LAN-WISS(Web Infoshop Service System)을 위한 보안 인증 모듈 설계 및 구현

백영미*, 이종훈*, 안경환*, 이현우**, 한기준*
*경북대학교 컴퓨터 공학과, **한국전자통신연구원 서비스네트워크연구부
{backjoo, abyss, khan}@netlab.ce.knu.ac.kr, hwlee@etri.re.kr, kjhan@bh.knu.ac.kr

Design and Implementation of Security Authentication Module for LAN-WISS

Young-Mi Baek, Jong-Hoon Lee, Kyung-hwan Ahn, Hyun-Woo Lee, Ki-Jun Han
Dept. of Computer Engineering, Kyungpook University,
ETRI, Service Network Department

요 약

본 논문은 웹 인포샵 서비스를 인터넷 전용선 사용자에게도 제공하기 위해 반드시 필요한 보안 인증 모듈을 설계 및 구현하였다. 보안 인증 모듈은 사용자의 요청 처리와 사용자의 인증 절차 및 암호화 기능을 수행하는 인증 에이전트와 사용자 정보를 암호화하여 전송하고 인증 에이전트로부터 수신한 응답을 처리하는 클라이언트로 구성된다. 이 때 사용된 암호화 알고리즘은 공개 키 암호법인 RSA알고리즘으로 사용자의 인증치를 보안 공격으로부터 보호한다. 유닉스 상에서 동작하는 인증 에이전트는 C와 JAVA로 구현했고 클라이언트는 JAVA와 JAVA APPLET으로 구현하였다. 현재 구현한 보안 인증 모듈과 웹 인포샵 서비스 시스템을 통합중이고 향후에는 과금 관리 기능, 시스템 관리 기능 등과 같은 부가 기능을 추가하여 최적화된 LAN-WISS를 완성 할 계획이다.

1. 서론

웹을 이용한 서비스의 대부분은 비 상업용이지만, 최근에 와서 엔터테인먼트 사이트, MP3 제공 사이트, 성인 사이트 등의 정보 제공 분야에서 상업용 사이트 수가 증가하고 있다. 현재 웹에서의 정보 제공 서비스는 신용카드를 이용한 과금 방법 등이 널리 행해지고 있다. 그러나 신용카드를 사용함으로써 발생하는 문제점과 비효율성으로 과금 방법의 한계에 부딪히고 있다.

이러한 문제를 해결하고, 웹 상에서 정보 제공 서비스의 활성화를 목적으로 한국통신에서는 웹 인포샵 서비스 시스템(Web Infoshop Service System)을 개발하여 운용중에 있다[1,2,3,4]. 그러나 현재 운용되고 있는 WISS는 전화망 가입자와 ISDN망 가입자에 대해여 웹 정보 제공업자(CP : Content Provider)의 서비스를 제공하므로 사용자의 이용에 제한이 있다. 이러한 한계를 극복하기 위하여 인터넷 전용선을 사용하는 이용자들을 수용할 수 있도록 대체 인증 및 대체 과금 기능을 제공하는 LAN-WISS(LAN-Web InfoShop Service System)의 개발이 제안되었다[10].

본 논문은 랜 사용자가 LAN-WISS를 통하여 CP 서비스를 제공받으려 할 때 개인 정보를 보호하는 보안 기능을 가지고 인증 절차를 수행하는 보안 인증 모듈을 설계하고 구현한다. 가장 중요한 기능인 개인 정보 보호는 적절한 암호화 방식을 이용하여 암호화된 사용자의 인증치를 LAN-WISS에 전달하여 올바른 인증치인지를 복호화하여 검사함으로써 제공한다. 여기에 사용한 암호화 방식은 RSA(Rivest, Shamir and Adleman) 알고리즘이다[5,6].

본 논문의 구성은 2장에서 기존의 WISS과 제안된 LAN-WISS 개념을 기술하고, 3장에서는 LAN-WISS의 보안 인증 모듈을 설계한 내용을 설명하였다. 4장은 구현한 모듈의 내용과 결과를 기술하였으며, 마지막으로 5장에서 결론 및 향후 연구 방향을 언급하였다.

