論文
8-4-6

웹서비스를 위한 지문인증 모듈에 관한 연구
(A Study on the Fingerprint Authentication Module for Web Services)

오 윤 탁(Yoon-Tak Oh)[1)]

요 약

인터넷 환경이 다양한 서비스 분야로 응용됨에 따라 보안에 대한 인식이 증가하고 있다. 웹서비스 상에서 이루어지는 사용자 인증 방식은 본인의 확인 없이 이루어지기 때문에 신뢰성, 안전성, 보안성 등이 문제가 될 수 있다. 이러한 문제를 해결하기 위해 사용자 아이디와 패스워드를 사용하거나 인증키를 사용하는 방법이 적용되어 왔다. 기존의 보안을 위해 사용되는 패스워드 및 인증키는 문자열의 조합으로 구성되어 있어 인증정보 유출이 쉽게 발생할 수 있고, 또한 해커들이 컴퓨터 해킹을 통해 인증정보를 쉽게 빼낼 수 있어 보안에 심각한 문제를 야기 시킬 수 있다. 본 논문에서는 웹 서비스 보안을 향상시키기 위하여 사용자의 고유한 생체 인식으로 이용되는 지문을 활용하여 웹서비스에 적용하는 모듈을 제안한다. 제안된 모듈은 사람의 고유한 특징인 지문인증을 사용하기 때문에 웹서비스 사용자의 본인을 정확히 확인할 수 있어 인증정보 유출이나 해커들의 해킹으로부터 보안성이 철저하게 유지될 수 있다. 따라서 제안된 방식이 웹서비스에 적용되는 기존의 패스워드나 인증번호 방식보다 보안성이 우수하다.

키워드 : 보안, 모듈, 지문인증

ABSTRACT

As the internet environment is applied in the various service field, the recognition on security is increasing. Because the authentication methods for web service user do not confirm person oneself, the serious problems of reliability, safety and security can be caused. In order to solve this problems, the authentication methods of user id and password or authentication key is used. Because the password and authentication key using the existent authentication methods for security is composed of a string, authentication information can easily hacked or leaked by hackers, and the serious problems of security can be caused. In this paper, in order to improve the web security, an authentication module using the fingerprint that have the unique properties of person is proposed. As the proposed module makes use of fingerprint authentication, the security of the web service user from hackers can be maintained. The proposed method is more excellent than the existent method in the web security.

Keywords : Security, Module, Fingerprint Authentication

논문접수 : 2007. 9. 15.
심사완료 : 2007. 10. 4.

1) 정회원 : 안산1대학 인터넷정보과 교수

1. 서론

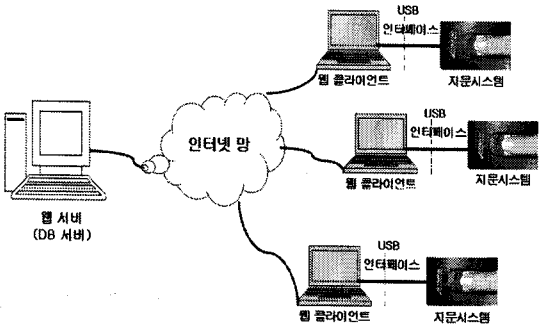
인터넷의 급속한 성장으로 기존에 기업에서 주로 이용되는 클라이언트 서버 환경이 웹기반 서비스 환경으로 천이되면서 웹서비스 응용이 다양해지고 있다. 최근 인터넷의 사용이 크게 확대되면서 인터넷 상거래, 인터넷 금융결재, 인터넷 게임, 원격교육, 원격 테스트 등 웹응용 서비스가 사회, 경제, 교육, 문화활동 등 산업전반에 확산되고 있다. 이러한 인터넷의 확산과 더불어 해커들이 개인정보를 해킹하여 부정적인 방법으로 사용함으로서 개인들의 피해 사례도 늘어나고 있다. 특히 금융 관련 부분이나 중요 정보를 다루는 분야에서 인터넷 해킹 문제는 매우 큰 사회적, 경제적인 문제로 대두되고 있다[1]-[3]. 따라서 인터넷 상에서 이루어지는 다양한 업무를 안전하고 신뢰성 있게 효율적으로 처리하기 위해 정보보안 문제에 대한 해결책이 당면과제이다. 지금까지 인터넷 쇼핑, 인터넷 게임, 원격교육, 원격테스트 등에 주로 사용되는 사용자 인증 방법은 개인 아이디와 패스워드 또는 인증키에 기반을 둔 방식이 활용되고 있다[5]-[7].

