안전한 로그인을 위한 소프트 보안카드 기반 다중 인증 시스템

Multi-Factor Authentication System based on Software Secure Card-on-Matching For Secure Login

이형우
한신대학교 컴퓨터공학부

Hyung-Woo Lee(hwlee@hs.ac.kr)

요약

로그인 과정에서는 사용자의 ID와 Password를 기반으로 시스템에 대한 사용권한을 확인하고 접근 권한을 부여한다. 하지만 로그인 과정에서 입력된 ID와 Password 정보는 패킷 스니핑 또는 키 로그(Key log) 프로그램 등을 이용하여 악의적인 공격자에 의해 노출될 수 있다는 취약점이 있다. 웹서버 또는 웹메일 시스템 등에 등록된 ID와 Password가 노출된다면 이는 개인 프라이버시 문제와도 연결되어 매우 심각한 문제를 야기한다. 본 연구에서는 기존의 ID/Password 기반 로그인 기법과 더불어 소프트웨어 형태의 보안카드를 핸드폰에 설치하여 유무선망을 통한 다중 인증(Multi-factor authentication) 기법을 제시한다. 제안한 소프트웨어 형태의 보안카드 기반 로그인 기법은 ID/Password와 함께 부가적으로 바이오 정보를 이용할 수 있으며 사용자의 핸드폰에 소프트 형태의 보안카드를 생성/전송/저장하게 된다. 따라서 제안한 시스템을 사용할 경우 기존의 ID 및 Password 정보에 대해 각 개인별 바이오 정보 기반 일회용 패스워드(Biometric One-Time Password) 방식으로 소프트 보안카드를 생성할 수 있으며 이를 이용하여 웹 및 인터넷 로그인 과정을 수행하기 때문에 보다 안전한 다중 인증 시스템을 구축할 수 있다.

■ 중심어 : | 로그인 | 다중인증 | 보안카드 | 바이오정보 | 인증시스템 |

Abstract

Login process uses both ID and password information to authenticate someone and to permit its access privilege on system. However, an attacker can get those ID and password information by using existing packet sniffing or key logger programs. It cause privacy problem as those information can be used as a hacking and network attack on web server and web e-mail system. Therefore, a more secure and advanced authentication mechanism should be required to enhance the authentication process on existing system. In this paper, we propose a multi-factor authentication process by using software form of secure card system combined with existing ID/Password based login system. Proposed mechanism uses a random number generated from the his/her own handset with biometric information. Therefore, we can provide a one-time password function on web login system to authenticate the user using multi-factor form. Proposed scheme provide enhanced authentication function and security because it is a 'multi-factor authentication mechanism' combined with handset and biometric information on web login system.

■ keyword : | Login | Multi-factor Authentication | Security Card | Biometric Information | Authentication System |

* 본 연구는 한신대학교 학술연구비 지원에 의해 수행되었습니다.
접수번호 : #080917-002
접수일자 : 2008년 09월 17일
심사완료일 : 2009년 01월 23일
교신저자 : 이형우, e-mail : hwlee@hs.ac.kr

I. 서 론

IT 강국에 걸맞게 많은 인터넷 관련 서비스가 제공되고 있다. 그중 홈페이지를 통한 서비스는 최근 급증하고 있으며 대부분의 서비스가 웹 환경에서 제공되고 있다. 기업들은 모두 웹 기반 서버 및 서비스를 제공하고 있으며 회원 가입 단계를 거쳐 서비스를 제공하고 있으며 그중 결재를 통해 서비스를 제공하는 곳도 있다. 따라서 웹사이트에 대한 접근 및 사용자 인증을 위해서는 ID/Password 기반의 인증 체계를 사용하여 시스템에 대한 로그인 및 서비스 사용 권한을 부여하고 있다.

하지만 기존의 ID/Password 기반 로그인 시스템은 간단하게 해당 시스템에 로그인을 할 수 있다는 장점이 있지만 공격자가 스니핑(sniffing)을 통해 쉽게 ID와 Password를 알아내어 로그인 할 수 있다는 단점이 있다. 이러한 문제를 해결하기 위해 다양한 로그인 기법들이 연구중이다.

기존의 기법중 로그인 할 경우 클라이언트에 프로그램을 다운 받는 방식과 다운 받은 클라이언트에 공개키 암호화 방식을 추가시킨 방법들이 제시되었다. 하지만 이 기법들은 클라이언트 PC에 따라 로그인 환경이 달라진다는 등의 문제점이 있다. 그리고 ID와 Password로 로그인을 한 후 다른 부가적 정보를 가지고 로그인하는 Single Sign On(SSO) 기법 등에 대해서도 연구되고 있으며, 바이오 정보 등과 같은 부가적 정보를 이용하여 인증의 과정을 거치는 것을 다중 인증(Multi-factor Authentication) 과정에 대해서도 연구기되고 있다.

본 연구에서는 기존의 인증 방법을 개선하여 은행에서 사용하는 보안카드를 접목/개선한 인증 시스템을 제안한다. 사용자 인증 과정에 있어 ID와 Password만을 사용하는 것이 아니라 회원 가입시 핸드폰으로부터 발급 받은 보안카드의 번호및 바이오 정보를 이용하여 사용자 인증과정을 수행한다. 이러한 소프트 보안카드(Soft Secure Card)를 이용한 사용자 인증기법은 인증과정을 다중으로 수행하게 되며 사용자의 ID와 Password가 누출이 되더라도 핸드폰 기반 소프트 보안카드 번호와 바이오 정보 등이 일치해야 최종 인증을 통과할 수 있기 때문에 더욱더 안전한 인증 체계를 제공한다.