2. 관련 연구

웹 인포샵 서비스[1,2,3,4]란 웹 환경을 이용하여 다양한 종류의 정보를 정보 사용자에게 제공하고 그 대가를 받는 가상 상점의 일종이다. 이런 서비스를 제공하는 WISS는 사용자와 CP간을 연결하여 대체 인증 기능과 대체 과금 기능을 수행하는 서비스를 제공한다.

대체 인증 기능은 유료 웹 서비스를 사용하기 위하여 그림 1과 같이, 사용자가 입력해야 하는 인증치를 WISS가 대신 입력해 주어 사용자의 편의성을 높여주며, 대체 과금 기능은 WISS에서 사용자의 전화번호로 과금하여 대신 징수함으로써 과금 회수률을 높인다. 이러한 기능으로 CP 사업자는 기존에 이뤄지던 사용자에 대한 개별 관리

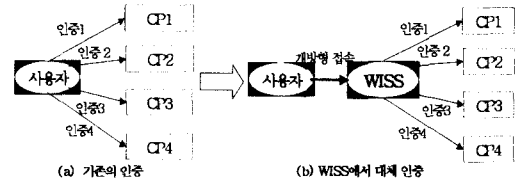


그림 1. 기존의 인증과 대체 인증 비교

와 과금에 대한 부담을 덜 수 있다.

그림 2는 LAN-WISS에서의 대체 인증 개념 모델로, 사용자와 CP 서버 사이에 위치하는 인증 에이전트가 CP 서버에서 해야 할 사용자에 대한 인증을 대신 해주는 개념이다. 이러한 개념이 실제 적용되기 위해서는 사용자와 인증 에이전트간에 정보가 보장되는 폐쇄망이어야 한다[2].

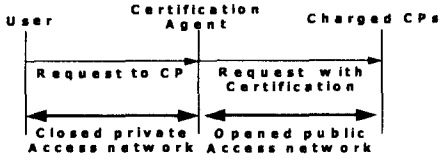


그림 2. 대체 인증 개념 모델

실제 인증 메커니즘이 적용되는 부분은 인증 에이전트이다. 사용자와 인증 에이전트사이에 사용자 정보의 보안이 제공되면서 인증 절차가 이루어지면, 사용자는 여러 CP서버에 대해서 각기 다른 인증을 유지 할 필요 없이 인증 에이전트와 단 하나의 인증 관리만 유지하면 된다[1,2].

3. LAN-WISS 보안 인증 모듈 설계

현재 상용화되어 서비스 중인 WISS는 DB, Warpd, Wdbd, Wcmabd, Waobd로 구성되어있는데[2], 사용자는 WISS의 서비스를 받기 위해 WISS로 프록시를 지정해야 한다[7,8,9]. 이 WISS에 랜 사용자에 대한 대체 인증 기능, 대체 과금 기능, 정보 보호 기능을 부여하기 위하여 그림 3과 같이 보안 인증 모듈인 Lwuad(LAN-WISS User Authentication Demon)를 추가한다

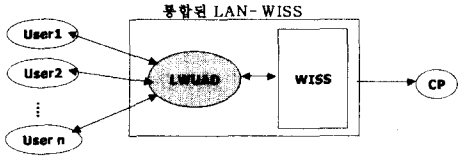


그림 3. WISS와 LWUAD의 연동

다음 그림 4는 LAN-WISS 시스템에서 Lwuad와 통합되었을 경우의 시스템의 모듈간의 연관 관계를 나타낸 것이며, 그림 5는 사용자의 LAN-WISS 접속부터 CP 연결까지 메시지 흐름과 동작 과정을 나타내었다.

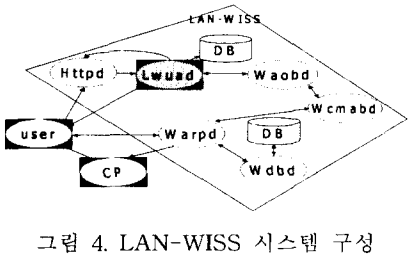


그림 4. LAN-WISS 시스템 구성

LAN-WISS는 IP 주소로 사용자를 구분하므로, 불법적인 사용과 IP 도용을 막기 위해 세션 단위로 관리된다.

가령, 로그인의 경우 세 개의 HTTP 세션을 가지는데 내용은 다음과 같다.