개인 패스워드나 인증키에 기반을 둔 기존의 방법은 관리자 및 사용자측면에서는 사용하기 쉽고 편리하지만 인증정보의 유출이 쉽게 일어나고 또한 해커들이 다양한 방법으로 인증정보를 해킹함으로서 웹서비스 보안성에 심각한 문제를 야기 시킬 수 있다. 이러한 문제점을 개선시키는 대표적인 방법으로 생체인식을 활용한 기법이 오랫동안 연구되어 왔다. 생체인식 방법은 국가 비밀기관, 대기업, 보안업체 등에서 비밀정보를 취급하는 담당자의 인증을 하기 위한 방법으로 활용되고 있다. 생체인식 방법은 대상자 본인의 유일한 생체적 특징을 이용하기 때문에 기존의 웹서비스에서 사용되는 인증정보 보다는 개인 인증의 보안성을 매우 향상 시켜준다. 현재 연구되고 있는 생체인식 분야로는 홍채인식, 정맥인식, 지문인식 분야로 나눌 수 있으며 편리성, 안정성, 신뢰성, 경제성을 고려해 볼 때 지문인식을 활용한 제품이 개인인증 방법으로 가장 적합 한 것으로 인식되고 있어 지문인식을 이용한 개인인증이 여러 분야에서 실용적으로 활용되고 있다[8]. 생체인식의 지문인증 방법을 웹서비스 보안문제에 적용한 기법으로 클라이언트에 지문인증 모듈을 사용하여 지문인증을 처리하는 방법이 연구되어 웹서비스의 신뢰성, 안전성, 보안성을 높였다[9]. 아울러 지문인증 모듈을 지문시스템에 내장하여 클라이언트의 부하를 줄이는 연구가 필요하다.

따라서 본 논문에서는 웹 서비스 보안성을 높이고 클라이언트 부하를 줄이기 위한 지문인증 모듈을 제안한다. 이를 위해 제2장에서는 웹 서비스를 위한 지문인증 모듈을 제안하고, 제3장에서는 웹 서버와 클라이언트의 모듈 기능을 제시한다. 그리고 제4장에서 클라이언트와 지문시스템의 모듈 기능을 제시하고, 제5장에서 결론을 맺는다.

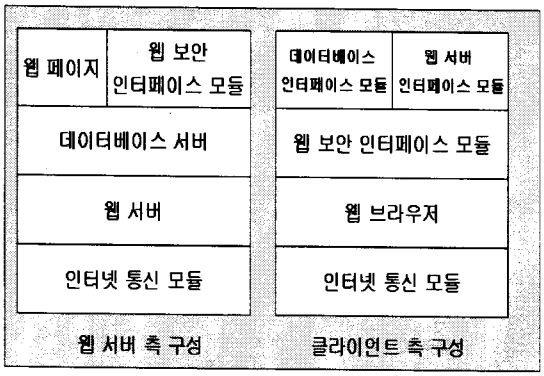
2. 웹 서비스 지문인증 모듈

인터넷 망에서 사용자가 웹 서비스를 이용하여 웹 서버에 접근하기 위한 지문인증 구성은 그림 1과 같다. 웹 서버는 데이터베이스 서버와 연동되어 있고 인터넷 망과 연결되어 클라이언트에 웹 서비스를 제공한다. 데이터베이스 서버는 지문시스템으로 부터 제공된 인증정보를 저장한다. 웹 클라이언트는 사용자의 인증 접속을 위하여 지문시스템으로 부터 인증정보를 받아 서버와 인증확인을 통해 서비스를 지원한다. 웹 클라이언트와 지문시스템간의 인터페이스는 USB 인터페이스를 사용한다.

