

안전한 전자상거래를 위한 가상카드번호 생성시스템의 개발에 관한 연구

A Study on the Development of a Virtual Card Number Generation System to Safety EC

최준기*, 이종광**, 강영창***

Joon-Kee Choi*, Jong-Kwang Lee** and Young-Chang Kang***

요 약

본 논문에서는 안전한 전자상거래를 위해 가상카드번호 생성시스템에 대한 연구를 진행하였다. 통신망 보안의 필요성이 급격히 증가하고 있는 추세에 맞추어, 전자상거래의 양 및 질적 팽창에 따른 안전한 상거래의 필요성도 더욱 증가하고 있다. 실제카드번호를 네트워크상에 노출시키는 대신 가상카드번호를 생성하여 노출시킴으로써 해킹의 위험을 원천적으로 차단할 수가 있다. 다양한 실험을 통하여 이를 증명하였다.

Abstract

In this paper, we research a virtual card generation system to secure e-commerce. Network security has increased the need to meet rapidly growing trend. And the amount and quality of e-commerce expansion due to the need for secure commerce transactions has increased even more. Instead of exposing the actual credit card number, we expose a virtual card number on the network. It can prevent the risk of hacking. We proved that through various experiments.

Key words : Network security, E-commerce, VCS, Shopping mall, Hacking

I. 서 론

20세기의 ‘플라스틱 혁명’ 또는 ‘제3의 화폐’로 불리는 신용카드 제도는 미국에서 처음 개발된 이후 현금을 대신하는 지불수단으로 여러 나라에서 널리 이용되어 왔다. 우리나라의 신용카드 역사는 짧은 편인데, 1990년 이후부터는 급속하게 증가하고 있다. 앞으로 신용카드 또는 이를 대체할 수 있는 전자지불

수단이 계속 증가할 전망이다[1].

그 이유는 매출의 명확성과 공정한 세금부과를 위하여 국가차원에서의 신용카드 사용 장려정책으로 인한 신용카드 사용이 보편화 되고 있고 특히, 전자지불 시스템 중 신용카드 결제 시스템의 연구가 많이 진행되고 있어, 안전한 수단으로 자리매김하고 있기 때문이다[2][3].

인터넷 상에서 전자 지불 과정 즉, 전자상거래는

* 인덕대학 비서과(Dept. of Secretary & Information, Induk University)

** 에이치기술루션 연구소(Research Center of HG Solution)

*** 가천의과학대학교 정보기술학과(Dept. of Information Technology, Gachon University of Medicine & Science)

· 제1저자 (First Author) : 최준기 · 교신저자(Corresponding Author) : 강영창

· 투고일자 : 2009년 12월 29일

· 심사(수정)일자 : 2009년 12월 30일 (수정일자 : 2010년 2월 8일)

· 게재일자 : 2010년 2월 28일

판매자 서버에 접속한 후 상품 검색 단계, 지불단계, 상품 획득 단계 그리고 판매자와 금융기관 사이의 실제 화폐로 전환하는 단계로 나눌 수 있다[4]. 이 과정에서 정보의 공유와 개방을 목표로 개발된 인터넷이 갖고 있는 근본적인 취약성 때문에 거래내용, 신용카드정보, 은행계좌정보 혹은 비밀번호 등의 중요정보들이 쉽게 노출 될 수 있다[5]. 최근들어 관련 기술들이 발전하고 있지만 온라인 상에서 개인 정보의 노출 위험은 항상 존재하고 있다고 볼 수 있다[6][7][8].

본 논문에서는 이러한 단점을 근본적으로 제거하기 위하여 안전한 전자상거래 시스템의 개발에 대해 연구한다. 즉, 온라인 결제 시에 신용카드 정보의 노출 위험 때문에 실제 카드번호가 아닌 가상카드번호를 노출시킴으로써 카드정보 도용을 원천적으로 차단하고자 한다. 따라서, 가상카드번호를 생성하는 알고리즘에 중점을 두고 전반적인 시스템을 구성한다.

II. 개발 배경 및 목적

온라인 상에서 일반적인 카드 결제 과정을 도식적으로 표현하면 다음 그림 1과 같다.

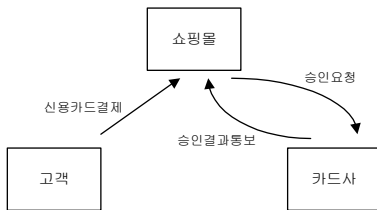


그림 1. 카드 결제 과정
Fig. 1 Process of a Credit Card Approval

고객이 쇼핑몰에서 구매를 위해 신용카드정보를 입력하면 결제가 이루어지고 쇼핑몰에서는 카드사에 신용카드결제에 대한 승인요청을 한다. 마지막으로 카드사는 이를 승인한다. 최근들어 대부분의 쇼핑몰들은 안심클릭과 공인인증서를 통해 결제가 이루어지기 때문에 비교적 안전하다고 할 수 있지만, 해킹 사고의 위험은 항상 존재하고 있다. 그리고, 쇼핑몰 자체의 보안 정책에 따라 고객관리를 하는 경우에는

특히 위험하다고 할 수 있다. 만일 고객의 신용카드 정보가 해킹된다면 이에 대한 피해는 막대할 수 밖에 없다. 이러한 위험을 방지하기 위하여 고객이 쇼핑몰에서 결제하는 과정에서 실제 카드번호를 가상카드번호로 바꾸어 결제가 이루어진다면 이를 효과적으로 방지 할 수 있다. 이를 도식화하면 다음 그림 2와 같다.

