안전한 인트라넷 구축에 관한연구

최향창*, 노봉남
*전남대학교 전산학과

e-mail:hcchoi@athena.chonnam.ac.kr

A Study on Secure Intranet Development

Hyang-Chang Choi*, Bong-Nam Noh*
*Dept of Computer Science, Chon-nam University

요약

웹 기술의 발전으로 기업에서는 인트라넷을 이용해 기업의 시스템을 구축하여 기업내의 업무처리의 효과를 증대시키고 있다. 이러한 인트라넷은 보통 외부 망과 내부 망 사이에 방화벽을 두어 안전성을 제공 한다. 하지만 이것만으로는 내부의 적은 막아낼 수 없다. 본 논문에서는 이러한 인트라넷을 기업에 적용할 때 내부의 불법적인 사용자에 대한 접근을 막아내기 위한 안전한 서비스를 제공할 수 있도록 구축하는 방법에 대해 제안한다. 방법은 역할 기반 접근제어모델과 사용자 접근에 대해 사용자 인증서를 포함하여 보내는 기술을 이용하여 시스템을 구축한다.

1. 서론

정보통신은 급속한 발전을 거듭했고 이것으로 말미암아 기업은 인트라넷을 사용해서 작업 능률을 향상 시키고 있다. 인트라넷은 웹 기술을 이용하기 때문에 확장성이 좋다. 처음에 인트라넷은 인사이동이나, 복리후생을 처리하는 데에 그쳤지만 현재에는 웹 기술의 발달로 인트라넷의 처리능력이 높아짐에 따라 기업 데이터베이스와 연계, 전자회의 등의 구현이 가능하다.

이렇게 중요한 인트라넷을 안전하게 보호하는 것은 무엇보다 중요하다. 인트라넷의 안전성을 높이기위해서 내부 사용자를 인증하고 역할 기반 접근제어 모델을 적용해서 기업에 적합한 보호를 할 수 있도록 제안한다. 이러한 방법을 통해서 클라이언트 사용자를 먼저 인증하고 이 사용자가 접근할 수 있는 권한에 의해 보호된 접근만을 허용하고자 한다.

이 논문의 구성은 2절에서 인트라넷의 내부 사용자들을 위한 안전이 필요한 이유에 대해 설명하고 3절에서는 관련 기술에 대해 알아보고 4절에서는 안전한 인트라넷 시스템에 대해 설계하고 5절에서는 이에 대해 실험한 내용에 대해 제시한다. 6절에서 제안한 시스템의 효과에 대해 검증해보고 7절에서 결론을 제시한다.

2. 인트라넷(Intranet)

2.1 인트라넷의 활용

인트라넷은 웹 기술을 이용해서 기업이나 특정단체에서 사용할 내부 정보 시스템을 구축한다. 예로 들면 전자 폼에 의한 자동문서 생성과 전자결재, 전자회의 등이 있다.

2.2 기업이나 단체에서 인트라넷을 적용하는 이유

웹 브라우저를 기반으로 사용 하고 있어서 거의 모든 플랫폼에서 사용이 가능하다. 또한 웹 툴들이 인트라넷과 기존 데이터베이스 애플리케이션 상호간에 연결해주는 강력한 메커니즘을 가지고 있어 기존 시스템과의 연계가 쉽다. 또한 같은 프로그램을 여러 기종의 하드웨어에서 사용할 수 있으므로 필요 소프트웨어 개발이나 유지 보수비용의 많은 절감 효과가 있다. 이러한 이유로 인해 현재 기업이나 단체에서는 인트라넷을 기업에 적용한다.

2.3 인트라넷 보안

인트라넷은 방화벽을 이용해 그룹의 외부네트워크에 대한 보호를 한다. 따라서 외부적으로 들어오는 요구들에 대해서는 방화벽에서 제공하는 안전을 따른다. 이러한 점으로 인해 내부 보안이 소홀해지기 쉽다. 안전한 인트라넷은 외부와의 방화벽에 의한 보호뿐만 아니라 내부적인 공격에 대해서도 방어할 수 있어야 한다. 본 논문에서는 내부적인 보호에 중점을 두어 연구한다.

