플러그인 프로그램을 이용한 보안 데이터 전송 모듈 설계 및 개발

윤재우*, 강창구*, 하경주*, 장승주**

*전자통신연구원 부호기술부, **동의대 컴퓨터공학과

Design and Development of Data Security Module using Plug In Program

Yoon Jae-Yoo*, Kang Chang-Gu*, Ha Kyung-Ju*, Jang Seung-Ju**

*ETRI Code Division, **Dongeui Univ., Dept. of Computer Engineering

요 약

본 논문은 인터넷 web browser(Netscape Communicator 또는 Netscape Navigator)기능에 문서 보안 기능 등을 통해서 안심하고 web page를 사용할 수 있는 클라이언트 환경을 제공한다 보안 모듈을 사용하여 보안 web 데이터 전송을 수행한다. 본 보안 모듈의 특징은 소프트웨어적으로 보안 환경을 사용하든 하드웨어적으로 보안 환경을 사용하든 독점적인 환경에서 웹 보안 기능을 제공할 수 있는 장점을 가진다. 일반적으로 보안이 절실히 요구되는 환경은 인트라넷이 구축된 경우이다. 이런 인트라넷 환경에서는 본 논문에서 제안하는 보안 기능을 사용할 경우 독점적인 보안 기능을 제공할 수 있다. 그리고 일반적인 인터넷 환경에서도 편리하게 보안 기능을 사용할 수 있는 장점을 갖는다. 본 논문은 인터넷 환경에서 보안을 만족하기 위하여 서버, 클라이언트 양쪽에서 모두 보안 모듈을 가져야 한다. 본 논문은 클라이언트 측에서 필요한 보안 모듈의 설계 및 구현 내용에 대해서 언급한다.

1 서론

플러그인 프로그램 기능은 인터넷을 사용하는 사용자들에게 너무나도 편리한 기능이다. 플러그인 프로그램 기능이 나타나면서 사용자들은 특정 프로그램의 원천 코드(source code)가 없이도 자신이 추가시키고자 하는 기능에 대해서 쉽게 프로그램 가능하다.

플러그인 프로그램 기능은 넷스케이프 네비게이트에서 제공되는 기능이다. 넷스케이프 네비게이트 플러그-인은 브라우저의 코드 부분이면서 동적으로 로드되는 코드 모듈이다. 즉 플러그인이 로드되면 브라우저 코드의 직접적인 부분이 된다. 이 기법은 가능한 최고의 속도를 제공하지만 보안성과 플랫폼의 독립성이 부족하다. 따라서 플러그-인은 다른 결함없이 구성된 웹 페이지 같으므로 적절한 플러그-인을 가져온 후에 사용자들은 그 플러그-인이 동작 중인지 종종 알기 어렵다.

플러그-인 모듈들은 오브젝트 코드이므로 그들을 완전히 컴파일할 수 있는 언어로 작성해야 만 한다. 특히 윈도우인 경우에는 개발 환경이 DLL(Dynamic Link Library)을 생성하는 동시에 컴파일된 리소스를 가지고 완성시킬 수 있어야만 한다

플러그-인 모듈로 작성할 수 있는 언어는 Visual C++ 언어를 가능한 사용하도록 권장한다. 플러그-인 모듈이 처음 개발될 때 Visual C++ 환경에서 개발되었기 때문이다. 물론 자바(Java)언어로 작성을 할 수도 있다.

플러그-인 기능은 이미지 뷰어, 도큐먼트 뷰어, 프리젠테이션, 애니매이션, 3-D, audio, video 등의 응용 프르그램 개발을 넷스케이프 네비게이트 웹 브라우저에서 하고자 할 경우 유용한 기법이다.

본 연구 논문은 넷스케이프의 플러그-인 기능을 이용하여 웹 보안 모듈을 설계 및 개발한다. 최근에 인터넷의 급속한 확산은 사용자들에게 안전한 데이터 전송을 보장하는 웹 환경이 절실히 필요하게 되었다. 이러한 환경을 쉽게 제공하기 위하여 넷스케이프 네비게이트 웹 브라우저를 이용한 보안 모듈을 플러그-인 프로그램 기능을 이용하여 제공한다.

