2000년 한국정보처리학회 추계 학술발표논문집 제7권 제2호

LAN 사용자의 웹 인포샵 서비스를 위한 보안 인증 시스템의 설계 및 구현

이종훈*, 백영미*, 안경환*, 류원**, 한기준*
*경북대학교 컴퓨터공학과
**한국전자통신연구원서비스네트워크연구부
{abyss, backjoo, khan}@netopia.knu.ac.kr,
wlyu@etri.re.kr, kjhan@bh.knu.ac.kr

A Design and Implementation of Security Authetication System For LAN-WISS

Jong-Hoon Lee*, Young-Mee Baek*, Kyung-Hwan Ahn*,
Won Lyu**, Ki-Joon Han*
*Dept of Computer Engineering, KyungPook National University
**ETRI, Service Network Dept

요 약

본 논문에서는 웹 상에서 대체 인증 및 대체 과금의 방법을 제공하는 웹 인포샵 서비스를 LAN 사용자로 확대하기 위한 신뢰성 있는 사용자 인증 시스템을 설계하고 구현하였다. 이를 위해서는 사용자와 서버간의 키 교환에 의한 암호화/복호화 과정을 통해 네트웍상에서 사용자 정보를 보호할 수 있다. 암호화/복호화 알고리즘으로는 RSA 알고리즘을 사용하였고 이를 위한 모듈로는 사용자측은 JAVA 애플릿으로 구현하였고 서버쪽의 인증 에이전트는 JAVA로 구현되었으며 웹 인포샵 서비스 시스템과의 인터페이스는 C로 구현되었다.

1. 서론

월드와이드웹(World Wide Web)은 클라이언트/서버 구조에 기반을 둔 문서 배분 시스템으로 지난 수년간 급속한 성장세를 유지해 왔으며[1], 쉬운 구축법과 사용자에게 친숙한 인터페이스로 사용자층을 넓혀왔다[2,3]. 근래에 들어서는 인터넷 쇼핑몰, 엔터테인먼트, 성인사이트, 인터넷 방송국등 정보제공분야에서 상업용 사이트의 수가 증가하고 있다[4]. 그러나 웹에서의 정보제공서비스는 과금 방법의 비효율성으로 인하여 많은 발전을 해 오지 못한 것이 사실이다. 개인별 회원가입과 한 달 단위의 정액 요금제도 등의 불편함은 많은 사용자로 하여금 회원 가입이나 사용을 꺼리게 했다. 또 정보제공업자는 유료화를 위해 개인 사용자를 관리해야 하며 각 사용자에 대한 과금 생성 및 추징까지도 담당하여야 한다. 사용자 역시 각각의 사이트에 대한 인증을 받아야 하므로 인증에 대한 불편함이 생기게 된다.

이러한 유료화의 문제점을 해결하고, 웹상에서 정보제공서비스의 활성화를 목적으로 한국통신에서는 웹 인포샵 서비스 시스템(Web Infoshop Service System)을 운용중에 있다. 웹 인포샵 서비스란 웹 인포샵 서비스 시스템을 이용하여 유료 웹 서비스를 제공하는 것으로 사용자와 웹 서비스 제공업자(CP;Content Provider) 간을 연결하여 대체 인증기능과 대체 과금 기능을 수행하여 주는 서비스이다[5,6,7,8]. 웹 인포샵 서비스의 특징은 전화망을 통한 종량제 과금과 과금의 납부, 수납, 관리 업무를 인포샵 운용자가 대행하여 주는 것이다. 그러나 현재 WISS는 전화망 가입자와 ISDN 가입자로 한정되어 있다. 따라서 LAN 가입자의 웹 인포샵 서비스를 위해서는 신뢰성있는 사용자 인증이 이뤄져야 한다. 본 논문에서는 이러한 사용자 인증을 위한 시스템을 설계하고 구현하였다.

본 논문의 구성은 2장에서는 기존의 WISS와 제안된 LAN-WISS에 대해 설명하고 3장에서는 사용자 인증을 위한 보안 시스템을 설계하고 4장에서는 구현한 내용과 결과를 설명하고 5장에서는 결론 및 향후 과제를 다루었다.

2. 전용선 사용자를 위한 웹 인포샵 서비스

웹 인포샵 서비스는 다양한 종류의 정보를 정보 제공자에게 제공하고 그 대가를 받는 가상상점의 일종으로 이를 제공하기 위해서는 WISS는 사용자와 CP간을 연결하는 대체인증기능과 대체과금기능을 수행하는 서비스를 제공해야 한다.

대체인증기능을 위한 웹 인포샵 서비스를 인터넷 전용선에서 제공하기 위해서는 그림 1과 같이 WISS와 CP 간에는 기존의 HTTP 1.0 기본 인증법을 사용하는 것은 동일하며 사용자와 WISS간에는 특별한 방법으로 사용자 인증을 거쳐야 한다.

