Bluetooth를 이용한 안전한 지불 시스템에 관한 연구

서대희*, 이임영
* 순천향 대학교 정보기술공학부
e-mail : 1636711@hitel.net

A Study on secure payment system applying Bluetooth

Dae-Hee Seo* Im-Yeong Lee
Soonchunhyang Univ. Division of Information Technology Eng.

요약

최근 근거리 무선 통신에 대한 연구가 활발히 진행 되면서 근거리 무선 통신의 규격으로 자리잡고 있는 Bluetooth는 많은 연구가 진행되고 있는 한 분야이다. Bluetooth는 기존 근거리 통신이 가지지 못한 여러 가지 장점들을 가지면서 SIG그룹을 중심으로 많은 연구가 진행중에 있으며 많은 응용분야에 적용하기에 충분한 근거리 무선 통신 기술이다.

따라서 본 논문에서는 Bluetooth 여러 가지 응용 기술중 안전한 지불 시스템을 제안한다. 본 논문에서 제안한 지불 시스템은 사용자를 중심으로 사용자가 승차하고 있는 자동차를 하나의 piconet으로 하여 자동차에서 사용자가 무선 mobile 기기를 이용하여 주유소에서 자동차에 주유를 한 뒤 이를 결제하는 시나리오를 바탕으로 안전한 지불 시스템을 제안하였다.

1. 서 론

동전과 지폐로 대별되던 화폐에 신용카드가 나오면서 화폐의 혁명이 시작되었다. 이른바 플라스틱 머니로 불리며 급속한 확산속도를 보이던 신용카드는 국민 1인당 1장 이상을 소유할 정도로 대중화된 화폐로 자리 잡고 있다. 최근에는 정보통신 및 컴퓨터 기술의 발달로 신용카드, 전자 자금 이체, 인터넷 뱅킹 등 현금대체 결제 수단이 보편화되고 있다.

한편 기술 발전과 인터넷에 대한 이용자의 폭발적인 증가에 힘입어 간단한 메시지 송·수신 단계에 머물던 무선인터넷 서비스는 이제 기업 업무용으로까지 서비스 폭이 넓어지고 있다. 무선 인터넷 시장에서 컨텐츠 유료화에 따른 수익 창출에 대한 기대가 모아지고 있는 가운데 근거리 무선 통신을 이용한 무선 전자상거래(Mobile Commerce)가 이슈로 부각되고 있다[1][4].

이처럼 인터넷 환경에서 유·무선 전자상거래가 활발하게 이루어지고 있지만 지불 수단의 미비로 인해 전자상거래 활성화에 많은 영향을 끼치고 있다. 따라서 근거리 무선 전자상거래에서 안전하고 신뢰할 수 있는 전자화폐 시스템이 필요하다.

따라서 본 논문에서 최근 근거리 무선 통신의 표준으로 자리 잡고 있는 Bluetooth를 이용하여 안전하고 신뢰할 수 있는 지불 시스템을 제안한다.

본 논문의 2장에서는 최근 많은 연구가 진행중에 있는 Bluetooth와 응용 기술에 대하여 살펴본 뒤 3장에서는 근거리 무선 통신 기술인 Bluetooth를 무선 지불 시스템에 적용하기 위한 보안적인 요구사항 및 Bluetooth 보안 서비스에 대해서 논하고자 한다. 4장에서는 Bluetooth를 이용한 전자 지불 시스템에 대하여 제안하고 5장에서는 기존 Bluetooth가 가지는 보안적 취약점을 기반으로 제안 방식을 분석한 후 6장에서는 결론을 맺고자 한다.[1]

2. Technology Review

2.1 Bluetooth 개요

Bluetooth는 1994년 에릭슨의 이동통신그룹이 휴대폰과 주변기기 사이의 소비전력이 낮고, 가격이 싼 무선 인터페이스를 연구하기 시작하면서 비롯하였다. 그 후 에릭슨, 노키아, IBM, 도시바, 인텔, 모토로라, 마이크로소프트, 루슨트 테크놀로지, 3COM 등 9개의 주도그룹인 SIG(Special Interest Group)을 중심으로 현재 2000여개 이상의 기업들이 회원으로 가입된 상태이며, 국내 참여 기업도 70여 곳에 이르고 있는 실정이다.

