PDA를 이용한 모바일 뱅킹 시스템

Mobile Banking Systems Using Personal Digital Assistants

안 건 호*, 양 수 철*, 추 영 열**

* 동명정보대학교 컴퓨터공학과(전화:(051)610-8404, 팩스:(051)610-8847, E-mail : dazzi11@hanmail.net)
** 동명정보대학교 컴퓨터공학과(전화:(051)610-8398, 팩스:(051)610-8847, E-mail : yychoo@tit.ac.kr)

Abstract : In mobile Internet banking service through wireless local area network, security is a most important factor to consider. We describe the development of mobile banking service using Personal Digatal Assistant (PDA). In order to increase the strength of encryption, we adopted hybrid approach where both of the public key algorithm and the secret key algorithm are used during the transaction among PDA, banking server and authentication server.

Keywords : 암호화, 소켓통신, 무선통신, 인증, 뱅킹 서비스

Ⅰ. 서 론

현재 무선 통신의 발전으로 각종 서비스를 휴대전화(Wireless Phone), PDA(Personal Digital Assistant) 등을 통해서간, 장소에 구애 받지 않는 환경이 제공되고 있다. 이미 국내의 이동전화 사업자들은 PDA를 통하여 위치정보, 교통정보, M-Commerce, 실시간 컨텐츠 제공등 기존 단말기로는 충분히 제공하지 못했던 서비스를 제공하고 있다. 이러한 환경은 기존 PC(Personal Computer)를 기반으로 한 인터넷 환경에 변화를 가져오게 되었다. 현재 PC를 이용한 인터넷 뱅킹과 폰뱅킹은 이미 상용화되어 있고 무선LAN을 이용한 금융 행위가 무선 장비의 성능향상으로 확산되고 있다.

모바일 뱅킹이란, 무선(wireless)을 이용하여 이동전화, PDA 등의 단말을 통해 이동 중에도 온라인(on-line) 금융서비스를 수행함을 의미한다. 이러한 서비스로는 모바일 지불(Mobile payment), 계좌통합(Account aggregation), 인터넷 빌링(EBPP), 금융포탈(Financial portal), 증권 거래 등이 있다. 하지만 이러한 모바일 기기를 이용한 전자 상거래의 눈부신 발달과는 대조적으로, 보안의 취약성이 대두되고 있다. 이 문제점은 TCP/IP의 도청에 대한 취약성에 기인한다. 이러한 문제점을 보완하고자, Netscape사에서 제안된 SSL (Secure Socket Layer)가 실질적인 웹 보안솔루션의 표준으로 인식되고 있는 실정이다. 하지만 SSL또한 슬래퍼 웜(Slapper Worm)등 공격형 웜 바이러스에 취약점을 가지고 있다. 또한 로밍 (roaming)시 연결이 이전될 때의 보안의 지속성 등에서 아직 완벽하지 못한 상태이다. 통신에서의 보안을 위해서는 암호화가 기본적으로 사용되고 나아가 인증, 디지털 서명 등이 요구된다[1][2][10].

암호화 방식은 크게 두 가지로 분류할 수 있다[2][3].

첫 째, 비밀키 알고리즘(대칭키 알고리즘)은 데이터의 암호화, 복호화에 동일한 키를 사용하는 알고리즘을 말한다. 송.수신자가 안전하게 통신하기 전에 반드시 키에 대한 공유가 필수적이다. 속도, 처리 능력면에서 공개키 알고리즘 보다 우월 하다고 볼 수 있겠다. 반면, 이 알고리즘의 단점으로는 알고리즘의 안전성이 키에 의존하기 때문에 키가 유출되면, 누구나 해독이 가능하다는 것이다.

둘 째, 공개키 알고리즘(비대칭 알고리즘)은 암호화, 복호화 시 사용되는 키가 서로 다른 것을 사용한다. 암호화하는 속도와 복호화 하는 속도가 차이가 나며, 이 알고리즘은 세션키 교환, 메시지 전자서명 등에 유용하게 사용된다. 이 알고리즘은 인증서의 형태로 배포 된다. 서로 다른 키쌍을 갖기 때문에 키에 안전성에 의존하는 비밀키 알고리즘과 대조된다.

