무선 환경에서 전자서명을 이용한 전자영수증 발급시스템

박근홍 박철 조성제 우진운
단국대학교 전산통계학과
{rooty71 pcman sjcho jwwoo}@dankook.ac.kr

A System for Issuing Electronic Receipt based on Digital Signature in Wireless Environment

Keunhong Park Chel Park Seongje Cho Jinwoon Woo
Dept. of Computer Science and Statistics, Dankook University

요 약

최근 휴대폰 보급의 활성화에 따라 무선인터넷 사용 및 무선 환경에서의 전자 상거래가 빠르게 증가하고 있다. 유선 환경상에서와 마찬가지로 무선 환경상에서의 전자상거래 역시 소비자와 판매자가 서로를 신뢰할 수 있는 시스템이나 기법이 필요하다. 무선환경에서의 보안을 위해 WML 전자서명과 WPKI 등 여러 가지 방법들이 활발히 연구중이나 단말기 성능 제한과 WAP 게이트웨이에서 데이터 변환으로 인한 보안문제 등과 같이 현실적으로 많은 문제점을 가지고 있다. 본 논문에서는 보다 높은 신뢰도를 얻을 수 있도록 유선환경과 무선환경을 접목시킨 신뢰성 있는 전자영수증 발급시스템을 제안한다. 본 시스템에서는 전자 서명을 이용한 전자영수증을 발급함으로써 판매자 및 소비자의 신원을 보장하고 판매자의 부인봉쇄효과를 갖는다. 또 무선 단말기의 단점을 보완하고자 신뢰할 수 있는 검증 서버를 설치하여 영수증 검증 및 보관기능을 제공한다.

1. 서론

무선 데이터 서비스, 즉 무선 인터넷에 대한 수요가 급증하고 있는 가운데, 무선 인터넷이 보다 활성화되기 위해서는 유선인터넷에서 제공되는 것과 같은 다양한 응용 서비스들이 개발되어야 한다. 현재 인터넷에서 가장 주목받으며 활발하게 제공되고 있는 서비스는 전자상거래 서비스이며 이동통신 환경에서도 금융, 증권, 경매 등과 같은 전자상거래에 관련된 서비스가 주요 서비스 아이템으로 자리잡아가고 있다. 최근, 이동 전화를 통한 주식 매매 및 은행 거래 등이 확산되면서 고속 데이터 전송에 의한 무선 인터넷이 각광받는 분야로 떠오르기 시작했다. IMT-2000등의 발전을 통해 무선 인터넷은 급격히 발전할 것으로 전망되며 2004년엔 무선 인터넷 이용자가 유선 인터넷 이용자의 수를 뛰어 넘을 것으로 전망된다[1]

그러나 무선인터넷에서 전자상거래를 비롯한 데이터 서비스가 성공적으로 제공되기 위해서는 반드시 해결해야 될 문제가 있는데, 바로 보안 문제이다[2]. 보안 기술은 기존의 유선 인터넷에서도 가장 중요한 기술 요소 가운데 하나로 취급되고 있다. 과거의 이동통신에서는 도청만이 보안문제의 쟁점이었지만 증권이나 인터넷 뱅킹과 같은 단순한 정보 서비스를 뛰어넘는 상거래 활동이 이루어지는 데이터 서비스에서는 사용자 인증, 데이터 무결성 보장 등 해결해야 할 문제가 많다[3].

현재 WAP 포럼에서는 무선 환경에 적합한 보안 프로토콜로서 인터넷 보안 메커니즘인 SSL과 TLS에 기반 하여 작성된 WTLS를 제공한다. 하지만 WTLS는 기밀성, 사용자 인증, 데이터 무결성 등의 보안서비스는 제공되는 반면 효율성에 관한 문제로 인해 전자상거래에 필수적인 부인봉쇄의 기능은 제공하지 않는다[4]. 부인봉쇄기능을 제공하는 대표적인 서비스는 공개키 암호 방식을 이용한 전자서명이다. 전자서명은 자신만의 고유한 암호화키를 이용하여 생성되므로 사용자 인증 및 부인봉쇄의 효과를 갖고 해시 함수를 이용하여 데이터의 무결성을 검증할 수 있다. 그러므로 전자서명을 통한 인증서비스는 전자상거래의 거래 안정성 및 신뢰성 확보에 필수적인 요소이다[5].

