인터넷 웹 환경에서 보안 데이터 전송을 위한 분산 시스템 설계 및 개발

강창구*, 윤재우*, 하경주*, 장승주**
*전자통신연구원 부호기술부, **동의대 컴퓨터공학과

Design and Development of Distributed Internet Web Security System

Kang Chang-Gu*, Yoon Jae-Yoo*, Ha Kyung-Ju*, Jang Seung-Ju**
*ETRI Code Division, **Dongeui Univ., Dept. of Computer Engineering

요 약

Web 보안 기능 중에서 가장 기본적이면서 중요한 보안 기능은 데이터의 암호 및 복호이다. 본 과제는 인터넷 web browser(Netscape Communicator 또는 Netscape Navigator)기능에 보안 모듈을 이용한 자료 및 문서 암호 기능을 통해서 안심하고 web page를 사용할 수 있는 시스템을 제공한다. 보안 모듈을 사용하지 않는 일반적인 web 데이터 전송 환경에는 SSL 프로토콜을 이용하여 web 데이터 전송을 수행한다. 서버가 보안 모듈을 가지고 있는 경우는 web을 통해 주고 받는 데이터에 대해서 보안 모듈 내에 존재하는 암호 및 복호하는 알고리즘을 사용한다. 이런 방식을 사용할 경우에 일반적으로 많이 사용하는 DES 알고리즘의 사용으로 쉽게 구현이 가능하다. 그러나 이러한 보안 모듈이 상호 연동해서 동작되기 때문에 이 모듈이 없이는 웹 상에 원하는 자료에의 접근이 불가능하다. 또한 이 방식은 기존의 방식이 갖는 보안 기능의 공개성 문제점을 극복하면서 완전한 보안 웹 환경을 제공해준다.

1. 서론

기존 상용 제품 web browser(netscape communicator, MS-explorer 등)는 보안 기능의 제공을 위하여 SSL(Secure Socket Layer) 프로토콜을 이용한 소프트웨어적인 문제 해결 방식을 사용하고 있다. 그러나 인터넷 web 환경에서 주고 받는 자료에 대한 기존 방식의 해결로는 강력한 접근 통제가 어렵다는 것이다. 따라서 보안 모듈을 이용한 강력한 보안 기능을 제공하는 접근 통제 기법을 제공해야 한다.

기존에 소프트웨어 방식을 이용한 web 보안 해결 방식의 프로토콜로는 SSL, SEA, S-HTTP 등이 있다. 현재 가장 많이 사용되고 있는 소프트웨어 보안 프로토콜로 SSL이다 기존의 소프트웨어를 이용한 web 보안 기능은 원천적인 접근 자체를 막을 수 가 없다. 원천적으로 접근이 허용되는 사용자에 대해서만 선별적으로 이루어지도록 하기 위하여 보안 모듈 개념을 도입해야 한다. 보안 모듈을 이용한 web 보안 기법의 기본적인 개념은 web host에 보안 모듈이 있고 이 모듈에서 제공하는 보안 기능을 이용한 API(Application Program Interface)가 있다. 클라이언트도 web host에 있는 자료에 접근하기 위해서는 보안 모듈이 있어야만 서버에 접근이 가능하다. 클라이언트에서도 서버의 보안 모듈과 동일한 기능의 인터페이스를 할 수 있는 API를 사용하여 서버와 연결한다.