본 논문의 2장에서는 기존의 안전한 로그인을 위한 기법 관련 연구들과 그 문제점들을 제시한다. 3장에서는 기존의 문제점들을 보안하기위한 모델을 제시하며, 4장과 5장에서는 바이오 정보 기반 제안 모델 접목 방식과 구현결과 및 성능평가를 수행하였다. 마지막으로 6장에서 본 모델의 장점과 안전한 로그인을 위한 앞으로의 연구 방향을 제시한다.

II. 관련연구

대부분의 웹서비스에서는 ID와 Password만으로 사용자에 대한 인증을 수행한다. 따라서 아래 [그림 1]과 같이 웹 인증 과정에서 전송되는 ID와 Password는 Ethereal을 통해서 너무나 쉽게 스니핑 할 수 있다.

기존의 로그인 방식에는 [그림 1]과 같은 ID와 Password가 쉽게 노출 되는 문제점이 있기에 다양한 로그인 방법들이 연구 중이다.

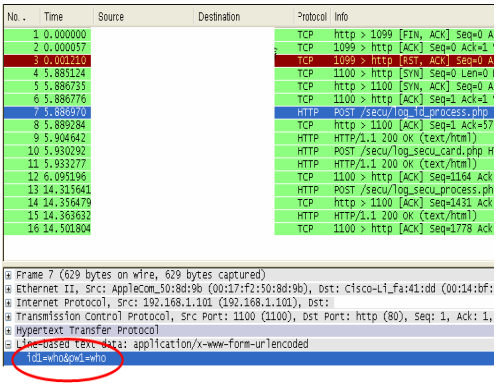

그림 1. 로그인 스니핑

1. 로그인 클라이언트 다운로드 방식

로그인 클라이언트 다운로드 방식은 웹서비스를 받고자 하는 사이트에서 간단한 클라이언트 프로그램을 작성하여 배포하는 것이다. 이것은 기존의 사이트에서 ActiveX 콘트롤러나 기타 다양한 프로그래밍을 통해

만들어 놓은 프로그램을 제공하고 있다.

이 기법의 장점은 로그인 클라이언트 프로그램의 보안적 문제나 버그에 대해 사이트 접속만으로 쉽게 수정할 수 있다는 것이다. 그리고 이동이 잦은 사용자의 경우 웹사이트 접속만으로 원하는 PC에 바로 설치가 가능하다. 이 방식은 스크립트 프로그래밍을 통해 자동으로 설치되는 방식을 제공할 수 있으며 편리함을 제공한다.

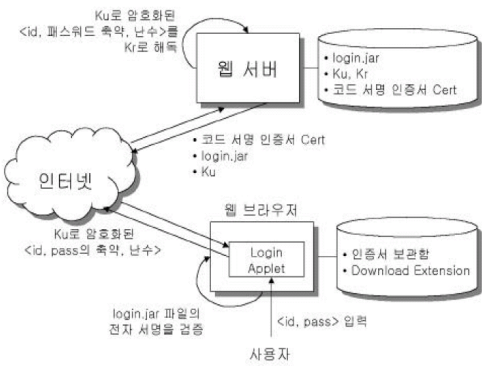

그림 2. 클라이언트 로그인 방식 및 구조

하지만 온라인 배포인 만큼 악의적인 사용자가 로그인 클라이언트의 수정을 통해 배포할 경우 사용자 정보나 파일을 훔쳐가는 코드를 내장할 수가 있다는 단점이 있다. 그리고 클라이언트 크기가 크거나 네트워크 속도가 느린 경우 로그인 클라이언트의 설치에 시간이 많이 소요된다는 단점이 있다.

2. 인증서 기반의 로그인 시스템

현재 대부분 인터넷으로 사용하는 은행의 경우 계좌이체나 결제를 위해 인증서를 사용하고 있다. 이 인증서는 대부분 결제 시스템에서 사용되고 있지만 몇몇 시스템에서는 로그인 시스템으로도 사용하고 있다. 이 기법은 각자 다른 인증서를 발급받게 된다는 점을 이용하여 본인인증을 한번 더 거치게 된다. 이 인증서는 불법 복제 및 수정이 어렵기 때문에 안전한 로그인을 제공하고 있다.

하지만 이 기법은 사용자의 PC에 저장이 되게 되며 다른 PC에서 로그인 할 경우 인증서를 가지고 다녀야 하는 단점이 생긴다. 그리고 인증을 위한 프로그램 설치에서부터 각기 다른 인증서의 선택 등 복잡한 인증과정을 거치게 된다.

그림 3. 기존의 인증서를 통한 로그인

3. 일회용 암호를 이용한 국산 암호 인증 시스템

로그인 및 사용자 인증이 필요한 시스템에서는 ID/Password를 사용한다. 이는 사용자가 지정할 수도 있지만 매번 변경되는 일회용 패스워드 방식을 사용할 수도 있다. 이와 같이 로그인 및 사용자 인증 과정에서 매번 변경되는 패스워드 값을 1회에 한하여 사용하여 인증하는 방식을 OTP(One Time Password)라고 한다. 이 방식은 인증 요청시 미리 저장된 경로를 통해 새로운 암호를 알려 주며 매번 갱신이 되기 때문에 스니핑이나 재전송의 공격에 강하다. 하지만 이 방식은 매번 바뀌는 암호를 받기위해 다른 통신에 연결을 해야 하기 때문에 상당한 불편을 감수해야만 한다[4].

