이언트 영역에 쿠키 값으로 저장시킨다. 따라서 사용자는 매 접속시마다 새로운 인증쿠키 값을 갖게 된다. 인증 쿠키 값을 저장할 때 사용자의 ID도 쿠키 값으로 저장시킨다. 이때 생성되는 사용자 인증 쿠키 값은 그림 7과 같다.

사용자가 로그아웃하면 기존의 인증과 무결성을 위한 쿠키는 모두 삭제되어야 하는데 사용자가 로그아웃을 통하지 않고 종료했다면 쿠키 값은 사용자의

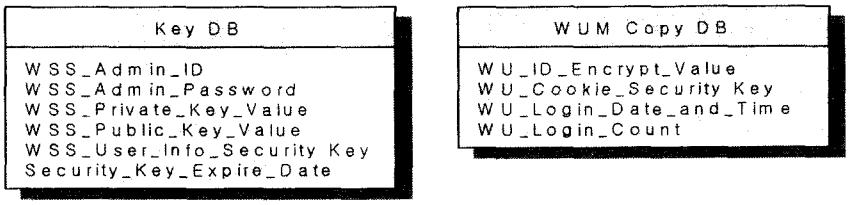


그림 5. 웹 서비스 시스템에서 유지하는 정보

표 1. 사용자의 가입요구 후의 CSMS의 사용자 정보

저 장 내 용		생성자	생성	저장
(1)	접속 ID(유일성 보증)	사용자	1	5
(2)	사용자가 제공한 Password를 MD5로 해싱한 데이터	CSMS	4	5
(3)	쿠키 보호 키	사용자	1	5
(4)	일시(최근에 WU 인증쿠키 생성이나 폐기될때 시간)	CSMS	4	5
(5)	CSMS 접속 횟수(접속 종료시 기존정보에 +1)	CSMS	4	5

표 2. 사용자의 가입요구 후의 WSS의 사용자 정보

저 장 내 용		생성자	생성	저장
(1)	사용자 접속 ID를 WSS에서 제공한 사용자 정보 보호키로 AES 사용 하여 암호화한 ID	CSMS	4	6
(2)	쿠키 보호 키	사용자	1	6
(3)	일시(최근에 WU 인증쿠키 생성이나 폐기될때 시간)	CSMS	4	6
(4)	CSMS 접속 횟수(접속 종료시 기존정보에 +1)	CSMS	4	6

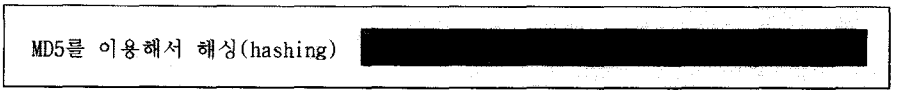


그림 7. 사용자인증 쿠키 구성 값

클라이언트 영역에 그대로 남게 된다. 따라서 쿠키 보호를 위해서 사용했던 기존의 쿠키 값이 남아있는지 확인하고 쿠키 값의 무결성 보호를 위해 쿠키 보호 시스템과 웹 서비스 시스템에서 제공한 인증을 위해 사용되었던 모든 쿠키 값을 제거한다. 다음으로 그림 7과 같은 인증쿠키 값을 웹 사용자 시스템에 저장시킨 후에 쿠키 보호키 관리시스템에서는 웹 서비스 시스템의 URL로 사용자의 접속을 연결시켜 준다.

웹 서비스시스템은 사용자가 로그인 과정을 끝내고 웹 서비스시스템에 연결되었을 때 안전하게 쿠키를 사용할 수 있도록 한다. 웹 연결이 HTTP 프로토콜을 사용하므로 쿠키를 사용하기 이전에 쿠키 보호키 관리 시스템에서 제공받은 사용자 인증 쿠키를 가져와 이것을 MD5로 해싱하여 사용자를 인증한다. 사용자에 대한 인증과정에서 먼저 접속한 사용자의 ID가 필요한데 접속한 사용자 시스템의 ID 쿠키를 가져오고 ID를 쿠키 보호키 관리 시스템의 WSS 비밀키로 AES을 이용하여 암호한 후 이 암호화된 ID를 이용하여 해당 사용자의 정보를 가져온다. 그리고 인증쿠키를 생성하고 사용자로부터 얻은 인증 쿠키와 비교함으로써 일치하면 사용자의 무결성을 보장할 수 있다. 인증이 완료되면 해당 사용자의 쿠키 보호키를 얻어 와서 사용자가 제공한 데이터 값을 암호화하여 재사용을 위해 사용자의 클라이언트 영역에 저장하거나 이미 저장된 쿠키 값을 복호화하여 사용한다. 각 쿠키데이터의 무결성은 이때 보증되는데 쿠키의 데이터영역이 변화되면 복호화 할 때 원래의 사용자 데이터를 얻을 수 없기 때문에 만약 공격자가 쿠키 데이터를 수정하였다 할지라도 원래의 데이터를 알 수 없으므로 쿠키의 무결성이 보장된다. 또한 쿠키 데이터 값이 AES를 이용하여 암호화 되어있으므로 쿠키 정보가 노출되었다 할지라도 데이터의 비밀성이 보장된다.

