The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 16, No. 1, pp.1-5, Feb. 29, 2016. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2016.16.1.1
JIIBC 2016-1-1

올인원 서비스에서 자동적인 고객 인증 기법

Automatic Client Authentication Method in All-In-One Services

김남윤*

Namyun Kim*

요 약 최근 신용 카드, 멤버쉽 카드, 쿠폰 등을 모아서 관리할 수 있는 올인원 서비스가 활성화되고 있다. 특히 오프라인 결제와 연계하여 O2O(Online to Offline)의 핵심 서비스로 등장하고 있다. 이러한 기업과의 모바일 상거래를 위해서는 고객의 인증 작업을 거쳐야 하는데, 고객이 기업별로 아이디/패스워드를 저장하거나 입력하는 작업은 매우 번거롭다. 따라서 본 논문에서는 올인원 서비스에서 자동적으로 고객을 인증하는 기법을 제안한다. 회원 등록시 고객은 기업으로부터 인증 티켓을 수신한 후, 단말기에 저장한다. 인증 티켓에는 고객의 아이디와 패스워드가 기업용 대칭 키로 암호화되어 있으며 서비스 요청시 인증 티켓을 전달함으로써 자동적으로 인증 절차가 이루어진다.

Abstract The all-in-one service, for example, mobile wallet enables users to have credit card, membership card, and coupon in one place. It has been one of important o2o services with offline payment. In order to take advantage of mobile commerce, it is necessary to authenticate clients automatically without entering their passwords. This paper proposes an automatic client authentication method in all-in-one service. At registration, clients receives and stores an authentication ticket from a company, which contains an user's identifier and password encrypted by company's symmetric key. Client can be authenticated by transferring authentication tickets to companies at service requests.

Key Words : All-In-One Services, Client Authentication, Authentication Ticket, Symmetric Cryptography

Ⅰ. 서 론

최근 금융과 IT 기술이 결합되는 핀테크 시대를 맞이하여 빅 데이터 등을 활용해 고객에게 맞춤식 혜택 정보를 제공하는 동시에 가맹점과의 상생을 실현할 수 있는 다양한 서비스 및 연구가 진행되고 있다[1,2]. 한 예로서 카드사뿐만 아니라 이동통신사들도 전자 지갑[3]을 통해 신용카드, 멤버쉽 카드, 각종 쿠폰/티켓 등을 모아서 관리할 수 있는 올인원(All-In-One) 서비스를 제공하고 있다. 즉, 복잡한 카드 혜택과 멤버십, 쿠폰 할인 정보를 하나로 모아 오프라인 결제 시 이용자 혜택을 극대화 시켜 주는 서비스라고 할 수 있다. 이와 같이 하나의 모바일 앱에서 다양한 가맹점 서비스를 제공하기 위해서는 몇 가지 보안 요구 사항이 존재한다.

첫째, 사용자들이 가맹점에서의 포인트 점수나 쿠폰 등을 조회하기 위해서 가맹점별로 패스워드나 공인 인증서 비밀번호를 입력하는 불편함이 없이 자동적으로 인증이 이루어질 수 있어야 한다. 가맹점별 패스워드를 따로 기억하기 어려울 뿐만 아니라 모바일 단말기에서 패스워드를 입력하기는 너무 불편하기 때문이다.

*정회원, 한성대학교 정보시스템공학과
접수일자: 2015년 11월 14일, 수정완료: 2016년 1월 7일
게재확정일자: 2016년 2월 5일

Received: 14 November, 2015 / Revised: 7 January, 2016 / Accepted: 5 February, 2016
*Corresponding Author: nykim@hansung.ac.kr
Dept. of Information System Engineering, Hansung University, Korea

둘째, 올인원 서비스를 제공하는 업체가 고객과 가맹점간의 데이터를 파악할 수 없도록 기밀성을 제공하여야 한다. 이러한 데이터는 주로 사용자의 개인 정보이기 때문에 고객과 가맹점을 제외한 제 3의 업체에서는 해독이 불가능하도록 하여야 한다.