그리고 Bluetooth 스펙도 99년 1.0을 발표한 이래로 2001년에 2.0을 공개할 예정으로 있었으나 현재까지 미발표된 실정이다. 현재 Bluetooth는 발전하는 단계에 있으며 Bluetooth의 무한한 잠재력을 믿고 국내의 기업 뿐만 아니라, 세계의 우수 기업들이 대거 참가를 하고 있다. 하지만 현재의 Bluetooth는 많은 부분의 보완을 필요로 하고 있다. 기존의 가전기기에 설치하여 사용하기 위해서는 단가를 낮추어야 하고 짧은 전송거리도 늘려야 한다. 또한 간단한 데이터 전송과 음성 전송만을 할 수 있지만, 화상회의 등 고속의 데이터 전송량을 필요로 하는 장소에서 사용하기 위해서 데이터 전송량을 늘릴 수 있는 방법도 개발되어야 한다.

이처럼 현재 Bluetooth는 시작단계에 있는 기술이기 때문에 모든 사람의 욕구를 충족 시킬 수는 없다. 하지만 과거 컴퓨터가 연구소나 공공기관에서만 사용하는 전유물에서 현재 누구나 편리하게 이용할 수 있는 개인 생활용품으로 변모했던 것처럼 Bluetooth도 앞으로 다가올 첨단 멀티미디어 세상에 커다란 영향을 미칠 기술로 기대되어지고 있다[1][2][3].

2.2 전자상거래를 위한 지불 시스템

무선인터넷은 공중망(PSTN) 혹은 인터넷망으로 접속한 후 보안 과정을 거치는 형태로 서비스가 이루어진다. 따라서 유선 인터넷 보다 더 많은 불법 해킹이나 개인정보 유출과 같은 문제가 발생할 수 있는 것이 무선 인터넷이다. 국내에서 사용하는 무선 기술은 보안성 면에서 다소 뛰어난 코드분할다중접속(CDMA)방식을 채택하고 있지만 사용자의 안전한 무선 인터넷 서비스 제공을 위해서는 현재의 보안 서비스보다 보다 안전한 보안 모듈

1) 본 연구는 정보통신부의 ITRC 사업에 의해 수행된 것임.

이나 솔루션이 필요하다.

무선 지불 분야도 무선 인터넷에서 해결해야 할 주요 과제 중 하나다. 디지털 정보뿐 아니라 쇼핑몰 등을 통해 물건을 사고 팔 때 결제 서비스가 제대로 지원되지 못하면 서비스 자체가 힘들기 때문이다. 지불 서비스 역시 기지국과 연동된 별도 지불, 결제 게이트웨이나 시스템을 통해 가능하다. 물론 이를 위해서는 WAP와 같은 무선 프로토콜에 기반한 솔루션 개발이 뒤따라야 한다.

또한 유선과 마찬가지로 사이버 공간에서 사용할 수 있는 전자화폐, 전자지갑 등 각종 사이버 머니도 필요하다.

더욱이 은행이나 신용카드와 같이 금융 기관과 전산망을 서로 맞물려야 하는 시스템 통합 단계를 거쳐야 한다[4].

3. 보안적 요구사항 및 분석

현재의 Bluetooth 기술은 사용자의 중심이 되는 mobile 디바이스간에 이루어지는 무선 통신 서비스이다.

따라서 Bluetooth를 무선 지불 시스템에 적용하기 위해서는 사용자의 프라이버시 보호를 위하여 여러 가지 보안적인 요구사항이 필요할 뿐만 아니라 지불 시스템이 가져야 하는 보안적 요구사항도 필요하게 되며, 이러한 보안적 요구사항은 다음과 같다[5][6].

