제20회 한국정보처리학회 추계학술발표대회 논문집 제10권 제2호 (2003. 11)

PDA 에서 이미지를 이용한 인증방안 및 전자지불 프로토콜 설계

최용식*, 전영준*, 신승호*
*인천대학교 컴퓨터공학과
e-mail : mars@incheon.ac.kr

A Design of Electronic Payment Protocol and Using Image authentication scheme on PDA

Yong-Sik Choi*, Young-Jun John*, Seung-Ho Shin*
*Dept. Of Computer Science & Engineering, University of incheon

요 약

PDA 는 터치패드 방식의 문자 입력을 한다. 따라서 사용자에게 긴 입력을 요구할 때 불편한 환경을 제공한다. 따라서 이미지의 특정 지점을 마우스로 선택함으로 문자입력을 대신하여 인증을 함으로써 편리한 환경을 제공한다. 보안을 제공하기 위하여 초기 이미지에 따른 이미지의 배열 정보 및 입력된 값을 해시코드화 하여 인증 및 키교환이 안전하게 이루어진다. HASH 와 SEED 암호화 알고리즘을 적용하여 효율적이고, 전송 메시지의 무결성을 보장하며 내부 참여자에 의한 정보 유출이 있더라도 안전한 전자지불 프로토콜 시스템을 설계 및 구현하였다.

1. 서론

정보통신 산업의 발달로 인하여 인터넷을 사용은 학술 및 연구를 대상으로 한 정보 공유 목적에서 마켓팅의 대상으로 보고 상업적으로 이용하고 있다. 유선 인터넷상에서는 인터넷 뱅킹, 온라인 쇼핑몰등 각종 물건을 판매하고 대금을 지불하는 전자 지불 시스템이 이루어지고 있다. 개인용 컴퓨터 등의 고정 단말기를 기반으로 하는 전자지불 시스템의 형태에서 벗어나 이동성, 휴대성을 제공하는 무선 서비스의 형태가 증가하고 있다. 무선인터넷의 발달과 사용자의 증가로 인하여 유선 인터넷에서 제공하는 서비스를 무선인터넷으로 확장한 모바일 서비스가 크게 증가하고 있다. 휴대폰은 주로 소액결제 시스템에 사용되며, PDA 의 경우는 증권, 은행의 일부 서비스를 제공하고 있다. 아직까지는 초기 단계이기 때문에 서비스의 내용이 다양하지 못하고, 보안상의 문제와 하드웨어 장비의 제약이 많다. 그리고 인증 및 정보보호 등에 관한 정보가 쉽게 노출되는 문제점이 있다. 이러한 문제점을 해결하기 위해서는 지불 정보 및 구매 정보의 기밀성을 보장하고, 디지털 서명을 이용한 전송데이터에 대한 무결성을 제공하며, 디지털 서명과 인증서를 제공하여 위험 요소로부터의 대비책이 필요하다. 또한, 모발일 단말기는 낮은 CPU 파워, 적은 메모리를 제공하며 터치패드 기반의 입력방식을 따르고 있다. 터치패드 방식은 긴 문자 입력을 요구할 때 불편한 환경을 제공한다. 이미지의 특정 지점을 마우스로 선택함으로 문자입력을 대신하여 인증을 함으로써 편리한 환경을 제공한다. 보안을 제공하기 위하여 초기 이미지에 따른 이미지의 배열 정보 및 입력된 값을 해시코드화 하여 인증 및 키교환이 안전하게 이루어진다. HASH 와 SEED 암호화 알고리즘을 적용하여 효율적이고, 전송 메시지의 무결성을 보장하며 내부 참여자에 의한 정보 유출이 있더라도 안전한 전자지불 프로토콜 시스템을 설계 및 구현하려고 한다.

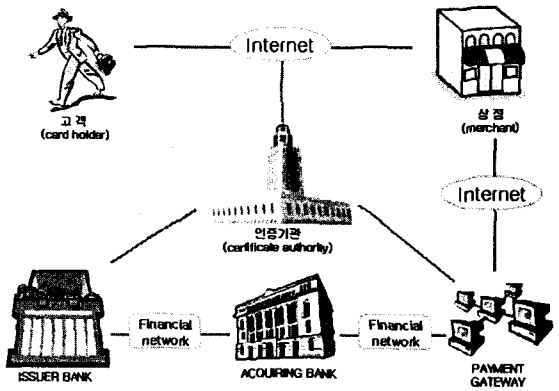
본 논문의 구성은 다음과 같다. 2 장에서 관련연구로서 전자지불 프로토콜과 패스워드 인증에 대하여 기술하고 3 장에서 제안된 이미지 기반 인증 및 전자지불 프로토콜의 설계 및 효율성을 분석하며 4 장에서 결론을 맺는다.