셋째, 네트워크를 통한 재생공격(reply attack)[4]에도 안정적으로 동작하도록 설계되어야 한다.

본 논문에서는 이러한 보안 요구 조건을 만족할 수 있는 고객 인증 기법을 제시한다. 고객은 멤버쉽 카드 등을 등록할 때 기업 혹은 가맹점에 인증 티켓을 요청한다. 기업은 고객을 유일하게 식별할 수 있는 정보 예를 들면, 전화번호를 바탕으로 고객의 아이디와 패스워드를 추출한 후, 이를 기업용 대칭키를 통해 암호화하여 인증 티켓(Authentication Ticket)을 생성한다. 이러한 인증 티켓은 고객에게 전달된다. 고객은 기업별 인증 티켓을 저장하는 테이블을 유지하며 기업에 서비스 요청시 인증 티켓을 전달함으로써 자동적으로 인증 절차가 이루어질 수 있다. 즉, 기업은 인증 티켓을 수신한 후, 기업용 대칭키로 해독하여 아이디와 패스워크가 DB에 저장된 값과 일치하면 인증하게 된다.

본 논문의 구성은 다음과 같다. 2절에서는 인증과 관련한 보안 기술을 소개하고 3절에서는 올인원 인증 프로토콜에 대해 기술한다. 마지막으로 4절에서 결론 및 향후 연구 과제에 대해 기술한다.

II. 고객 인증 기술

본 논문에서는 고객과 서버와의 통신 시 웹 보안 기술인 SSL(Secure Sockets Layer)[5]을 기본적으로 가정한다. 본 논문에서는 고객 인증 기술을 대상으로 하며 일반적인 고객 인증 기술은 다음과 같다.

1) 패스워드: 가장 보편화된 인증 방법으로서 사용자만이 인지하고 있는 비밀번호를 통해 인증하는 방법이다. 비록 보안상의 여러 문제가 존재하지만 재발 급이 쉽고 비용이 저렴하기 때문에 널리 사용되는 방법이다. 그러나 올인원 서비스에서 다수의 가맹점마다 비밀번호를 입력하는 것은 불편할 뿐만 아니라 사용자가 기억하기도 어려운 문제가 존재한다.
2) 대칭키(Symmetric Key)에 기반한 인증: 고객과 가맹점간의 대칭키를 공유하고 있다는 가정 하에, 가맹점이 일회용 난수(random number)를 전송했을 때 고객이 난수를 대칭키로 제대로 암호화할 수 있는지를 통해 인증하는 방식이다. 대칭키 암호는 Triple DES[6], AES[7] 암호가 사용될 수 있다. 이 인증 방법은 사전에 고객이 다수의 가맹점과 미리 대칭키를 공유해야 하는 문제가 존재한다.
3) 공개키(Public Key)에 기반한 인증: 고객이 개인키를 알고 있음을 통해 인증하는 방법으로서 가맹점이 일회용 난수를 전송했을 때 고객은 난수를 개인키로 암호화하여 전송한다. 가맹점은 암호화된 난수를 고객의 공개키로 풀어서 일회용 난수가 제대로 나온다면 고객을 인증하게 된다. 대표적인 공개키 암호 알고리즘으로는 RSA[8]가 있다. 이러한 방식은 고객이 모바일 단말기에 공인 인증서와 개인키를 보관해야 하고 인증서 비밀번호를 입력해야 하는 불편함이 존재한다. 모바일 환경에서 매번 비밀번호를 입력하기보다는 자동적이고 투명하게 고객을 인증할 수 있는 프로토콜이 필요하다.

본 논문에서는 미리 대칭키를 공유하지 않고 매번 비밀번호를 입력하지 않으면서도 자동적으로 고객을 인증할 수 있는 프로토콜을 제시한다.