- 무결성 : Bluetooth를 이용해 지불이 이루어질 경우 지불 정보 데이터에 대한 무결성이 보장되어야 한다. 그러나 Bluetooth 자체 제공 서비스에서는 무결성을 위한 보안 서비스를 제공하지 않는다.
- 기밀성 : 지불 데이터에 대해 기밀성이 보장이 이루어져야 한다. 그러나 Bluetooth 자체 제공 서비스에서 제공하는 기밀성 서비스는 보안 키에 의존하고 있으나 보안 키를 생성하는 PIN 번호에 대한 길이 및 보안 키 분배가 이루어질 때 Man-in-the-middle attack에 대한 위험이 있다.
- 부인봉쇄 : Bluetooth를 이용하여 상호간 지불 사실에 대한 부인을 막을 수 있는 부인 봉쇄가 이루어져야 한다. 현재의 Bluetooth에서는 기기에 대한 인증은 이루어지나, 사용자에 대한 인증은 이루어지지 않는다.
- 상호인증 : 지불이 이루어지는 각 객체들간에 상호인증을 통하여 안전한 지불 관계가 이루어지도록 해야 한다. Bluetooth 기술 내역서에서는 객체들에 대한 인증이 이루어지지 않을 뿐 아니라 단지 조회 과정을 거쳐 Bluetooth 통신이 가능한지에 대한 과정만을 거친다.

4. Bluetooth를 이용한 안전한 지불 시스템

본 제안 방식은 사용자의 mobile 디바이스간에 안전한 정보 교환을 통해 사용자를 중심으로 하나의 piconet이 형성했으며, 사용자는 자신의 자동차에 주유를 위해 주유소와 Bluetooth 통신을 이용해 지불을 하고자 하는 시나리오이다.

본 논문에서 Bluetooth의 piconet을 형성하는 각 객체들은 25시간마다 갱신되는 WPKI 인증서를 가지고 있다. 또한 piconet master와 slave는 사전에 비밀키 K를 공유하였으며 이를 기반으로 그룹 서명값을 이용한 안전한 piconet을 형성하였다고 가정한다.

제안 방식의 구성 객체는 노트북, Mobile Phone, AP(Access Pointer), 은행(Bank)으로 구성된다.

제안 방식의 구성 객체는 다음과 같이 구성된다.

- 노트북 : 사용자를 중심으로 형성된 piconet의 master
- Mobile Phone : 사용자를 중심으로 형성된 piconet을 구성하는 slave로써 Mobile wallet을 포함하고 있다.
- AP : Bluetooth 통신을 위하여 주유소에 설치된 Access Pointer
- 은행 : Bluetooth 통신을 이용한 지불이 이루어질 때 사용자의 Mobile wallet을 발행하고 지불을 처리하는 객체

4.1 시스템 계수

다음은 Bluetooth를 이용한 전자 지불 시스템을 구성하는데 필요한 시스템 계수를 기술한다.

* (노트북 : N, Mobile Phone : H, AP : A, 은행 : B)

p_*, q_* : ECC 암호 알고리즘을 기반으로한 *의 공개키, 비밀키($p \geq 128$비트,[$q = aP$, $P \in E(Z_p)$])

g, η : 모든 객체가 공유한 시스템 계수

h_* : *가 생성한 안전한 해쉬값

r_* : 각 해당 개체의 의사 랜덤수

T_* : *의 타임 스탬프

$H()$: 안전한 해쉬 알고리즘

G : Base Point

R_*, S_* : *가 생성한 ECDSA 서명값

$ID_{infor.}$: *의 정보

EC : 타원곡선 암호 알고리즘

E : 관용 암호 알고리즘

S_j : Bluetooth piconet 그룹키 서명값

TD_* : *의 Transction Data로서 사용일시, 금액에 대한 내용을 포함하고 있는 Data 형식

PI_* : *의 지불 정보 (Payment Information)

$(TD_N \| PI_N)_{res}$: 지불에 관한 영수증 정보

$V@\_\#\$$: $의 키로 암호화 되어 @에서 #로 전송되는 암호화된 값

4.2 프로토콜

4.2.1 초기 설정 단계

사용자가 Bluetooth 지불을 이루기 위하여 초기에 자신을 중심으로 형성된 piconet의 master를 은행에 등록하여 은행과 master간에 세션키를 공유하는 단계이다.