실제 인증을 처리하는 방식에서는 두가지 알고리즘을 혼합하여 쓰는 혼합방식(Hybrid)이 많이 사용되고 있다. 구현된 프로그램에서는 발생된 16개의 난수배열을 공개키로 암호화하고, 이 난수배열로부터 세션키를 유도하여 로그인 문자열에 비밀키 암호화를 수행한다. 메시지의 무결성을 검증 가능케 하는 해쉬의 기능을 활용하여 복호화 측에서도 위.변조유무 파악이 용이하였다[2][3].

본 논문은 PDA를 이용한 은행 거래에서 사용자의 보안을 위해 공개된 2개의 암호화 방식을 기초로 모바일 뱅킹 시스템 (PDA Internet Banking System, PIBS)을 구현하였다.

본 논문은, 공개된 암호 라이브러리를 이용하여 고객과 은행이 원하는 확실한 보안 서비스를 제공할 수 있고, 편의성을 제공하는 안전한 인터넷 뱅킹 시스템의 설계 및 구현에 대하여 기술한다. 본 논문은 다음과 같이 구성되어있다.

Ⅱ. PIBS의 구성

본 시스템은 크게 무선통신 구간과 유선통신 구간으로 나뉘어지는데, 무선 통신구간에서는 PDA로 은행 서버에 접속하여서 회원 인증 및 데이터 통신을 할 수 있

도록 설계되었다. 유선통신 구간에서는 인증 서버와 은행 서버간의 실시간 인증서 확인이나 무선으로 받았거나 요구되어 지는 데이터를 전송하고 업데이트 하는 기능을 가진다.

이 시스템에서의 특징은 인터넷 뱅킹을 하면서 인증이나 암호화 부분에서 가중되는 PDA 모바일 기기의 제약적인 것들에 대해서 부담을 줄이고자 중간의 은행 서버를 만들어서 인증서버와 통신하게 만들었다. 인증만 된다면 사용자의 데이터를 받을 수 있도록 은행 서버기능을 하도록 설계되었다. 크게 은행 서버와 인증서버와의 통신, PDA와 은행 서버간의 통신으로 나눌 수 있다. 그리고 PIBS의 전체적인 구조를 살펴보면, 무선 통신 환경에서 뱅킹 전용 프로그램 상에서 사용자에게 편리성과 안정성을 제공할 수 있는 인터페이스 부분과 하부에서 보안 서비스를 제공하기 위해서 독립적인 프로그램 형태로 구성된 암호 프로그램 부분으로 구성된다. 하부의 응용 프로그램 부분은 암호 부분, 키 분배 부분, 인증서 발급 및 관리에 관한 부분으로 세분화되어 구성된다[3].

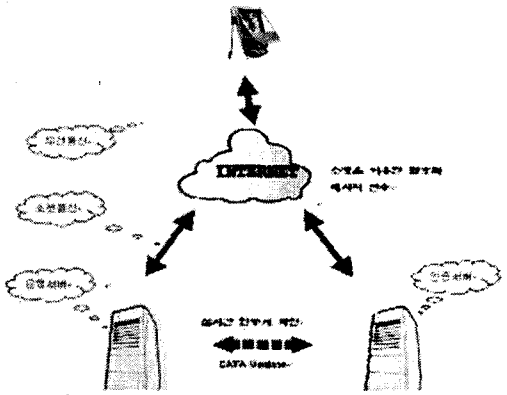

그림1. PDA BANKING SYSTEM 전체 구성도

1. PDA

PDA의 뱅킹 프로그램에서는 사용자 인터페이스와 무선통신에 중점을 두었다. 먼저 사용자가 로그인을 하면 무선 통신을 통한 은행서버에 접속 요구를 하고 응답을 기다린다. 계좌조회 창에서는 서버에서 정보를 전송 받아 계좌번호 및 사용자 정보 확인을 하고 이체처리 시에는 개인카드의 코드번호 확인 후 번호를 전송한 후 서버로부터 응답 후 다음 실행한다. 암호화 모듈을 통해 모든 정보를 암호화해서 전송한 후 수신시 복호화 모듈을 통해 복호화 해서 컨트롤에 데이터를 나타내어준다.