앞서 설명한 로그인 시스템들과 같이 재전송이나 로그인 클라이언트의 역 컴파일, 그리고 인증서 기반 로그인 시스템의 취약성과 같은 문제를 해결하기 위해 특정한 소프트웨어의 설치가 필요 없는 로그인 방법으로 보안카드 기반 이중인증 메카니즘을 제안한다. 본 연구에서 제안한 시스템은 안전한 로그인을 위해 핸드폰과 연계된 소프트 보안카드 기반 인증 기능을 제공하기 위해 웹서버 및 인증 서버로 구성이 되며, 보안카드 발급 및 보안카드기반 로그인 모듈로 구성된다.

III. 제안 모델

1. 회원 가입 및 로그인을 위한 보안카드 발급

1.1 회원가입

안전한 로그인을 위한 보안카드 기반 인증시스템은 웹서버 및 인증 서버로 구성이 되며, 보안카드 발급 및 보안카드기반 로그인 모듈을 이용하게 된다. 기본적으로 작동하는 순서는 아래와 같다. 일반적으로 홈페이지에서 제공되는 로그인 관련 홈페이지를 Login.html 파일이라고 가정하였을 경우 사용자가 입력한 ID/Password 정보는 확인 과정에 해당하는 Log_ID_Process 모듈로 전송되어 ID/Password에 대한 정보와 사전에 기록된 정보를 확인하고, 이를 통해 소프트 형태의 보안카드 모듈로 전달된다. 보안카드 모듈에서는 사용자에 대한 확인 과정을 수행하여 최종적인 다중 인증 과정을 수행하게 된다.

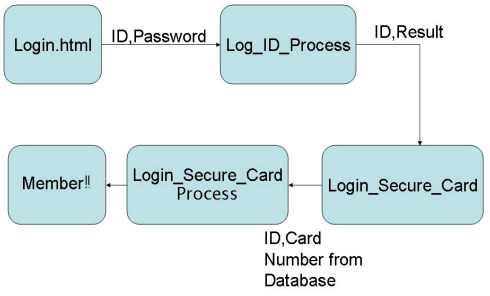

그림 4. 본 연구에서 제안한 모델의 작동방식

본 연구에서 제안한 회원가입 및 소프트 보안카드 발급 단계는 다음과 같다. 웹 시스템을 기반으로 작동하는 로그인 시스템일 경우 아래 그림과 같이 사용자에 대한 회원가입 과정을 수행하며, 핸드폰과 연계하여 소프트 보안카드 발급 요청 과정을 통해 일차적으로 사용자에 대한 인증 과정을 수행하고 핸드폰 내에 소프트 보안카드 정보를 생성하고, 키 값을 발급받게 된다.

이때 발급되는 키 정보는 부가적으로 바이오 정보와 연계하여 생성 가능하며 이에 대한 절차 등에 대해서는 4장에서 제시한다.

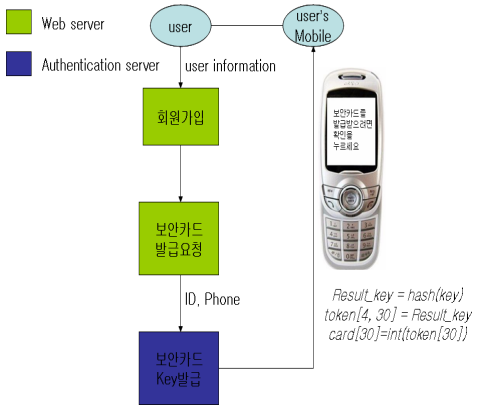

그림 5. 회원 가입 및 소프트 보안카드 발급 모듈

본 시스템은 로그인을 위한 시스템이기 때문에 회원가입을 필요로 한다. 일반적으로 기존의 회원 가입의 절차와 유사하며 필요조건으로서 핸드폰 번호와 생년월일을 입력하여야 한다. 처음 로그인시 ID와 생년월일을 입력하며 입력된 ID와 생년월일이 일치할 경우 보안카드와 비밀번호를 입력하게 된다. 보안카드의 경우 핸드폰을 통해 보안 카드가 발급되기 때문에 핸드폰 번호는 필수 입력 사항이 된다.

다음 의사코드는 회원 가입을 위한 코드이다. Member_Information 이라는 회원 정보를 위한 구조체 변수가 선언이 되며 필수정보 입력을 판단하기 위한 Result 변수가 선언된다.

```
/* 입력 : 사용자 정보
출력 : 회원가입 신청결과 */
Bool Join(){
    Struct Member_Information Join_Member;
    Bool Result;
    Input( Join_Member.ID,
           Join_MemberPassword,
           Join_Member.Birthday,
           Join_Member.PhoneNumber
           etc...);
    Result=Check_Blank( Join_Member.ID,
                        Join_MemberPassword,
                        Join_Member.Birthday,
                        Join_Member.PhoneNumber);
    return Result;
}
```

Input()은 사용자로부터 정보를 입력받는 함수이며 파라미터는 회원 가입시 입력되는 정보들이다. Check_Blank()는 필수정보의 확인을 위한 함수이다. Check_Blank()의 파라미터에는 필수정보인 ID, Password, Birthday, PhoneNumber를 전달한다.

1.2 WIPI를 통한 소프트 보안카드 발급

현재 핸드폰의 WIPI 플랫폼을 이용하여 핸드폰에 프로그램을 다운로드할 수 있다. 본 연구에서는 WIPI를 통해 프로그램의 주소를 메시지에 입력하여 보낼 경우 핸드폰에 바로 관련 프로그램을 다운로드할 수 있다. 연결된 핸드폰은 프로그램뿐만 아니라 보안카드 번호를 생성하기 위해 개인 비밀(Secret)에 기초하여 마스터 키(Master Key)값을 생성하고 이를 전송하게 된다.

```
/* 입력 : ID, PhoneNumber
출력 : Message, Key */

void Send_Message(ID,PhoneNumber){
    Master Key = Key_Generate(ID, Secret);
    Send(PhoneNumber,Master Key);
}
```

보안카드를 발급하는 모듈에서는 ID와 핸드폰 번호를 입력받으며 Key 생성을 위한 변수를 선언한다. ID에 따라 고유의 키가 Key_Generate()를 통해 생성이 되며 생성된 Key는 핸드폰번호와 함께 Send모듈로 전송된다. Send 모듈은 핸드폰으로 보안카드 프로그램과 생성된 고유의 키를 전송한다.