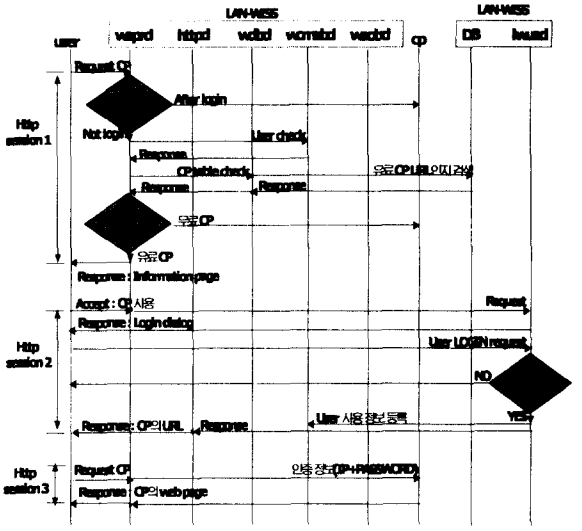


그림 5. LAN-WISS 로그인 동작 과정 및 메시지 흐름

첫 번째 세션은 사용자의 로그인 여부와 요청한 CP사용이 유료 CP인지, 무료 CP인지 확인하는 과정이다.

두 번째 세션은 로그인하지 않고 유료 CP 사용을 요청한 사용자에 대한 인증 과정이다. 즉, 사용자의 유료 CP 사용의 요청으로 세션이 시작되면, 요청을 수신한 Lwuad는 로그인 창을 사용자에게 전송한다. 사용자 웹 브라우저의 로그인 창에 사용자가 정보를 입력하여 개인 정보가 전송될 때, 기존의 HTTP 1.0에서 지원하는 기본 인증법만으로는 보안상 매우 취약하므로, 공개키 암호 알고리즘인 RSA를 사용하여 랜 사용자와 LAN-WISS간에 개인 정보를 보호한다. 암호화할 때, 각 사용자에 대해서 세션 단위로 키를 생성함으로써 보안성을 더욱 높인다. 또한 RSA의 단점인 처리 속도 문제를 보완하기 부가적인 작업을 추가한다. Lwuad에서는 수신한 사용자 정보를 복호화하여, 사용자 인증 과정을 통해 사용자 인증 절차가 올바르게 종료하면, 인증된 사용자에 대한 정보를 관리하도록 Wcmabd에게 요청한다.

마지막 세션은 인증치를 CP로 보내고 사용자와 CP를 연결하는 것이다.

4. 보안 인증 모듈의 구현

Lwuad는 사용자의 인증과 기존의 WISS와의 연동을 담당하는 인증 에이전트와 사용자와의 연동을 위한 클라이언트로 구성되어있다. 인증 에이전트는 JAVA와 C로 구현하여 유닉스 상에서 동작하고 클라이언트는 JAVA와 JAVA APPLET으로 구현하여 사용자의 웹 브라우저에서 실행된다. 개인 정보를 보호하기 위해 공개 키 암호법인 RSA 알고리즘으로 암호화하여 전송한다[5,6].

4.1 인증 에이전트

인증 에이전트는 클라이언트 통신 모듈, 요청 처리 모듈, 데이터 베이스 처리 모듈, 기존 WISS와의 연동 모듈, 복호화 모듈, 키 분배 모듈로 구성된다. 각 처리 모듈의 기능은 표 1과 같다.