2. 은행 서버

은행 서버의 구성은 무선 통신 구간과 유선 통신 구간의 중간의 AGENT 역할을 하는 서버로서 무선 기기들이 접속할 수 있는 다중 소켓과 RC4 알고리즘을 이용한 암호화 모듈과 DB에 접속하여 검색 및 업데이트를 하기 위해 ADO와 ODBC를 이용하였다[4-6]. 인증 서버와의 실시간 인증 확인을 위한 인증 모듈 크게 4가지로 나눌 수 있다. 기능은 PDA 프로그램의 취약점을 보완하기 위한 서버이고 중개자 역할을 하는 서버이기도 하다.

3. 인증 서버

인증 DB와 암호화되어 송수신할 수 있는 암호화 모듈로 구성된다. 인증서버는 회원가입 요구를 받으면 인증서버에 저장하고 인증서를 만들어 배포한다. PDA에서 로그인 시 은행서버로부터 받은 암호화된 문자열을 복호화하고 인증 DB와 비교 후 PDA로 응답을 보내준다. 인증서버는 인증서를 은행서버로 전송하고 실시간 인증서 확인 기능을 가지고 있다.

III. 기능 설계 및 구현

1. 기능 설계

1.1 모바일 뱅킹 전체 흐름

본 논문의 모바일 뱅킹시스템은 기본적으로 클라이언트(모바일 단말기), 은행서버, 인증서버 3개체로 구성되어 있다. 구현된 모바일 뱅킹시스템의 처리흐름은 그림 2와 같다.

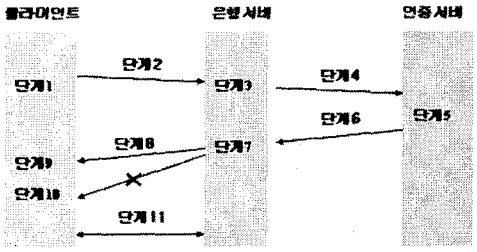

그림2. 모바일 뱅킹 처리 흐름도

(1) 로그인을 행한다. 이 때 로그인 문자열(ID + Password)을 비밀키 암호화를 사용한다.
(2) 암호화된 문자열을 소켓으로 전송한다.
(3) 전송된 문자열을 비밀키로 복호화 한다.
(4) 난수배열을 발생시키고 이 데이터를 해쉬하여 세션키를 발생시켜 로그인 문자열을 암호화 하고, 난수배열은 인증서의 공개키로 암호화 시켜 메시지를 토큰과 함께 조립한 후 인증서버로 소켓전송을 한다
(5) 인증서버에서는 공개키로 암호화된 난수배열과 세션키로 암호화된 로그인 문자열을 토큰을 근거로 적절히 분리시켜서 먼저 난수 배열의 암호문을 인증서의 비밀키로 복호화 한 후, 복호화된 데이터를 해쉬한 후 세션키를 발생시켜 로그인 문자열을 복호화 한다.
(6) 복호화 결과 인증된 사용자인지 아닌지 데이터베이스의 레코드와 비교작업을 한 후, 그 결과를 은행서버로 전송한다.
(7) 은행서버는 전송된 결과 값(True/False)을 가지고

클라이언트로부터의 연결요청을 수락 또는 거부하게 된다.

(8) 수락할 경우 단계9번, 거부할 경우 단계 10을 수행한다.

(9) 수락하였을 경우 정상적인 인터넷뱅킹을 수행하게 된다. 단계11을 수행한다.

(10) 접속이 거부된다.

(11) 인터넷뱅킹을 수행하게 되는데, 클라이언트에서의 원격 데이터베이스의 직접적인 연결이 아니라, 클라이언트가 질의어(Query Language)를 비밀키로 암호화 시켜서 소켓 전송을 하고, 은행서버에서 이를 전송받아, 질의를 대행하고 그 결과 또한 비밀키로 암호화 시켜 응답을 하는 방식으로 데이터베이스 연동을 수행한다.

구현된 프로그램에 사용된 라이브러리는 Microsoft CryptoAPI이다[8][9]. 서론에서 논하였던 기존 웹 기반에서의 뱅킹시스템에서의 취약점을 보완하고자, 웹이 가지는 범용성을 지양하고, 데이터의 암호화를 통하여 보안성을 강화하기 위해 윈도우 기반으로 작성하였다.

1.2 PDA와 서버간의 처리흐름

PDA와 서버간의 처리 흐름은 그림 3과 같다.