1.3 로그인을 위한 소프트 보안카드 프로그램

로그인을 하기 위해서는 인증을 위해 일회용 패스워드가 필요하기 때문에 보안카드 기반 인증 과정을 수행해야 한다. 보안카드 번호는 4자리 숫자로 이루어지며 30개의 번호가 생성된다. 이 번호들은 여러 방식을 이용하여 마스터 키(Master Key)를 생성하게 되며 보안카드내 생성된 번호들은 겹치지 않도록 생성한다.

본 시스템에서는 핸드폰에 프로그램 설치시 받은 고유의 Key값을 가지고 120자리의 Key를 생성하며 생성된 Key값을 4자리씩 토큰화 시켜 30개의 카드번호를 생성할 수 있으며, 또한 각 개인별 바이오 정보를 이용하여 마스터 키 값을 생성할 수 있다.

```
/* 입력 : Key
출력 : CardNumber[] */

void Create_CardNumber(Key){
    String CreateKey;
    int CardNumber[30];
    CreateKey=Hash(key);
    CardNumber[]=Token(CreateKey);
}
```

위 코드는 핸드폰에 들어가는 WIPI 플랫폼 기반의 프로그램중 일부분이다. 회원가입시 전송받은 고유의 Key 값이 파라미터로 전달이 되며 고유의 Key 값을 통해 생성될 값이 CreateKey로 선언된다. CardNumber[]는 생성된 카드번호를 저장할 배열변수이다. 입력된 고유의 Key 값은 Hash()함수를 통해 120자리의 번호가 생성이 되어 CreateKey로 반환된다. 반환된 CreateKey는 Token()함수를 통해 4자리씩 나누어 CardNumber[]로 저장되게 된다.

```
Result_key = hash(key)
token[4, 30] = Result_key
card[30]=int(token[30])
```

이렇게 발급된 숫자의 경우 총 9^4개의 경우를 가지기 때문에 단순 입력이나 추측으로는 예측하기 어렵다.

이와 같은 방식을 적용하여 기존 로그인 방식의 보안 취약성을 보완하기 위해 본 연구에서 제시하는 기법의 전체적인 구조는 다음 그림과 같으며, 각 단계별 세부 과정을 통해 로그인 과정에서의 다중 인증을 통한 보안성을 향상시키고자 하였다.

소프트 보안카드를 핸드폰 내에 포함시켜서 작동시키는 것은 인증서버를 중심으로 인증 과정을 거치는 방법보다 개인 보안성을 높일 수 있으며, 핸드폰 자체의 사용자 확인 기능에 부가적으로 보안카드 체계를 접목

할 수 있기 때문에 보다 안전한 다중 인증 방식을 구축할 수 있다는 장점이 있다.

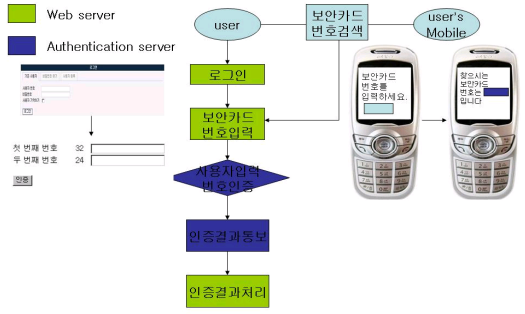

그림 6. 로그인을 위한 보안카드 로그인 모듈

2. 발급된 보안카드와 ID/PW를 통한 로그인

2.1 ID,생년월일을 통한 로그인

처음에는 기본적으로 ID와 생년월일을 입력하도록 한다. Password를 먼저 입력하지 않는 이유는 Password를 스니핑으로 부터 보호하기 위해서 이다. Password는 보안카드를 입력할 때 같이 입력하게 된다. ID와 생년월일 통해 로그인이 성공할 경우 보안카드 번호 체크 페이지로 넘어 갈수 있다. 로그인 부분은 기존의 사이트에서 그대로 사용할 수 있게 하기 위하여 큰 변화를 주지 않았다. 기존의 회원제 서비스를 제공하는 사이트의 로그인 모듈을 약간의 수정으로 사용할 수 있다.

```
/* 입력 : ID, Birthday
출력 : 1차로그인결과 */

Bool Login_ID_Birthday(){
    String ID, Birthday;
    Bool Result;
    Input( ID, Birthday);
    Result = Compare( ID, Birthday);
    return Result;
}
```

위 코드는 첫 번째 ID와 생년월일을 이용한 로그인의 코드이다. ID와 생년월일을 입력받기 위한 변수가 선언이 되며 결과를 반환하기 위한 Result변수가 선언이 된다. Result변수에 따라 보안카드 로그인으로 넘어 갈지 다시 로그인 페이지로 갈지 결정된다. Input()함수를 통해 ID와 생년월일을 입력 받는다. 그리고 회원정보가 입력된 데이터베이스와 Compare()함수를 통해 비교를 하게 된다. 그 결과는 Result에 저장되어 반환된다.