3.2 URL 노출 방지기법

기업에서 내부 사용자를 위해서 내부문서를 배포하는데 있어서 웹 기술을 사용하면 내부문서의 위치인 URL을 알아낼 수 있는데 이러한 URL 정보도 침입하고자 하는 공격자에게는 중요한 정보가 된다. 따라서 이러한 문제점을 미연에 방지하기 위해 사용자에게 내부문서의 URL을 노출시키지 않도록 하는 방법에 대해서 설계한다. 여기서는 이러한 방법을 위해 역할기반 접근통제를 도입하고 SFS-HTTP를 이용한 사용자 URL 인증 기술을 응용하여 보호를 할 수 있도록 제안한다[4,5,13]. 이 내부 보호 시스템의 구

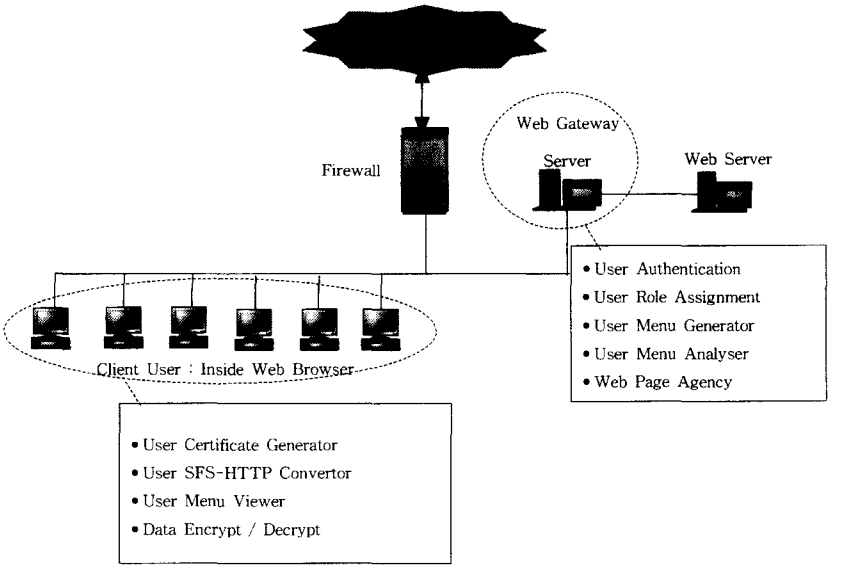


그림 8. 내부보호 시스템의 구성

성은 그림 8과 같다.

3.2.1 내부 웹 브라우저 (IWB : Inside Web Browser)

내부 사용자의 보안을 위해 설계된 내부 웹 브라우저인 IWB(Inside Web Browser)는 웹 브라이져(그림 9)의 기능을 가지고 있어서 인트라넷으로 구현된 모든 응용에 대해서 사용할 수 있으며, 사용자 인증을 위한 정보와 IWB의 무결성을 보증하기 위해 IWB 인증 번호 입력란을 제공한다.