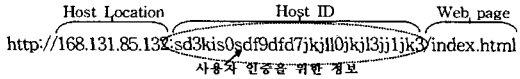
3. 관련연구

여기서는 SFS-HTTP의 방법과 역할 기반 접근 모델에 대해서 알아본다.

3.1 SFS-HTTP[1]

3.1.1 Self-Certifying URLs

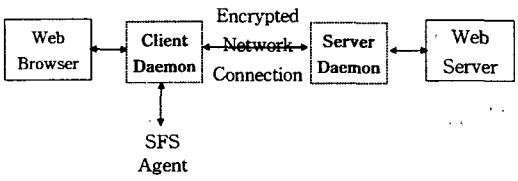
SFS-HTTP는 URL에 사용자 인증서를 추가하여 보내는 방법이다. 이것은 [그림 1]과 같은 형태로 보낸다.



[그림 1] SFS-HTTP의 일반적인 구성

3.1.2 SFS-HTTP 시스템의 구성

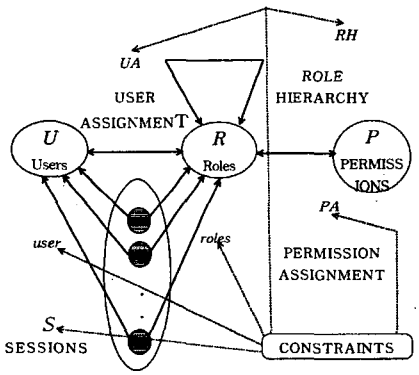
웹 브라우저에서 웹 서버에 접속하고자 할 때 먼저 클라이언트 데몬으로 보내면 클라이언트 데몬에서는 SFS Agent를 통해 사용자 인증서를 보내게 하고 암호화된 네트워크 연결을 통해 서버 데몬과 통신한다. 서버 데몬은 사용자 인증이 되면 웹 서버에서 자료를 받아 클라이언트 데몬으로 전송하고 클라이언트 데몬은 클라이언트 웹브라우저에 결과 화면을 보여준다. 이 것은 [그림 2]와 같다.



[그림 2] SFS-HTTP system

3.2 역할기반 접근 통제 모델[2]

조직 내에 같은 역할(role)을 가지고 있는 사람들은 같은 일을 처리한다. 이러한 이유로 인해 역할에 의해 접근권한을 준다면 개개의 사람들에 관한 시스템 접근규칙을 관리하기가 쉬어지므로 조직 내에 적용하기가 좋은 기법이다. 이것은 [그림 3]과 같다.



[그림 3] 역할기반 접근 제어모델

3.2.1 역할(role)

역할은 조직의 규정이나 규칙에 의해 정의되어지는 업무의 기능을 의미한다. 따라서 조직에서 같은 역할을 부여받는 사용자들에게 동일하게 제공된다.

3.2.2 세션(session)

사용자가 세션을 통해 자신에게 배정된 역할들 중의 일부 또는 전체를 수행할 수 있다. 세션과 결합된 역할을 활성역할(active role)이라고 한다. 이러한 활성역할은 세션의 사용자의 배정된 역할의 집합에 포함되는 특성을 만족해야 한다.

3.3.3 사용자 배정(user assignment)

사용자 배정과 권한 배정은 다대다 관계이다. 사용자가 정보 객체들에 실행할 수 있는 연산들을 직접 사용자에게 부여하고 사용자가 해당 역할의 구성원이 됨으로서 객체에 대한 연산을 수행할 수 있다.