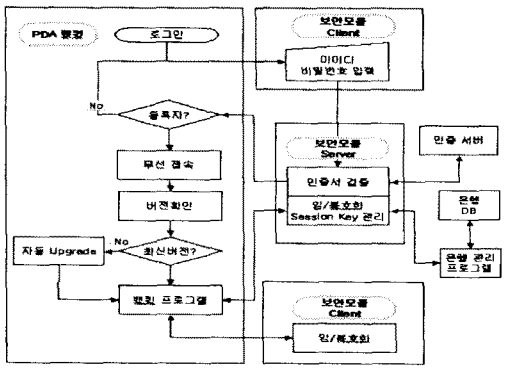

그림 3. PDA와 은행서버간의 처리절차

사용자가 로그인을 하면 무선통신을 통해 인증확인을 하게 되고 인증 확인이 되지 않는다면 은행에 등록을 한 후 뱅킹 서비스를 이용할 수 있다. 인증 확인시 보안 모듈을 통해서 세션키로 암호화 시킨 후 서버에서 실시간 인증 확인을 한다. 인증확인이 된 고객은 버전확인을 하고 업그레이드를 한다. 다음 뱅킹프로그램을 이용할 수 있고 모든 데이터 송수신은 보안 모듈을 통해서 서버와 통신하게 된다.

2. 구현

2.1 구현 환경

PDA에서 적용되는 프로그램은 Window CE 3.0 기반 환경에서 개발되었고 은행서버와 인증서버는 Window XP환경에서 구현하였다. 데이터 베이스는 SQL SERVER를 ADO와 ODBC로 연동시켰다[5-9].

PDA와 은행 서버간의 통신은 무선 인터넷을 사용하여 액세스 포인트에 접속해서 컴퓨터 IP로 접근을 하는 무선 통신을 이용하였고 은행과 인증 서버간의 통신은 유선 통신구간으로 소켓통신으로 각 토큰들로 데이터를 구별하여 전송하는 방식으로 구현하였다.[2]

암호화 모듈을 구현하기 위해서 은행서버와 인증서버 간에는 비밀키 알고리즘의 RC4를 사용하여 암호화, 복호화 시켰고 PDA와 은행 서버 간에는 독자적인 알고리즘을 만들어 PDA의 제약조건에 상관없이 사용할 수 있도록 만들었다.

2.2 PDA와 서버간의 통신 및 암/복호화 구현

PDA에서 로그인시 ID와 Password를 조합한다. 그리고 암호화시 사용되는 세션 키의 배열은 클라이언트 - 은행서버에서 동일하게 보유하고 있다. ID+<토큰>+Password+<토큰>으로 된 문자열을 세션 키로 암호화 하고 그 세션 키 배열의 인덱스 값과 로그인 모드를 뜻하는 모드 문자를 덧붙여 전송하게 된다. 결국 로그인시 전송되는 문자열은 다음과 같다.

모드+<토큰>+세션 키의 인덱스 값+<토큰>+ 암호화된 로그인 문자열<토큰>형태로 은행서버로 전송된 문자열은 은행서버에서는 이 문자열을 암호화 하기전 모드문자를 분석하여 모드 필드를 추출하여 인증모드임을 확인하고 세션키의 인덱스 값으로 세션키 배열에서 키를 추출하여 암호화된 로그인 문자열을 복호화 한다. 그리고 데이터베이스 서버에 질의문으로 해당 ID와 Password로 질의하여 인증서 이름을 추출해 내고, 그 인증서 이름에 맞는 인증서를 이용하여 암호화를 수행 한다.

PDA-은행서버 간 암호화시 세션키 값을 문자열로 변환하고 각 자릿수마다 ASCII값을 취해 그 값을 더한 것을 각 문자열의 문자마다 가중치를 두어 토큰들로 조립되고, 복호화시 동일한 세션키로 가중치를 다시 빼고 그것을 문자열로 재복원하는 방법을 사용하였다. 그리고, 이러한 알고리즘은 인증 후 사용자의 금융거래 시에도 유용하게 사용될 수 있다.

2.3 서버 측 암/복호화 구현

RC4를 응용한 인증서버와의 암호화와 PDA와 암호화모듈로 구성된다. 서버 간의 암호화 과정은 그림 4와 같다.