서버는 IWB 인증번호를 랜덤하게 생성 후 IWB 접속IP와 쌍으로 유지하여 저장한 후 해당 IWB에 전송하고 사용자의 접속이 요청되면 해당 IWB 인증

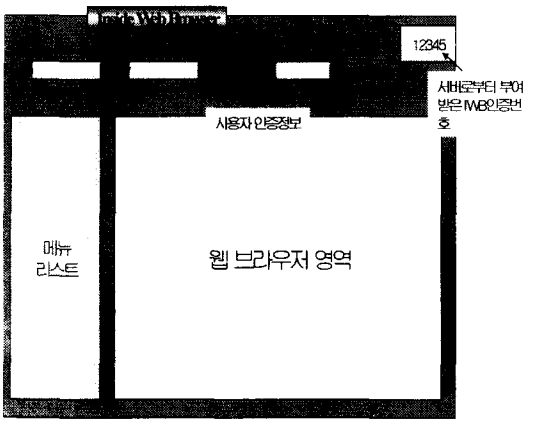


그림 9. 내부 웹 브라우저

번호를 서로 비교함으로써 정상적인 IWB임을 보증한다. 사용자 인증이 완료 되어지면 IWB는 URL정보가 없는 단지 사용자가 접근 가능한 메뉴리스트만 보여준다. IWB의 무결성 보증이 끝나면 웹 게이트웨이 서버는 웹 게이트웨이의 개인키를 가지고 IWB 인증번호를 MD5를 거쳐 해쉬하고 IWB에 전송한다.

IWB의 내부모듈인 사용자 인증 생성기(User Certificate Generator : UCG)는 인증서를 생성하고 이 인증서를 통해서 로그인 과정 후에 사용자를 인증하는 모듈이다.

사용자 메뉴 뷰어(User Menu Viewer)는 웹 게이트웨이 서버에서 보내져온 사용자 접근 가능 웹 페이지 목록 주소들을 사용자들이 사용할 수 있도록 버튼으로 만들어서 화면상에 보여주는 모듈이다.(그림 10)

데이터 암호화 및 복호화(Data Encrypt / Decrypt) 모듈은 과업을 수행중 웹 게이트웨이로 보내는 데이터를 암호화하고 웹 게이트웨이로부터 받은 암호화된 데이터를 복호화할 때 사용되는 모듈이다.

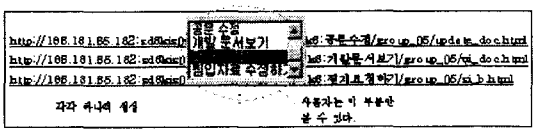


그림 10. 사용자 메뉴뷰어에 의해 생성된 메뉴

3.2.2 웹 게이트웨이 서버

내부 웹 브라우저(Inside Web Browser)를 통해 접속해오는 사용자 요구를 분석하여 처리하는 서버로서, 이 서버에 의해서만 웹 서버에 접속가능하고 웹 서버로 받은 결과를 사용자에게 전송하는 웹 게이트웨이 역할을 한다. 여러 가지 모듈 중 사용자 역할 부여 처리 모듈(그림 11의 ①)은 가져온 사용자의 역할등급을 가지고 이 권한에 해당하는 과업을 가져와서 사용자 메뉴 생성기에 넘기는 기능을 수행하고 사용자 메뉴 생성기 모듈은 User Role Assignment로부터 얻어온 자료를 SFS-HTTP 형으로 변환한다(그림 11의 ②, ③).

4. 시스템의 구현 및 분석

쿠키보호 시스템의 구현환경은 다음의 표 3과 같다.

이 시스템은 운영체제로서 Linux와 Windows2000, 시스템에서 사용되는 정보저장을 위해서 Mysql데이터베이스를 사용했다. 관리자 로그인 기능의 구현은 Kylix를 통해 만들었고 내부사용자가 사용하는 내부 웹 브라우져는 Delphi 언어를 사용했으며 사용자에 대한 접속이나 암호화 인증에 관해서는 php4를 사용했다. 이 시스템은 안전하게 쿠키를 사용하기 위해 쿠키 사용자의 사용자 인증기능과 쿠키의 노출에 의한 보호기능 그리고 위조문제를 해결하는 쿠키 정보의 무결성을 제공한다.

표 3. 구현환경

운영체제	WOW Linux 7.1 / Windows2000	
하드웨어	CPU	ML330, Intel Pentium III
	RAM	256
개발도구	데이터베이스	Mysql
	사용언어	Delphi Kylix php4 Java Script

사용자 로그인과정을 수행한 후의 쿠키 정보는 그림 12에서 보여준다.

쿠키를 암호화하는 키 관리 서버를 두기 때문에 여러 개의 웹 서비스 시스템과의 연계가 가능하다. 또한 기존에 안전한 쿠키(Secure Cookies)와 다르게 사용자 각각이 자신의 쿠키 비밀키를 유지함으로써 보다 강화된 사용자 프라이버시를 제공할 수 있다.