3.3.4 역할계층(role hierarchy)

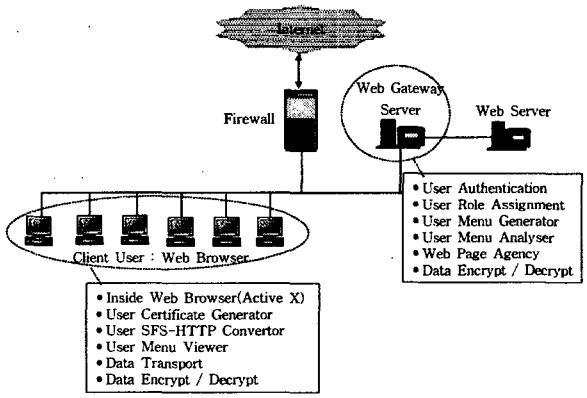
역할에 배정되어진 권한들 사이의 포함관계를 나타내고 있는 역할들 간의 부분순서의 관계이다. 이것은 사용자가 컴퓨터 시스템을 통하여 시스템 내의 정보를 사용하는 객체로 본다. 권한은 이 객체에 대한 실행 가능한 연산의 집합이다.

3.3.5 제약조건(constraints)

모든 구성 요소들 간에 적용되어진다. 이것은 각 구성요소가 가지는 특성에 대한 제한사항이나 조건 등을 기술한다.

4. 설계

이 시스템은 SFS-HTTP의 기법과 역할기반 접근 모델을 적용해서 시스템을 설계한다. 이 인트라넷 시스템의 구성은 다음과 같다.



[그림 4] 시스템 구성도

4.1 일반 사용자(Client User)

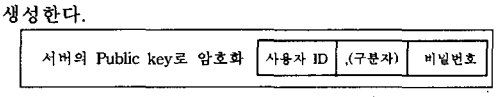
일반 사용자는 인터넷 웹 브라우저를 통해 웹 서버에 접속하기 위해서 웹 게이트웨이 서버(Web Gateway Server)를 사용한다. 웹 게이트웨이 서버와 상호 동작하기 위해 다음과 같은 기능을 하는 클라이언트 모듈이 필요하다.

4.1.1 Inside Web Browser

웹 브라우저를 통해 웹 게이트웨이 서버에 접속할 때 Com과 Active X를 이용해 웹 브라우저 안에 또 다른 웹 브라우저를 생성한다. 이것의 기능은 웹 게이트웨이 서버가 웹 서버에 접속해서 얻어낸 결과를 화면상에 나타낸다.

4.1.2 User Certificate Generator

사용자 인증서를 생성하는 모듈이다. 이 모듈은 웹 게이트웨이 서버의 공개키를 가지고 [그림 5]와 같은 인증서를 생성한다.



[그림 5] 사용자 인증서 생성 구조

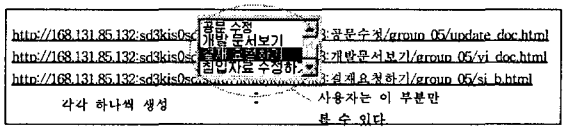
공개키 값은 Inside Web Browser에 변수 값으로 포함되어 있다. 또한 여기서는 사용자 세션키를 생성한다. 이 생성 방법은 [그림 7]의 5와 같다.

4.1.3 User SFS-HTTP Convertor

위에서 생성된 인증서를 3.1에서 보여준 [그림 1]과 같이 변형시키는 모듈이다.

4.1.4 User Menu Viewer

Web Gateway Server에서 보내져온 사용자 접근 가능 웹 페이지 목록 주소들을 사용자들이 사용 할 수 있도록 버튼 화 시켜서 화면상에 보여주는 모듈이다. 단 사용자가 목록 주소를 볼 수 없도록 HTML언어가 아닌 ActiveX에 의해 구현된 리스트 박스에 하나씩 동적으로 추가시키는 모듈이다. 단 목록 주소를 대표하는 이름만 볼 수 있다. 이것의 생성 예는 [그림 6]에서 보여준다.



