# 온라인 환경의 인터넷 안전결제에서 ISP 생성시 안전한 신원확인을 위한 인증 알고리즘 설계

전영호, 전문석
숭실대학교 컴퓨터학부
e-mail:dean83, mjun@ssu.ac.kr

# A Design of Authentication Algorithm for Safe Identification on Generating ISP in Online Environment Internet Secure Payment System

Young-Ho Jeon, Moon-Seog Jun
Dept of Computer Science, Soong-sil University

요 약

인터넷의 발달로 인하여 다양한 온라인 카드 지불 방식이 생겨나게 되었다. 그 중, 기존의 국민카드와, BC카드의 카드 결제 방식인 ISP(Internet Secure Payment) 시스템에서 ISP를 생성하는 과정이 현재의 인증 방법으로는 잠재적인 취약점이 있음을 발견하고, 이에 본인 인증을 강화하는 프로토콜을 제안한다.

## 1. 서론

인터넷의 발전에 따라 전 세계적으로 전자상거래의 비중이 날로 높아만 가고 있다. 오프라인으로만 살 수 있었던 과거와는 달리, 홈쇼핑, 통신 판매, 인터넷등 다양하면서도 새로운 방법으로 상품을 구입하는 것이 가능해졌다. 그에 따라 지불 수단 역시 어음, 수표, 현금이 위주였던 과거에는 없었던 폰뱅킹, 계좌이체와 카드사용등이 활성화 되었다. 하지만 이중 가장 활성화 된 것은 바로 전 세계적으로 표준화가 되어있는 카드의 사용이다. 국내에서도 이러한 카드의 활성화는 예외가 아니다. 물건을 구입할 수 있는 방법은 여러 가지지만 결재를 하는 과정에서의 카드의 사용은 편리함과 더불어 2010년 상반기 현재 전체 결제 건수의 60%를 웃돌고 있다.

하지만 최근 사고사례에 따르면 특정 카드사의 시스템인 ISP 결재 시스템에서 필요한 ISP를 만드는데에 실물 카드의 정보와 비밀번호 4자리만 있으면 30만 원 이하의 결재가 연속적으로 가능한 점을 악용하여 다양한 사고들이 발생하고 있는 추세이다.

따라서 ISP 생성 시에 카드 정보와 비밀번호만으로 ISP를 만들 수 있는 현재의 발급 프로세스를 잠재적인 위험을 방지하고 보다 안전한 발급을 위한 연구가 필요한 시점이다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구로 커버로스(Kerberos)와 ISP(Internet Secure Payment)에 대해 알아보고 3장에서는 커버로스를 이용한 강화된 ISP 발급 시스템에 대하여 제안하며 4장에서는 결론을 기술한다.

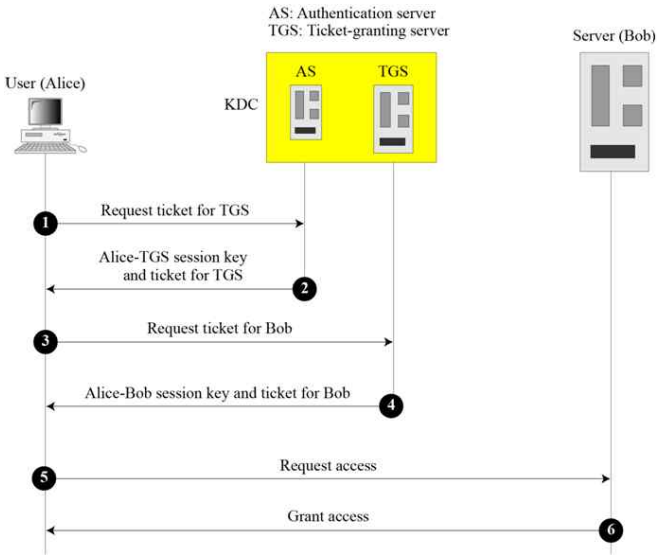
## 2. 관련연구

### 2.1. 커버로스(Kerberos)

커버로스는 인증 프로토콜이며 동시에 KDC(Key Distribution Center)이다. 많은 시스템에서 이 커버로스를 사용하는데, 이 이름은 문을 지키는 그리스 신화의 머리가 셋이 달린 개의 이름에서 따온 것이

다. 초기의 설계는 MIT에서 하였으며 이후 여러 버전으로 업데이트 되었다.[1]

커버로스 프로토콜에서는 3개의 서버를 사용한다. 하나는 인증 서버(Authentication Server)이고, 다른 하나는 티켓-발급 서버(Ticket Granting Server), 그리고 실제로 서비스를 위해 쓰이는 응용서버(Application Server)로 구성 되어 있다.