대체과금의 경우 유료 CP에 대한 각 사용자의 사용료의 부과와 회수등의 관리업무를 대신해 주는 것으로 CP 업자들에게 과금에 대한 부담을 줄일 수 있다.

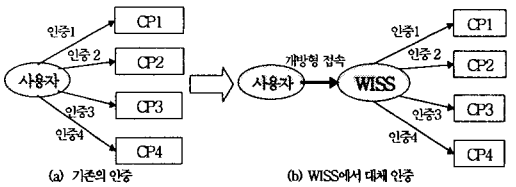

그림 1. 기존의 인증과 대체 인증 비교

그림 2는 전용선 사용자의 웹 인포샵 서비스(LAN-WISS)를 위한 시나리오에 대한 흐름도이다.

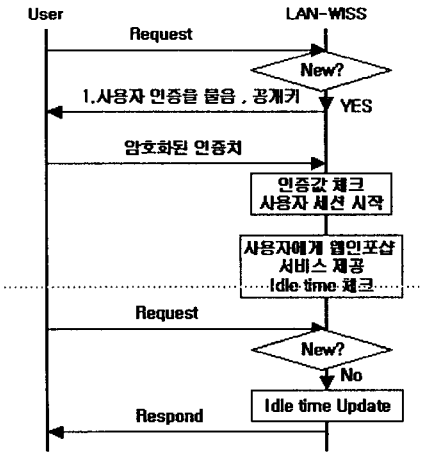

그림 2. LAN-WISS의 인증 시나리오

3. LAN-WISS에서의 사용자 인증 시스템 설계

현재 HTTP 1.0에서 지원하고 있는 사용자 인증 방법은 기본인증법이다. 기본 인증법은 사용자의 ID와 패스워드를 단순히 Base64 인코딩 방법을 사용하여 인코딩해 보내는 것으로 보안상 매우 취약한 약점을 가지고 있다. LAN-WISS에서 사용자와 WISS간의 인증에 사용 가능한 방법으로 기본 인증법을 사용할 수 있으나 사용자가 개인적으로 가지는 인증값은 각 개인의 고유의 것이고 쉽게 주기적으로 바꿀 수 있는 성질의 것이 아니므로 보안상 취약한 기본 인증법을 사용하는 것은 무리가 있을 수 있다. 따라서 LAN-WISS와 사용자간에는 보다 특별한 보안메카니즘이 적용되어야 한다. 또한 IP 주소를 사용자를 구분하는 기준으로 사용함으로써 불법적인 IP 도용을 막기 위해 사용자 세션 개념을 도입하여 사용자가 로긴한 순간부터 로그아웃할 때까지 관리한다.

LAN-WISS의 사용자 인증을 위한 보안 메카니즘으로 RSA알고리즘에 의한 암호화/복호화 방식이다[9,10].그리고 순수 JAVA에 의한 사용자측의 JAVA 애플릿과 서버측의 JAVA 어플리케이션으로 구성된다.

3.1 LAN-WISS의 구성

현재 상용화되어 서비스 중인 WISS는 Warpd, Wdbd, Wcmabd, Waobd, DB로 구성된다[8]. 사용자 인증을 위해서는 기존 WISS에 그림 3과 같이 Lwuad(LAN-WISS User Authentication Demon)을 추가한다.

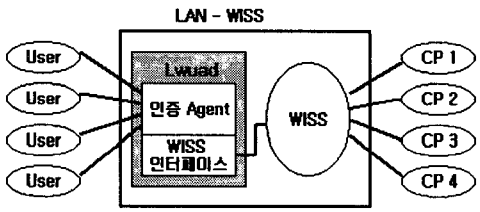

그림 3. Lwuad와 WISS의 통합

Lwuad는 사용자 인증과 이 인증된 결과로써 사용자의 IP 주소를 메시지큐를 통해 WISS에게 넘겨주게 된다. 그리고 사용자는 웹 브라우저의 프록시를 WISS의 URL로 지정해야 한다. LAN-WISS 보안 시스템은 그림4와 같이 LAN 사용자와 WISS간의 사용자 인증을 위하여 RSA 알고리즘에 의해 인코딩함으로써 완벽한 보안을 보장해 줄 수 있는 방법을 사용한다. LAN-WISS 보안 시스템은 서버, 암/복호 AGENT, 그리고 DB 테이블로 구성된다.