(1) Bluetooth piconet의 master인 노트북은 은행에 VN_Bq_N를 전송한다.

$$Q_N = r_N \times G$$

$$h_N = H(Q_N \| ID_{info_N})$$

$$VN\_Bq_N = EC_{q_N}(Q_N \| ID_{info_N} \| T_N \| h_N)$$

(2) 은행은 piconet master의 공개키 서명을 확인한 뒤 master의 정보인 ID_{info_N}과 Q_N을 저장하고 VN_Bq_B를 master에게 전송한다.

$$Q_B = r_B \times G$$

$$h_B = H(Q_B \| ID_{info_B})$$

$$VB\_Nq_B = EC_{q_B}(Q_B \| ID_{info_B} \| T_B \| h_B)$$

Bluetooth master인 노트북과 은행은 다음과 같은 세션키 χ를 계산하여 비밀스럽게 공유한다.

- 노트북 : $\chi = r_N \times Q_B = r_N \times r_B \times G$
- 은행 : $\chi = r_B \times Q_N = r_B \times r_N \times G$

4.2.2 지불 프로토콜 진행 단계

초기 인증과정을 거친 후 Mobile Phone은 wallet을 기동하고 지불정보 수신대기를 위한 모드로 동작하게 된다. AP는 특정 phone 접속을 위한 지불 내역을 전송하게 된다.

전송된 지불 정보는 Mobile Phone을 통하여 piconet master의 인증과정을 거쳐 은행에게 전송된 후 은행의 승인 과정을 통하여 AP와 piconet master인 노트북에게 지불에 대한 결과를 전송하게 된다. 이상의 프로토콜 과정을 통하여 안전한 Bluetooth 지불이 이루어진다.

(1) 주유소에 설치된 AP는 Mobile Phone에 지불 정보를 요청하며 지불 정보 수신을 위한 대기모드로 전환한다.

$$(ID_{info_A} \| TD_A)$$

(2) 지불 정보를 요청 받은 Mobile Phone은 해당 piconet의 master인 노트북에게 VH_N_K를 전송한다.

$$VH\_N_K = E_K(ID_{info_A} \| TD_A \| T_H \| R_H \| S_H \| S_j)$$

(3) Piconet의 master인 노트북은 전송된 VH_N_K를 사전에 공유된 세션키 K로 복호화 하여 지불 정보와 전송

한 slave의 그룹 서명을 확인한 뒤 VN_H_χ를 Mobile Phone에게 전송한다.

$$VN\_B_\chi = E_\chi(TD_M||PI_M||R_M||S_N||T_N)$$

$$h_N = H(VN\_B_\chi)$$

$$VN\_H_K = E_K(VN\_B_\chi||h_M||R_N||S_N)$$

(4) Mobile Phone는 전송받은 VN_H_K를 세션키 K로 복호화 한 뒤 VN_B_χ를 임시 버퍼에 저장한 뒤 VH_Aq_H를 AP에게 전송한다.

$$VH\_Aq_H = EC_{q_H}(VN\_B_\chi||T_H)$$

(5) AP는 전송된 VH_Aq_H를 Mobile Phone의 공개키로 서명을 확인한 뒤 은행의 공개키로 암호화 하여 VA_SP_B를 은행에 전송한다.

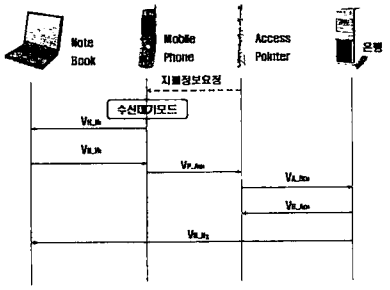
$$VA\_SP_B = EC_{p_B}(VN\_B_\chi||S_A||R_A)$$