Web 보안 기능 중에서 가장 기본적이면서 중요한 보안 기능은 데이터의 암호 및 복호이다. 본 논문은 인터넷 web browser(Netscape Communicator 또는 Netscape Navigator)기능에 보안 모듈을 이용한 자료 및 문서 암호 기능을 통해서 안심하고 web page를 사용할 수 있는 기능을 제공한다. 보안 모듈을 사용하지 않는 일반적인 web 데이터 전송 환경에는 SSL 프로토콜을 이용하여 web 데이터 전송을 수행한다 서버에 보안 모듈을 가지고 있는 경우는 web을 통해 주고 받는 데이터에 대해서 암호 및 복호하는 부분을 보안 모듈에서 제공하는 알고리즘을 사용한다. 이런 방식을 사용할 경우에 기존의 방식에서 사용하는 암호, 복호 방식은 일반적으로 많이 사용하는 DES 알고리즘의 사용으로 쉽게 데이터 해독이 가능하다. 그러나 보안 모듈을 이용한 암호, 복호 방식은 보안 모듈을 갖지 않을 경우는 어떤 경우라도 데이터의 해독이 불가능하다는 장점이 있다.

위에서 제시한 개발된 제품의 응용 분야로는 인터넷 web을 통해서 많은 문서나 데이터가 흘러다니게 되는데 인터넷 웹 상에 흘러다니는 데이터의 안전한 전송을 원할 경우에 사용할 수 있다 Web page로 구축된 환경을 이용하여 전송되는 데이터 나 문서를 특정한 사람이나 특정한 조직에 대해서 만 접근이 가능하도록 접근된 데이터를 해독할 수 있도록 함으로써 원천적으로 문제가 되고 있는 불특정 다수자에게 중요한 정보나 자료가 흘러 들어가는 경우를 막을 수 있다

2. 서버와 클라이언트의 동작

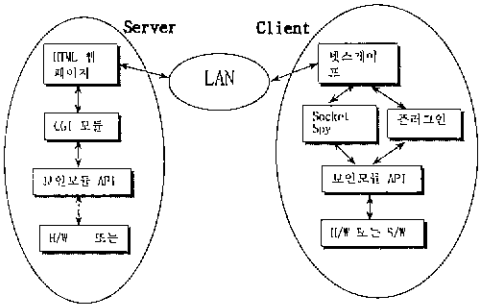
웹 환경에서는 대부분의 경우 서버에서 클라이언트로 데이터를 전송하는 경우가 대부분이다. 대부분의 웹 페이지가 이와 같은 상황에 의한 클라이언트에 정보를 제공하는 기능을 담당한다. 우리가 네트웍을 통해 웹을 항해하다 보면 서버에서 데이터를 받는 경우가 대부분이지만

클라이언트에서 서버로 데이터를 전송하는 경우도 있다. 예를 들어 웹 페이지 상에 사용자 개인의 정보를 입력하거나 게시판에 글을 올릴 경우가 이에 해당된다. 게시판은 누구나 다 보아도 아무런 상관이 없지만 개인의 신상 혹은 금융 정보(신용카드번호) 같은 중요한 데이터의 경우는 어느 누구에게도 보여 져서는 안된다. 이러한 문제를 해결하기 위해서 보안 모듈을 이용해서 웹 서버로 전송하게 되면 개인의 중요한 정보가 유출되는 것을 막을 수 있다.

첫번째 경우 서버의 CGI 프로그램은 웹 페이지 상의 특정 데이터를 암호화하는 기능을 수행했다. 그러나 두 번째 경우는 클라이언트의 넷스케이프 웹 브라우저에서 서버로 전송되는 메시지를 암호화하여 서버로 전송해야 한다. 웹 서버에서는 [그림 1]과 같이 클라이언트에서 암호화되어 넘어온 데이터를 복호화하는 기능을 수행한다. 클라이언트의 넷스케이프 웹 브라우저는 Socket spy 프로그램을 사용하여 데이터를 암호화한다. Socket spy 프로그램은 웹 브라우저에서 발생되는 메시지를 가로채기 하는 역할을 담당한다 Socket spy 에서 가로채기 한 일반 형식의 메시지를 서버로 안전하게 전송하기 위하여 보안 모듈 API를 통해서 암호 한 후 서버로 전송한다. 클라이언트에서 메시지를 암호할 경우에도 보안 모듈을 이용한다 Socket Spy 프로그램은 기존의 윈속(Winsock) 프로그램의 기능을 그대로 이용하고 단지 클라이언트에서 서버에 데이터를 보내는 순간 암호화 기능을 수행한다.