그림 4. LAN-WISS 보안 시스템의 구성

서버의 클라이언트 처리 모듈은 클라이언트와의 소켓 통신을 통해 클라이언트와 메시지를 주고 받고 사용자로부터 로그인, 로그아웃, 사용자등록, 사용자 정보변경등의 요청을 처리하고 데이터베이스 처리모듈은 소수 테이블, 사용자 관리 테이블, 로그인 관리 테이블등의 관리를 한다. 그리고 공개키 분배 모듈은 클라이언트가 공개키 요청을 할 때 클라이언트에게 공개키 분배를 하고 암/복호 AGENT 통신 모듈은 비밀키/공개키 생성, 암호화, 복호화등의 작업을 수행하는 AGENT와 통신을 담당한다. 암/복호 AGENT는 DB 접근을 통해 비밀키/공개키를 생성하고 암/복호화에 관계된 기능을 담당하는 모듈이다.

LAN-WISS는 그림 5와 같이 세 개의 HTTP 세션을 가진다. 첫 번째 세션은 사용자의 로그인 여부와 요청한 CP사용이 유료 CP인지 무료 CP인지를 확인하는 과정이다. 두 번째 세션은 로그인 하지 않고 유료 CP 사용을 요청한 사용자에 대한 인증과정이다. 즉 사용자의 유료 CP 사용의 요청으로 세션이 시작되면, 사용자는 인증을 위한 JAVA 애플릿을 로드하게 된다. 사용자는 이 JAVA 애플릿과 서버와 암호화된 메시지의 교환으로 인증여부를 결정받게 된다. 그리고 세 번째 세션은 인증치를 CP로 보내 대체 인증을 WISS가 하고 사용자와 CP를 연결하는 것이다.

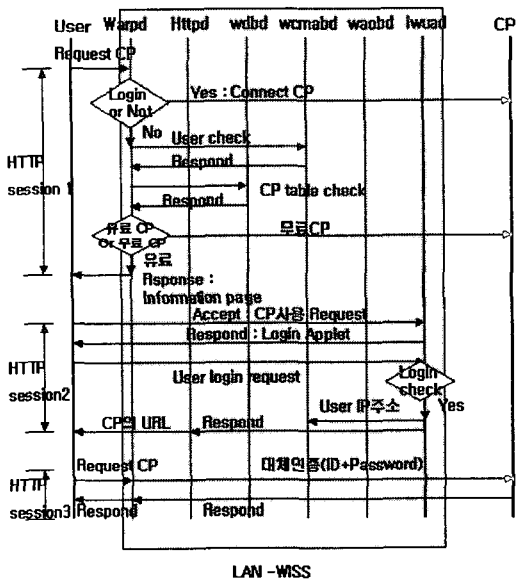

그림 5. LAN-WISS 로그인 메시지 흐름도

3.2 보안 모듈

앞에서 언급한 Lwuad의 기능중 가장 핵심적인 기능으로 사용자 인증을 위한 보안기능이다. 이는 공개키와 비밀키의 쌍에 기반을 둔 암호화 및 복호화 알고리즘인 RSA 알고리즘에 기반을 두고 있다 [9,10]. 사용자가 인증을 받기 위해 우선 서버에게 키를 요청하면 JAVA 인증 에이전트는 키 생성모듈에 의해 생성된 키 쌍중 비밀키를 제외한 공개키를 JAVA 애플릿으로 전송한다. JAVA 애플릿은 수신된 공개키로 사용자의 ID와 비밀번호를 암호화함으로써 네트웍상에서 전송중에 사용자의 ID와 비밀번호가 노출되는 우려를 막을 수 있다. JAVA 애플릿과 인증에이전트는 공개키와 비밀키로서 JAVA의 BigInteger클래스를 사용하므로 제한된 키의 한계를 벗어날 수 있다. 그리고 JAVA 인증 에이전트는 암호화된 메시지의 복호화를 통해 사용자 인증의 여부를 결정하고 그 결과로 사용자의 IP 주소를 WISS에게 넘겨준다.

3.3 사용자 인증 모듈

사용자 인증을 위해서 LAN-WISS는 사용자가 유료 CP에 대해 여러개의 브라우저를 동시에 사용할 수도 있으므로 사용자의 IP 주소에 대해 인증 여부를 결정한다. 이 경우 Lwuad는 사용자가 입력한 ID와 비밀번호를 DB에 저장된 데이터와 확인하는 검증과정을 거쳐 확인이 되면 Warpd에게 인증된 IP 주소를 넘겨준다. Warpd는 사용자 IP 주소가 정상적으로 로그인된 사용자라면 유료 CP에 대해 대체 인증과정을 수행한다.

Lwuad의 JAVA 인증 에이전트와 Warpd와의 메시지 전달은 C로 구현한 인터페이스 서버를 통해서 이뤄지는데 인터페이스 서버는 JAVA 인증 에이전트로부터의 결과를 메시지큐를 통해 Wcmabd에게 전달하고 DB 접근에 대한 제어를 한다.