III. 모바일 전자 상거래를 위한 올인원 서비스

1. 올인원 서비스 구조

올인원 서비스란 신용 카드, 멤버쉽 가드, 쿠폰 등을 하나의 모바일 앱에 통합 저장 관리하는 서비스이다. 올인원 서비스를 제공하는 웹 서버, 모바일 앱, 기업 가맹점 서버로 구성되는데, 그림 1은 올인원 서비스의 구성 요소를 보여주고 있다.

그림 1. 올인원 서비스의 구조
Fig. 1. The Service Architecture of All-In-Service

올인원 서비스를 제공하는 웹 서버와 모바일 앱간에는 멤버쉽 관리 서비스를, 모바일 앱과 가맹점 서버간에는 가맹점 서비스를 제공한다. 멤버쉽 관리 서비스는 가맹점에 대한 모든 정보를 바탕으로 해당 멤버쉽을 제공하고 가맹점 서비스는 특정 멤버쉽에 대한 세부 서비스(예: 포인트 조회)를 제공한다. 웹 서버와 모바일 앱, 모바일 앱과 가맹점 서버간의 통신시에는 SSL을 통해 보안 채널을 설정 후, 메시지를 주고 받는다. 올인원 서비스의 세부적인 흐름은 다음과 같다.

1) 모바일 앱은 관심있는 멤버쉽 정보를 요청한다. 예를 들면, 항공사, 패밀리 레스토랑, 주유소 등에 대한 멤버쉽을 요청한다.
2) 웹 서버는 가맹점에 대한 모든 정보를 저장하고 있으며 고객이 요청한 멤버쉽을 검색한 후, 전달한다. 멤버쉽 정보로는 UI, 멤버쉽별 웹 페이지, 가맹점 서버 IP 주소 등을 포함한다.
3) 모바일 앱은 멤버쉽에 대한 인증 티켓이 있는지를 파악한 후, 없을 경우 인증 티켓을 가맹점 서버에 요청한다. 인증 티켓은 개인 신분증 역할을 수행하며 고객 인증에 사용된다. 가맹점 서버는 고객의 전화번호에 해당되는 사용자 정보를 데이터베이스에서 검색한 후, 암호화하여 인증 티켓을 생성한다. 인증 티켓에는 사용자 아이디와 패스워드를 가맹점 대칭키로 암호화함으로써 외부에 노출되지 않는다.
4) 모바일 앱은 포인트 조회, 쿠폰 조회와 같은 서비스 요청시 인증 티켓을 가맹점 서버에 전송함으로써 인증을 받는다. 가맹점 서버는 인증 티켓을 대칭키로 해독한 후, 아이디와 패스워드를 추출한다. 데이터베이스에 저장된 값과 비교하여 인증 테스트를 수행한 후, 해당 서비스를 모바일 앱으로 전송한다.

2. 고객 인증 프로토콜

고객을 인증하기 위해서는 인증 티켓을 요청하는 단계와 인증을 수행하는 단계로 나눌 수 있다. 각 단계에서 HTTPS를 통해 미리 세션 보안을 설정한 후, 메시지를 송수신한다. 그림 2는 고객 인증 프로토콜에서 각 단계에서 송수신되는 메시지를 보여주고 있다.