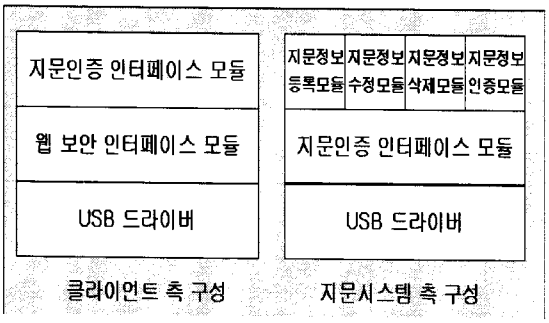


(그림 48) 웹 서비스 지문인증 구성

웹 서비스 지문인증을 구현하기 위해 본 논문에서 제안한 웹 서비스 지문인증 모듈은 웹 서버와 클라이언트간의 보안을 지원하기 위한 모듈과 클라이언트와 지문시스템간의 지문인증 절차를 수행하기 위한 모듈로서 다음 그림 2, 3에 보여주고 있다.



(그림 49) 웹 서버와 클라이언트간의 모듈



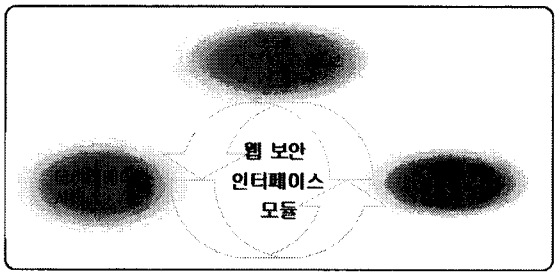
(그림 50) 클라이언트와 지문시스템간의 모듈

3. 웹 서버와 클라이언트간의 모듈

웹 서버와 클라이언트간의 모듈은 그림 2에서 보여주고 있는 것처럼 웹 서비스 보안을 제공하는 모듈들로 구성되어 있다.

3.1 웹 서버 모듈

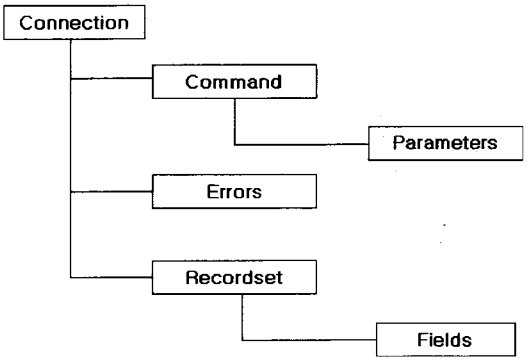
웹 서버측 모듈 구성은 웹 서비스를 제공하기 위한 웹 페이지, 웹 보안을 지원하기 위한 웹 보안 인터페이스 모듈, 웹 보안 정보를 저장하기 위한 데이터베이스 서버가 있다. 그리고 웹 페이지를 운영 및 관리하는 웹 서버, 클라이언트와 통신을 지원하는 인터넷 통신 모듈이 있다. 웹 페이지는 웹 서비스 제공자가 구축하는 정보로서 인터넷 쇼핑, 인터넷 게임, 원격교육, 원격테스트, 포탈 정보 페이지 등 서비스 종류에 따라 다양한 웹 페이지가 제공될 수 있다. 웹 서버와 클라이언트간의 웹 보안 인터페이스 모듈은 그림 4에서 보여주고 있는 것처럼 클라이언트에서 지원하는 지문인증 정보를 송수신하기 위한 모듈로서 웹 서버측에서 클라이언트 측으로 다운로드 되는 액티스 엑스 컨트롤 형태로 존재한다. 이러한 액티스 엑스 컨트롤은 웹 서버에 접속하는 다수의 클라이언트들에게 서비스를 지원하기 위해 개발된 응용으로서 웹 서버와 독립적인 컨트롤이다. 데이터베이스 서버는 웹 보안 정보를 관리 및 저장하는 서버로서 MS-SQL 서버, 오라클 데이터베이스 서버, MySql 등 다양한 데이터베이스 서버를 적용할 수 있다. 웹 서버는 웹 페이지를 관리하고 인터넷 서비스 기능을 제공하며 아파치 서버, IIS(Internet Information Server) 서버 등이 이용될 수 있다.