무선 보안을 위해 연구중인 WPKI의 경우 단말기 성능 제한으로 인해 암호화와 복호화에 많은 시간이 소요되는 단점이 있으며 WML Script에 의해서 생성된 전자서명은 WAP 게이트웨이를 통과하면서 인터넷에 적합한 형식으로 변환되어야 하기 때문에 보안상에 큰 허점이 생긴다. 그러므로 이동통신에서의 보안은 무선 네트워크 환경에 대한 고려뿐만 아니라 이동통신 단말기 등의 주변기기의 성능도 고려해야 한다. 위의 사항을 고려해 볼 때 단순히 무선 네트워크를 통한 보안은 그 실효성이 없으며 반드시 유선 인터넷과의 연동을 고려해야 한다[3].

본 논문에서는 전자상거래의 활성화를 위해선 필수적인 무선 네트워크 보안에서 이동통신 단말기의 문제점을 보완하기 위해 신뢰할 수 있는 검증서버를 이용한 전자영수증 발급시스템을 제안한다. 전자상거래에서 전자영수증의 역할은 소비자를 보호하고 상거래의 신뢰성을 높이는 데 기여할 것이며 검증서버는 무선 인터넷의 보안상의 약점과 부족한 기기의 성능을 보완하는데 큰 기여를 할 것이다.

2. 관련 연구

2.1 공개키 기반구조

공개키 암호 시스템[4]은 비대칭키 암호 시스템이라고도 불리며, 수학적 함수를 기반으로 하여 비밀키 암호 시스템과 달리 키 쌍이 존재하여 하나의 키는 누구든지 사용할 수 있도록 공개하며 다른 하나는 자신만이 비밀스럽게 보관하는 방식을 입컫는다. 이때 공개하는 키를 공개키(public key)라고 하며 비밀스럽게 보관하는 키를 개인키(private key)라고 한다. 특히, 인터넷과 같은 공개 네트워크상에서 키 관리와 분배의 문제점을 해결할 수 있다. 즉, N명의 사람들과 암호화 통신을 하기 위해서 비밀키 암호 시스템에서는 N(N-1)/2개의 키가 필요하게 되나, 공개키 암호 시스템에서는 각 사용자당 2개씩의 키만 필요하게 되므로 전체적으로 2N개의 키들만이 필요하게 된다.

그러나 키 사이즈가 크다는 단점과 2진수를 10진수로 변환하기 위한 연산시간이 길어서 암호화와 복호화에 많은 시간이 소요되는 단점이 있다. 공개키 암호를 이용한 송신자와 수신자간의 암호 통신 과정은 그림 1과 같다.

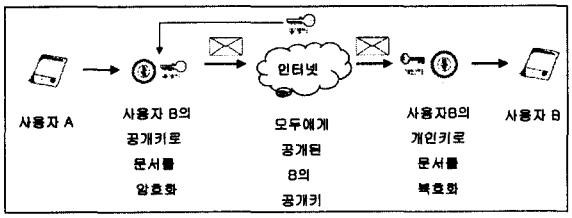

그림 1. 공개키 암호 시스템

2.2 전자서명

공개키 암호 방식에서 응용된 분야로 송신자가 자신의 개인키로 암호화한 암호문을 수신자가 송신자의 공개키로 복호화 함으로써 이루어진다. 송신자 A의 개인키를 아는 사람은 오직 송신자 A뿐임으로 송신자 A의 공개키로 확인되어지는 서명을 한 사람은 오직 송신자 A뿐이다.

전자 서명은 전자화된 문서의 메시지 내용이 수정 및 변조되지 않았음을 보장하는 동시에 메시지의 주체인 사용자들이 진정하다는 것을 제 3자가 확인할 수 있게끔 하는 인증 방식이다. 전자서명을 생성하는 방식은 다음과 같이 분류된다[7].

● RSA(Rivest-Shamir-Adleman) : 1978년에 제안된 공개키 암호 방식의 알고리즘으로 큰 자리 합성수를 소인수 분해하는 것의 어려움을 이용한 방법

● DSA(Digital Signature Algorithm) : DElGamal(이산대수 계산의 어려움을 이용)방식에 기초하는 전자서명 알고리즘으로 DSS(Digital Signature Standard)의 핵심 알고리즘이다.

2.3 해쉬함수

해쉬함수는 다양한 길이의 입력을 고정된 짧은 길이의 출력으로 변환하는 함수로서 전자서명을 생성 시 전체 문서를 암호화하는 것은 어려움이 있으므로 해쉬함수를 이용하여 전체 입력을 고정된 짧은 길이의 출력으로 변환하여 암호화한다[4]. 해쉬함수는 다음의 두 가지가 널리 쓰인다(표 1 참조).

● SHA : SHA(Secure Hash Algorithm)은 미국 표준 FIPS PUB 180으로 공포된 알고리즘으로 MD4 알고리즘에 기반을 두고 있다.