2.2 보안카드를 통한 로그인

보안카드를 통한 로그인페이지는 ID와 생년월일을 통한 로그인이 성공할 경우 보여준다. 보안카드의 번호를 입력하는 화면은 하나의 보안카드 의 Index번호와 비밀번호 입력창을 보여준다. 해당 Index번호와 연결이 되는 카드의 번호를 입력하면 입력된 번호와 비밀번호를 암호화 하여 전송하게 된다. Index번호에 따른 카드번호는 회원가입시 핸드폰에 저장된 프로그램을 통해 알 수 있게 된다.

```
/* 입력 : ID, CardNumber, Password
출력 : 2차 로그인 결과 */

Bool Login_CardNumber_Password(ID){
    String CardNumber, Password;
    Bool Result;
    String EncodeData;
    print( Random_Card_IndexNumber );
    Input( CardNumber, Password);
    EncodeData=Encoding(CardNumber,Password);
    Result = Compare( ID, EncodeData);
    return Result;
}
```

카드번호와 비밀번호를 통한 로그인 모듈에서는 카드번호와 비밀번호를 입력받기 위한 변수가 선언이 되며 결과를 출력하기 위한 Result가 선언이 된다. 우선 Print()함수를 통해 랜덤하게 생성한 카드의 Index번호인 Random_Card_IndexNumber를 출력한다. 출력된 Random_Card_IndexNumber에 맞추어 사용자가 CardNumber와 Password를 입력하게 되며 입력된 CardNumber와 Passwrod는 Encoding()함수를 통해 암호화과정을 거친다. 암호화과정을 통해 생성된 data는 EncodeData에 저장되며 암호화된 EncodeData와 ID를 Compare()함수에 전달하여 사용자정보가 저장된 서버와 비교를 하게 된다. 비교 결과는 Result함수에 전달되어 반환하게 된다.

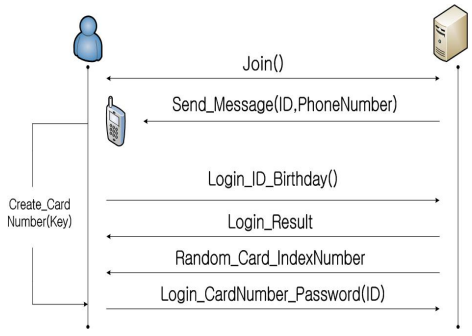

그림 7. 전체적인 모듈 흐름도

V. 바이오 정보 기반 다중 인증

앞에서 제시한 핸드폰 기반 소프트 보안카드에서 사용하는 키를 생성하기 위해 다음과 같은 바이오 정보 기반 키 생성 모델 및 기법을 적용할 수 있다.

1. 바이오 정보 기반 키생성 모델

1.1 사용자 바이오 정보

사용자 바이오정보는 고유하기 때문에 각 사용자의 신분 정보를 대신할 수 있는 특성을 갖으며 전자서명 키를 생성하기 위해서 사용자가 임의로 선택하는 비밀 값과 함께 사용된다. 바이오정보와 사용자 비밀 값을 같이 사용함으로써 전자서명 키를 취소하고 재등록할 수 있는 특성을 갖게 된다.

1.2 바이오 정보 기반 개인키/공개키 쌍 생성

사용자 비밀 값은 전자서명 키 생성 단계에서 사용자에 의해서 직접 설정하는 값으로 키 생성 시에 사용자 비밀 값을 초기값(initial vector)으로 해서 매번 서로 다른 전자서명용 개인키/공개키 쌍을 생성할 수 있다. 이때 생성되는 키쌍은 기본의 RSA/ElGamal 알고리즘 등과 접목하여 ITU-T SG17에서 표준으로 채택된 X.1088(X.tdk) 방식을 적용하여 암호학적으로 안전한 개인키/공개키 쌍을 생성할 수 있다.

전자서명용 개인키 생성을 위해서 해쉬 함수를 사용한다. 사용자 비밀 값과 바이오정보를 해쉬 함수의 입력으로 받는다. 사용자 비밀 값을 조정하여 전자서명 개인키로 사용할 수 있는(적용되는 디지털 서명 알고리즘에 따라서 공개키 및 개인키 생성 조건이 서로 상이함) 해쉬 결과 값을 찾아낸다.

전자서명 개인키 보호를 위해서 퍼지볼트 기법을 이용하여 생성된 개인키에 대해 보호/은닉하여 안전하게 저장/관리할 필요가 있다. 바이오 정보로부터 생성된 개인키를 안전하게 저장하고 공개키 부분에 대해서는 X.509 기반 인증서로 공개함으로써 개인키를 이용한 전자서명 및 사용자 인증 모듈에 적용 가능하다.

2. 바이오 정보 기반 개인키/공개키 생성 방법

2.1 바이오 인증서 기반 키쌍 생성 방식

아래 그림과 같이 바이오 정보로부터 개인키/공개키 쌍을 생성하고 이를 안전하게 저장하는 구조를 형성할 수 있다. 개인에 대한 바이오 정보를 입력받아 기존에 저장되어 있는 정보와 비교하고 인증이 성공한다면 바이오 정보로부터 공개키/개인키 쌍을 생성하는 과정을 수행한다. 생성된 개인키에 대해서는 안전한 형태로 보호/저장하고 공개키 정보는 기존의 X.509 기반 PKI 인증서 형식으로 공개한다.