[그림 6] User Menu Viewer에 의해 생성된 메뉴

4.1.5 Data Transport

웹 게이트웨이로 보내는 데이터를 SSL 프로토콜을 이용해서 전송한다.

4.1.6 Data Encrypt / Decrypt

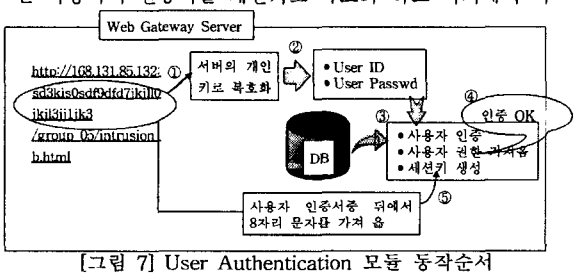
웹 게이트웨이로 보내는 데이터를 암호화하고 웹 게이트웨이로부터 받은 암호화된 데이터를 복호화 할때 사용되는 모듈이다. 이것은 세션키에 의해 암호화 되고 복호화 된다.

4.2 웹 중계 서버(Web Gateway Server)

내부 웹 브라우저(Inside Web Browser)를 통해 접속해 오는 사용자 요구를 분석하여 처리하는 서버이다. 이 서버에 의해서만 웹 서버에 접속가능하고 웹 서버로 받은 결과를 사용자에게 전송하는 역할을 한다.

4.2.1 User Authentication

사용자를 인증한다. SSL[5] 프로토콜을 통해 전송되어 온 사용자의 인증서를 개인키로 복호화 하고 여기에서 나



[그림 7] User Authentication 모듈 동작순서

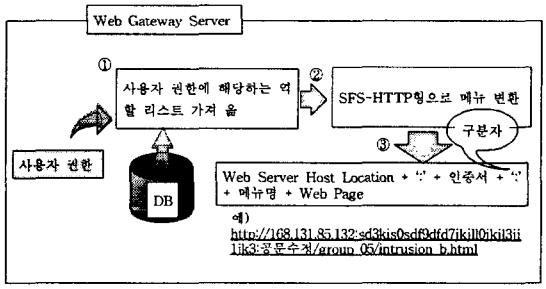
온 사용자 ID와 비밀번호에 의해 사용자를 인증하고 인증되면 사용자의 역할과 사용자의 세션키(Session key)를 얻어온다. 사용자의 세션키는 Web Gateway Server와 Inside Web Browser간의 암호화된 통신을 하기 위한 비밀 키 이다. 이것은 [그림 7]에서 볼 수 있다.

4.2.2 User Role Assignment

가져온 사용자의 권한을 가지고 이 권한에 해당하는 역할을 가져와서 User Menu Generator에 넘긴다[그림 8].

4.2.3 User Menu Generator

User Role Assignment로부터 얻어온 자료를 SFS-HTTP 형으로 변환한다[그림 8].



[그림 8] 사용자 메뉴 생성을 위한 준비과정

4.2.4 User Menu Analyser

사용자가 [그림 6]과 같은 메뉴를 통해 접속을 요청하면 이에 해당하는 메뉴의 값을 받아 이 값을 분석해서 웹 서버(Web Server)에 요구하는 모듈이다.

4.2.5 Web Page Agency

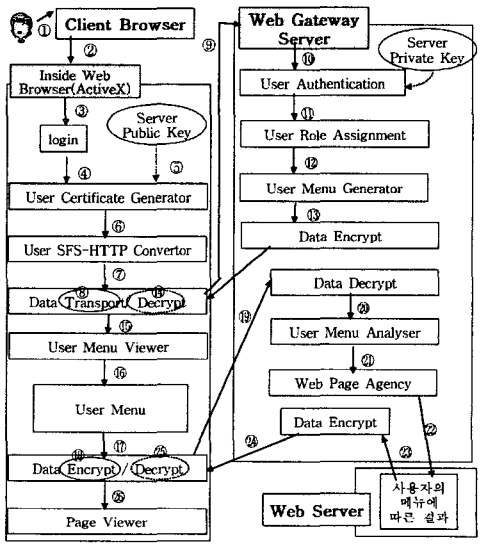
웹 서버로부터 받은 결과를 Inside Web Browser에 보내주는 역할을 한다.

