논문 2004-41SP-6-12

무선 인터넷에서 보안을 위한 인증방안에 관한 연구

(A Study on the authentication scheme for Security of Wireless Internet)

최 용 식*, 강 찬 희**, 신 승 호*

(Yong Sik Choi, Chan Hee Kang, and Seoung Ho Shin)

요 약

모바일 단말기는 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. HASH와 SEED 암호화 알고리즘을 적용하여 효율적이고, 전송 메시지의 무결성을 보장하며 내부 참여자에 의한 정보 유출이 있더라도 안전한 전자지불 프로토콜 시스템을 설계 및 구현하였다.

Abstract

The continuing development of the information technology industry and wireless networking has increased the use of mobile device, which provides both portability and mobility. As follows, demands for extended services within the wireless Internet are increasing rapidly. Because it still in its initial stages of development, the wireless Internet presents continuing problems in security and limitations in the content of services. Furthermore, most mobile equipment utilizes the touch pad input method. This input method is inconvenient when a user needs to input a long sentence. This has led to the more convenient development of image selection by using a pen mouse. In order to provide security under these conditions, a HASH code may be used to transmit an array of information and input values, created by the image input at the early stages. Thus, authentication and key exchange are completed securely. Messages are encoded and transmitted, preventing both information drain by insiders and interference from outside.

Keywords : Hash Code, security, mobile equipment, wireless

I. 서 론

정보 정보통신 산업은 아날로그 통신 시대에서 디지털 통신 시대로의 변화에 따라 통신 단말기는 급속히 소형화, 경량화 되고 있으며, 단순한 통신수단에서 개인용 컴퓨팅 기기로 발전해 일상생활의 필수품으로 자리잡아가고 있다. 휴대가 간편한 음성 위주의 기능에 더하여 데이터 위주의 무선 인터넷 및 컴퓨팅 기술들이 추가되고 있는 상황이다. 즉, 유무선 네트워크 통합 및 대역폭 확장과 더불어 고객의 요구 다양화는 이동통신 기능과 컴퓨팅 기능들의 통합화를 이끌어나가고 있다. 최근에서 무선 지불 수단을 제공하는 휴대폰, PDA 등 이동통신단말기 기술이 발전함에 따라 오프라인 상점에서도 전자 지불 수단의 활용이 크게 증가하고 있다. 최근에는 전자상거래뿐만 아니라 교통, 유통, 금융, 교육 등 여러 산업분야에 널리 적용되고 있다. 모발일 단말기는 낮은 CPU파워, 적은 메모리를 제공하며 터치패드 기반의 입력방식을 따르고 있다. 터치패드 방식은 긴

* 정회원, 인천대학교 컴퓨터 공학과
(Dept. of Computer Engineering, University of incheon)
** 정회원, 상지영서대학교 디지털 정보과
(Dept. of Digital Information Of Sangji Youngseo Colleage)
※ 본 연구는 과학기술부 지정 동북아 전자물류 연구센터의 지원에 의한 것입니다
접수일자: 2004년6월18일, 수정완료일: 2004년11월4일

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 입력된값을 해시코드화 하여 인증 및 키 교환이 안전하게 이루어진다. HASH와 SEED 암호화 알고리즘을 적용하여 효율적이고, 전송 메시지의 무결성을 보장하며 내부 참여자에 의한 정보 유출이 있더라도 안전한 전자 지불 프로토콜 시스템을 설계 및 구현하려고 한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서 관련연구로서 전자 지불 프로토콜과 패스워드 인증에 대하여 기술하고 Ⅲ장에서 제안된 이미지 기반 인증의 설계하며 Ⅳ장에서 결론을 맺는다.

Ⅱ. 본 론

1. SET(Secure Electronic Transaction)

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 전자증명서등을 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.50을 기반으로 한 인증서 방식을 이용하여 거래 행위의 실질적인 주체인 카드소지자와 상인 간에 상호 인증을 제공한다. SET에서의 인증서는 실제로 컴퓨터상에서 취급하는 데이터이며, 여기에는 본인의 이름, 신용카드의 이름 외에 통신에 필요한 암호 키의 정보도 일부 포함된다.