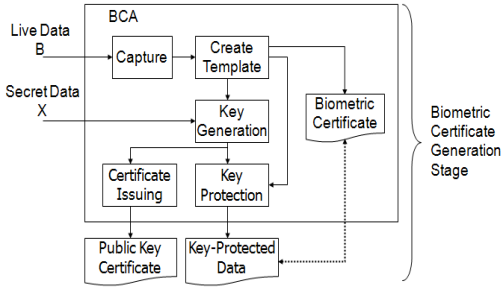

그림 8. 바이오 정보 기반 키쌍 생성 단계

사용자는 핸드폰 등에 부가장치로 제공되는 바이오 정보 입력장치를 통해 자신의 바이오 정보를 입력한다. 입력된 바이오 템플릿 정보에 앞에서 정의된 사용자 비밀 값(Secret Data)을 이용하여 개인키/공개키 쌍 생성 과정을 수행한다. 이때 RSA 등의 공개키 암호화 알고리즘을 적용하여 생성된 개인키 및 공개키 쌍에 대해서 공개키 정보는 X.509 기반 공개키 인증서 형태로 저장

되며, 개인키 정보는 안전성을 높이기 위해 바이오 인증서와 연계하여 안전한 형태로 저장된다.

바이오 정보를 이용하여 키를 생성할 경우 클라이언트 서버 과정에서 송수신되는 메시지 등에 대한 암호 과정에 적용할 수 있으며, 바이오 정보를 이용하여 일회용 패스워드를 생성할 수 있다. 이와 관련한 구체적인 바이오 인증서 생성 과정은 다음 그림과 같다. 최근 ITU-T에서 표준으로 채택된 X.1089(X.tai)를 기반으로 하였으며 바이오 정보를 대상으로 인증서를 생성하고 여기에 개인의 바이오 키 생성 관련 정보를 저장/관리할 수 있다.

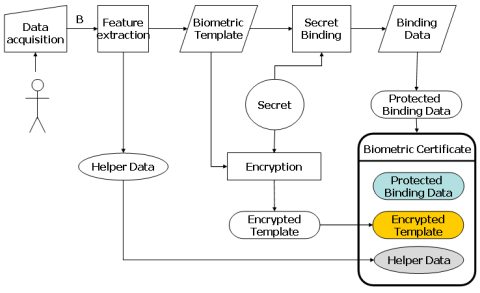

그림 9. 바이오 정보 기반 바이오 인증서 생성 단계

이에 아래 그림과 같이 바이오 인증서를 토대로 다중 인증에 사용할 수 있는 키 정보를 생성할 수 있다. 3장에서 제시한 핸드폰 기반 다중 인증 구조에서 사용자에 대한 다중 인증 기능을 제공하기 위해 아래 그림과 같이 사용자 개인의 바이오 정보를 이용하여 키 값을 생성하고, 이를 소프트 보안카드에 적용하는 구조이다.

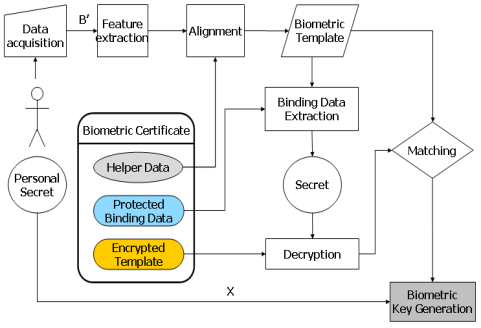

그림 10. 바이오 인증서 기반 키쌍 생성 단계

2.2 바이오 키 기반 인증 메시지 서명 구조

기존에 안전하게 저장된 키 값을 추출하고 이를 사용하여 메시지에 대한 전자서명 또는 암복호화 과정을 수행할 수 있다. 정보보호 기법에 바이오 인증 기법을 접목하기 위하여 제안한 모델에서는 보정 함수를 사용한다. 보정 함수는 동일한 사용자의 서로 다른 바이오 이미지로부터 고유한 특징점을 추출할 수 있도록 도와준다. 공개키 생성 모델에서 개인키 보호를 위하여 퍼지 볼트 등의 기법을 적용하여 protected 템플릿에 개인키 정보를 은닉한다. 바이오 정보를 기반으로 디지털 키를 사용하여 메시지에 대한 암복호화 기능을 제공할 수 있다. 바이오 기반 암복호화 방식에서 수신자의 공개키를 CA 인증서로부터 받은 후에 안전한 통신을 위해 보내고자 하는 메시지에 대한 암호화 과정을 수행한다. 복호화 과정에서는 바이오 기반 인증 과정을 수행한 후에 개인키를 추출하고 수신된 인증 메시지에 대해 전자서명을 적용하는 과정은 아래 그림과 같다.

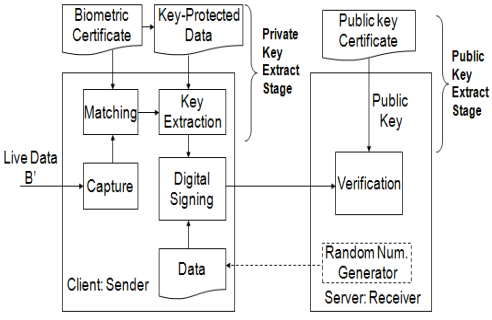

그림 11. 바이오 정보 기반 인증 메시지 전자서명 구조

VI. 구현 및 성능평가

본 실험은 리눅스 시스템에서 이루어 졌으며 웹서버는 Apache, 데이타베이스 서버는 Mysql, 시스템 언어로는 PHP를 사용하였다. 현재 대부분의 웹사이트는 ID, Password만을 비교하기 때문에 한번 누출된 ID와 Password만을 가지고 다른 사람인 것처럼 인증을 받을 수 있다. 본 연구에서 제시한 보안카드 기반 인증 시스템의 전체적인 작동방식을 살펴보면 다음 그림과 같다.