본 연구는 한국과학재단 지정 인천대학교 동북아전자물류연구센터의 지원에 의한 것입니다.

2. 관련연구

2.1 SET

SET(Secure Electronic Transaction)은 인터넷과 같은 open network에서 안전하게 상거래를 할 수 있도록 보장해주는 지불 프로토콜이다. SET 프로토콜은 메시지의 암호화와 개인을 인증(Authentication)하는 전자 증명서등을 통해서 인터넷상에서 안전한 전자상거래가 이루어질 수 있도록 하고 있다. 즉, 메시지 암호화를 통하여 전자상거래에 참여하는 카드소지자의 계좌번호 및 신용카드 번호와 지불 정보 등 민감한 정보의 노출을 방지하며, 전자서명 및 해쉬 함수를 이용하여 모든 메시지 내용의 무결성(integrity)을 보장하는 한편, X.50 를 기반으로 한 인증서 방식을 이용하여 거래 행위의 실질적인 주체인 카드소지자와 상인간에 상호 인증을 제공한다. 예를 들면 신용카드를 이용할 경우에는 물건을 사는 사람이 정말로 신용카드 회원인지를 증명할 필요가 있다. SET 에서는 이러한 목적으로 인증서를 사용한다. 인증서는 실제로 컴퓨터상에서 취급하는 데이터이며, 여기에는 본인의 이름, 신용카드의 이름 외에 통신에 필요한 암호 키의 정보도 일부 포함된다.



[그림 1] SET 지불 프로토콜

[그림 1]과 같이 SET 을 이용한 상거래 트랜잭션에 참여하는 구성원은 카드소지자(Cardholder), 상인(Merchant), 지불게이트웨이(Payment Gateway), 그리고 인증기관(CA; Certificate Authority)으로 정의되어 있으며, 신용카드 사 또는 제 3 자에 의해서 운영되는 지불게이트웨이는 금융기관 네트워크를 통하여 은행과 연결된다. SET 프로토콜 명세는 다양한 하드웨어 및 소프트웨어 플랫폼 간에 동작할 수 있도록 하기 위하여 ASN.1 을 이용하여 기술되어 있다.

2.2 SEED

SEED 는 대칭키 암호알고리즘으로 블록 단위로 메시지를 처리하는 블록 암호 알고리즘이다. 대칭키 블록 암호알고리즘은 비밀성을 제공하는 암호시스템의 중요 요소이다. n비트 블록 암호화 알고리즘이란 고정된 n 비트 평문을 같은 길이의 n 비트 암호문으로 바꾸는 함수를 말한다. 이러한 변형 과정에 암• 복호키를 적용하여 암호화와 복호화를 수행한다.

블록 암호 알고리즘은 Feistel 구조로 설계된다. 블록 암호화 알고리즘은 DES, FEAL, LOKI, MISTY, Blowfish, CAST, Twofish 등이 있다. Feistel 구조란 각각 t 비트인 블록으로 이루어진 2t 비트 평문 블록이 r 라운드(r≥1)를 거쳐 암호문으로 변환되는 반복 구조를 말한다. 반복 구조란 평문 블록이 여러 라운드를 거쳐 암호화되는 과정을 말한다. 라운드 함수 란 암호키로부터 유도된 각 서브키를 입력으로 하여

$L_i = R_{i-1}$, $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$ 를 통해

$(L_{i-1}, R_{i-1}) \xrightarrow{K_i} (L_i, R_i)$ 로 바꾸어 주는 함수를 말한다. 또한, 전체 알고리즘의 라운드 수는 요구되는 비도와 수행 효율성의 상호 절충적 관계에 의해 결정된다. 보통 Feistel 구조는 3 라운드 이상이며, 짝수 라운드로 구성된다.

2.3 HASH

해쉬함수는 원문의 무결성을 검증할 때 사용되며, 전자 서명에도 사용된다. 해쉬함수는 단방향 성질 때문에 다이제스트된 메시지로부터 원문을 구해낼 수 없다. 암호에서의 해쉬함수와 일반적인 해쉬함수와의 차이점은 다음과 같다. 일반적으로 해쉬 함수는 임의 길이의 평문 데이터를 정해진 길이의 데이터로 줄여주는 함수 이다. 하지만 암호에서 사용하는 해쉬함수는 이와 같은 성질이외에 다음의 성질을 추가적으로 요구한다. 약한 충동 회피성은 해쉬함수 h 에 대하여 특정 값 a 와 h(a)값이 주어졌을때, h(b)=h(a)를 만족하는 a 와 서로 다른 b 를 찾기 어렵다. 강한 충동 회피성은 해쉬함수 h 에 대해서 특정 값 h(b)=h(a)를 만족하는 a, b 를 찾기 어렵다. 단 방향 성질은 h(a)값을 알 때, a 값을 알기 어렵다. 즉 원문 a 로부터 a 의 해쉬값인 h(a)는 쉽게 구할 수 있지만 해쉬값만 가지고는 원문을 알아내기 어렵다.