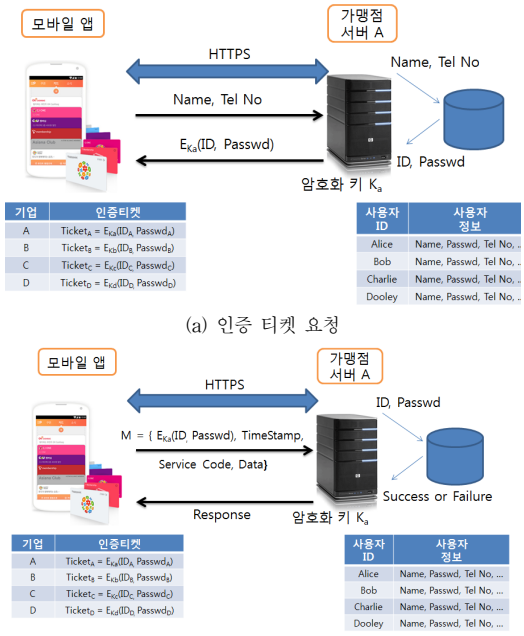

그림 2. 고객 인증 프로토콜
Fig. 2. Client Authentication Protocol

1) 인증 티켓 요청: 모바일 앱은 사용자 이름과 전화번호를 이용하여 가맹점 서버에 인증 티켓을 요청한다. 이 때 가맹점 서버는 DB를 접속하여 사용자 ID와 패스워드를 추출한 후, 가맹점 서버의 대칭 암호화키 K를 사용하여 암호화하여 인증 티켓을 생성한다.

$$\textit{인증 티켓} = E_k(\textit{Client ID, Client Passwd})$$

(E_k 는 가맹점 암호화 키)

모바일 단말기에는 "인증 티켓 테이블"이 저장되어 있으며, 인증 티켓은 가맹점 키로 암호화되어 있기 때문에

가맹점만이 해독할 수 있음에 주목해야한다.

한편, 가맹점은 고객 ID에 해당되는 바코드 이미지를 인증 티켓과 함께 전송할 수 있으며 바코드 이미지는 제품 및 서비스 구매시 포인트 누적을 위해 사용될 수 있다.

2) 고객 인증 및 서비스 요청: 고객이 포인트 조회, 사용 내역 조회시 서비스 요청 메시지를 전송한다. 요청 메시지는 인증 티켓과 서비스 요청 데이터를 포함하고 있다. 고객이 서비스 요청 M 의 구성은 다음과 같다.

M = { 인증 티켓, TimeStamp, Service Code, Service Data }

(TimeStamp는 현재 시각,
Service Code는 포인터 조회,
쿠폰 수신 등 서비스를 구분하는 코드)

가맹점은 서비스 요청 메시지를 수신하였을 때, 인증 티켓을 해독한 후 티켓에 포함된 아이디와 패스워드를 데이베이스에 조회함으로써 인증 절차를 수행한다. 한편, 타임 스탬프는 모바일 단말기의 현재 시각으로 재생 공격 방지용으로 사용된다.

3. 보안성 분석

본 논문에서 제안한 고객 인증 프로토콜의 보안성 분석은 다음과 같다.

1) 고객 인증: 기업은 인증 티켓에 기반하여 고객을 인증한다. 인증 티켓에는 사용자 ID와 패스워드로 구성되어 있고 기업용 대칭키로 암호화되어 있다. 기업마다 상이한 암호화키를 사용하기 때문에 동일한 사용자라고 하더라도 인증 티켓은 서로 다르다. 기업은 인증 티켓 수신시 자신의 대칭키로 해독한 후, 사용자 ID와 패스워드를 비교함으로써 쉽게 인증이 가능하다. 한편, 클라이언트는 인증 티켓을 단말기에 저장하고 있기 때문에 비밀번호 입력같은 명시적인 인증절차 없이 투명하게 인증을 할 수 있는 장점이 있다.
2) 재생공격: 외부 공격자가 서비스 요청 메시지를 저장해 두었다가 나중에 그 메시지를 재생하여 사용할 수 있다. 이러한 방법으로 외부 공격자는 사용자의 인증 티켓없이도 인증 받을 수 있다. 이러한 재생 공격을 방지하기 위해서 서비스 메시지에는 타임스탬프를 사용한다. 가맹점 서버는 일정 시간 범위를 벗어나는 요청은 거부한다. 따라서 공격자가 서비스 요청 메시지를 획득하더라도 재생 공격이 불가하다.
3) 기밀성: 고객과 기업간에는 HTTPS를 이용하여 메시지를 암호화하므로 외부 공격에 안전하다. 한편, 인증 티켓은 올인원 웹 서버의 개입없이 고객과 기업간에만 전송되기 때문에 안전하게 전달될 수 있는 장점이 있다.

