웹에서의 데이터 기밀성을 위한 암호방식 적용방안 및 응용

김동현*, 안선후**, 이성주***

A Study on the Implementation of Cryptography Scheme for Secure Data Transmission on WWW

Dong-Hyun Kim, Sun-Hoo An, Sung-Ju Lee

본 연구는 순천청암대학 교내 학술진흥연구비 지원에 의해 수행 되었음

요 약

본 논문에서는 기존의 HTTP 프로토콜에 의해 서버와 클라이언트 간에 송수신하기전에 응용계층에서 전송되는 메시지를 RSA공개키로 암호화한다. 또한, 넷스케이프 브라우저에 어플리케이션 프로그램의 지원과 플러그인 확장 기술을 사용하여 암호 모듈을 접속시킴으로써 WWW에서 안전한 데이터 전송이 가능한 정보보호 시스템을 구현하였다. 이러한 기술을 통하여 키 관리 및 암호화 전송절차가 간결하고 용이하게 되었고, 암호화 통신에 소요되는 시간이 단축되었다.

Abstract

In this study, the messages sent at application layer are encrypted by using RSA Public Keys before sending. Then we developed the information security system devised for the secure WWW data transmission by extending the functions of the Netscape browser and by using application programs such as Java applications and by using the plug-in methods. Not only can these technologies reduce and make it easier to

* 순천청암대학 컴퓨터정보과학부 교수
** 광주대학교 공학석사
*** 조선대학교 컴퓨터공학부 교수
접수일자 : 2000년 7월 8일

perform key management or encryption transmission process, but they can also reduce the processing time of encryption correspondence.

Ⅰ. 서 론

인터넷은 세계 최대의 통신 네트워크로서 그 사용이 급격히 증가하고 있는 추세이다. 인터넷은 정보의 바다라 불릴 만큼 방대한 양의 데이터를 포함하고 있기 때문에 사용자들이 인터넷을 통해서 자신이 원하는 데이터를 찾아내고 서로 주고받는다는 것은 그리 쉽지 않은 작업이다. 이러한 문제점으로 인하여 인터넷은 점차 그 사용의 한계를 드러내고 있었다. 그러나 1989년 유럽의 CERT에서 제한된 WWW의 도입은 이러한 문제점을 해결하기 위한 방안으로 고려되기 시작하였고 이후 이에 대한 연구가 진행되었다. 결과적으로 GUI 기반의 WWW 브라우저인 모자익이 발표되었고 이후 넷스케이프, 마이크로소프트 익스플로어등이 공개되면서 인터넷은 새로운 전기를 맞이하게 되었다. 이러한 WWW 브라우저들은 WWW의 접근 메커니즘으로 하이퍼링크를 제공함으로써 사용자는 단지 마우스를 누르는 단순한 작업을 통하여 자신의 원하는 데이터를 손쉽게 얻을 수 있게 되었다. 사용이 간단하다는 점 이외에도 WWW은 다양한 형태의 멀티미디어 데이터를 처리 할 수 있는 기능을 제공함으로써 그 사용자들에게는 네트워크를 사용하기 위한 일종의 Total-Solution으로 인식되고 있다.[1][3][8]

이러한 WWW의 사용 증가 추세에서 반드시 고려되어야 할 사항은 WWW이 가지고 있는 보안상의 문제점들이다. WWW은 인터넷이 가지고 있던 보안상의 문제점들을 그대로 물려받았기 때문에 데이터 전송시의 기밀성이나 무결성을 보장받을 수 없다. 따라서 전송되는 데이터에 대한 추가적인 보안 메커니즘이 고려되지 않는 한 데이터 보호가 요구되는 분야나 상업적인 용도로의 이용은 불가능 할 것이다. 예를 들면 군사 기밀이나 기업간의 정보 교환, 전자 상거래, 홈뱅킹 등의 분야에서 불법적인 사용자에 의 한 정보 유출이나 변조를 막을 수 없다면 상당한 혼란만 초래 할 것이다. 위와 같은 보안상의 문제점을 해결하기 위한 방안으로 1994년 EIT 사에서는 S-HTTP라는 새로운 형식의 HTTP 프로토콜을 제안하였다. 이와 비슷한 시기에 넷스케이프사에서는 SSL 프로토콜을 제안함으로써 WWW 보안 문제 해결에 새로운 전환점을 맞이하게 되었다. S-HTTP는 WWW의 기반 프로토콜인 HTTP의 기반이 되는 TCP/IP 레벨의 암호화 모듈을 제공함으로써 데이터의 보호를 시도하였다. S-HTTP나 SSL의 경우 모두 기본적인 아이디어는 데이터의 암호화 송수신이라는 면에서 서로 일맥상통 하지만 암호화 모듈이 적용되는 범위가 서로 다르다는 차이점이 있다.[5]