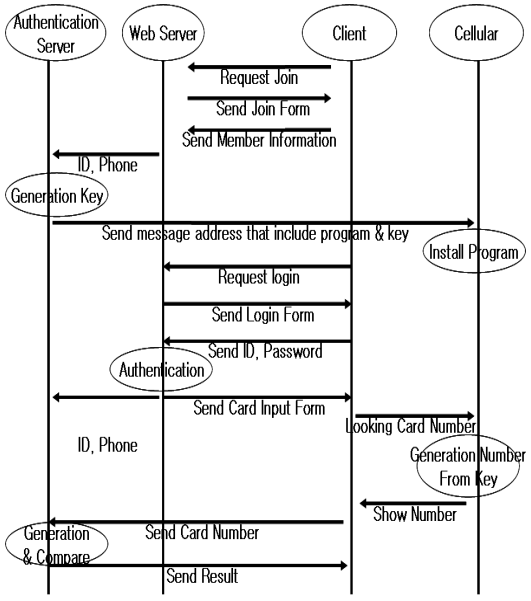

그림 12. 본 연구에서 제시한 모듈 실행 단계

위 그림은 휴대폰 기반 소프트 보안카드 방식을 적용한 다중 인증 구조에 대한 것으로 세션키를 생성하는 과정에서 일반적인 비밀값 기반의 암호학적 대칭키를 사용할 수도 있고, 바이오 정보와 연계된 개인키/공개키를 사용할 수 있다. 사용자는 WIPI 등의 모듈이 탑재되어 부가적인 SW를 설치/운용할 수 있는 핸드폰을 가지고 있으며 바이오 인증서 등과 연계될 수 있는 인증서버에 접속하여 다중 인증 과정을 수행하게 된다.

또한 본 연구에서는 아래 그림과 같이 웹 로그인 관련 시스템을 구축하였으며 이를 통해 기존의 기법보다 개선된 인증 체계를 제공할 수 있다.

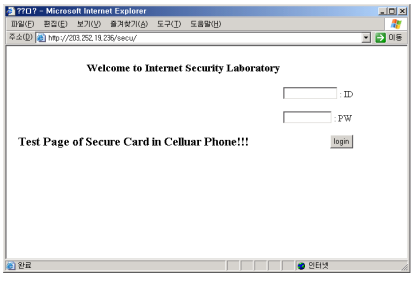

그림 13. 기본적 로그인 화면

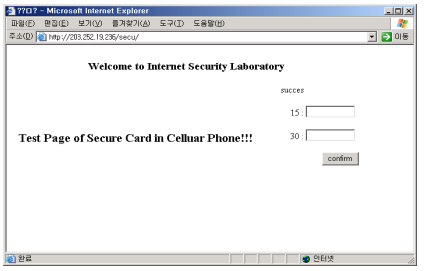

그림 14. 보안카드 입력 화면

현재 대부분의 웹사이트는 ID, Password만을 비교하기 때문에 한번 누출된 ID와 Password만을 가지고 다른 사람인 것처럼 인증을 받을 수 있다. 하지만 본 연구에서 제시한 기법을 이용할 경우 사용자에 대한 바이오 정보와 연계하여 키를 생성하게 되며, 생성된 키 값 정보는 핸드폰 기반 소프트 보안카드 생성 과정에 적용되어 보다 안전한 인증 시스템에 적용 가능한 구조이다.

본 논문에서 제시한 모델에서 송수신되는 패킷 정보를 스니핑하여 분석한 결과는 다음과 같다. 다음 그림에서와 같이 캡춰된 패킷 내용을 분석해 보면 전송되는 데이터가 해쉬 방식으로 변환되었으며 바이오 키 값을 이용하여 전자서명되어 전송된다. 따라서 전송되는 메시지 자체에 대한 인증 및 송신자에 대한 부인봉쇄 기능도 제공할 수 있다. 결국 인증 시스템에서의 안전성을 높일 수 있었다.

본 연구에서 제시한 기법은 기존의 휴대폰 기반 인증에서 가장 간단하게 nonce 값을 이용하여 로그인 사용자의 신원을 확인하는 방법보다 안전성을 높일 수 있다. nonce 값을 전송하기 위해서는 별도의 안전한 채널을 통해 nonce 값만을 전송하고 이를 통해 일회용 세션키 또는 일회용 패스워드(OTP) 값을 생성할 수 있으나. 이 경우 이른바 대포폰 및 비 인가된 핸드폰 등에 의해 불법 사용될 수 있다는 문제점이 있다. 하지만, 본 연구에서 제시한 기법인 경우 단순히 nonce 값을 생성하는 것 대신에 핸드폰 내 소프트 보안카드에 기반한 1차적 인증 과정을 수행하고, 추가로 바이오 정보 등을 이용한 다중 인증 모듈로도 적용 가능하다는 장점이 있다.

물론 본 연구에서 제안한 핸드폰 기반 소프트 보안카드 기법인 경우 바이오 정보와 연계하지 않을 경우 기

존의 nonce 기반 사용자 인증 방법으로도 활용 가능하다.

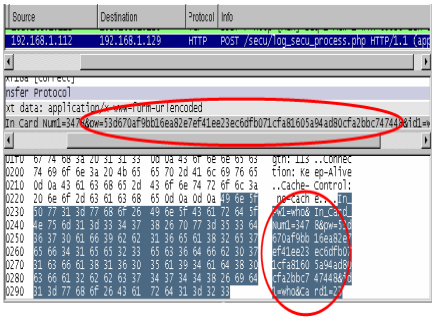

그림 15. 로그인 정보 스니핑

본 연구에서 제시한 기법을 기존의 인증 시스템과 비교 분석한 결과는 다음 표와 같다. 본 연구에서 제시한 소프트 보안카드 기반 로그인 기법은 기존의 로그인 기법에 사용되는 기본정보를 사용하며 부가적 정보를 이용하여 다중 인증(Multi-factor Authentication)을 제공한다. 물론 본 연구에서 제시한 기법은 바이오 정보 등과 같은 부가적 정보 입력을 필요로 하고 있으며, 1회 생성된 소프트 보안카드 정보는 기존의 보안카드와 유사하게 30개의 숫자 조합으로 생성된다는 제한을 가지긴 하지만 사용자가 요청하거나 로그인할 때마다 매번 다른 번호를 생성/입력하게 되기 때문에 일회용 패스워드(One-Time Password) 기능을 제공한다.