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

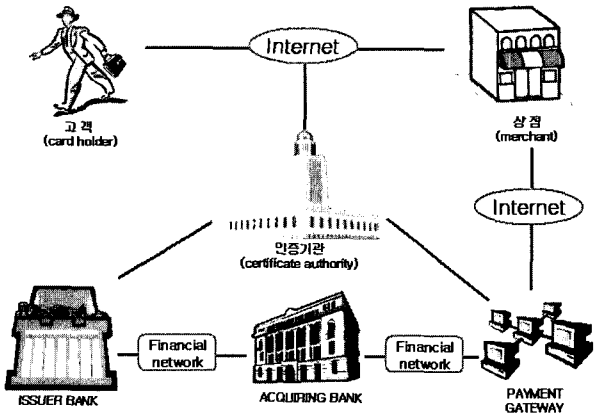


그림. 1. SET 지불 프로토콜
Fig. 1. SET Payment Protocol.

2. SEED

SEED는 대칭키 암호알고리즘으로 블록 단위로 메시지를 처리하는 블록 암호 알고리즘이다. 대칭키 블록 암호알고리즘은 비밀성을 제공하는 암호시스템의 중요 요소이다. n비트 블록 암호화 알고리즘이란 고정된 n비트 평문을 같은 길이의 n비트 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 t비트인 블록으로 이루어진 2t비트 평문 블록이 r라운드($r \geq 1$)를 거쳐 암호문으로 변환되는 반복 구조를 말한다. 반복 구조란 평문 블록이 여러 라운드를 거쳐 암호화되는 과정을 말한다.

라운드 함수란 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 3라운드 이상이며, 짝수 라운드로 구성된다.

3. HASH

해쉬함수는 원문의 무결성을 검증할 때 사용되며, 전자서명에도 사용된다. 해쉬함수는 단방향 성질 때문에 다이제스트된 메시지로부터 원문을 구해낼 수없다. 암호에서의 해쉬함수와 일반적인 해쉬함수와의 차이점은 다음

과 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 h에 대하여 특정 값 a와 h(a)값이 주어졌을 때, h(b)=h(a)를 만족하는 a와 서로 다른 b를 찾기 어렵다. 강한 충동 회피성은 해쉬함수 h에 대해서 특정 값 h(b)=h(a)를 만족하는 a, b를 찾기 어렵다. 단 방향 성질은 h(a)값을 알 때, a 값을 알기 어렵다. 즉 원문 a로부터 a의 해쉬 값인 h(a)는 쉽게 구할 수 있지만 해쉬 값만 가지고는 원문을 알아내기 어렵다.

해쉬알고리즘은 크게 DES와 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.

4. WTLS, WPP

WTLS는 WAP의 보안 프로토콜 으로서 인터넷 프로토콜에서 TCP의 보안을 위해 사용하는 TLS를 무선 환경에 맞도록 최적화 한 것이다. WTLS는 TLS와 마찬가지로 인증, 암복호화, 무결성 검증 기능의 보안을 제공한다. WPP 프로토콜은 SET을 기초하여 무선인터넷에서 신용카드 지불을 할 수 있도록 제안된 지불 프로토콜이다. WPP는 신용카드 정보를 보호하기 위해서 스마트카드 기술과 WAP의 WTLS를 사용한다.

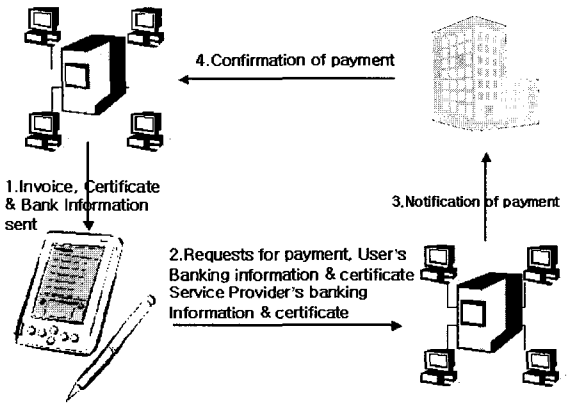


그림 2. WPP 지불 프로토콜
Fig. 2. WPP Payment Protocol.

Fig 2와 같이 WPP지불 프로토콜은 사용자, 사용자의 은행, 서비스 제공자, 서비스 제공자의 은행으로 구성된다. WPP 지불 프로토콜은 WAP의 WTLS를 사용하여 무선구간의 보안을 제공한다. 이와 같은 연결은 WAP 단말기와 유선환경에 존재하는 서버를 연결하는 WAP Gateway를 통하여 연결된다. WAP Gateway는 WTLS-SSL 프로토콜 변환 시 암호화된 메시지가 복호화 되어 원본 메시지의 유출의 위험이 있다. 즉, 종단간의 보안을 제공하지 못한다. 그러므로 WPP 지불 프로토콜도 같은 문제점이 있다.