본 논문에서는 WWW 보안상의 문제점을 해결하기 위한 방안으로 모든 데이터를 처리하는데 있어서 데이터 보안 시스템을 통하여 특정 응용분야에서만 사용되는 암호화기법을 제공함으로써 WWW 통신의 오버 헤드를 줄일 수 있다. 이는 데이터의 암호화가 특정 그룹이나 회원위주의 관리 시스템 내에서 수행되는 전송이나 서비스에만 적용된다는 것을 의미한다. 인터넷이 정보의 공유를 주장한다는 점이나 사용 증가로 인한 전송률의 저하를 고려한다면 이러한 방식의 암호화 전송 방식은 여러 가지 장점을 가질 수 있다. 본 논문에서 제시된 데이터 보안 시스템은 공개키 암호 방식을 이용하여 구현하였다.

Ⅱ에서는 공개키 암호화 방식과 키관리 방식에 대해서 살펴보고 Ⅲ에서는 WWW 보안 및 RSA 암호방식 적용에 관한 설계를하고 Ⅳ에서는 공개키 암호 방식에 기반한 WWW 데이터 보안 시스템의 구현에 대하여 기술한다. 그리고 마지막으로 Ⅴ에서는 결론을 맺는다.

Ⅱ. 관련연구

1. 공개키 암호방식

1976년 W.Diffie와 M.E. Hellman이 논문 'New Directions in Cryptography'에서 최초로 제시한 공

개키 암호 방식은 기존 암호학의 상식을 뛰어넘는 혁신적인 발상으로 키의 일부를 공개함으로써 키 관리의 어려움을 해결하고자 하는 방식이다. 관용 암호 방식은 송·수신자가 동일한 키에 의하여 암호화와 복호화 과정을 수행하므로 키를 안전하게 전송하고 보관함에 있어 어려움이 야기된다. 이에 비하여 공개키 암호 방식은 암호화할 때 사용하는 키(일명 암호화키 또는 공개키)와 복호화할 때 사용하는 키(일명 복호화 키 또는 비밀키가 달라서 공개키는 공개하고 비밀키만 안전하게 유지하는 방식이다(암호화 키 ≠ 복호화 키). 즉 A가 B에게 비밀 통신을 하고자 하는 경우, A가 공개키 디렉토리(예: 전자 게시판등)에 공개된 B의 공개키를 가지고 송신할 내용을 암호화하여 B에게 전송하면 B는 자신만이 가지고 있는 비밀키를 이용하여 암호문을 복호화 한다. 따라서 관용 암호 방식에서 전제로 하였던 키의 안전한 분배는 필요 없게 된다.[1][2]

만약 n명이 비밀 통신을 하려면 관용 암호방식에서는 한 명당 (n-1)개의 키가 필요하므로 총 $nC_2 = 1/2 \cdot n \cdot (n-1)$ 개의키가 필요하나 공개키 암호 방식은 한명 당 두 개의 키가 필요하므로 2n개의 키면 충분하다. 예를 들면 1천여명의 가입자를 가진 관용 암호 방식은 1/2 * 1,000 * 999 = 499,500개의 키가 필요하지만 공개키 암호 방식은 1천개의 공개키와 1천개의 비밀키만 있으면 충분하다. 일반적으로 공개키 암호 방식을 구성하는 방법으로는 수학적으로 어려운 문제(NP 문제)로 알려진 다음의 세 문제를 가장 많이 사용한다.[1]

[정의 1] 소인수 분해 문제

주어진 합성수 n의 소인수들을 찾는 문제로 n의 자리수가 매우 큰 경우(10^{150}이상)에는 n의 소인수를 효율적으로 찾는 알고리즘이 아직까지는 존재하지 않는다고 알려져 있다.

[정의 2] 이산대수 문제

소수 p가 주어지고 $y \equiv g^x \pmod p$인 경우, 역으로 $x \equiv \log_g y \pmod p$인 x를 계산하는 문제이다. 여기서 x를 법 p상의 y의 이산대수라 한다. p가 매우 큰(2^{512}이상)소수이고 g의 위수 k 가 2^{140}이상인 경우, x, g, p가 주어졌을 때 p가 비교적 큰 정수라 해도 y는 고속 지수계산 알고리즘을 사용하여 쉽게 구할 수 있지만 y, g, p가 주어졌을 때 $x \equiv \log_g y \pmod p$인 x를 구하는 문제는 어려운 것으로 인정되고 있다. (여기서, g의 위수는 k는 $g^k \equiv 1 \pmod p$를 만족하는 최소의 양의 정수).