4.2.6 Data Encrypt / Decrypt

내부 웹 브라우저(Inside Web Browser)로 보내는 데이터를 암호화하고 내부 웹 브라우저(Inside Web Browser)로부터 받은 암호화된 데이터를 복호화 할때 사용되는 모듈이다. 이것은 세션키에 의해 암호화 되고 복호화 된다.

4.3 전체적인 흐름

이 시스템의 전체적인 흐름은 [그림 9]와 같다.

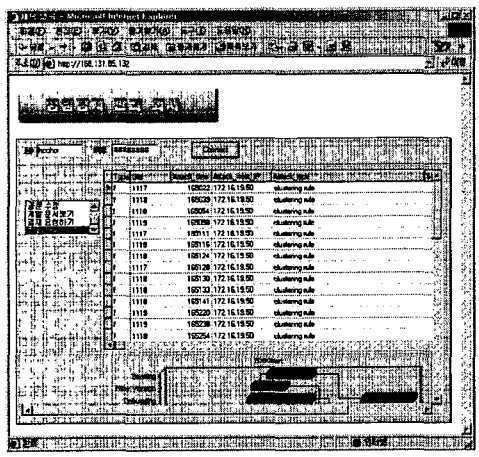


[그림 9] 시스템의 전체적인 흐름

위에서는 번호 순서대로 흐름을 나타낸 것이다. 사용자 메뉴가 생긴 후부터는 시스템이 종료되기 전까지 사용자의 메뉴 요구에 따라서 ⑰ ~ ㉖ 을 반복한다.

5. 구현

구현은 NT시스템을 이용하였다. 침입탐지 회사에서 처리해야 할 일반적인 작업에 대해 예시하여 구현했다. 내부 웹 브라우저를 통해 역할서버(Role Server)와 접속하는데 역할 서버는 사용자의 인증서를 자신의 개인키로 복호화하고 이 복호화 된 결과를 통해 사용자를 인증하고 사용자의 ID에 의해서 이 사용자의 역할을 판별하고 사용자 역할을 지정한다. 이 지정된 역할을 가지고 사용자가 조직 내에서 사용할 수 있는 업무에 대한 메뉴를 동적으로 생성하여 사용자의 웹 브라우저로 전송한다. 이때 사용자의 내부 웹 브라우저에서 이것을 받아내어 사용자 메뉴를 구성한다. 또한 서로 간에 통신할 때 각각 인증서를 가지고 생성한 세션키로 암호화된 통신을 한다. 주요한 실행화면은 [그림 10]과 같다.



[그림 10] 구현 예제 화면

6. 시스템의 효과

위와 같은 방법에 의해 개발된 인트라넷은 다음과 같은 장점을 갖는다.

6.1 역할기반 접근제어

역할기반 접근제어 방법에 의해 접근하게 되므로 사용자들의 관리가 쉬어진다. 역할 기반 접근제어 방법에 의해 사용자를 위한 각각의 메뉴 리스트들을 부여한다. 역할 기반이 아니고 개개의 사용자에게 업무를 적용하는 시스템이라면 개인별로 메뉴를 구성하기위해 많은 시간과 자원이 소비 될 것이다. 이러한 점으로 미루어 볼 때 개인별로 각각 업무를 유지하는 것 보다 역할에 의해 유지관리 하는 것이 더욱 효과적이다.