Ⅲ. 실 험

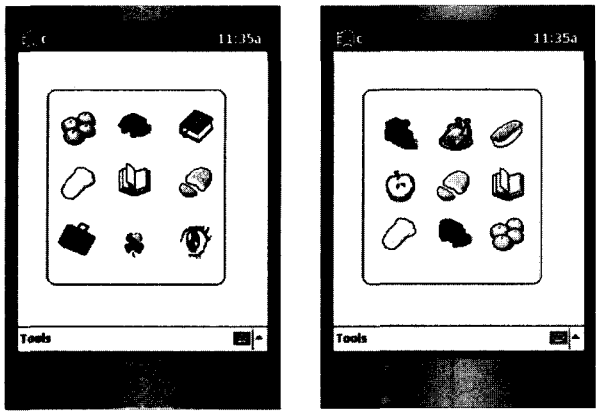
1. 제안된 인증 시스템

가. 이미지를 활용한 패스워드 입력

PDA는 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. 숫자 기반의 패스워드는 짧은 키 길이에 의하여 사용자가 기억하기 쉽고 입력하기 편리하나 짧은 키 길이로 인하여 보안상의 위험이 있고, 문자 기반의 패스워드는 숫자 기반에 비하여 긴 입력 길이로 숫자기반에 비하여 안전한 패스워드 입력 방식이 있다. 하지만 문자 기반의 패스워드 입력 방식은 터치패드 기반의 PDA에서는 입력하기 불편하다. 이에 짧은 입력을 가지면서 강한 보안성을 제공하기 위하여 이미지를 선택하는 것을 통하여 편리하고 짧은 키 길이의 입력을 하고 각각의 이미지 값에 암호화된 Hash Code를 할당하여 입력 정보를 보호함으로써 강력한 보안을 제공한다.

1) 이미지 배열의 생성

이미지를 통한 입력 인터페이스는 입력이 용이하며 사용자는 의미를 갖는 이미지를 기억하므로 사용자의 기억에 의존하는 낮은 엔트로피(entropy)에 대하여 유용하다. 보안을 제공하기 위하여 각각의 이미지에 매핑되는 값을 HASH Code화 하여 클라이언트 모듈에 설치한다. Fig 3과 같이 사용자가 의미를 갖는 이미지를 기억하고 각각의 이미지 값은 HASH Code가 할당되어 있으므로 사용자는 패스워드를 기억하기 쉽고 안전한 인증절차를 할 수 있다.



User A Interface User B Interface

그림 3. 입력 인터페이스
Fig. 3. Input Interface.

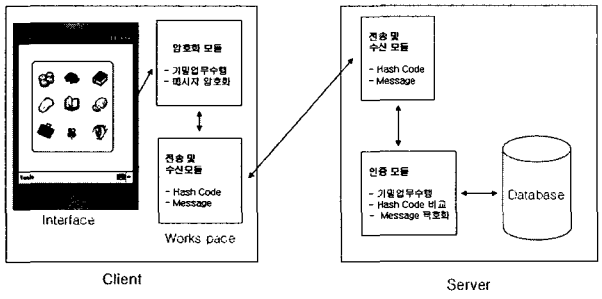


그림 4. 인증 시스템
Fig. 4. Authentication System.

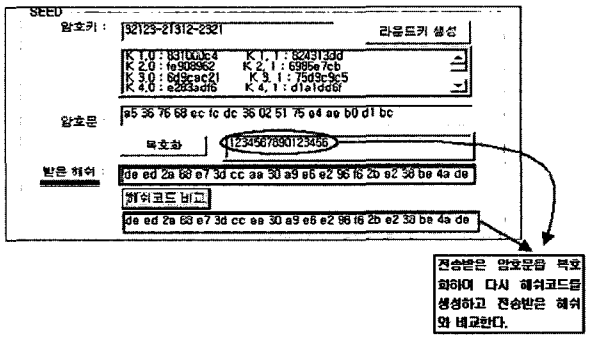


그림 5. Hash Code 비교
Fig. 5. Comparing Hash Code.

나. 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 인증 보를 HASH Code화 하고 지불 정보를 SEED 암호화 알고리즘을 적용하여 암호화하여 전송 메시지의 무결성을 보장하며 효율적이고, DC/LC에 대하여 안전하다. 그리고 128비트를 지원하므로 안전도를 충분히 제공한다.

암호화된 인증 정보를 받아 전송된 메시지를 비교하는 인증 시스템은 Fig 4와 같다.

Fig 5에서는 전송된 HASH Code를 서버에 저장되어 있는 HASH Code 값과 비교하여 일치하면 인증이 올바르게 이루어졌다고 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.