[정의 3] 이차 잉여류문제

gcd(x, n) = 1인 정수 x에 대하여 이차 합동식 $w^2 \equiv x \pmod n$가 해를 가질 때 x를 법 n에 관한 이차 잉여라 하고 이 합동식이 해를 가지지 안을 때 x를 법 n에 관한 이차 비잉여라고 한다. x, n에 대하여 x가 이차 잉여인지 이차 비잉여인지를 결정하는 문제를 법 n상에서 이차 잉여류 문제라 하고 이 문제는 소인수 분해 문제와 동치임이 알려져 있다.[1][5][8]

2. 암호화 키관리

관용암호계에서는 조립과 번역에 각각 같은 열쇠를 사용하고, 암호화의 대상이 바뀔 때마다 다른 열쇠를 사용하기 때문에 안전관리에 필요한 열쇠 수가 대단히 많아지게 된다. 이 때문에 열쇠의 계층적인 관리 시스템을 도입하여 열쇠 그 자체를 다른 열쇠로 암호화하여 보관하는 등, 본질적으로 관리해야하는 열쇠의 수를 감소시키고, 가능하다면 일원화할 필요가 있다. 이와 같은 열쇠를 마스터키라 부른다. 이에 반해 공개 열쇠 암호 계에서는 조립용 열쇠는 공개되기 때문에 번역용 열쇠만을 비익하면 된다. 따라서, 관리해야하는 열쇠의 수는 관용암호계와 비교해 볼 때 더작지만, 각 별개의 열쇠를 사용하는 것보다는 공통으로 대체할 수 있는 간단한 마스터 열쇠가 있으면 관리를 일원화하기가 용이하다.[1][5]

Ⅲ. WWW 보안 및 RSA암호방식적용 및 설계

WWW은 1989년 팀 버너스에 의해 제안되어 그동안 모자익과 넷스케이프등의 사용자 인터페이스를 편리하게 설계한 브라우저의 출현으로 널리 퍼져 나가기 시작했다. 인터넷은 초기에 전문가들만이 사용했던 이유로 군사, 교육, 연구용으로 사용되었지만, 이제는 소비자들의 편리성과 기업의 이해 관계가 부합되어 상거래에까지 사용되고 있다.

그러나, WWW의 근간인 인터넷은 본래 개방형 시스템을 기반으로 설계되었기 때문에 WWW 또한 보안의 측면에서는 취약한 것으로 알려지고 있다. 일반 시민들의 상거래 수단으로까지 사용되고 있는 WWW의 보안 문제는 더 이상 간과할 수 없는 사항으로써, 본 절에서는 WWW이 가져야 할 보안 요구 사항을 알아보고, 암호 기술을 이용한 WWW 보안에 대해 살펴본다.[10]

1. WWW 보안 요구사항

WWW에서 이루어져야 할 보안 요소로 다음과 같은 것을 정의 할 수 있다.

(1) 시스템 보안

WWW의 암호화 통신을 구현하기 전에, WWW 프로그램 자체에 보안 통로를 갖지 않도록 해야한다. 보안 통로이란, 불법 침입자가 시스템에 접근할 수 있게끔 하는 시스템의 허점을 뜻한다.

(2) 기밀성

WWW의 통신 내용을 클라이언트 사용자와 서버 즉, 통신의 두 당사자만이 파악할 수 있도록 하는 기능을 말한다.

(3) 서버 인증

WWW 통신을 할 때 클라이언트가 접속한 서버가 실제도 의도했던 서버인지를 확인시켜 주어야 한다.

(4) 클라이언트 인증

서버에 대한 인증 작업이 필요하듯이 클라이언트 사용자에 대한 인증 작업이 필요하다. 문서에 대해 접근 제어를 전혀 하지 않는다면 문제가 되지 않지만 특정인에게만 서비스를 제공해 주고자 한다면 접속한 클라이언트 사용자가 적합한 사용자인가를 확인하는 절차가 필요하게 된다.

(5) 무결성

서버와 클라이언트에 대한 인증이 완료되고 서로의 공개키와 세션키를 이용하여 암호통신을 한다고 해서 모든 보안 요구 사항이 충족되지는 않는다.[3][5][8][11]

2. 암호 기술을 이용한 WWW 보안

앞에서는 현재 사용되고 있는 WWW의 보안 요소들을 알아보았다. 하지만 보다 강력한 보안 요구사항들을 만족시켜 주기 위해선 현재의 HTTP에 알고리즘을 추가시킨 방법이 필요하다. 암호 알고리즘을 사용하는 것만이 문서의 기밀성과 무결성, 사용자 및 서버의 인증을 보장해 줄 수 있는 방법이다. 하지만 WWW에 암호 알고리즘을 추가시키는 작업이 매우 어려운 것으로 간주되고 있는데 그 이유는 다음과 같다.