(그림 51) 웹서버와 클라이언트간의 웹 보안 인터페이스 모듈

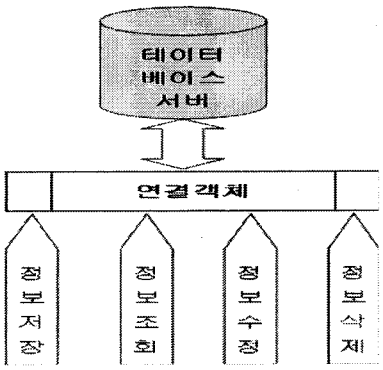
3.2 클라이언트 모듈

클라이언트측 모듈 구성은 웹 서버에서 엑티스 엑스 컨트롤 형태로 다운로드 되는 웹 보안 인터페이스 모듈이 있으며 여기에는 웹 서버측의 데이터베이스 서버에 접속하기 위한 데이터베이스 인터페이스 모듈과 웹 서버에 접속하기 위한 웹 서버 인터페이스 모듈이 있다. 그리고 웹 서버에 저장된 웹 페이지를 접속하기 위한 웹 브라우저와 인터넷 망을 통해 웹 서버에 접속하기 위한 인터넷 통신 모듈이 있다. 클라이언트의 웹 브라우저가 웹 서버에 최초로 접속하여 웹 서비스를 이용하면 웹 보안 인터페이스 모듈이 다운로드되어 설치된다. 웹 보안 인터페이스 모듈의 웹 서버 인터페이스 모듈은 웹 서버와 데이터를 주고받기 위한 모듈로서 페이지와 정보를 교환한다. 데이터베이스 인터페이스 모듈은 클라이언트 측에서 처리하는 데이터를 액세스하기 위한 모듈이다. 이러한 각각의 인터페이스 모듈들은 상호 작용하여 웹 서비스에서 인증 기능을 제공한다. 데이터베이스 인터페이스 모듈은 지문인증 관련 정보를 데이터베이스에 저장, 조회, 수정, 삭제 등의 기능을 담당한다. 데이터베이스 인터페이스 모듈이 웹 서버의 데이터베이스와 인터페이스를 하기 위해 그림 5에서 보여 주고 있는 것처럼 ADO(ActiveX Data Object) 객체를 사용한다. Connection 객체는 데이터 제공자에게 연결할 때 사용하는 객체이고, Recordset 객체는 질의를 통해 얻어낸 레코드를 관리하기 위해 사용되는 객체이다. 그리고 Command 객체는 SQL 질의문이나 저장 프로시저 등을 통해서 수행된 결과를 관리하는 객체이고, Error 객체는 데이터베이스 액세스에 에러가 발생 했을 경우 그 내용을 관리하는 객체이다.



(그림 52) ADO 객체 모델

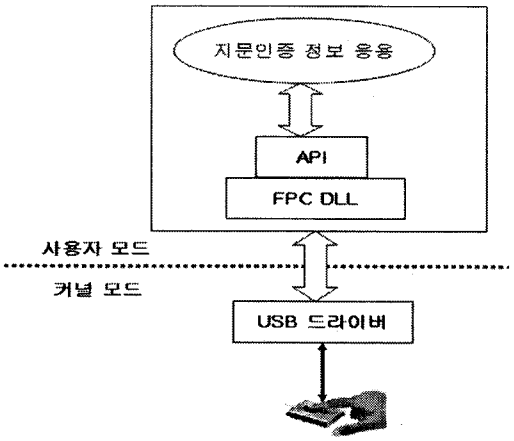
데이터베이스 인터페이스 모듈 다음 그림 6에서 보여주고 있는 것처럼 연결객체를 통해 데이터베이스에 연결한 후 정보 저장, 조회, 수정, 삭제 기능을 제공한다.