6.2 사용자 관리

사용자는 역할서버가 SFS-HTTP 방법에 따라 부여한 사용자 메뉴 리스트를 통해 본인이 업무에 접속하게 되므로 시스템 접속에 따른 불법 사용자에 대해 보호 할 수 있다. 예를 들어 사용자 ID와 비밀번호를 알지 못하면 사용자 메뉴 리스트를 생성할 수 없으므로 불법 적인 사용자에 대해 안전하게 관리할 수 있다.

사용자는 인증 후 시스템에 접속할 수 있으므로 사용자별로 작업을 처리하기 위해 접속한 시간 등을 사용자의 인증서를 통해 로그를 기록하게 할 수 있다. 이 자료는 사용자를 보다 좋은 역할에 위치할 수 있도록 사용자의 적성을 검사하는 데에도 사용될 수 있다. 이것이 가능한 이유는 인트라넷은 기업용 시스템이고 역할 기반에 의해 분류되어 있으므로 사용자의 프라이버시에는 침해가 되지 않는다고 볼 수 있다.

6.3 시스템 보호

악의적인 사용자가 웹 서버에 무리를 주기위해 도스 공격을 한다고 할지라도 사용자 ID와 비밀번호를 알지 못하면 공격하기 힘들다. 예를 들어 불법적인 사용자가 시스템에 대해 도스(Dos) 공격[3]을 시도할 때 사용자의 ID와 비밀번호가 틀린 접속이 들어온다면 이것에 대한 발신 주소를 확인하여 조치할 수 있다. 또한 이것은 인트라넷이므로 도스 공격에는 무리가 있다.

6.4 스푸핑(spoofing)[3] 공격에 대한 보호

내부에서 특정 클라이언트가 서버임을 속이는 스푸핑 공격을 한다고 할지라도 SFS-HTTP 방법에 의해 통신하므로 어떤 사용자가 이 가상의 악의적인 웹 서버에 접속한다고 할지라도 암호화된 인증서를 해독하지 못하면 이것 또한 공격 방법이 될 수 없다.

6.5 스니핑(sniffing) 공격에 대한 보호

SSL 프로토콜과 사용자 세션키를 사용해서 암호화된 통신을 하므로 안전하다.

7. 결론

인트라넷을 구축하는데 있어서 소홀하기 쉬운 내부보안을 강화하는 방법에 대해 연구를 해보았다. 이 방법은 내부 사용자를 보호하는 방법에 SFS-HTTP방법에 역할기반 접근제어 모델을 사용해 사용자 역할에 따른 메뉴를 사용자에게 전송해 줌으로서 사용자 메뉴에 의한 웹 접속만을 허용 받게 제한함으로서 시스템의 웹 페이지 정보의 오용을 막을 수 있도록 설계되었다. 또한 악의적인 사용자가 주로 사용하는 스푸핑과 스니핑 공격에 대비 하고 있다. 또한 이 시스템의 모든 연결과정은 사용자 인증서를 기반으로 하므로 사용자별 시스템 업무 활용정도를 인증서가 의미하는 사용자별로 모니터링 할 수도 있다. 또한 이것은 조직 내에서 발생하는 악의적인 사건에 대한 사후처리에 대한 로그로도 활용될 수도 있다. 다음에는 보다 높은 보호를 제공하는 인트라넷 시스템에 대해 연구해보겠다.

8. 참고문헌

[1] Michael Kaminsky and Eric Banks, "SFS-HTTP: Securing the Web with Self-Certifying URLs", MIT, 1999
http://www.pdos.lcs.mit.edu/~kaminsky/sfs-http.ps

[2] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein and Charles E. Youman, "Role-Based Access Control Models", IEEE Computer Vol29,Number2 , pp. 38-47, 1996

[3] Anonymous, "Maximum Linux Security", SAMS, 1999.

[4] H.X. Mel and Doris Baker, "Cryptography Decrypted," Addison Wesley, 2001.

[5] E. Rescorla, "SSL and TLS," Addison-Wesley, 2001.