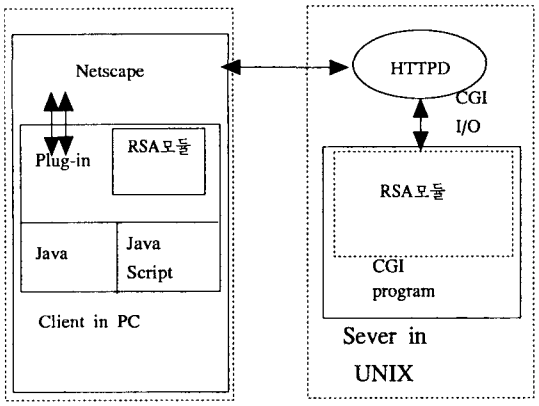
- 새로운 표준이 제정되어야 할 정도로 HTTP와 HTML의 확장이 필요하다.
- 브라우저와 서버 양쪽에 암호화 알고리즘을 추가시켜야 한다.
- 존재하는 암호화 알고리즘들은 심각한 취약점이 발견될 수 있으므로 앞으로 개발될 알고리즘을 수용할 수 있어야 한다.
- 몇몇 나라에서는 암호화 기술의 수출입을 제한하고 있어서 암호화 알고리즘의 사용이 자유롭지 못하다.
- WWW에 암호화 기술을 추가하기 전에 키의 인증을 전담하고 관리할 기구등의 다른 요소가 미리 설계되어야 한다.
- WWW은 전체 네트워크 중에서 극히 적은 부분을 차지하고 있기 때문에 WWW에 국한되지 않은 네트워크 전체를 지원해 줄 수 있는 기술이 필요하다.

3. RSA 암호방식 적용에 관한 설계

(1) 공개키 기반 WWW 보안 시스템 설계

공개키 암호 방식을 이용한 WWW보안 시스템의 전체적인 구성도 이다. 공개키 암호방식의 도입을 위하여 RSA암호 알고리즘을 사용하며 Ⅲ에서 기술된 LiveConnect 기법을 이용하여 넷스케이프와 암호 모듈과의 데이터 교환을 구현하였다.

전체적인 구조를 살펴보면 클라이언트의 경우 플러그인과 자바와 자바스크립트로 구성된 암호화 적용 모듈이 넷스케이프에 Embeding 되며 PC 사용자를 대상으로 한다. 플러그인과 자바와 자바스



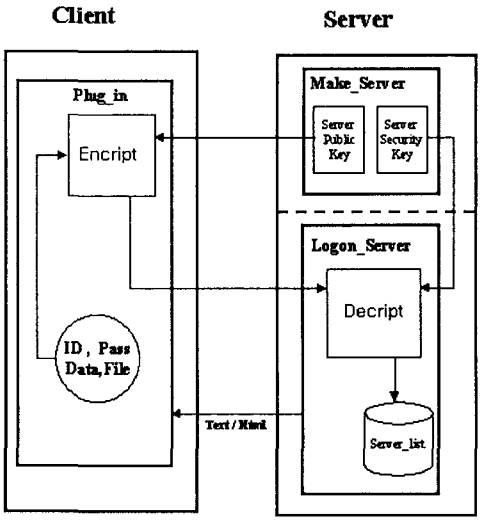
〈그림 1〉 공개키 암호방식에 기반한 WWW 데이터 보안 시스템 구성도

크립트 사이의 데이터 교환을 위하여 3장에서 언급한 LiveConnect 기법이 사용된다. 암호화 적용모듈 중 플러그인 부분은 데이터 암호화를 수행하기 위하여 RSA 모듈을 포함하며 넷스케이프와의 실질적인 데이터 교환과 제어 기능을 수행한다. 서버는 HTTPD와 RSA 모듈을 포함하는 CGI 프로그램으로 구성되며 UNIX 시스템 상에서 동작한다. 클라이언트와 서버 사이의 데이터 전송은 HTTP 프로토콜을 그대로 이용하며, 물론 암호화를 기본으로 한다.

(2) RSA 암호화 방식과 프로토콜 설계

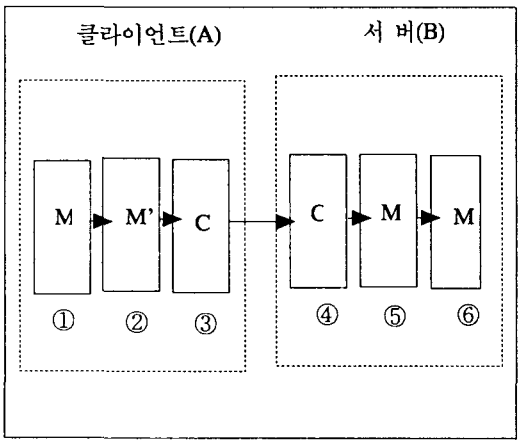
RSA공개키 방식을 사용하여 데이터 암호화 시스템의 구성도를 설명하도록 한다. 데이터 암호화 시스템의 구성도를 살펴보면 <그림 2>와 같다.