기존 상용 제품web browser(netscape communicator, MS-explorer 등)는 보안 기능의 제공을 위하여 SSL(Secure Socket Layer) 프로토콜을 이용한 소프트웨어적인 문제 해

결 방식을 사용하고 있다. 그러나 인터넷 web 환경에서 주고 받는 자료에 대한 소프트웨어적인 방식의 해결로는 강력한 접근 통제가 어렵다는 것이다. 기존에 소프트웨어 방식을 이용한 web 보안 해결 방식의 프로토콜로는 SSL, SEA, S-HTTP 등이 있다. 현재 가장 많이 사용되고 있는 소프트웨어 보안 프로토콜로 SSL 이다.

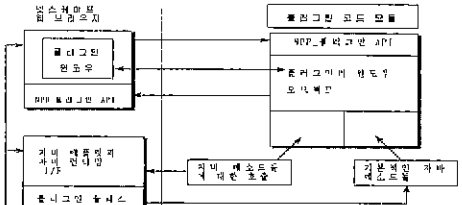
2. 플러그-인 프로그램 구조

넷스케이프 네비게이터에서 서버와 클라이언트 사이에 데이터를 주고받는 포맷으로 MIME 타입을 사용한다. MIME(Multipurpose Internet Mail Extension)타입은 전자우편에서 추가적인 데이터 타입을 다루기 위하여 만들어지고 전세계적인 표준으로 이용되고 있다. 플러그-인은 리소스가 내재된 MIME 정보를 이용하여 네비게이터에 의해 등록된다 MIME은 다음과 같은 헤더 필드들을 정의한다

MIME 버전
컨텐트 타입
컨텐트-전송-인코딩
컨텐트-ID
컨텐트-기술

넷스케이프 네비게이터의 플러그-인 구조는 동적으로 로드되는 코드모듈을 기본으로 동작한다. 이들 모듈은 반드시 네비게이터가 초기화하는 동안에 네비게이터가 읽는 플러그-인 디렉토리나 서브 폴더내에 있어야 한다 네비게이터가 HTML 을 통해서 웹에 내재된 MIME 타입을 발견했을 때는 적절한 코드모듈로 로드된다.

임베드된 플러그-인 인 경우에 HTML EMBED 태그는 네비게이터에게 웹 페이지 상에서 플러그-인 윈도우의 크기를 알려준다. 이 윈도우는 플러그-인을 대신해서 네비게이터가 생성한다. 플러그-인의 인스턴스는 플러그-인이 로드될 때 NPP_New API 를 호출하여 생성된다. 플러그-인은 다수의 인스턴스를 생성하면서 여러 번 로도될 수가 있기 때문에 한 웹 페이지가 한 플러그-인의 인스턴스를 여러 번 가지는 경우가 일반적이다. 데이터 스트림은 네비게이터 플러그-인 구조에서 아주 중요한 개념이다. 대부분의 플러그-인은 서버로부터 처리하기 위하여 데이터를 받지만 다른 경우에서는 렌덩 처리 형태로 데이터를 요구하기도 한다. 또한 네비게이터에서는 LiveConnect 를 제공한다. LiveConnect 는 플러그-인, 자바 애플릿, 자바스크립트 사이의 통신을 제공하면서 플러그-인 구조를 확장시켰다. 자바 런타임 인터페이스(JRI - Java Runtime Interface)는 이들 사이에 중요한 역할을 수행한다.네비게이터 플러그-인 구조는 다음과 같다



[그림 1] 플러그-인 프로그램 구조

네비게이터 플러그-인 구조는 플러그-인 코드모듈, 네비게이터, 자바 애플릿, 자바 런타임 인터페이스, 자바스크립트, HTML 로 이루어진다. 플러그-인 인터페이스의 핵심은 플러그-인 API 이다. 이들 API 중에서 네비게이터의 메소드인 경우는 NPN_로 시작하며 플러그-인의 메소드인 경우는 NPP_로 시작한다 그리고 LiveConnect 는 자바와 자바스크립트를 플러그-인에 결합시킨다.

<LiveConnect>

네비게이터 LiveConnect 를 통해서 자바, 자바스크립트, 플러그-인들을 결합시킬 수 있다. LiveConnect 에 대한 새로운 플러그-인 메소드는 NPP_GetJavaClass, NPN_GetJavaEnv, NPN_GetJavaPeer 이다. LiveConnect 에서 수행할 수 있는 일은 다음과 같다.

플러그-인에서 자바 메소드를 호출
자바에서 플러그-인 메소드들을 호출
자바스크립트에서 자바 메소드를 호출
자바에서 자바스크립트를 호출

<Runtime Loading>

네비게이터가 처음 실행될 때 먼저 플러그-인 디렉토리 내의 코드모듈을 확인한다. 이때 네비게이터는 플러그-인이 가지는 리소스 정보를 파싱한다. 네비게이터에 Help|About 에서 플러그-인 코드모듈과 관련한 정보를 볼 수 있다.