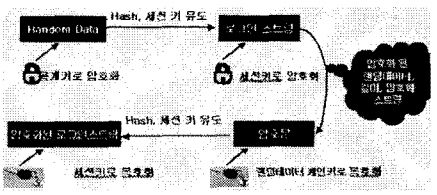

그림 4. 인증 서버간의 암호화 처리

먼저 RC4를 응용한 암호화 알고리즘은 랜덤 데이터를 공개키로 암호화해서 그 길이와 함께 첨부하고, 랜덤 데이터를 해쉬해서 세션키를 생성한다. 대칭키 방식, 비대칭키 방식 둘 다 이용한 혼합방식을 사용함으로서 위. 변조로부터 보안성 강화를 할 수 있다.

PDA의 암호화는 먼저 키를 난수 함수를 이용하여 생성시킨 후 키를 공개키로 암호화하고 암호화된 값을 전송할 문자열을 비밀키로 암호화한 데이터와 합해서 전송하는 방식으로 구현되었다.

2.4 PDA클라이언트

사용자 로그인과 동시에 서버로부터 다운로드 되어 실행된다. 서버가 열리면 특정 포트를 서버 소켓으로 열고 승인 응답을 기다린다. 승인 응답을 받는 동시에 은행 서버에서는 고객에 대한 정보를 PDA로 전송을 하고 전송 받은 데이터들을 복호화해서 스트링을 토큰으로 나누어 컨트롤에 나타내어준다. 모든 뱅킹 행위를 하다가 각 트랜잭션에 맞게 암호화 모듈을 거쳐 스트링을 전송해주고 그 결과를 받아 처리해준다.

Ⅳ. 결 론

본 논문은 인터넷 사회라고 불리는 현대 사회에서 은행 업무를 가정이나 사무실에서 처리할 수 있도록 해 주는 인터넷 뱅킹 시스템을 좀 더 사용자에게 편의성을 제공할 수 있도록 하기위해 모바일 기기인 PDA를 이용한 뱅킹 시스템을 구현하였다.

PIBS는 보안상으로 비밀키 방식의 RC4를 변형시키고 자체 알고리즘을 구현하여 기존의 암호화보다 더 강한 암호화를 제공한다. 기존의 세션키를 암호화하는 방식이 아닌 랜덤 데이타를 이용하여 한 번 더 암호화하는 방식으로 보안강도를 더 높였다. 그리고 사용자들의 다중 접속을 위해 다중 소켓방식으로 구현하였고 PDA에의 사용자 인터페이스는 PDA의 메모리 제약조건으로 인해 간단하고 편리하게 구성을 하였다. 자체 제작된 암호화 모듈을 바탕으로 설계 및 구현한 응용 프로그램 부분을 고객이 사용하기에 편리하도록 최대한의 편의성을 제공할 수 있다.

향후에 PIBS는 뱅킹 업무만이 아닌 주식 및 부동산 등과 같은 금전적인 목적물을 인터넷상에서 매매할 때에도 보안상의 서비스를 제공하기 위해서 사용 가능하다. 기타의 보안상의 데이터 전송을 위한 응용 분야에 활용하기 위해서 암호처리 알고리즘과 신분 인증 알고리즘을 적용하여 응용한다면 보안이 필요한 보다 많은 분야에서 이용할 수 있을 것이다.

참고문헌

[1]김진묵, 암호 라이브러리를 이용한 안전한 인터넷 뱅킹 시스템 설계 및 구현, 배제대학교 석사학위 논문, 1999.

[2]William Stallings, Cryptography and Network Security: Principles and Practice, 2nd Edition, Prentice Hall, 1999

[3]강선명, 熱血講義 Visual C++ 암호화 프로그래밍, 프리렉

[4]김화종, 컴퓨터 네트워크 프로그래밍, 홍릉출판사

[5]김병세,이이표, Microsoft Visual C++ Bible 6.0, 삼양출판사

[6]MS SQL SERVER 2000 개발팁, microsoft SQL server 2000 resource kit

[7]우철웅, SQL server 2000 programming

[8]Bondi,Richard / John Wiley & Sons, Cryptograghy for Visual Basic : A Programmer's Guide to the Microsoft CryptoAPI; Incorporated

[9]Douglas Boling, PROGRAMMING Microsoft Wwindows CE 2nd Edition

[10]Mc Graw Hill, Behrouz A. Forouzan, Data Com munications and Networking 2nd edition