해쉬알고리즘은 임의의 길이의 비트 열을 고정된 길이의 출력값인 해쉬코드로 압축시키는 알고리즘으로써 다음의 특성을 갖는다.

(1) 주어진 출력에 대하여 입력값을 구하는 것이 계산상으로 불가능하다.

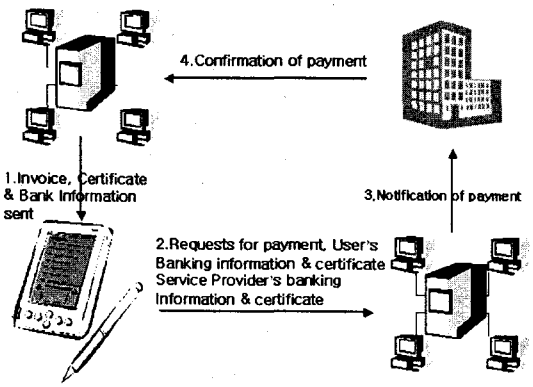
(2) 주어진 입력에 대하여 같은 출력을 내는 또다른 입력을 찾아내는 것이 계산상 불가능하다.

(3) 같은 출력을 내는 임의의 서로 다른 두 입력 메시지를 찾는 것이 계산상 불가능하다.

해쉬알고리즘은 크게 DES 와 같은 블록 암호알고리즘에 기초한 해쉬알고리즘과 전용 해쉬알고리즘으로 나눌 수 있다. 블록 암호알고리즘을 이용한 해수알고리즘은 이미 구현되어 사용되고 있는 블록 암호알고리즘을 사용할 수 있다는 장점이 있으나, 대부분의 블록 암호알고리즘의 경우 속도가 빠르지 않을 뿐더러 이를 기본함수로 이용한 경우 블록 암호알고리즘보다 훨씬 속도가 떨어지므로 현재는 대부분의 응용에서 전용 해쉬알고리즘이 주로 이용된다.

2.4 WTLS, WPP

WTLS 는 WAP 의 보안 프로토콜으로서 인터넷 프로토콜에서 TCP 의 보안을 위해 사용하는 TLS 를 무선환경에 맞도록 최적화 한것이다. WTLS 는 TLS 와 마찬가지로 인증, 암복호화, 무결성 검증 기능의 보안을 제공한다. WPP 프로토콜은 SET 을 기초하여 무선 인터넷에서 신용카드 지불을 할 수 있도록 제안된 지불 프로토콜이다. WPP 는 신용카드 정보를 보호하기 위해서 스마트카드 기술과 WAP 의 WTLS 를 사용한다.



[그림 3] WPP 지불 프로토콜

[그림 3]과 같이 WPP 지불 프로토콜은 사용자, 사용자의 은행, 서비스 제공자, 서비스 제공자의 은행으로 구성된다. WPP 지불 프로토콜은 WAP 의 WTLS 를 사용하여 무선구간의 보안을 제공한다. 이와같은 연결은 WAP 단말기와 유선환경에 존재하는 서버를 연결하는 WAP Gateway 를 통하여 연결된다. WAP Gateway 는 WTLS-SSL 프로토콜 변환 시 암호화된 메시지가 복호화되어 원본 메시지의 유출의 위험이 있다. 즉, 종단간의 보안을 제공하지 못한다. 그러므로 WPP 지불 프로토콜도 같은 문제점이 있다.

2.5 패스워드에 기초한 인증

패스워드의 선택 범위와 길이는 사용자의 기억력에 의해 제안되는 낮은 엔트로피(entropy)를 가지므로 공격자가 패스워드로 유추되는 단어들을 사전화하고, 오프라인에서 이 단어들을 차례로 대입하여 정당성을 확인하는 오프라인 사전 공격에 취약하다.