3. 보안 모듈의 설계

3.1 보안 모듈 시스템 구조

본 논문은 웹 환경에서 안전한 데이터 송.수신을 보장하기 위하여 설계 및 개발되었다. 웹 환경 중 클라이언트 노드에서 동작되는 보안 기능의 설계 및 구현 모듈을 중심으로 다룬다. 웹 환경에서 데이터를 주고 받는 경우 인터넷을 통해서 자료가 흘러다닌다. 인터넷을 통해 흘러다니는 중요한 자료가 제 3 자에게 흘러들어갈 경우 심각해진다. 최소한 제 3 자에게 자료가 흘러들어가더라도 이 자료를 브지 못하도록하는 것이 중요하다.

기본적으로 웹 환경은 클라이언트-서버 환경이다. 클라이언트-서버 환경에서 자료를 제공하는 측은 서버 컴퓨터이고 이 자료를 이용하는 측은 클라이언트 시스템이다. 서버 컴퓨터에는 데이터가 저장되어 있고 이 데이터를 클라이언트가 필요로 할 경우 보내주는 역할을 한다. 웹 환경에서는 대부분 HTML을 이용하여 서버에 자료들이 구축되어 있다 HTML 을 이용한 자료 저장에서 자료 양이 많을 경우는 CGI 를 이용한 파일로 구축하게 된다.

본 논문은 웹 환경의 클라이언트-서버 구조에서 보안 기능 만족을 위한 모듈을 중심으로 동작되는 프로그램들을 설명한다. 본 논문에서의 서버는 기존의 웹 서버에서 제공되는 기능과는 조금 개념이 다르다. 웹은 누구에게나 공개되어 있지만 여기서 말하는 서버는 어느 특정인 또는 특정 단체에게만 접근을 허용하는 보안 기능을 갖는 웹 서버이다. 또한 기존의 웹 서버는 보안 기능을 위한 접근 제어를 위하여 소프트웨어적인 방법을 사용했지만, 여기서는 암호화 기능을 갖는 보안 모듈을 이용하여 접근 통제가 이루어진다. 보안 모듈을 이용한 접근 통제는 소프트웨어적인 방법보다 보안 접근 통제가 훨씬 강력하다. 보안 모듈을 갖지 않을 경우 어느 누구도 웹 서버에 접근 자체가 불가능해진다 기존의 소프트웨어 적인 방법은 소프트웨어 프로그램이 있으면 접근이 불가능하지만 접근 가능한 소프트웨어를 구할 수 있는 경우는 접근이 가능하다는 것이다.

웹 페이지의 정보는 일반 문서와 동일하게 작성되어 있다 이 문서는 일반 형식의 파일로 되어 있고 보안 모듈의 보안 기능을 사용한다. 보안 모듈이 갖는 보안 기능을 사용하기 위해 보안 모듈 API 인터페이스를 사용한다. 일반 문서로 작성된 자료 내용들은 직접 웹 페이지에 일반 텍스트나 이미지 형태로 직접 나타나지 않고 보안 모듈을 이용하여 자료의 상호 변환이 이루어진 후 데이터가 화면에 나타나게 된다 이 일반 문서로 작성된 자료가 보안 모듈을 사용하기 위하여 CGI(common gateway Interface)프로그램 모듈을 사

용하게 된다. CGI 프로그램은 HTML 언어로 해결할 수 없는 기능을 제공하기 위한 목적으로 만들어졌다. 클라이언트로부터 서버에 접속될 경우 자동적으로 CGI 프로그램이 동작하여 일반 문서의 내용이 보안 모듈 API 를 통해서 보안 모듈의 암호 기능을 이용하여 암호화된 문서로 변환한다. 이 암호화된 문서는 접근이 허용된 클라이언트에게 인터넷을 통해서 전달된다.