그림 13은 내부문서 URL 은닉시스템의 예시로서, 사용자는 웹 게이트웨어 서버로부터 웹 게이트웨이로의 접속에 사용될 내부 웹 브라우저(IWB)를 다운받아 시스템에 설치한 후 IWB를 통해 사용자 인증과정을 생성하고 암호화 및 복호화에 사용되는 세션키를 얻어내어 사용자 메뉴 뷰어를 통해 문서를 사용한다.

5. 결 론

기업에서는 인트라넷에서 웹 기술을 사용하는데

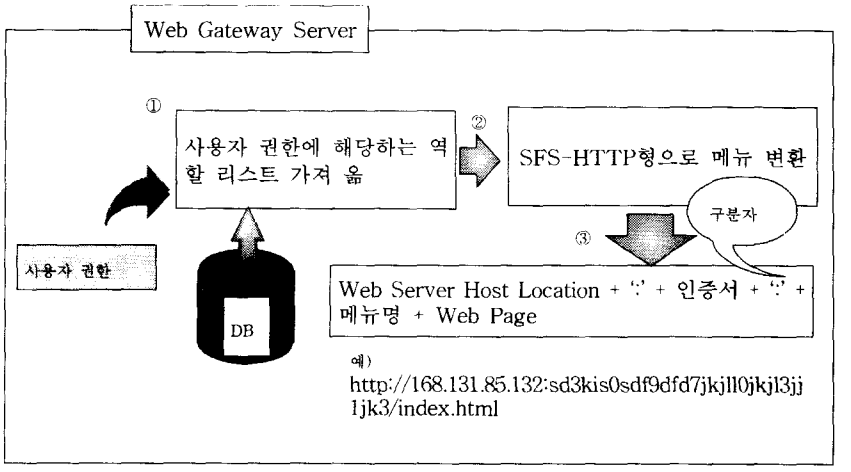


그림 11. 사용자 메뉴 생성을 위한 준비과정

그림 12. 쿠키 로그인 과정 수행 후 쿠키 정보

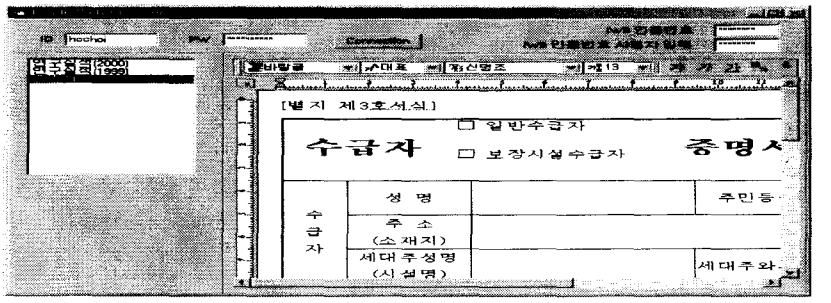


그림 13. 내부문서 URL 은닉시스템 사용자 화면 예시

있어서 소프트웨어 개발이나 유지비용의 절감효과가 있으나 불법적인 공격에 많은 취약점을 가지고 있다. 이중에서 외부의 사용자에 대한 공격으로 빈번하게 발생하는 쿠키 공격과 내부사용자의 내부문서 노출 문제를 해결하기 위해 시스템을 제안하고 구현했다.

이 시스템은 외부의 일반 사용자를 위해 쿠키 보호를 제공하기 위해 쿠키 보호키 관리시스템을 사용한다. 따라서 이 시스템의 사용으로 인해서 쿠키 정보가 클라이언트 영역에 암호화되어 저장됨으로써 쿠키 사용에 따른 사용자 정보를 공격자에게 노출하지 않을 수 있다. 또한 쿠키 보호키 관리시스템을 두어 쿠키를 안전하게 보호하기 위한 키 관리를 별도로 함으로써 기존에 사용되고 있는 웹 서비스 제공 사이트에 쉽게 적용될 수 있고 또한 사용자 사생활을 강화하기 위해 정보데이터를 관리시스템 간에 분리하여 유지함으로써 외부로 데이터베이스가 노출되는 사건이 발생한다 하더라도 사용자의 사생활이 보호되도록 하고 있다. 이 시스템은 암호화 방식을 사용해서 쿠키의 무결성, 비밀성, 사용자에 대한 인증을 제공한다.