표 1. 기존 시스템과의 비교분석 및 평가

종류 / 기능	클라이언트 다운로드	공개키 기반	인증서 기반	제안기법
ID 및 Password 입력	O	O	X	O
부가정보입력	X	X	O	O
Multi-factor Authentication	X	X	X	O
One-Time Password	X	X	X	O

VII. 결론

대부분의 연구는 현재 얼마나 안전하게 통신을 하느냐에 관심을 가지고 새로운 기술의 개발에만 집중할 뿐 현재 구현된 기술의 보안성 향상 및 안전성 부분을 중요시하고 있지 않는 경향이 있다. 따라서 현재 대부분의 기업 및 사용자에게 제공되는 로그인 시스템인 경우 대부분 동일하거나 유사한 ID와 Password로 로그인을 하고 있는 경우가 많다. 결국 개인 프라이버시 정보 유출의 문제점이 발생하고 있다.

또한 최근 널리 공개된 패킷 스니핑 툴 등을 이용하여 네트워크 상에 전송되는 패킷을 누구나 손쉽게 캡쳐할 수 있으며, 기존 TCP/IP 기반 프로토콜의 특성상 보안 모듈 등이 패킷 헤더 구조 등에 적용되어 있지 않기 때문에 웹 로그인 과정 등에 포함된 ID 및 Password 정보 등을 공격자는 손쉽게 획득할 수 있다. 이러한 문제점을 보완하기 위해 주기적으로 ID/Password 정보를 변경해야 하는데 이 또한 상당히 번거로운 일이 되고 있다.

따라서 본 연구에서는 소프트 보안카드 방식을 통해 기존 웹 시스템 및 인터넷 관련 로그인 과정에서의 안전성을 향상시키기 위한 방법을 제시하였다. 본 연구에서 제시한 소프트 보안카드 시스템은 현재 로그인 시스템의 큰 수정 없이 적용이 가능하며 개인별 고유한 바이오 정보 및 개인이 소유하고 있는 핸드폰 시스템 등과 연계하여 사용자와 전체 웹 기반 시스템의 안전함을 향상 시킬 수 있다. 앞으로 다양한 형태의 바이오 정보와 연계하여 다중 인증 서비스를 제공할 수 있는 방안에 대한 연구가 필요할 것으로 생각된다.

참 고 문 헌

[1] 장혜진, '클라이언트 다운로드 방식의 안전한 로그인 프로세스의 설계 및 구현', 상명대학교 산업과학연구소 논문집, Vol.11 No.1, pp.345-348, 2001.

[2] 서종원, 조제경, 이형우, 'Spam mail 방지를 위한 SMS(Short Message Service) 송신자 인증 방법에 관한 연구', 2006년도 한국정보보호학회 동계학술대회, Vol.16, No.2, pp.234-238, 2006.

[3] M. Stuart, S. Samuil, and S. Shreeraj, '웹해킹(공격과방어)', 피어슨에듀케이션코리아, 2006.
[4] 추성호, 제갈명, 박홍성, "일회용 암호를 이용한 국산 암호 인증 시스템", 멀티미디어학술회의 논문집, Vol.5, No.1, pp.127-131, 2002.
[5] A. K. Jain, A. Ross, and S. Prabhakar, "Fingerprint matching using minutiae and texture features," to appear in the International Conference on Image Processing(ICIP), Greece, 2001(10)
[6] O. Peter, "Biometric generation of digital keys," Mini Symposium, DMIS-BUTE, 2001
[7] P. Janbandhu and M. Siyal, "Novel biometric digital signatures for Internet-based applications," Information Management & Computer Security, Vol.9, No.5, pp.205-212, 2001.
[8] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, Vol.21, pp.120-126, 1978.
[9] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms," IEEE Transactions on Information Theory, Vol.IT-30, No.4, pp.469-472, 1985.
[10] P. Tuyls and J. Goseling, "Capacity and examples of template-protecting biometric authentication systems," Proceedings of BioAW 2004, Lecture Notes in Computer Science 3087, Springer-Verlag, pp.158-170, 2004.
[11] X. Boyen, Y. Dodis, J. Katz, R. Ostrovsky, and A. Smith, "Secure remote authentication using biometrics," Advances in Cryptology - EUROCRYPT 2005, Lecture Notes in Computer Science 3494, Springer-Verlag, pp.147-163, 2005.

저 자 소 개

이 형 우(Hyung-Woo Lee) 정회원

- 1994년 2월 : 고려대학교 컴퓨터학과(이학사)
- 1996년 2월 : 고려대학교 컴퓨터학과(이학석사)
- 1999년 2월 : 고려대학교 컴퓨터학과(이학박사)
- 1999년 3월 ~ 2003년 2월 : 백석대학교 정보통신학부 교수
- 2003년 3월 ~ 현재 : 한신대학교 컴퓨터공학부 교수

<관심분야> : 정보보호, 네트워크보안, 무선랜, 침입탐지/차단, 웹 보안 기술, 컨텐츠 보호