4. 사용자 인증 시스템 구현

Lwuad는 사용자의 인증과 보안을 위한 인증 시스템과 기존의 WISS와 연동을 위한 C 인터페이스 에이전트 그리고 사용자를 위한 JAVA 애플릿으로 구성된다. JAVA로 구현된 인증 시스템과 C로 구현한 WISS 인터페이스 서버는 유닉스상에서 동작하고 사용자 JAVA 애플릿은 사용자의 웹 브라우저에서 동작한다.

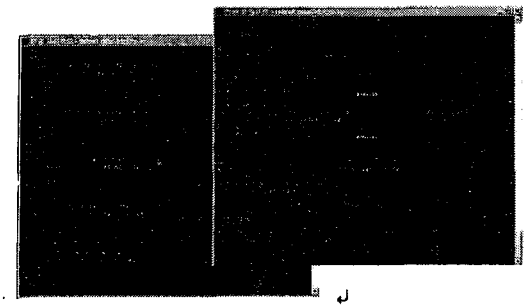

그림 6 LAN-WISS 보안시스템 서버

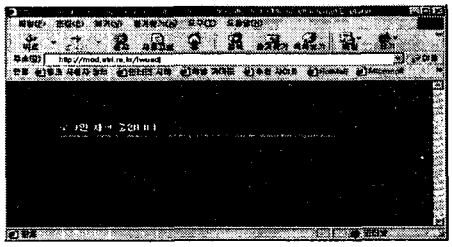

그림 7 LAN-WISS 보안 시스템
클라이언트

5. 결론 및 향후 과제

본 논문에서는 전용선 사용자를 위한 웹 인포샵 서비스인 LAN-WISS에서 사용자 인증을 위한 보안 시스템을 구현한 내용을 기술하였다. LAN-WISS는 WISS가 가지는 대체 인증 기능과 대체 과금 기능을 LAN 사용자까지 확대시키려는 것이 목적으로 이를 위해선 필수적으로 LAN 사용자에 대해서 신뢰할 수 있는 사용자 인증이 이뤄져야 한다. 이는 사용자 인증에 있어 RSA 알고리즘에 의해 보안화함으로써 부정사용자들의 개입을 막을 수 있고 유료 CP에 대해 대체 인증이 가능하다.

LAN-WISS 보안 시스템에서 구현된 RSA암호 알고리즘은 순수 JAVA에 의해 구현되었으므로 키 크기에 의한 RSA 알고리즘의 본질적 약점을 충분히 개선하였다. 향후 LAN-WISS는 사용자 인증을 위한 보안 시스템과 웹 인포샵 서비스 시스템을 통합하고 과금관리기능, 시스템 관리 기능등과 같은 부가 기능을 추가함으로써 사용자와 CP를 위한 최상의 기능을 수행할 수 있을 것이다.

*본 논문은 한국통신에서 출연한 'RAS형 AICPS 개발' 과제의 연구결과물중 일부입니다.

참고문헌

[1] O'callaghan,D.,"A central cashing proxy server for WWW users at the University of Melbourne"Proceedings of AusWeb95, March, 1995

[2] T.Berers-Lee et al.,"The WOrld-Wide Web," Commun. ACM, vol.37, pp.76-82, aug.1994

[3] Henning Schulzrinne, "World Wide Web: Whence, Whither, What Next?," IEEE Network, pp.10-17, march/April 1996

[4] Admir Herzberg, Hilik Yochai, "MiniPay:Charging per Click on the Web," Sixth International World Wide Web Conference, pp239-253, April, 1997

[5] Chang Woo Yoon, Dae-Ung Kim, "Providing Fast and Time Predictable Web Inforshop Services in Real Time System," ISCOM'97, Taiwan, pp241-244, December 1997.

[6] Chang Woo Yoon,"Vicarious Certifiation and Billing Agent for Web Information Service," ICOIN'98, Japan, January 1998.

[7] 윤장우,"웹 인포샵 서비스 시스템을 이용한 웹 사이트 유료화 방법," 1998 통신학회 추계종합학술논문집, pp927-930, 1998.11.

[8] 윤장우, 이현우, "내장형 시스템엣의 웹 인포샵 서비스 제공 방법," 1999 COMSW'99. pp235-238, 1999.7

[9] Douglas R. Stinson, *CRYPTOGRAPHY : Theory and Practice*, CRC Press, 1995.

[10] William Stallings, *Network and Internetwork Security*, Prentice-Hall, 1995

[11] Charles Broooks, Murrary S. Mazer, Scott Meeks, Jim Miller, "Application-Specific Proxy Servers as Http Stream Transducers," Fourth International World Wide Web Conference, pp539-548, December, 1995.

[12] Jeffery K. MacKie-Mason, Hal R. Varian, "Some FAQs About Usage-Based Pricing," Second International World Wide Web Conference, pp302-311, December, 1993.

[13] Louis Perrochon, Andera Kennel, "W3-Access for Blind People," Fourth International World Wide Web Conference Poster Session pp92-93, December, 1995.