(6) 은행은 전송받은 VA_SP_B를 자신의 개인키를 이용하여 복호화 한 뒤 AP의 서명값을 확인하고 VN_B_χ를 초기 설정단계에서 piconet master와 공유했던 세션키 χ를 이용하여 복호화 한 뒤 TD_N, PI_N과 master의 서명값을 확인함으로써 piconet master를 인증한 뒤 TD_N, PI_N를 저장하고 VB_Ap_A를 AP에게, VB_N_χ는 노트북에 전송한다.

$$VB\_N_\chi = E_\chi(R_B||S_B||T_B||(TD_N||PI_N)_{res})$$

$$VB\_Ap_A = EC_{P_A}(VB\_N_\chi||S_B||R_B||T_B||\chi)$$

(8) Access pointer와 piconet master인 노트북은 각각 전송 받은 VB_Ap_A와 VB_N_χ를 복호화 하여 piconet msater와 은행을 인증하며 Access pointer는 $(TD_M||PI_N)_{res}$을 확인하여 이를 저장한다. 이상의 프로토콜의 전체적인 흐름은 그림 1과 같다.



(그림 1) Bluetooth를 이용한 안전한 지불 시스템

5. 제안 방식 고찰

본 논문에서 제안된 지불 프로토콜은 다음과 같은 보안적 특징을 가지고 있다.

- 무결성 : 안전한 해쉬 함수 H와 time stamp T를 이용한 데이터의 무결성을 유지할 수 있다.
- 기밀성 : 공개키 암호 방식을 사용하여 기밀성을 유지하고자 하였으며 계산 능력을 고려하여 타원곡선 암호 알고리즘을 이용한 방식을 이용하였다.
- 부인봉쇄 : 각 객체간의 부인 봉쇄를 위하여 공개키 서명 방식과 ECDSA 방식을 mobile 환경에 적용하여 각 객체간의 부인 봉쇄가 가능하다.
- 상호인증 : 초기 piconet 형성에서의 그룹 키를 이용한 piconet 구성 객체들과의 안전한 상호 인증뿐만 아니라 은행과의 초기 상호 인증 단계을 통하여 안전한 지불 프로토콜이 진행되기 위한 과정을 제안하였다.

6. 결론

본 논문에서는 최근 근거리 무선통신의 표준으로 자리 잡고 있는 Bluetooth를 이용한 여러 가지 응용 방법 중에서 전자상거래에 적극 활용이 가능한 지불 프로토콜을 제안하였다.

현재 무선 환경에서 제공되고 있는 여러 가지 응용 서비스들은 유선에 비해 취약한 보안적 문제점들이 지적하고 있어 실제 전자상거래 환경에 적용하기엔 많은 문제점이 있다.

그러나 본 논문에서 제안하는 지불 프로토콜은 안전성 및 실제 적용이 가능한 프로토콜로서 사용자에게 안전한 무선 전자상거래를 제공하기 위한 하나의 방법으로 활용할 수 있으리라 사료된다. 향후, 본 논문의 고려사항에서 보안적인 요구사항을 좀 더 확대해 안전성과 효율성을 고루 갖춘 지불 프로토콜에 대한 계속적인 연구가 필요할 것이다.

참고문헌

[1]. http://www.bluetooth.or.kr
[2]. http://www.bluetooth.com/developer/specification/specification.asp
[3]. http://www.niksula.cs.hut.fi/~jiitv/bluesec.html (Juha T.Vainio, "Bluetooth Security", jssmd 2000.)
[4]. J.Camenisch, U Maurer, and M. Stadler. "Digital Payment Systems with Passive Anonymity-Revoking Trustees." Computer Security -ESORICS 1996.
[5]. 전자지불시스템 요구사항(한국전산원 번역), StGallen 대학교 경영정보연구소, 1996.
[6]. 장석철, "분할성 및 익명성 제어를 갖는 네트워크형 전자화폐 시스템에 관한 연구", 순천향대학교 석사 학위 논문, 2001.
[7]. 이임영 "전자상거래와 보안 입문", 생능출판사, 2001.
[8]. Alfred J Menezes, Paul C, Oorschot, and Scott A. "HANDBOOK of APPLIED CRYPTOGRAPHY", CRC, 1996.