암호된 문서를 전달받은 클라이언트는 암호화 된 문서를 복호하기 위하여 플러그인 모듈을 이용한다. 플러그인 모듈은 넷스케이프 웹 브라우저에서 사용하는 기법이다. 플러그인 모듈은 암호된 문서를 웹 서버로부터 전달받아서 복호를 해야 한다 복호를 하기 위하여 플러그인 모듈은 보안 모듈의 API 를 호출한다. 보안 모듈 API 는 보안 모듈의 복호 기능을 수행하기 위한 인터페이스이다. 암호된 문서를 넘겨받은 넷스케이프 네비게이트 웹 브라우저는 플러그-인 기능을 사용하여 암호화된 문서를 복호화하는 모듈이 실행 되도록 한다. 복호 모듈을 통해서 클라이언트의 사용자는 정상적인 문서의 내용을 볼 수 있다. 위의 내용은 [그림 2]와 같이 나타낼 수 있다

[그림 2] 서버에서 클라이언트 데이터 전송모델

[그림 2]와 같은 상황은 웹 서버에서 클라이언트로 데이타를 일방적으로 전송하는 경우가 해당된다. 대부분의 웹 서버에 존재하는 페이지는 이와 같은 상황에 의하여 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 클라이언트 사용자 정보를 웹 서버로 전송하게 되면 개인의 중요한 정보가 유출되는 것을 막을 수 있다.

4. 플러그인(Plug in)

4.1 플러그인 등록

클라이언트에서 넷스케이프 네비게이트로 접속했을 때 서버의 HTML 에서 제공하는 CGI 파일로부터 읽어들이는 문서 정보의 형식에 따라 클라이언트의 넷스케이프 네비게이트는 그에 맞는 플러그인 으로 등록된 프로그램 모듈을 넷스케이프 네비게이트가 설치된 디렉토리 내에서 찾게된다. 실행된 플러그인은 넷스케이프 네비게이트 웹 브라우저 속에 포함되거나 분리되어 윈도우에 나타난다 본 논문에서는 tex 타입의 문서를 서버에서 암호화 해서 클라이언트로 보내주면 클라인트에서는 암호화된 문서를 그대로 보여주는 것이 아니라 암호화된 문서를 복호화해 주는 플러그 인을 호출한다. 먼저 플러그인 모듈을 실행 할 수 있도록 하기 위하여 플러그 인을 넷스케이프 네비게이트 웹 브라우저가 설치된 디렉토리 내에 설치해야 한다. 플러그-인은 넷스케이프 네비게이트 웹 브라우저의 디렉토리에 설치를 해야 한다. 이 디렉토리 내에 Nppcm.dll 플러그인과 암/복호를 기능 수행을 위한 보안 모듈이 설치되어야 한다. Nppcm.dll 플러그-인 모듈이 동작하면서 암/복호화 기능 수행을 하는 보안 모듈을 이용하게 된다.

플러그인 모듈을 넷스케이프 네베게이트 웹 브라우저에 복사한 후 플러그인 모듈이 제대로 등록되었는 지를 확인해야 한다. 플러그인이 제대로 등록되었는를 확인하는 방법은 넷스케이프 웹 브라우저를 실행시킨 상태에서 help 메뉴에서 "About Plug-ins"를 실행하면 된다.

5. 결론

본 논문은 웹 환경에서 데이터를 주고 받을 경우 제 3 자로부터 안전성을 보장하기 위한 목적으로 연구되었다. 이러한 연구 결과물은 최근에 인터넷 사용의 증가로 인한 부작용인 보안 문제를 말끔히 해결할 수 있다. 본 연구 논문의 결과를 적용할 수 있는 응용 분야로 정부 기관이나 회사 등 어떤 조직 내에서 중요한 정보를 web page 로 구축해 둔 모든 사이트가 적용가능 하다. Web page 로 구축하게되면 불특정 다수가 여기에 접근이 가능하다. 특정한 조직 내에 보안 모듈을 갖지 않은 사용자는 web page 에 접근이 불가능할 뿐만 아니라, 접근이 되더라도 암호된 자료를 가져가더라도 복호가 불가능하기 때문에 자료를 볼 수 없다. Web page 가 일반화되면서 이러한 환경을 필요로 하는 단체나 회사, 정부 기관들이 급증하고 있다. 본 논문은 인터넷 웹 페이지 상의 보안 시스템 구축을 위한 클라이언트 시스템에서 필요한 보안 기능의 구축에 대해서 언급하였다. 클라이언트 시스템에서 보안 기능은 보안 모듈을 이용한다. 보안 모듈을 클라이언트 시스템에서 동작시키기 위하여 플러그-인 프로그램 기능을 이용해야 한다.

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

- HTML 과 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

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

[10] Peter D. Hipson, "윈도우 NT 서버", 사이버출판사, 1997 년 3 월

[11] 김경만, "IIS 로 웹서버를 구축하자", 정보시대, 1997 년 4 월

[12] Peter Dyson, "INSIDE SECRETS IIS 4", 삼각형, 1998 년 5 월