[그림 1] 커버로스 서버 기본 구성도

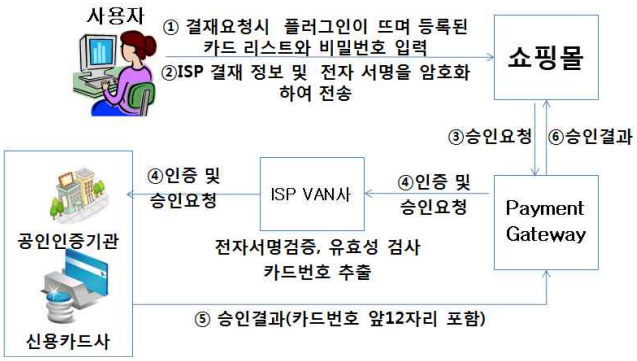
인증서버는 커버로스 프로토콜의 KDC이다. 각 사용자는 인증서버에 등록을 하고 사용자 ID와 패스워드를 발급한다. 인증서버는 사용자의 ID와 대응되는 패스워드에 대한 데이터베이스를 가지고 있다. 사용자를 검증하고 Alice와 티켓-발급 서버 사이에 사용될 세션 키를 발급하고 티켓-발급 서버에게 티켓을 발급한다.

티켓-발급 서버는 실질 서버에게 티켓을 발급해준다. 또한 Alice와 Bob 사이에 사용할 세션 키를 제공한다. 커버로스는 티켓을 발급하는 것과는 별개로 독립된 사용자 검증을 한다. 이렇게 하면 비록 Alice가 자신의 ID를 인증서버와 오직 한 번만 검증하지만 Alice는 티켓-발급 서버에 여러 차례 접속할 수 있으며 서로 다른 여러 실제 서버에 접속할 때 사용할 티켓을 획득할 수 있다.

실질 서버는 사용자에게 서비스를 제공한다. 커버로스는 개인-대-개인 인증용으로는 사용되지 않는다.[2][3]

### 2.2. ISP(Internet Secure Payment)

ISP(Internet Secure Payment)서비스는 모든 거래에 대하여 암호화 통신을 하고, 거래 당사자 확인을 위한 전자인증서의 사용, 전자 결제 지불 대행사(Payment Gateway) 에서의 금융거래정보 저장 및 해독 금지, 금융기관과 PG업체의 접속은 전용회선을 사용하는 등 전자 서명법 및 전자금융 안전 대책 기준 권고사항을 충족하고 있으며 인터넷 안전결제(ISP)인증서 및 전자서명을 통해 보안요건을 충족하고 있다.[4]




[그림 2] 인터넷 안전결재(ISP) 결재 흐름도

(1) 구매자가 상품을 구매후에 KB/BC카드로 결재를 할 경우에 ISP 화면이 나타난다. 이미 등록된 카드 리스트가 나타나며 ISP 비밀번호를 입력하고 결제를 요청한다. 30만 원 이상인 경우에는 공인인증서 창이 뜨고 공인인증서 암호를 입력한다.

(2) ISP 결제 정보 및 전자서명을 암호화 하여 전송한다.

(3) 암호화된 ISP 정보를 PG를 통하여 ISP VAN사에 승인 요청을 한다

(4) ISP VAN사는 전자서명을 검증하고, 인증서에 대한 유효성 검사와 카드 번호를 추출한 후 해당 카드사에 승인요청을 한다.

(5) 카드사가 PG로 승인결과를 전송한다.

(6) PG는 구매처에 승인결과를 보내주고 카드 거래내역 조회 서비스를 위한 카드번호 앞자리 12자리를 보내준다.