서버는 클라이언트에서 암호화된 문서가 전송되면 HTML 로부터 이 메시지를 받아서 CGI 모듈에 전달된다. CGI 모듈로 전달된 암호 메시지는 보안 모듈 API를 통해서 보안 모듈 복호 기능을 이용한다.

일반적으로 사용하는 개념인 서버에서 클라이트로 자료가 전송되는 경우에 서버에서 서버의 CGI 모듈을 이용하여 암호된 데이터를 클라이언트에 전송한다. 암호된 데이터를 받은 클라이언트는 플러그인 모듈을 통해서 데이터를 받는다. 받은 데이터는 보안 모듈을 통해서 복호가 이루어진다. 복호가 끝난 데이터는 화면에 뿌려지게 된다.



[그림 1] 클라이언트에서 서버에 데이터 전송모델

그러므로 서버의 CGI 프로그램은 데이터를 암호화하고 복호화하는 기능을 수행한다.

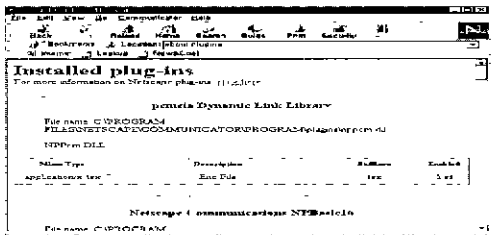
3. 플러그인(Plug in)

3.1 플러그인 등록

클라이언트에서 넷스케이프로 접속했을 때 서버의 HTML 에서 제공하는 CGI 파일로부터 읽어들이는 문서 정보의 형식에 따라 클라이언트의 넷스케이프는 그에 맞는 플러그인 으로 등록된 프로그램 모듈을 넷스케이프가 설치된 디렉토리 내에서 찾게된다. 실행된 플러그인은 넷스케이프 웹 브라우저 속에 포함되거나 분리되어 윈도우에 나타난다. 본 논문에서는 tex 타입의 문서를 서버로부터 암호화해서 클라이언트로 보내주면 클라이언트에서는 암호화된 문서를 그대로 보여주는 것이 아니라 암호화된 문서를 복호화해 주는 플러그 인 모듈을 호출한다.

먼저 플러그인 모듈을 실행 할 수 있도록 하기 위하여 플러그 인 프로그램 모듈을 넷스케이프 웹 브라우저가 설치된 디렉토리 내에 설치해야 한다. 플러그-인은 넷스케이프 웹 브라우저의 디렉토리에 설치를 해야 한다. 이 디렉토리 내에 nppcm.dll 플러그인 모듈과 서버로부터 받은 암호된 문서를 복호하는 기능을 갖는 보안 모듈 API 함수가 호출하는 EtriCApi.dll 과 EtriCApi.lib 파일을 복사한다 Nppcm.dll 플러그 인 파일이 동작하면서 EtriCApi.dll 파일과 EtriCApi lib를 이용하게 된다.

플러그인 모듈을 넷스케이프 웹 브라우저에 복사한 후 플러그인 모듈이 제대로 등록되었는 지를 확인해야 한다. 플러그인이 제대로 등록되었는를 확인하는 방법은 다음 그림과 같이 넷스케이프 웹 브라우저를 실행시킨 상태에서 help 메뉴에서 "About Plug-ins"를 실행하면 다음과 같은 화면이 나타날 것이다.