내부문서 URL 은닉 시스템은 자신의 인증서를 URL에 포함시켜 전송함으로써 각각의 접속에 대해서 사용자의 인증을 제공하며, 역할기반 접근제어 방법을 이용하여 사용자가 접근 가능한 메뉴를 생성하므로 사용자에 대한 관리가 쉽고 개개의 사용자에게 업무를 적용하는 시스템보다 많은 시간과 자원의 낭비를 줄일 수 있는 장점을 갖는다. 또한, 사용자 관리에 있어서 사용자는 역할 서버가 SFS-HTTP 방법에 따라 부여한 사용자 메뉴 리스트를 통해 본인이 업무에 접속하게 되므로 시스템 접속에 따른 불법 사용자에 대해 보호할 수 있다.

참 고 문 헌

[1] J. Park and R. Sandhu, "Secure Cookies on the Web," IEEE Internet Computing, 2000.

[2] J. Park, "A Secure-Cookie Recipe for Electronic Transactions," http://citeseer.nj.nec.com/par99securecookie.html, 1999.

[3] Simon Perkins, "Internet Cookies: Security Implications," http://citeseer.nj.nec.com/perkins00internnet.html, 2000.

[4] Ravi S. Sandue, Edward J, Coyne, Hal L. Feinstein and Charles E. Youman, "Role-Based Access Control Models," IEEE Computer, Volume 29. Number 2, pp. 38-47, 1996.

[5] Joon S. Park, Ravi Sandue, SreeLatha Ghanta, "RBAC on the Web by secure cookies," In Proceedings of the IFIP WG11.3 Workshop on

Database Security, 1999.

[6] Fielding R, Gettys J, Mogul J, Frystyk H, Masinter L, Leach P and T Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1," RFC2616, June 1999.

[7] R. Fielding and L. Montulli, "Defending Against Sequence Number Attacks," RFC1948, January 1996.

[8] Edward W. Felten, Dirk Balfanz, Drew Dean, and Dan S. Wallach, "Web Spoofing," An Internet Con Game Technical Report 540-96, February 1997.

[9] D. Kristol and L. Montulli, "HTTP State Management Mechanism," RFC2109, January 1997.

[10] H.X. Mel and Doris Baker, "Cryptography Decrypted," Addison Wesley, 2001.

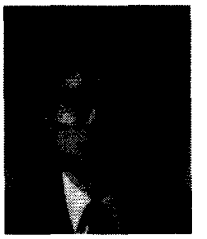
[11] R. C. Merkle, "A Certified Digital Signature," In CRYPTO'89, 1989.

[12] E. Rescorla, *SSL and TLS*, Addison-Wesley, 2001.

[13] Michael Kaminsky and Eric Banks, "SFS-HTTP: Securing the Web with Self-Certifying URLs," MIT, 1999.

[14] Anonymous, *Maximum Security : A Hacker's Guide to Protecting Your Internet Site and Network,* Sams, Second Edition, September 1998.

[15] Anonymous, *Maximum Linux Security: A Hacker's Guide to Protecting Your Linux Server and Workstation,* Sams, October 1999.



최 은 복

1992년 전남대학교 전산학과 졸업(이학사)
1996년 전남대학교 전산통계학과 졸업(이학석사)
2000년 전남대학교 전산통계학과 졸업(이학박사)
2001년 순천제일대학 인터넷정보학부 전임강사
2002년~현재 전주대학교 정보기술컴퓨터공학부 전임강사
관심분야 : 통신망관리, 정보보안, 엑티브 네트워크 등

최 향 창

2000년 8월 광주대학교 컴퓨터공학 학사
2002년 8월 전남대학교 전산학이학 석사
2003년 3월~현재 전남대학교 정보보호 박사과정
관심분야 : 유비컴 보안, SSO, 통합보안관제

이 형 옥

1994년 2월 순천대학교 전산학과 졸업(이학사)
1996년 2월 전남대학교 전산통계학과 졸업(이학석사)
1999년 2월 전남대학교 전산통계학과 졸업(이학박사)
1999년 10월~2002년 2월 한국전산원(선임연구원)
2002년 3월~현재 순천대학교 컴퓨터교육과 전임강사
관심분야 : 그래프이론, 알고리즘, 병렬처리