(그림 53) 데이터베이스 인터페이스 모듈 기능

4. 클라이언트와 지문 시스템 간의 모듈

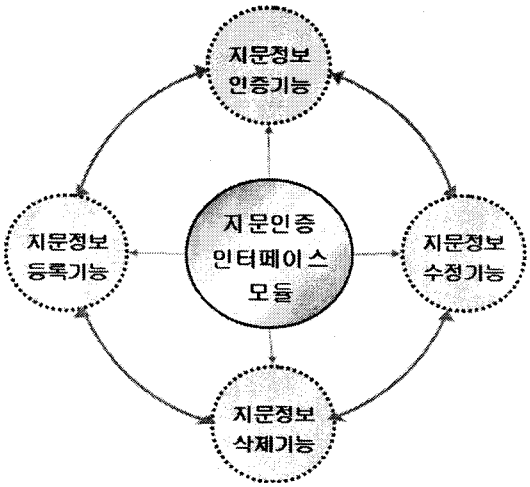
본 논문에서 정의한 클라이언트와 지문시스템 간의 지문인증 정보를 전달하기 위한 모듈은 그림 3에서 보여 주고 있는 것처럼 USB 드라이버를 통해 연결되어 있다. 클라이언트와 지문시스템간의 연동을 지원하는 웹 보안 인터페이스 모듈은 그림 7에 보여주고 있는 것처럼 지문시스템, USB 드라이버, FPC DLL(FingerPrint Control Dynamic Link Library), API(Application Programming Interface), 지문인증 정보간에 상호 관계를 가진다. 지문센서는 커널 모드에서 디바이스 드라이버에 의해서 제어되고 관리된다. 디바이스 드라이버는 지문센서에 종속되고 지문센서의 USB 인터페이스를 통하여 지문정보를 처리한다. FPC DLL은 지문인증 정보를 처리하기 위한 함수들의 집합이다. USB 드라이버를 제어하는 함수들은 디바이스 드라이버와 인터페이스를 통하여 지문인증 정보를 읽어오고 지문정보를 처리하여 결과 값을 API를 통해 지문인증 정보 응용으로 전달한다. FPC DLL에서 정의된 함수들은 API 함수들로써 지문정보 응용이 호출하여 사용한다. 이러한 API 함수들은 각각의 고유한 기능을 가지고 있으며 지문정보 응용함수들과 인터페이스를 통하여 상호 작용한다. 지문시스템의 모듈은 클라이언트와 지문인증 정보를 주고 받기 위해 지문인증 인터페이스 모듈과 지문정보를 등록, 수정, 삭제, 인증하기 위한 모듈들로 구성된다. 또한 지문시스템에는 하드웨어 구성으로 지문센서, CPU, 메모리 등이 존재한다. 지문센서는 사용자의 지문을 입력받은 하드웨어시스템이고 CPU는 지문인증 모듈들의 기능을 처리하며 메모리는 지문인증 정보를 저장한다.



(그림 54) 웹 보안 인터페이스 모듈 기능

4.1 지문인증 인터페이스 모듈

지문인증 인터페이스 모듈은 클라이언트측과 지문시스템간의 상호 작용을 하기 위해 정의되었다. 사용자가 웹 서버에 접속하여 인증정보가 필요하면 그림 8에 보여주고 있는 것처럼 지문인증 인터페이스 모듈을 통해 지문시스템에 지문정보의 등록, 수정, 삭제, 인증을 요청한다.



(그림 55) 지문인증 인터페이스 모듈 기능

4.2 지문정보 등록 모듈

지문정보 등록 모듈은 그림 9에 보여주고 있는 것처럼 웹 서비스 사용자가 웹 서버에 사용자 등록을 하기위해 사용되는 모듈로서 기존의 웹 보안을 위해 사용되는 문자열 패스워드 대신에 FPW(Fingerprint PassWord)를 등록한다. 그리고 지문센서로부터 지문을 입력받아 지문정보의 FID(Fingerpring IDentification)를 생성하고 이 값을 기반으로 보안 알고리즘을 사용하여 FPW를 만든다. FID는 지문정보이기 때문에 용량이 커서 웹 서버의 데이터베이스에 저장하기에는 부하가 많이 걸림으로 지문시스템에 저장하고 FID를 기반으로 생성된 FPW를 클라이언트에 전달하여 웹 서버의 데이터베이스에 저장하도록 한다. 지문정보 등록처리 절차의 세부 단계는 다음과 같다.

① 웹 사용자가 웹서버의 사용자 등록 페이지에 접속하여 지문정보 등록을 요청한다.

② 웹 서버는 지문정보 등록을 위해 사용자 아이디에 대한 FPW 등록을 요구한다.

③ 클라이언트는 사용자 아이디를 입력받고 지문정보 등록 모듈에게 FPW를 요청한다.