[그림 2] 넷스케이프 웹 브라우저 상에서 플러그인의 정보 보기 화면

3.2 플러그인 동작

실제 플러그 인 모듈이 어떤 과정을 거쳐서 서버로부터 암호된 문서를 받아 클라이언트의 넷스케이프 웹 브라우저에 보여지는 지를 살펴보면 먼저 플러그인과 CGI 를 볼 수 있는 웹 페이지를 서버에 만들어 놓는다. 서버에서 웹 페이지를 만들 때 클라이언트에서 넷스케이프 웹 브라우저로 하여금 플러그인을 호출하려면 HTML 언어에 <EMBED> 필드를 추가해야 한다

4. FORM 태그와 CGI

클라이언트에서 서버에 데이터를 넘겨주는 경우 안전한 메시지 전송 과정에 대한 동작을 살펴보자. 이 과정은 FORM 태그를 통해서 이루어진다

4.1 FORM 태그

<FORM>태그는 클라이언트에서 사용자가 어떠한 데이터를 서버에게 보낼 수 있는 기능을 제공한다. 클라이언트에서 서버로 넘어온 데이터는 CGI 프로그램에 의해 처리된다. 간단한 <FORM>태그의 예제를 살펴보면 다음과 같다.

```
<form method=post
   action="http://203.241.201.110
```

```
    /cgi-bin/FormCGI.exe">
<p> 이          름: <input name="name"size="12">
<p> 주민등록번호:<input name="personalID" size="14">
<p> 전 화  번 호: <input name="tel" size="12">
<p> 삐삐/휴대폰: <input name="hp"size="13">
<p> 주          소: <input name="addr" size="50">
<p><input type=submit value="확  인">
  <input type=reset value="재입력">
</form>
```

첫번째 라인의 <FORM> 문은 입력되는 데이터에 대한 속성을 결정한다. 속성을 살펴보면 POST와 GET 방식이 있다. GET 방식은 클라이언트의 사용자가 입력 값이 환경변수에 저장되어 넘겨진다. 즉 입력 값들이 기본 URL에 붙은 인수로서 첨가되어 CGI 프로그램으로 값을 넘겨준다

4.2.1 CGI 프로그램 등록

웹 서버의 경우 클라이언트에서 넘어온 데이터를 복호화하는 CGI 프로그램을 cgi-bin 디렉토리에 복사한다. 웹 서버로 Window NT를 사용하기 때문에 FormCG.EXE 라는 CGI 프로그램을 "C:₩InterpubWwwwrootWcgi-bin" 디렉토리에 복사한다.

4.3 클라이언트에서 메시지 입력

클라이언트의 넷스케이프 웹 브라우저를 살펴보면 먼저 서버에서 제공된 FORM 태그를 통해서 화면에 데이터를 입력 받을 수 있는 화면이 나타난다. 이때 자신의 신상 정보를 입력한다. 입력하는 부분에 데이터를 모두 입력하고 확인 버튼을 누른다. 확인 버튼을 누르는 순간 클라이언트에서 입력한 데이터가 웹 서버로 전송된다. 확인 버튼을 누르기 전까지 클라이언트의 웹 브라우저에 입력된 메시지는 웹 브라우저의 임시 버퍼에 남아 있다. 그리고 확인 버튼을 누르는 순간 윈도우에서 제공하는 winsock 기법을 통해서 (wsock32.dll 파일) 웹 서버로 전송된다 웹 서버로 전송되기 전에 winsock00.dll 모듈을 이용하여 보안 모듈을 이용한 암호된 메시지가 전송될 있도록 작업을 한다.