클라이언트가 서버에 접속을 하면 서버의 MakeServerKey가 구동을 하여 공개키와 비밀키가 만들어져서 공개키를 클라이언트로 보내진다. 그러면 클라이언트의 플러그인에서 사용자로 하여금 ID와 Password를 입력 받아서 클라이언트의 비밀키와 서버의 공개키로 암호화 하여 서버에게 전송한다. 암호화된 데이터를 LogonServer에서 받는다. LogonServer에서는 클라이언트에서 보내온 암호문을 MakeServer에서 만들어진 서버의 비밀키와 클라이언트의 공개키를 이용하여 LogonServer의 Decript()의 함수에서 복호화하여 key_List 파일에 저장을 한다. 이때 정상적으로 저장이 이루어진다



〈그림 2〉 데이터 암호화 시스템 구성도

면 OK_Message(Text/Html)를, 저장되지 않았다면 NO_Message(Text/Html)를 클라이언트에게 보낸다. 이처럼 데이터와 파일도 <그림 2>의 구성도에 의해서 전달된다. 위와같이 데이터 암호화 시스템 구성도를 통하여 데이터 암호방식을 설계하면 <그림 3>과 같다.



〈그림 3〉 데이터 암호화 방식

① M은 원문 메시지 M이다.

② M = DA(M), 즉 A자신의 비밀키로 암호화

한 파일이다.

③ C = EB(M) = EB(DA(M)), 즉 M 을 수신자 B의 공개키로 암호화한 파일이다.

④ C 는 B가 A로부터 받은 암호문, 즉 C 는 이중 암호화된 파일이다.

⑤ M = DB(C), 즉 B 자신의 비밀키로 복호화한 파일이다.

⑥ M = EA(M) = EA(DB(C)), M 을 송신자 A의 공개키로 복호화 하면 원문 M 을 구할 수 있다.

Ⅳ. 구현 및 시험

공개키 암호 방식에 기초한 WWW 데이터 보안 시스템은 공개키 암호화 방식을 이용한 암호화 모듈로서 클라이언트/서버 모델이다. 클라이언트는 PC를 대상으로, 서버는 유닉스 시스템을 대상으로 구현되었으며 WWW 데이터 보안 시스템의 구현과 수행을 위한 시스템 환경을 살펴보면 <표 1>과 같다.

〈표 1〉 시스템 환경

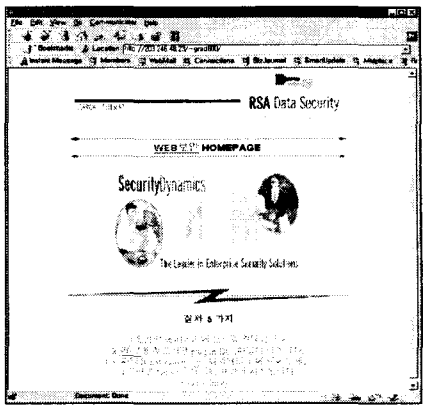
	운 영 체 체	프 로 그 래 밍 툴
서버	Sun OS 5.5 (Selab1)	c++ compiler, for Server's CI compiling
클라이언트	Windows 95	Visual C++ 5.0, for Client's plug-in DLL

본 시스템에서 사용되는 MIME 타입은 "application/RSA" 이며 DLL프로그램 내부에 지정되어 있어 사용자가 따로 지정할 필요가 없고 브라우저가 구동될 때 자동적으로 등록된다.

2. WWW 보안 시스템

(1) Web 보안 홈페이지 초기화면

여기에서는 클라이언트가 서버와 안전한 전송을 하기위한 시험환경 수칙 4가지를 이행하고 Web보안 부분을 클릭하면 서버와 접속할 수 있는 브라우저가 나오게 된다.