● MD5 : MD5 해쉬 알고리즘은 MD4의 개발자인 미국 MIT 공대의 Ron Rivest에 의해 개발되었다.

표1. MD5와 SHA의 차이점 비교

	MD5	SHA
처리 기본 단위	512 비트	512 비트
해쉬 값	128 비트	160 비트
최대 입력 메시지 크기	무한대	2^{64}
단계 수	64	80
사용되는 비선형 함수 개수	4	3
덧셈 상수 개수	64	4

3. 전자영수증 발급시스템

3.1 시스템 구조

사용자가 무선 쇼핑몰에 접속하여 쇼핑을 한 후 Payment Gateway를 통해 결재를 하면 영수증 발급 시스템에서 영수증을 발급한 뒤 전자서명을 생성한다. 영수증 발급 시스템은 영수증과 전자서명을 검증 서버로 전송한다. 검증 서버는 발급 시스템으로부터 전송된 전자서명과 영수증의 자료 무결성을 검사한 뒤 데이터베이스에 저장함과 동시에 리다이렉션된 무선인터넷 사용자에게 영수증 내역을 전송한다.

사용자가 영수증과 전자 서명을 전송 받기 위해 검증 서버에 유선 인터넷으로 접속하면 영수증 관리 프로그램과 검색된 영수증 내역을 전송 받을 수 있다. 이러한 시스템 구조를 나타내면 그림 2와 같다

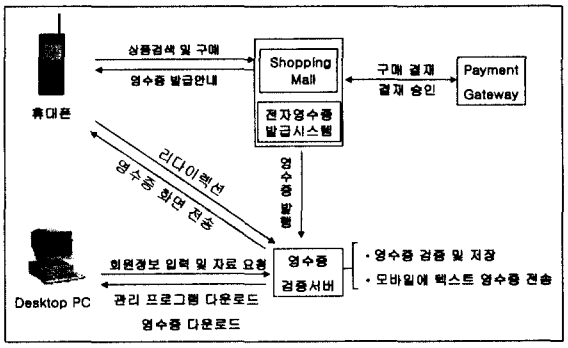

그림 2. 전자영수증 발급 시스템

3.2 전자 영수증

생성된 영수증을 해쉬함수로 축약한 뒤 개인키로 암호화하여 원래의 영수증과 함께 검증서버로 전송한다. 검증서버는 영수증을 수신한 뒤 공개키를 이용하여 전자서명을 복호하고 원래의 영수증을 해쉬함수를 이용하여 축약한다. 복호된 전자서명과 축약된 영수증을 비교하여 자료의 무결성을 검사한다. 영수증이 검증되면 수신한 영수증을 데이터베이스에 저장한다.

본 논문에서는 전자 영수증을 축약하는 알고리즘으로 SHA-1을 사용하였으며 전자 서명 생성 방식으로 DSA방식을 이용하였다.

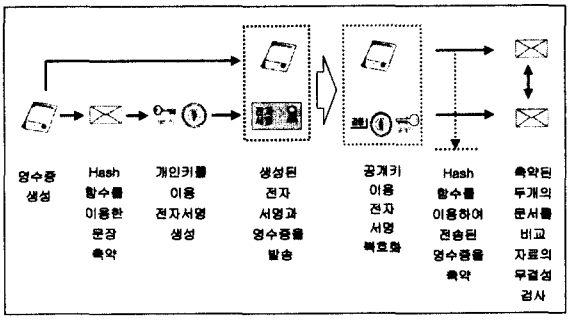

그림 3. 전자영수증과 전자서명의 생성 및 검증 과정

4. 구현 및 결과

본 논문은 Windows 2000 Server환경에서 구현되었으며 웹서버는 IIS 5.0과 Java Servlet엔진인 resin 2.0을 같이 설치하였다. 구현 언어는 WML과 ASP, Java를 사용하였고 데이터베이스는 MS SQL 7.0을 사용하였다.

무선 쇼핑몰은 무선 인터넷 서점을 구현하여 일련의 구매 과정을 수행하도록 하고 영수증 발급시스템은 ASP와 Java Servlet을 이용하여 영수증 및 전자서명을 생성하고 Java Socket을 이용하여 검증서버로 전송하는 역할을 수행한다. 검증서버는 Socket을 통해 전송된 전자 서명과 영수증을 Java Servlet을 이용하여 무결성 검사를 시행하고 자료 검증 결과가 이상이 없을 시 데이터베이스에 저장한다.