무선 PKI 에서는 인증서 요청 시 사용자 인증을 위해 사용자 아이디와 패스워드를 사용한다. 이때 패스워드는 WTLS 연결을 통해 보호되거나, 패스워드에 기초한 MAC(Message Authentication Code)를 이용해서 보호되고 있다. 전자는 WAP Forum 의 WPKI 표준에서 사용되는 방법이고, 후자는 국내 기술규격에 명시되어 있는 방법이다. 국내에서는 WTLS 의 오버헤드를 고려해서 이를 사용하지 않는 방안을 고안했고, 이에 따라 signText 와 패스워드에 기초한 MAC 을 이용해서 인증서 요청 형식을 정의하고 있다.

무선 인터넷을 위한 보안 프로토콜은 인증과 키교환을 주 목적으로 하며, 주로 인증서를 이용하여 설계되었다. 대표적인 것이 WAP(Wiresless Application Protocol) 포럼의 WTLS(Wireless Transport Layer Security)이며, 무선 인터넷에서 인증서의 효율적인 사용을 위하여 X.509 인증서가 아닌 WTLS 인증서를 이용한다. 무선 PKI(Public Key Infrastructure)를 통해 발급받은 인증서를 이용한 공개키 암호시스템 위에 설계되었다. 그러므로 인증서 관리의 불편함이 있고, 무선 PKI 의 완전한 구축이 이루어지지 않으면 사용이 어렵다. 패스워드에 기초한 인증 및 키 교환 프로토콜은 패스워드가 가지는 취약점, 즉 충분한 하지 않는 길이 그리고 랜덤성을 고려해서 오프라인 사전 공격에 강해야 한다.

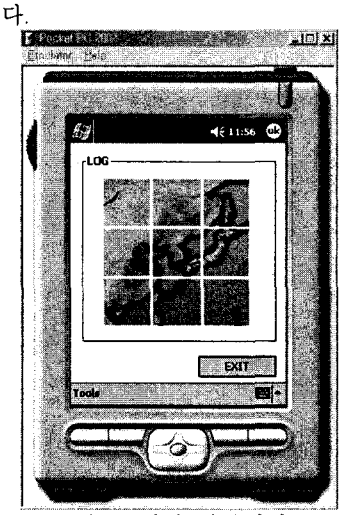
3. 제안된 인증 프로토콜 설계

3.1 이미지를 활용한 패스워드 입력

모바일 서비스는 휴대폰, PDA 등 무선 특화 단말기를 이용하여 빌링 및 지불 시스템에 접근하여 결제 서비스를 제공한다. 그러나 모바일 장비는 제한된 자원과 낮은 대역폭, 낮은 연산 처리 능력으로 인한 제약사항이 따른다. 따라서 짧은 키 길이, 빠른 키 생성, 적은 량의 메모리를 사용하면서도 강한 보안성이 보장되어야 한다. PDA 에서 문자 기반의 패스워들를 사용하는 것은 인터페이스가 터치패드 기반이기 때문에 긴 입력을 요구할 때 불편한 환경을 제공한다. 이에 문자 대신 화면에 나타난 이미지에서 특정 지점을 팬 마우스로 선택하는 것으로 인증 절차를 마치게 한다.

3.1.1 이미지의 배열의 생성

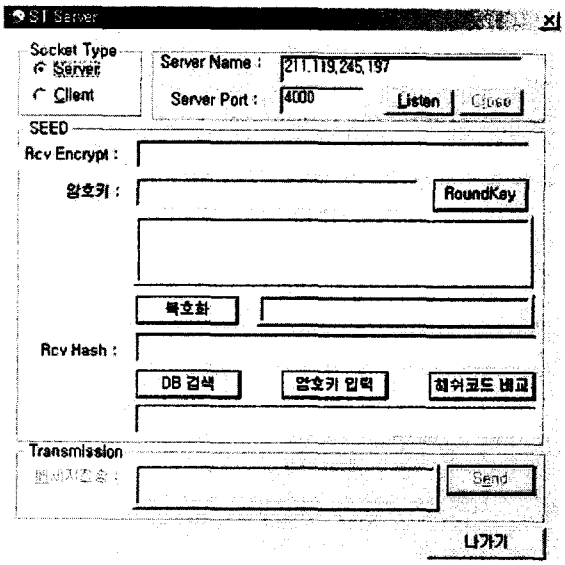
이미지를 통한 입력 인터페이스를 제공하여 사용자의 편의를 제공하며 이미지 위치 값을 랜덤하게 생성한 후 이미지의 배열 정보를 해쉬코드화 한다. 이미지 배열정보와 선택된 이미지의 값을 해쉬코드화 한다. 그리고, 지불정보를 SEED 를 통하여 암호화한다. 암호된 값을 전자지불 시스템에 전송하므로 도청 및 오프라인 사전공격에 대해 인증 및 키 교환이 안전하게 이루어 진다.