〈그림 4〉 Web보안 홈페이지 초기화면

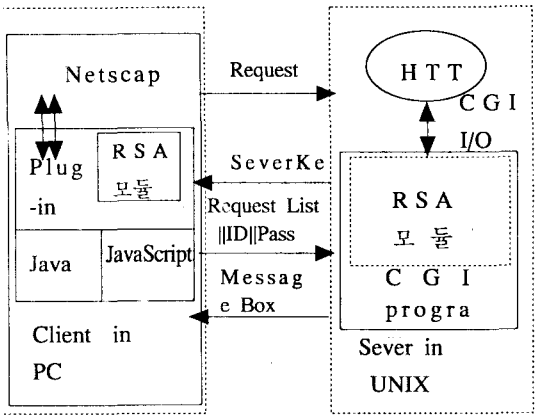
• 시험환경 수칙 4가지

1) 서버에서 제공하는 플러그인 DLL 파일을 다운로드받는다.
2) 다운로드 받은 파일을 넷스케이프/플러그인 디렉토리 밑에 저장한다.
3) DLL 파일이 저장된후 서버의 홈페이지를 다시 접속한다.
4) 접속한후 Web보안 부분을 클릭하면 데이터 보안 시스템인 브라우저가 보인다.

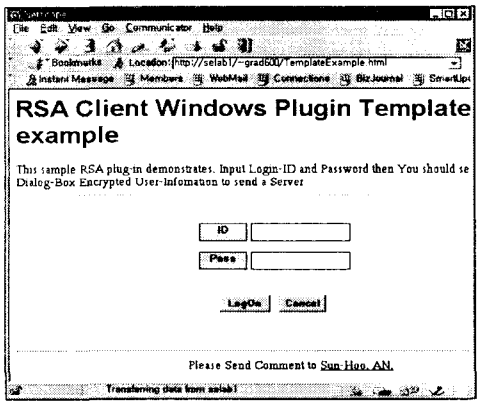
• 클라이어트에서 서버로 사용자 Logon

<그림 4>에서 사용자 Logon 수행과정을 보면 클라이언트가 서버의 웹보안 홈페이지에 들어오게 되면 서버는 자신의 공개키를 클라이언트에게 전송한다. 클라이언트가 서버의 공개키를 획득하고나서 클라이언트가 서버에게 사용자 Logon 정보를 주면 서버는 이에 사용자 유무를 확인하여 암호화 기능을 제공하는 메시지 박스를 준다. Logon 정보를 전송하는데 있어서 데이터의 암호화를 RSA암호화 기법을 이용하여 서버에게 안전하게 데이터를 전송한다.

사용자가 자신의 Logon 정보를 서버에게 전송할 때 일단 자신의 공개키를 서버에게 함께 보내게 된다. <그림 5>에서 사용자가 자신의 Logon 정보를 입력한 뒤 전송버튼을 누르게 되면 입력한 사용자의 ID에 맞게 공개키를 생성하여 서버에게 전송하여 준다. 이때 공개키 생성은 RSA모듈의 키관리 부분에 의해서 생성되고 이생성된 공개키는 서버의 비밀키에 맞게 생성된다. <그림 6>은 클라이

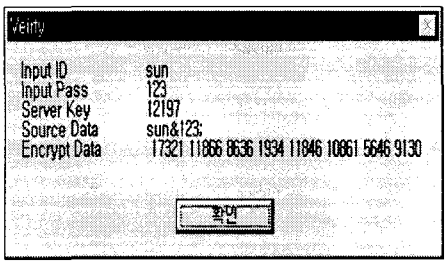


〈그림 5〉 사용자 Logon 수행과정



〈그림 6〉 사용자 Logon

언트가 서버에게 데이터를 보내기 이전해 해야할 키 생성과 서버키확인 문제를 나타내 주는 페이지이다. 이페이지에서 클라이언트와 서버간의 사용자 확인 유무가 결정된다.

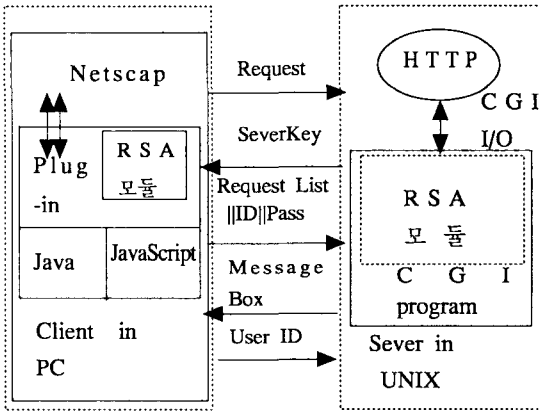


〈그림 7〉 Logon 정보 전송과정

클라이언트는 자신의 ID와 Password를 입력한후 Logon 버튼을 누르게 되면 서버의 사용자 logon정보와 일치하면 <그림 7>의 화면을 보여준다. logon 정보가 일치하지 않은면 다시 <그림 6> 사용자 Logon 페이지를 보여준다.