4.3.1 Socket Spy 모듈 등록

클라이언트에서 웹 서버에 전송될 데이터를 암호화하기 위해 socket spy 프로그램을 이용한다. Socket spy 프로그램은 웹 서버에서 요구하는 데이터를 클라이언트측 사용자가 입력하고 확인 버튼을 누르는 순간 클라이언트에서 웹 서버로 메시지가 전송되는 과정 중 win socket 을 통한 데이터 전송 이 이루어진다. 이때 실행되는 파일이 *wsock32.dll 이다.* *넷스케이프 웹브라우저에서* wsock32 dll 파일을 불러들이는 부분을 수정해서 socket spy 프로그램이 만든 wsock00.dll 파일을 이용하도록 수정해 주어야 한다. 이렇게 하기 위해서 Wsock00.dll 파일을 c'₩Windows₩System 디렉토리에 복사한다. Wsock00.dll 파일은 클라이언트에서 웹 서버로 전송되는 메시지를 암호하는 기능을 갖는다. netscape.exe 파일을 수정하기 위해 **file=>open=> 모든파일, Binary형식**으로 open 한다. socket spy 프로그램은 wsock32.dll을 그대로 이용하고 이 프로그램에서 wsock00.dll로 호출되도록 하였다. Wsock00.dll 에서는 넷스케이프 웹 브라우저에서 입력한 데이터를 받는다. 이 데이터를 받아서 암호화를 한다. 암호화를 할 때 보안 모듈 API 를 이용한다. Socket spy 프로그램이 정상적으로 수행되면 원래의 데이터가 암호화되어 서버로 전달된다 서버에서는 받아들인 데이터를 복호화하는 과정이 필요하다. 웹 서버에서 데이터 복호 기능은 FormCGI 모듈에서 이루어진다.

5. 결론

본 논문은 웹 환경에서 데이터를 주고 받을 경우 제3자로부터 안전성을 보장하기 위한 목적으로 연구되었다. 이러한 연구 결과물은 최근에 인터넷 사용의 증가로 인한 부작용인 보안 문제를 말끔히 해결할 수 있다.

본 논문은 웹 페이지를 사용하는 인터넷 환경에서 보안 데이터 전송을 보장하기 위한 분산 시스템 구조 및 개발 기능들에 대해서 설명했다. 보안 웹 기능은 서버-클라이언트 구조를 갖는다. 따라서 개발 기능도 서버와 클라이언트 각각에서 이루어져야 한다. 서버에서 개발되어야 하는 기능은 웹 페이지 데이터를 클라이언트로 보안 전송하기 위하여 보안 모듈을 이용하는 모듈과 클라이언트로부터 받은 보안 데이터를 복호해서 저장하는 모듈이 있다. 클라이언트에서 개발되어야 하는 기능은 서버로부터 받은 보안 데이터를 복호하기 위한 기능이다. 복호를 웹 브라우저 상에서 하기 위하여 플러그인 프로그램 기능을 사용해야 한다.

본 논문에서 개발한 웹 보안 프로그램 모듈은 다음과 같이 구성되어 있다.

- ♥ HTML과 표준 보안 모듈과의 암호 인터페이스를 위한 CGI 프로그램
- ♥ 클라이언트에서 웹 브라우저에 암호된 데이터를 표준 보안 모듈과의 복호 인터페이스를 위한 플러그인 프로그램
- ♥ 클라이언트에서 서버로 전달되는 암호된 데이터에 대한 표준 보안 모듈과의 암호 인터페이스를 위한 프로그램
- ♥ 클라이언트에서 서버로부터 받은 암호 데이터를 표준 보안 모듈과의 복호 인터페이스를 위한 CGI 프로그램

참고 문헌

[1] Zan Oliphant , "넷스케이프 플러그-인 프로그래밍", 인포북, 1997 년 6 월

[2] Ed Tittel, Mark Gaither, Sebastian Hassinger & Mike Erwin, "CGI 바이블", 영진출판사, 1997 년 8 월

[3] Stephen Asbury, "CGI HOW-TO", 대림, 1997 년 4 월

[4] Dwight&Niles, "예제로 배우는 CGI 프로그래밍", 인포북, 1997 년 5 월

[5] Charles Petzold, " Programming Windows 95", 교학사, 1996 년 10 월

[6] 이상엽, "Visual C++ programming Bible Ver 5.x", 영진출판사, 1997 년 8 월

[7] Michael Morrison 외 19 인, "Java Unleashed", 대림, 1996 년 7 월

[8] 김석주, "자바스크립트의 유혹", 가남사, 1996 년 10 월

[9] Cornell, Horstmann, "Core Java", 영한출판사, 1997 년 9 월