4. 기대효과

본 논문에서 제안한 인증 프로토콜은 다음과 같은 기대효과를 가진다.

1) 올인원 서비스에서는 다수의 가맹점에 서비스를 요청할 수 있는데, 제안한 인증 프로토콜은 고객과는 투명하게, 자동적으로 인증되기 때문에 고객의 편의성 증대된다.
2) 고객은 기업별로 따로 유지되는 개인 정보(포인트, 사용 내역)의 통합 관리할 수 있는 장점이 있다.
3) 고객 아이디에 해당되는 바코드를 저장한다면 오픈 라인 결제시 고객 카드를 쉽게 식별이 가능하기 때문에 모바일 커머스 활성화에 이바지할 수 있다.

Ⅳ. 결 론

모바일 단말기의 급속한 보급과 더불어 O2O 서비스에 대한 관심이 급증하고 있다. 본 논문에서는 신용 카드, 멤버쉽 카드, 쿠폰과 같은 정보를 통합하여 관리할 수 있는 올인원 모바일 서비스에서 고객 인증 프로토콜을 제시하였다. 이 프로토콜은 사용자의 명시적 개입없이 투명하게 인증이 이루어지고 재생 공격과 기밀성을 제공하는 장점이 있다. 모바일 커머스의 성장과 더불어 중요한 이슈가 될 것으로 예상된다. 향후에는 모바일 결제와 관련된 보안 이슈를 검토하고 설계할 예정이다.

References

[1] Byung-Rae Cha1, Sang-Hun Lee, Soo-Bong Park, Gun-Ki Lee, and Yoo-Kang, "Prototype Design of Mobile Micro-payment to Enhance Security by 2 Factor Authentication," International Journal of Security and Its Applications, Vol. 9, No. 8 2015.

[2] Jung-Oh Park, Byung-Wook Jin, "A Study on Authentication Method for Secure Payment in Fintech Environment," The Journal of IIBC, Vol. 15, No. 4, 2015.

[3] Susan Pandy, "Current Perspectives on the Mobile Wallet Evolution," Mobile Payments Industry Workgroup (MPIW), April 9-10, 2015.

[4] Sreekanth Malladi, Jim Alves-Foss, Robert B. Heckendorn, "On Preventing Replay Attacks on Security Protocols," Proc. International Conference on Security and Management, 2002.

[5] Mohammed A. Alnatheer, "Secure Socket Layer (SSL) Impact on Web Server Performance," Journal of Advances in Computer Networks, Vol. 2, No. 3, September 2014.

[6] S. Pavithra, Mrs. E. Ramadevi, "Study and Performance Analysis of Cryptography Algorithms," International Journal of Advanced Research in Computer Engineering & Technology, Volume 1, Issue 5, July 2012.

[7] Shanta, Jyoti Vashishtha, "Evaluating the Performance of Symmetric Key Algorithms: AES(Advanced Encryption Standard) and DES(Data Encryption Standard)," International Journal of Computational Engineering & Management, Vol. 15, Issue 4, July 2012.

[8] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," Communications of the ACM, 21:120-126, 1978.

저자 소개

김 남 윤(정회원)

- 1992년 2월 : 서울대학교 컴퓨터공학과 학사
- 1994년 2월 : 서울대학교 컴퓨터공학과 석사
- 2000년 2월 : 서울대학교 컴퓨터공학과 박사
- 1999년 9월 ~ 2002년 2월 : 삼성전자 무선사업부 책임연구원
- 2002년 ~ 현재 : 한성대학교 정보시스템공학과 교수

<주관심분야 : 웹 서비스, 모바일 서비스, 공개 SW>

※ 본 연구는 한성대학교 교내학술연구비 지원과제임