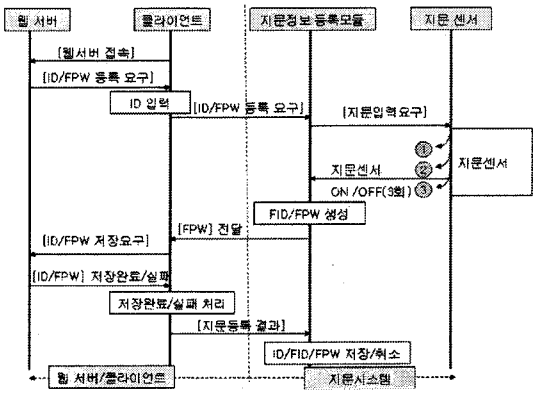
④ 지문정보 등록 모듈은 지문센서를 통해 지문입력을 요구하고 사용자가 지문을 입력한다.

⑤ 지문정보 등록 모듈은 사용자가 입력한 지문정보를 사용하여 FID를 생성하고 이 값을 기반으로 보안 알고리즘을 사용하여 FPW를 만들어 클라이언트에 전달한다.

⑥ 클라이언트를 웹 서버에게 사용자 아이디와 FPW를 웹 서버의 데이터베이스에 저장을 요청한다.

⑦ 웹 서버와 연동된 데이터베이스 서버는 사용자 아이디와 FPW를 데이터베이스에 저장하고 결과를 클라이언트에게 전달한다.

⑧ 클라이언트는 지문등록 결과를 지문정보 등록 모듈에게 전달한다. 지문정보 등록 모듈은 결과에 따라 지문시스템의 메모리에 아이디, FID, FPW를 저장한다.



(그림 56) 지문정보 등록 처리 절차

4.3 지문정보 인증 모듈

지문정보 인증 모듈은 웹 사용자가 웹 서버에 접속하기 위해 수행되는 절차로서 그림 10에 보여주고 있다. 기존의 웹 서비스에서는 사용자 아이디와 문자열 패스워드 및 인증키를 사용하여 접속하지만 지문정보 인증 모듈은 지문정보를 사용하여 웹 서버에 접속하도록 지원한다. 지문정보 인증 모듈은 웹 서버에 있는 FPW와 웹 사용자가 입력 지문정보의 FPW와 비교하여 인증여부를 결정한다. 지문정보 인증 처리 절차의 세부단계는 다음과 같다.

① 웹 사용자가 웹서버의 사용자 로그인 페이지에 접속한다.

② 웹서버는 지문정보 인증을 위해 웹 사용자에게 지문정보 인증을 요청한다.

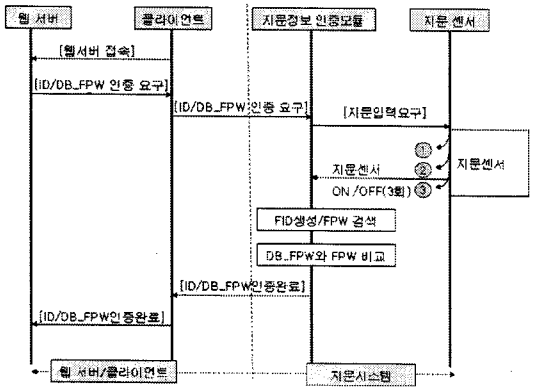
③ 클라이언트는 웹 사용자 아이디에 대한 DB_FPW를 검색하여 지문정보 인증모듈에게 인증을 요구한다. DB_FPW는 웹 서버의 데이터베이스에 저장된 사용자 FPW 이다.

④ 지문정보 인증 모듈은 지문센서를 통해 웹 사용자의 지문정보를 입력받아 FID를 생성한

다.

⑤ 지문정보 인증 모듈은 지문시스템의 메모리를 검색하여 FID에 해당하는 FPW를 검색하여 DB_FPW와 비교하여 인증을 처리하고 클라이언트를 통해 웹 서버에 인증 결과를 전송한다.

⑥ 웹 서버는 인증결과에 따라 웹 사용자의 웹 서버 접근을 결정한다.



(그림 57) 지문정보 인증 처리 절차

4.5 지문정보 수정 모듈

지문정보 수정 모듈은 웹 사용자가 본인의 FPW를 수정하기 위해 사용되는 모듈로서 그림 11에 보여 주고 있다. 이 모듈은 웹 사용자가 지문정보 인증 모듈을 통해 웹 서버에 접속한 후에 요구되는 기능이다. 지문정보 수정 처리 절차의 세부단계는 다음과 같다.

① 웹 사용자가 지문정보 인증절차를 통해 웹 서버에 접속한다.

② 웹 서버는 웹 사용자의 아이디에 대한 FPW 수정을 요청한다.