• Message post

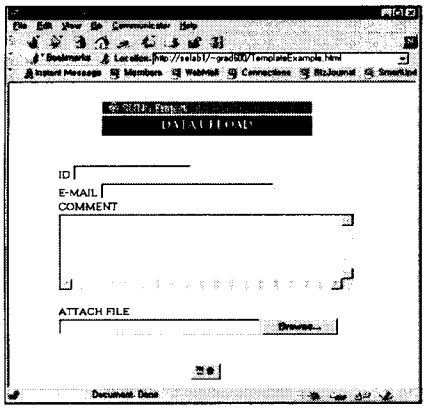
Message Post란 넷스케이프 화면의 사용자 입력란에 입력된 정보를 서버로 전송하는 기능이다. Message Post 기능이 수행되는 과정을 살펴보면 <그림 8>와 같다.



〈그림 8〉 Message post 수행과정

클라이언트가 서버에게 서비스 페이지를 요청하게 되면 서버는 이에 응답하여 암호화 기능을 제공하는 서비스 페이지를 전송하는데 이과정에서는 일반적인 WWW메커니즘처럼 암호화 과정없이 수행된다. 서비스 페이지를 수신한 클라이언트는 자신의 RSA ID와 사용자 입력란에 입력된 데이터를 암호화하여 서버에 전송한다. <그림 9>은 Message Post 기능을 수행하는 서비스 페이지를 나타낸다.

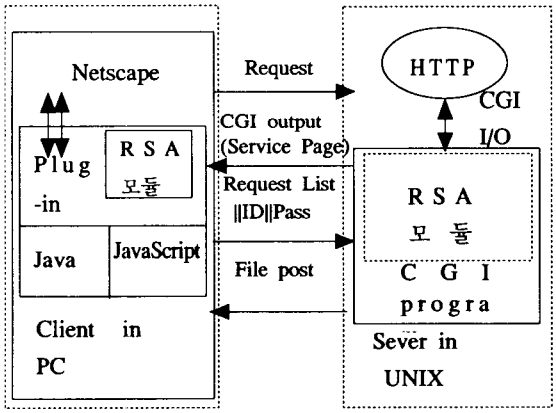
<그림 9> 에서도 ID를 입력할 때 Logon ID와 일치하여야 한다. 클라이언트가 "Message"의 입력란에 전송할 정보를 입력한후 "전송" 버튼을 입력된 내용이 암호화되어 서버로 전송되게 된다.



〈그림 9〉 Message post 와 File post

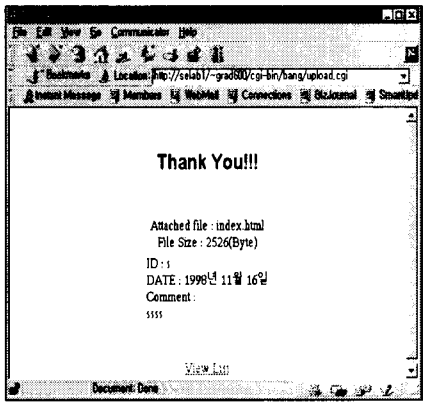
• File post

File post 란 클라이언트 시스템에 있는 파일을 서버로 전송하는 기능으로 File post 기능이 수행되는 과정을 살펴보면 <그림 10>와 같다.



〈그림 10〉 File post 수행 과정

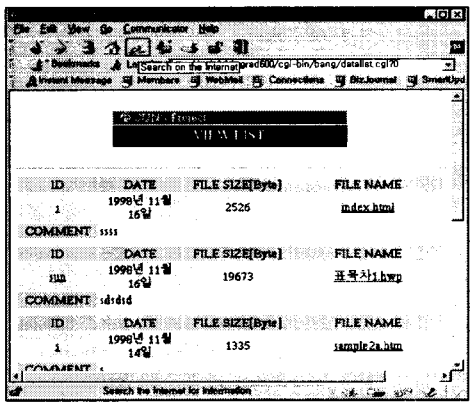
클라이언트가 서버에게 서비스 페이지를 요청하게 되면 서버는 이에 응답하여 암호화기능을 제공하는 서비스 페이지를 전송하는데 이과정에서는 일반적인 WWW 메커니즘처럼 암호화 과정 없이 수행된다. 서비스 페이지를 수신한 클라이언트는 자신의 RSA ID 와 전송할 파일을 암호화하여 서버에 전송한다. <그림 10>은 File post 기능을 수행하는 서비스 페이지를 나타낸다. <그림 10>에서도 RSA ID 입력되어야 한다. 클라이언트가 파일명을 입력한 후 "전송" 버튼을 누르면 해당 파일이 암호화되어 서버로 전송되게 된다. 이때 전송된 파일에서 사용자 ID와 RSA ID가 일치하게 되면 <그림11>에서 처럼 클라이언트가 작성된 내용이 화면에 나타나게된다. 이때 클라이언트는 자신이 보낸 Message 내용인지를 확인하면 서버의 CGI에 의해 자료가 저장되어지게 된다.