[그림 4] 입력 인터페이스

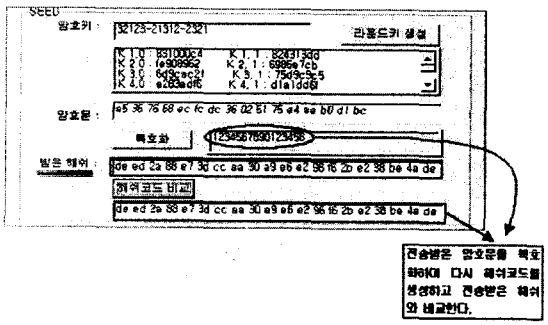
3.2 인증 시스템

사용자는 직접 금융 시스템으로 연결될 수 없으며 지불 시스템을 통하여 연결된다. 이와 같은 구조는 서버의 보안상의 취약점이나 내부 관련자에 의한 정보의 유출이 있을 때 보호될 수 없다. 이러한 구조적인 문제점을 해결하여 종단간의 보안을 제공하기 위하여 인증정보를 HASH Code 화 하고 지불 정보를 SEED 암호화 알고리즘을 적용하여 암호화하여 전송 메시지의 무결성을 보장하며 효율적이고, DC/LC 에 대하여 안전하다. 그리고 128 비트를 지원하므로 안전도를 충분히 제공한다.



[그림 5] 인증 시스템

암호화된 인증 정보를 받아 전송된 메시지를 비교하는 인증 시스템은 [그림 5]와 같다.



[그림 6] HASH Code 비교

[그림 6]에서는 전송된 HASH Code 를 서버에 저장되어 있는 HASH Code 값과 비교하여 일치하면 인증이 올바르게 이루어져다고 간주한다.

즉 원문의 내용을 모르더라도 HASH Code 값을 비교함으로써 인증 가능하다. 이것은 서버의 보안상 취약점이나 내부 관련자에 의하여 비밀정보의 유출이 있더라도 안전하게 인증할 수 있다.

4. 결론 및 향후 계획

PDA 는 제한된 자원과 낮은 대역폭, 낮은 연산 처리 능력으로 인한 제약사항이 따른다. 따라서 짧은 키 길이, 빠른 키 생성, 적은 량의 메모리를 사용하면서도 강한 보안성이 보장되어야 한다. PAD 에서는 터치패드 기반의 입력방식을 따르고 있다. 터치패드 방식은 긴 문자 입력을 요구할 때 불편한 환경을 제공한다. 이에 이미지의 특정 지점을 마우스로 선택함으로 문자입력을 대신하여 인증을 함으로써 편리한 환경을 제공한다. 보안을 제공하기 위하여 초기 이미지에 따른 이미지의 배열 정보 및 입력된 값을 해시코드화 하여 인증 및 키교환이 안전하게 이루어진다. HASH 와 SEED 암호화 알고리즘을 적용하여 효율적이고, 전송 메시지의 무결성을 보장하며 내부 참여자에 의한 정보 유출이 있더라도 안전한 전자지불 프로토콜 시스템을 설계 및 구현하였다.

참고문헌

[1] Wireless Application Protocol Wireless Transport Layer Security, WAP Forum, 6th of April, 2001.

[2] Wireless Application Protocol Public Key Infrastructure Definition, WAP Forum, 26th of Oct. 2000.

[3] VISA & Mastercard, "SET Electronic Transaction Specifiation", 1997

[4]임수철, 강상승, 이병래, 김태윤, "무선인터넷에서의 종단간 보안을 제공하는 신용카드 기반의 지불 프로토콜", 한국정보과학회 논문지 I VOL.29 NO.06 pp. 0645 ~ 0653, 2002. 12.

[5]양대현, 이석준, "무선 인터넷을 위한 패스워드 기반의 인증 및 키 교환 프로토콜", 한국정보과학회 논문지 I VOL.29 NO.03 pp. 0324 ~ 0332, 2002. 06.

[6]허재형, 신동규, "PDA 상에서의 전자 상거래 보안 솔루션", 정보처리학회 2002 년 춘계학술대회 VOL.09 NO.01 pp. 1349 ~ 1352, 2002. 04.

[7]김선형, 김태윤, "제 3 세대 이동 통신 시스템을 위한 인증 및 지불 기법", 정보처리학회 2002 년 추계학술대회 VOL.09 NO.02 pp. 0000 ~ 0000, 2002. 10.