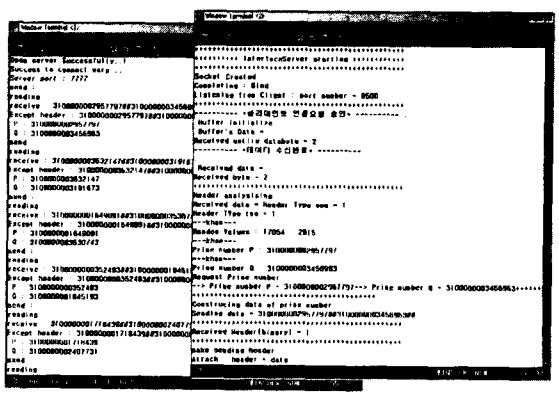
표 1. 인증 에이전트 모듈의 기능

모듈	기능	비고
클라이언트 통신 모듈	다중 사용자 지원 / 생성된 공개키 및 데이터를 수신 및 전송 - JAVA	소켓 통신
요청 처리 모듈	로그인, 암호변경, 로그 아웃, 사용자 등록 처리 - C/JAVA	
데이터 베이스 처리 모듈	사용자 정보와 과금을 위해 사용자의 데이터 사용량 혹은 사용 시간을 저장 - C	
WISS 연동 모듈	WISS에 인증된 사용자에 대한 정보 전달 사용자 정보 메시지 관리 요구 - C	메시지 큐를통한 통신
복호화 모듈	수신한 사용자 정보를 복호화 - JAVA	
키 분배 모듈	소수사용 비밀키/공개키 생성 - JAVA	RSA 알고리즘

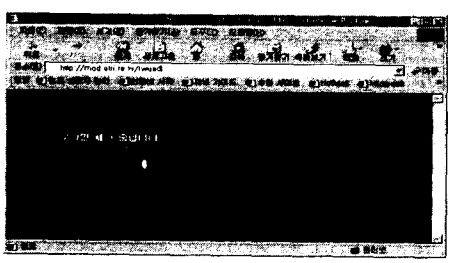
4.2 클라이언트

클라이언트는 사용자 개인 정보를 암호화하는 암호화 모듈과 에이전트와 소켓 통신을 하는 에이전트 통신 모듈이 있다. 웹 브라우저의 로그인 창으로 사용자가 사용자의 정보를 입력하면, 서버로부터 전송 받은 공개키로 암호화 모듈에서 사용자 정보를 암호화하여 Lwuad로 전송한다. Lwuad는 클라이언트로부터 전송된 인증치에 대한 인증 과정이 종료하면 인증 결과를 클라이언트로 전송하게 되는데 이 때, 전송 받은 메시지를 웹 브라우저에 출력한다. 사용자가 자신의 인증치를 자의로 노출시키지 않는 한 인증치는 안전하게 보관되며, 안전하게 전송될 수 있다.

그림 6은 Lwuad를 구현하여 테스트한 내용으로 인증에이전트의 왼쪽이 JAVA를 사용하여, 오른쪽이 C로 구현한 것이다.



(a) 인증에이전트



(b) 클라이언트

그림 6. 보안 인증 모듈 구현 결과

5. 결론 및 향후 과제

본 논문에서는 LAN-WISS를 위한 보안 인증 모듈을 인증 에이전트와 클라이언트로 구성하여 구현한 내용을 기술하였다. 인증 에이전트는 사용자 요청에 대한 처리를 하고, 개인 정보를 RSA알고리즘으로 암호화하고 기존의 WISS와의 연동을 고려하여 구현하였다. 클라이언트는 사용자측의 웹 브라우저에서 실행되고 사용자의 정보를 전송함에 있어 정보 보호를 위해 인증 에이전트로부터 받은 공개키로 암호화하여 전송하고 에이전트의 응답을 웹브라우저로 표현하는 기능을 수행한다. 이 인증 모듈의 구현으로 전화망 및 ISDN 망 가입자에게만 한정되어 있던 웹 인포샵 서비스를 인터넷 전용선 사용자에게도 제공할 수 있게 되었다. LAN-WISS의 보안 인증 모듈은 구현한 상태로, 현재 구현한 보안 인증 모듈과 WISS와의 통합 작업이 진행중이고, 향후에 과금 관리 기능, 시스템 관리 기능 등과 같은 부가 기능을 추가하여 최적화된 LAN-WISS를 완성 할 계획이다.

*본 논문은 한국통신에서 출연한 'RAS형 AICPS 개발' 과제의 연구 결과입니다.

참고 문헌

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

[2] 윤장우, 이현우, "내장형 시스템에서의 웹 인포샵 서비스 제공 방법," 1999 COMSW'99, pp235-238, 1997.7.

[3] Chang Woo Yooon, "Vicarious Certification and Billing Agent for Web Information Service," ICOIN'98, Japan, January 1998.

[4] Chang Woo Yoon, Dae-Ung Kim, "Providing Fast and Time Predictale Web Infoshop Services In Real Time System," ISCOM'97 Taiwan, pp241-244 , December 1997.

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

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

[7] 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.

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

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