③ 클라이언트는 사용자 아이디에 대해 지문정보 수정 모듈에게 DB_FPW 수정을 요청한다.

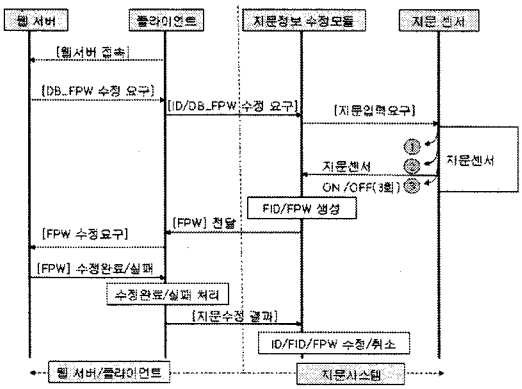
④ 지문정보 수정 모듈은 지문센서를 통해 웹 사용자의 지문입력 받는다.

⑤ 지문정보 수정 모듈은 웹 사용자가 입력한 지문정보를 사용하여 FID를 생성하고 이 값을 기반으로 보안알고리즘을 사용하여 FPW를 만들어 클라이언트에 전달한다.

⑥ 클라이언트를 웹 서버에게 사용자 아이디와 지문정보 수정 모듈에서 전송된 FPW를 웹 서버의 데이터베이스에 수정을 요청한다.

⑦ 웹 서버와 연동된 데이터베이스 서버는 사용자 아이디와 FPW를 데이터베이스에 수정하고 결과를 클라이언트에게 전달한다.

⑧ 클라이언트는 지문수정 결과를 지문정보 수정 모듈에게 전달한다. 지문정보 수정 모듈은 결과에 따라 지문시스템의 메모리에 아이디, FID, FPW를 수정한다.



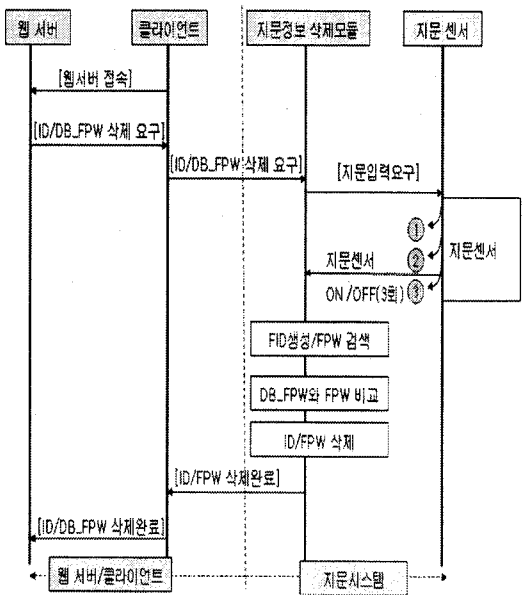
(그림 58) 지문정보 수정 처리 절차

4.5 지문정보 삭제 모듈

지문정보 삭제 모듈은 그림 12에 보여주고 있는 것처럼 웹 사용자가 웹 서버에서 회원등록을 취소하기 위해 사용되는 모듈이다. 이 모듈은 웹 서버의 데이터베이스에서 사용자 아이디와 FPW를 삭제하고 지문시스템에서 사용자 아이디, FID, FPW를 삭제한다. 지문정보 삭제 모듈의 세부적인 절차는 다음과 같다.

① 웹 사용자가 지문정보 인증절차를 통해 웹 서버에 접속한다.

② 웹 사용자는 웹 서버에게 회원등록 취소를 요청한다.
③ 웹 서버는 클라이언트를 통해 사용자 아이디와 DB_FPW를 지문정보 삭제 모듈에게 전송하여 삭제를 요청한다.
④ 지문정보 삭제 모듈은 지문센서를 통해 웹 사용자의 지문입력 받는다.
⑤ 지문정보 삭제 모듈은 웹 사용자가 입력한 지문정보를 사용하여 FID를 생성하고 이 값을 기반으로 보안알고리즘을 사용하여 FPW를 만들어 DB_FPW와 비교한다.
⑥ 지문정보 삭제 모듈은 지문시스템의 메모리에 FPW와 DB_FPW가 일치되는 값이 존재하면 사용자 아이디, FID, FPW를 삭제한다.
⑦ 지문정보 삭제 모듈을 지문정보 삭제결과를 클라이언트를 통해 웹 서버에 전달한다.
⑧ 웹 서버는 데이터베이스에서 사용자 아이디와 DB_FPW를 삭제한다.