〈그림 11〉 클라이언트가 전송한 데이터의 내용

• File List

전송된 데이터는 복호화 과정을 통하여 CGI 에 의해서 저장되어지게 되는데 이과정에서 서버는 클라이언트가 보낸시간과 날짜를 서버 타임에 의해서 기록하여준다. <그림 12>은 최종적으로 서버에게 클라이언트가 자료를 보내었는지를 확인하는 과정이다.



〈그림 12〉 전송된 자료 리스트

V. 결 론

본 논문에서는 정보 서비스의 다양화에 따른 정보보호 서비스에 대하여 기술하였으며, WWW상에서 정보보호 서비스를 구현하도록 제공하는 암호 기법에 대하여 기술하였다. 암호화 기법으로는 크게 관용키 암호 방식과 공개 키 암호 방식으로 구분될 수 있으나 본 논문에서는 공개키 암호방식에 근거한 WWW 데이터 보안 시스템의 설계와 구현에 대하여 기술하였다. 본 논문에서 제시된 WWW 데이터 보안 시스템을 구현하기 위해서는 브라우저와 Application 프로그램 사이에 데이터 교환을 담당하는 브라우저 확장 기법과 Application 프로그램에서 수행되는 암호화 기법에 대하여 기술하였다.

이러한 측면에서 본 논문에서 제시한 데이터 보안 시스템은 가상공간에서의 상거래 및 앞으로 시행될 전자주민카드등 정보제공 서비스에서 사용자의 데이터 무결성 및 기밀성 보장하는 모델로서 유용하게 사용 될 수 있을 것으로 사료되며, 향후 연구 과제로서는 공개키를 기반으로하는 정보보호 서비스의 문제점인 안전한 키 분배 및 관리에 대한 연구가 병행 되어져야 하며, 본 연구 결과는 앞으로 전개될 WWW을 기반으로 하는 전자상거래 및 EDI 시스템, 인트라넷 보안 모듈과 같은 특정 서비스 그룹 관리에 필요한 보안 시스템으로 응용할 수 있다.

〈참고문헌〉

[1] 박성준 : 「현대암호학」, 1997, pp.2~20

[2] 松井甲子雄 · 이현열 : 「컴퓨터 사용을 위한 암호 조립법 입문」 대영사, 1996, pp.133~178

[3] 박성준 : 「암호기술 및 응용/공개키 암호알고리즘」, '97 하계 정보보호센터 전문가 과정 교재, 1997, pp.2~15

[4] 황종선 · 허용도 : 「통신망 데이터 보호기술」, 1992 , pp.12~45

[5] 고준수 : 「Client-Server 에서의 User Authentication에 관한 연구」, 광주대학교, 1997 , pp.34~37

[6] 이상엽 : 「Visual C++ Programming Bible Ver5.0」, 영진출판사, 1997

[7] 유해영 · 우진운 : 「웹 페이지 작성과 디자인」, 이한출판사, 1998

[8] 정진욱 : 「암호학 이론」, "정보과학회지" 제7권 제5호, 1989.

[9] 남길현 : 「암호시스템의 특성과 활용」, "정보과학회지" 제7권 5호, 1989.

[10] 오창석 : 「인터넷상에서 WWW의 보안강화에 대한 설계 및 구현」, 건국대학교, 1996.

[11] 「정보보호 기술입문서」, "한국전자통신연구원" 최종연구보고서 별책 제14권, 1998

김 동 현(Dong-Hyun Kim)
1992년 광운대학교 공학석사
2000년 조선대학교이학박사수료
1999년~현재 벤처정보연구소장
2000년~현재 창업보육센터장
1996년~현재 순천청암대학 컴퓨터정보과학부 교수
*주관심분야 : 전자상거래시스템, 컴퓨터네트워크, 정보보안

안 선 후(Sun-Hoo An)
1996년 2월 광주대학교 공학사
1999년 2월 광주대학교 공학석사
* 주관심분야 : 전자상거래, 정보보안

이 성 주(Sung-Ju Lee)
1992년 광운대학교 전자계산학과(이학석사)
1998년 대구가톨릭대학교 전자계산학과 (이학박사)
1988년~1990년 조선대학교 전자계산소 소장
1995년~1997년 조선대학교 정보과학대학장
1981년~현재 조선대학교 컴퓨터공학부 교수
*관심분야 : 소프트웨어 공학, 프로그래밍 언어, 객체지향 시스템, 러프 집합