(7) 구매처는 구매자에게 지불결과를 보여준다.[5]

## 3. 제안하는 기법

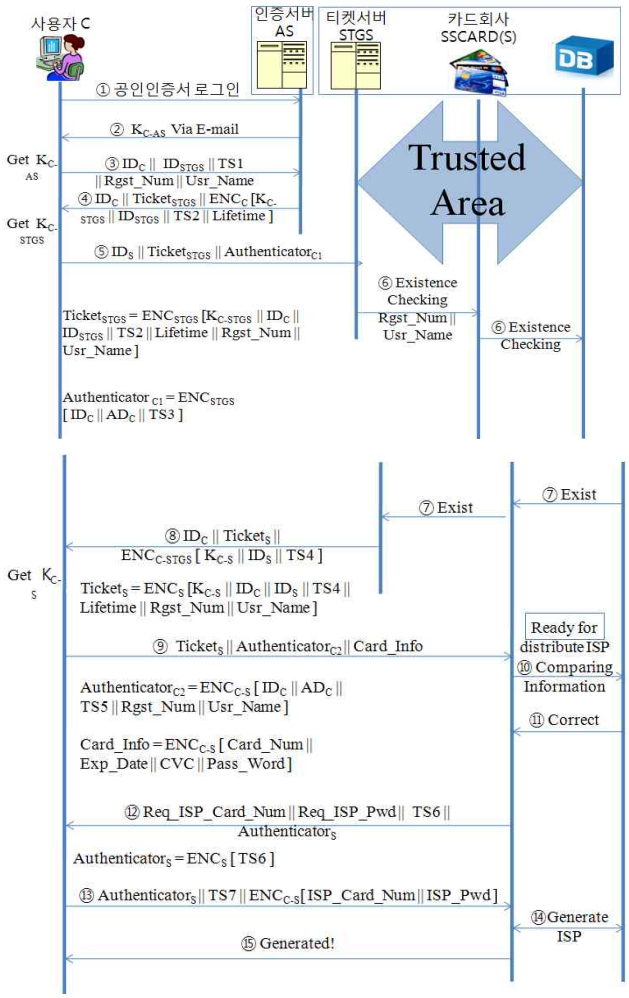
제안하는 기법은 크게 두 가지로 나눌 수 있다. 제

안 시스템 개요와 제안 인증 알고리즘이다.

### 3.1 제안 시스템 개요

실물 카드 정보와 비밀번호 4자리를 알고 있으면 만들 수 있는 현 ISP 생성 프로세스가 잠재적 위험 가능성이 존재한다고 판단되며, 이를 위하여 공인인증서 인증과 이메일을 사용하는 2 channel 인증을 제안하였다. 그리하여 강력한 한 번의 인증으로 여러 카드사의 ISP 생성을 가능하게 하는 싱글 사인온(Single Sign on) 형태의 생성을 제안한다.

### 3.2 제안 인증 알고리즘




[그림 3] 제안하는 시스템의 인증 알고리즘

(1) ISP를 발급하기 위한 가장 첫 단계로 우선 공인인증서를 통한 로그인을 한다.

(2) 그러면 카드 등록 시 기재했던 이메일 주소로 사용자와 AS간의 세션키 $K_{C\text{-}AS}$를 발급과 동시에 주민등록번호와 이름을 받을 수 있는 창을 띄우고 입력을 받는다.

(3) 사용자는 자신의 ID와 거래하고자 하는 TGS의 ID, 타임스탬프 TS1, 주민등록 번호, 자신의 이름을 입력한다.

(4) AS는 사용자로부터 받은 사용자의 ID와 TGS에게 전해줄 티켓, 사용자와 AS의 세션키로 암호화한 사용자와 TGS와의 세션키, TGS의 ID, 타임스탬프 TS2, 유효기간을 보내준다.

(4-1) TGS로 보내질 AS가 발행한 티켓에는 TGS의 공개키로 암호화 된 사용자와 TGS의 세션키, 사용자의 ID, TGS의 ID, 타임스탬프 TG2, 유효기간, 주민등록번호, 사용자 이름이 들어간다.

(5) 사용자는 TGS에게 카드회사의 ID와 AS로부터 받았던 티켓, 그리고 인증자를 보내준다.

(5-1) (5)에서 사용된 인증자는 TGS의 공개키로 암호화 된 사용자의 ID와, 주소, 타임스탬프 TS3을 보내준다.

(6) TGS는 (5)에서 받은 정보로 주민등록번호와 이름을 DB에서 찾아 존재를 확인한다.

(7) 존재를 TGS에 전달한다.

(8) TGS는 사용자에게 사용자의 ID와 카드사에게 전달할 티켓, 사용자와 TGS의 세션키로 암호화된 사용자와 카드회사의 세션키와, 카드회사의 ID, 타임스탬프를 보낸다.