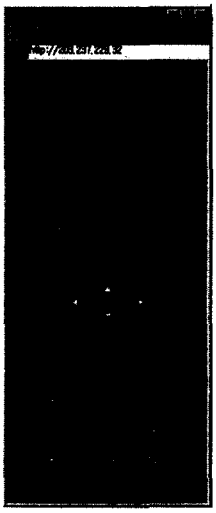

그림 4. 영수증 발급 화면

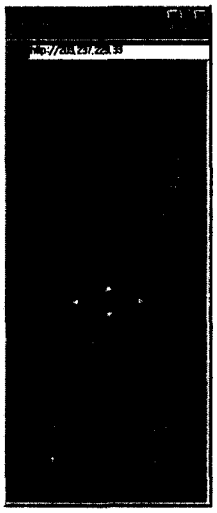

그림 5. 검증서버 확인화면

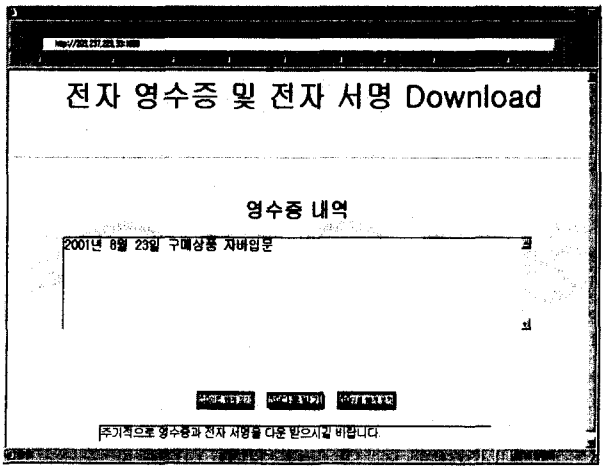

그림 6. 검증서버 다운로드 화면

무선 인터넷 사용자 인터페이스는 Phone.com에서 제공하는 에뮬레이터를 이용하여 구현하였으며 사용자는 유선 인터넷을 이용하여 검증 서버에 접속하여 사용자 인증 후 영수증과 전자 서명을 다운받을 수 있다.

그림 4는 영수증 발급 화면으로 구매 날짜와 상품명, 구매 숫자 등의 구매 정보를 보여준다. 발급 화면으로 가면 전자 서명이 생성되며 검증 서버를 연결하면 검증 서버로 리다이렉션 된다.

그림 5는 쇼핑몰에서 검증서버로 리다이렉션 된 후 검증된 영수증을 핸드폰 상에서 확인하는 화면이다.

그림 6는 검증 서버에 온라인으로 접속하여 영수증과 영수증 관리 프로그램을 다운받는 화면이다. 영수증은 10개 단위로 최근의 것부터 검색 할 수 있다.

5. 결론

현재 무선 인터넷을 이용한 전자상거래가 증가하고 있지만 기기의 성능이나 처리 속도, 효율성 등에 관한 문제로 보안에 관한 부분은 신뢰성을 갖지 못하는 실정이다. 무선 인터넷의 발전에 맞춰 전자 상거래를 보다 활성화하기 위해 여러 가지 보안에 관한 연구들이 활발히 진행되고 있다. 이러한 여러 가지 방법중 소비자의 권익 보호를 통한 전자상거래 활성화를 위해 본 논문에선 전자 영수증과 검증 서버를 제안하였다. 전자 서명을 이용한 전자 영수증은 소비자와 판매자간에 신뢰성을 높이고 거래의 투명성을 부여하게 된다. 또 검증서버를 이용함으로써 무선 인터넷 기기의 저장 공간 부족과 암호화 및 검증속도의 문제점을 보완하여 무선 인터넷 전자 상거래에 유선과 같은 보안을 제공할 수 있다. 이때, 전자 상거래를 위한 검증 서버는 이동통신 제공업자나 국가 인증기관 등의 신뢰할 수 있는 기관으로부터 제공되어야 한다.

참고 문헌

[1] 무선인터넷백서편찬위원회, 무선인터넷백서 2001, 소프트뱅크 미디어, 2000. 9.

[2] Soo Mee Foo 외 3인, Beginning WAP, WML, & WMLScript, Wrox Press Ltd, 2001

[3] Pekka Niskanen, Inside WAP Programming Applications with WML and WML Script, Addison-Wesley, 2000.

[4] 이만영 외 5인, 전자상거래 보안기술, 생능출판사, 1999. 8. 30

[5] Derek Hamner 외 3인, Java Network Programming, Manning Press, 1999

[6] Charles Arehart 외 12인 공저, Professional WAP, Wrox Press Ltd, 2001

[7] Jess Garms and Daniel Somerfield, Professional Java Security, Wrox Press Ltd, 2001, 5