(그림 59) 지문정보 삭제 처리 절차

5. 결론

본 논문에서는 인터넷 망에서 신뢰성, 안전성, 보안성을 향상시키는 웹 서비스를 제공하기 위하여 지문인증 모듈을 제안하였다. 제안된 지문인증 모듈은 웹 서버측 모듈, 클라이언트 모듈, 그리고 지문시스템측 모듈로 구성되어 있다. 웹 서버측 모듈과 클라이언트측 모듈은 웹 보안 인터페이스 모듈은 통해 접속이 이루어지고 클라이언트측 모듈과 지문시스템측 모듈은 지문인증 인터페이스 모듈을 통해 상호작용한다. 제안된 인증정보 모듈은 지문인증 정보인 FID를 웹 서버의 데이터베이스에 저장하지 않고 지문시스템의 메모리에 저장하므로서 웹 서버와 클라이언트의 부하를 줄일 수 있고 인증절차 속도를 향상 시킬 수 있다. 그리고 생체인식의 고유한 특징을 사용하기 때문에 웹 서비스 사용자의 본인을 정확히 확인할 수 있어 인증정보 유출이나 해커들의 해킹으로부터 보안성이 철저하게 유지될 수 있다. 따라서 제안된 방식이 기존의 사용자 아이디와 문자열 패스워드 및 인증키 방식보다 웹 보안성이 우수하다.
향후에는 본 논문에서 제안된 지문인증 모듈을 인터넷 상거래, 인터넷 금융결재, 인터넷 게임, 원격교육, 원격 테스트 등 웹 응용 서비스 분야에 적용하는 방법에 대한 연구가 필요하다. 또한 지문인식의 효율을 높일 수 있는 지문 인증 알고리즘에 대한 연구가 병행되어야 한다.

참고문헌

[1] MS, IBM, VeriSign(2002). Web Service Security(WS-Security).
[2] Bloor Research(2002). Web Services Gotchas.
[3] 이해규, 이상수, 김문규(2002). 웹 서비스 보안. 정보처리학회 논문지, 제9권 4호, pp.

36-45
[4] 정현철(2001). IP Fragmentation을 이용한 공격기술들. 한국정보보호진흥원.
[5] Todd Sunsted(2001). Building Security into Web Services.
[6] 김익수, 김명호(2003). 관리자 인증 강화를 위한 추가적인 패스워드를 가지는 보안커널모듈 설계 및 구현. 정보처리학회 논문지, 제10권 6호, pp. 675-682.
[7] 김덕령(2006). 휴대용 지문 인식 개인 인증 시스템 소프트웨어 구현에 관한 연구. 안산1대학논문집 24권, pp. 133-143.
[8] Anil K. Jain, Salil Prabhakar, Lin Hong, Sharat Pankanti(2000). *Filterbank-based fingerprint matching*. IEEE Transactions on Image Processing, vol.9, no.5, pp. 846-859.
[9] 오윤탁(2006). 지문인식을 이용한 웹 어플리케이션 인증시스템. 정보처리학회논문지:기술교육 제1권 제3호, pp. 237-243.
[10] A. Farina, Z.M. Kovacs-Vajna, Alverto Leone(1999). *Fingerprint Minutiae Extraction from Skeletonixed Binary Images*. Pattern Recognition, Vol.32, No.4, pp. 877-889.
[11] 차정희, 장석우, 김계영, 최형일(2003). 특징점의 연결정보를 이용한 지문인식. 정보처리학회 논문지, 제10-B권 7호, pp. 815-822.
[12] USB 인터페이스 장치의 설계(2004). 국제테크노정보연구소.

오 윤 탁
ytoh@ansan.ac.kr

1992년 한양대학교 전자계산학과 학사

1994년 한양대학교 전자계산학과 공학석사

1999년 한양대학교 전자계산학과 공학박사

1996년 ~ 현재 안산1대학 인터넷정보과 교수.

1996년 ~ 현재 정보처리학회 회원

관심분야 : 컴퓨터 네트워크, 정보보안, 지문인식