(8-1) (8)에서 보낸 티켓에는 카드회사의 공개키로 암호화 된 사용자와 카드회사의 세션키, 사용자 ID, 회사 ID, 타임스탬프 TS4, 유효기간과, 주민등록번호, 사용자 이름이 있다.

(9) 사용자는 (8)에서 받은 티켓, 인증자2, 카드 정보를 카드회사로 보낸다.

(9-1) (9)의 인증자2에는 사용자와 카드회사의 세션키로 암호화 된 사용자 ID, 주소, 타임스탬프 TS5, 주민등록번호, 사용자 이름이 들어있다.

(9-2) (9)의 카드정보에는 사용자와 카드회사의 세션키로 암호화 된 카드번호, 유효기간, CVC코드, 암호가 들어 있다.

(10) 이를 받은 카드회사는 DB에서 정보를 확인한다.

(11) DB에서 정보가 유효함을 확인한다.

(12) 정보를 확인한 카드회사는 사용자에게 실제로 ISP를 만들 카드의 정보를 요청하고 타임스탬프 TS6과 인증자S를 같이 보낸다.

(12-1) (12)의 인증자S에는 카드회사의 공개키로 암호화한 타임스탬프 TS6이 들어 있다.

(13) 사용자는 (12)에서 받은 인증자와 타임스탬프 TS7, 사용자와 카드회사의 세션키로 암호화된 ISP

카드 번호와, ISP 암호를 보내준다.
(14) 카드회사는 DB에 ISP 생성을 요청한다.
(15) 생성된 결과를 사용자에게 알려준다.

위에서 제안한 인증 기법은 우선 단순 실물 카드와 비밀번호 4자리만으로 ISP 생성을 불가능 하게 만들었고, 강력한 한 번의 인증으로 여러 카드사의 ISP 생성을 가능하게 하였다. 인증 서버를 카드사 외부의 공인된 기관으로 두어 카드사에 요구되는 트래픽을 감소 시켰으며, 기존의 커버로스 시스템과는 달리 카드회사마다 TGS서버를 두어 AS가 해킹 당했을 시에 TGS에서 AS를 거쳐 왔는지의 여부를 판단하게 하여 있을 수 있는 2차 피해 방지도 염두해 두었다.

## 4. 결론 및 향후 계획

인터넷 전자 결재가 활성화 되면서 사용자들은 다양한 방식의 결재를 사용하지만, 국제 표준화가 가장 잘 되어 있는 16자리방식의 카드를 사용한다.
하지만 일부 국내 카드사들이 시행하고 있는 한국형 시스템인 ISP의 생성 과정에 있어서 비교적 간편한 생성 절차에 대한 장점도 물론 존재 하지만, ISP 생성자를 위한 안전성, 보안성 및 악용 가능성은 아직도 해결해야 하는 문제로 남아 있다. 이 뿐만이 아니라, IC카드, 전자지갑, 지문인식 등 여러 가지 방법도 필요 하겠지만, 실질적으로 하드웨어 자원이 많이 필요 하지 않은 강화된 인증 방법을 사용하여 좀 더 안전한 전자거래가 가능해지도록 되어야 할 것이다.
본 논문에서는 ISP 생성과정을 커버로스로 이용한 강력한 인증을 할 수 있는 그런 메커니즘을 제안 하였다.

향후에는 이 시스템을 구현하여 이전의 생성 과정과 비교하여 악용 가능성을 평가해보고, 다른 방식의 강력한 인증에 대해서도 연구할 예정이다..

## 참고문헌

[1] Jason Garman, "Kerberos: the definitive guide", O'Reilly Media, Inc, 2003
[2] Behrouz A. Forouzan, "Cryptography and network security", McGraw Hill, 2007
[3] 김은환, "공개키를 이용한 커버로스 기반의 강력한 인증 메커니즘 설계", 정보보호학회논문지, 제 12권, 제 4호, pp. 67-76, 8월, 2002.
[4] 백은정, "전자지불시스템에서 구매자인증을 위한 ISP / 3D-Secure 프로토콜에 대한 연구", 한국컴퓨터종합학술대회, 제 32권, 제 1호
[5] KVP(Korea Virtual Payment), "인터넷 안전결재 서비스 소개자료", 2003.
[6] Mahesh Kumar Shikarpuri, "Single sign-on: the implementation of single sign-on in enterprise applications", Florida Institute of Technology, 2004