Ⅳ. 결 론

PDA는 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. 숫자 기반의 패스워드는 짧은 키 길이에 의하여 사용자가 기억하기 쉽고 입력하기 편리하나 짧은 키 길이로 인하여 보안상의 위험이 있고, 문자 기반의 패스워드는 숫자 기반에 비하여 긴 입력 길이로 숫자기반에 비하여 안전한 패스워드 입력 방식이 있다. 하지만 문자 기반의 패스워드 입력 방식은 터치패드 기반의 PDA에서는 입력하기 불편하다. 이에 짧은 입력을 가지면서 강한 보안성을 제공하기 위하여 이미지를 선택하는 것을 통하여 편리하고 짧은 키 길이의 입력을 하고 각각의 이미지 값에 암호화된 Hash Code를 할당하여 입력 정보를 보호함으로써 강력한 보안을 제공한다. 또한 SEED 암호화 알고리즘을 적용하여 효율적이고, 전송 메시지의 무결성을 보장하며 내부 참여자에 의한 정보 유출이 있더라도 안전한 전자지불 프로토콜 시스템을 설계 및 구현하였다.

향후 계획으로서는 이미지에 할당되는 Hash Code값을 안전하게 관리하는 관리기법과 사용자 화면에 보이는 이미지를 사용자가 사용할 때마다 다른 배열을 보이기 함으로써 좀더 안전한 클라이언트 모듈에 관한 연구가 필요하다.

참 고 문 헌

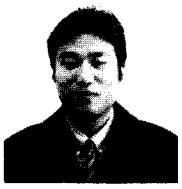
[1] Joshua D. Guttman, "Security Protocol Design via Authentication Tests", Computer Security Foundations Workshop, April 11. 2002.
[2] Amir Herzberg, "Payments and banking with mobile personal devices",
[3] B. Schneier and J. Kelsey, "Unbalanced Feistel

Networks and Block Cipher Design", Fast Soft -ware Encryption, Third International Workshop Proceedings (February 1996), Springer-Verlag, 1996, pp. 121-144.
[4] Geraldine Gray, "Virtual Credit Card Processing System", Principle and Practice of Programming in Java 2002
[5] SET Secure Electronic Transaction Setting the Stage for Safe Internet Shopping an enticing concept. http://www.mastercardintl.com/netechnology/set/
[6] Overview of the SET Protocol, http://www.seas.upenn.edu/~tcom500/commerce /set.htm
[7] Wireless Application Protocol Wireless Transport Layer Security, WAP Forum, 6th of April, 2001.
[8] Wireless Application Protocol Public Key Infra -structure Definition, WAP Forum, 26th of Oct. 2000.
[9] VISA & Mastercard, "SET Electronic Transac -tion Specifiation", 1997.
[10] 임수철, 강상승, 이병래, 김태윤, "무선인터넷에서의 종단 간 보안을 제공하는 신용카드 기반의 지불 프로토콜", 한국정보과학회 논문지 I VOL.29 NO.06 pp. 0645 ~ 0653, 2002. 12.
[11] 양대현, 이석준, "무선 인터넷을 위한 패스워드 기반의 인증 및 키 교환 프로토콜", 한국정보과학회 논문지I VOL.29 NO.03 pp. 0324 ~ 0332, 2002. 06.
[12] 허재형, 신동규, "PDA 상에서의 전자 상거래 보안 솔루션", 정보처리학회 2002년 춘계학술대회 VOL. 09 NO.01 pp. 1349~1352, 2002. 04.
[13]김선형, 김태윤, "제 3세대 이동 통신 시스템을 위한 인증 및 지불 기법", 정보처리학회 2002년 추계학술대회 VOL.09 NO.02 pp. 0000~0000, 2002. 10.

저 자 소 개

신 승 호(정회원)
1979년 경희대학교 전자공학과 (공학사)
1981년 경희대학교 전자공학과 (공학석사)
1985년 경희대학교 전자공학과 (공학박사)
1986년~현재 인천대학교 컴퓨터공학과 교수
<주관심분야: 컴퓨터 통신, 신호처리, 암호학>

강 찬 희(정회원)
1980년 경희대학교 전자공학과 (공학사)
1982년 경희대학교 전자공학과 (공학석사)
1994년 경희대학교 전자공학과 (공학박사)
1989년~현재 상지영서대학교 디지털 정보과 교수
<주관심분야: 영상처리, 컴퓨터 통신, 신호처리>



최 용 식(정회원)
2001년 인천대학교 컴퓨터공학과 (공학사)
2003년 인천대학교 컴퓨터공학과 (공학석사)
<주관심분야: 컴퓨터 통신, 임베디드 시스템, 암호학>