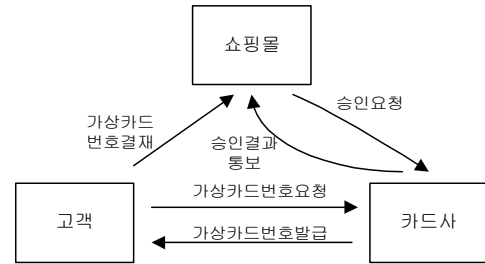


그림 2. 제안한 방법
Fig. 2 A Proposed Method

고객은 쇼핑몰에서 결제하기 전에 카드사로부터 가상카드번호를 발급받는다. 이것을 가지고 쇼핑몰에 가상카드번호로 결제하고, 쇼핑몰은 카드사에 승인을 요청 한다. 그림 2에서 보는것 처럼 실제 카드번호가 노출되는 것을 원천적으로 방지함으로써 네트워크상에서 안전한 거래가 이루어질 수 있다.

III. 안전한 전자상거래를 위한 가상카드번호 생성시스템의 개발

3-1 가상카드번호 생성시스템의 전체 구성도

가상카드번호 시스템(Virtual Card System, VCS)은 고객이 온라인 결제시에 실제 카드번호를 가상카드번호로 변환시켜 쇼핑몰이나 PG(Payment Gateway)사에 가상카드번호를 보냄으로써 실제 카드번호의 노출을 사전에 막는 시스템이다. 이때 인증을 위한 실제 카드번호와 가상카드번호의 매칭데이터는 해당카드사 또는 은행의 서버에만 저장되므로 원천적으로 유출을 차단할 수 있다. 전체 구성도는 그림 3과 같다.

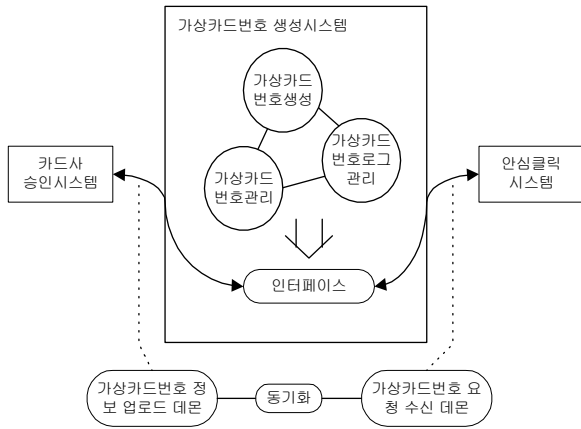


그림 3. 가상카드번호 생성시스템
Fig. 3 Virtual Card Number Generation System

가상카드번호 생성시스템은 최초에 안심클릭시스템으로부터 가상카드번호 생성 요청을 받게되고 이에 따라 가상카드번호를 생성한다. 결제를 위해 카드사 승인시스템으로 이미 생성된 가상카드번호와 실제 카드번호를 함께 전송한다.

3-2 시스템 흐름 및 분석

카드사의 가상카드번호 생성시스템을 중심으로 고객, 쇼핑몰(PG) 그리고 카드사의 결제 과정의 흐름을 그림으로 표현하면 그림 4와 같다.

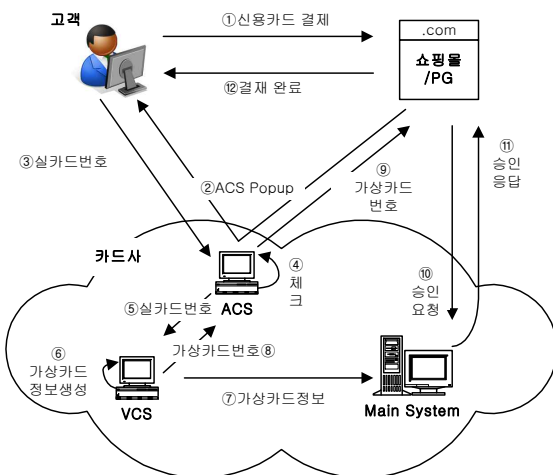


그림 4. 전체 시스템의 흐름
Fig. 4 System Overview

그림에서 원안의 번호는 결제의 흐름을 나타낸다.

그리고, ACS는 카드 결제시에 생성되는 팝업창인 안심클릭창을 생성하는 안심클릭 시스템을 의미한다. 최초 고객이 쇼핑몰이나 PG에서 결제를 하게되면 안심클릭 등의 팝업창이 뜨게 되고 결제과정이 이루어진다. 이 과정에서 카드사내에 있는 가상카드번호 시스템은 가상카드번호를 생성하고 이를 쇼핑몰이나 PG로 전송한다. 이를 가지고 카드사의 메인 시스템으로 승인요청을 한다. 결국 가상카드 번호 정보만이 승인시 필요하기 때문에 해킹 시 실제카드번호를 알 수가 없다.

3-3 가상카드번호의 정의

가상카드번호의 일련번호 16자리를 다음과 같이 정의하였다.

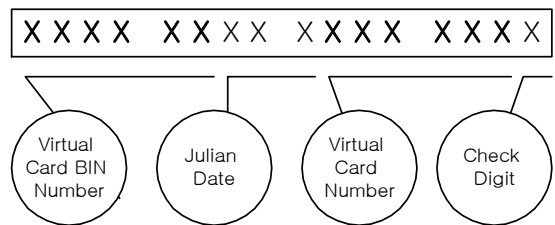


그림 5. 가상카드 번호 구성
Fig. 5 Formation of Virtual Card Number

그림 5에서 가상카드빈(BIN)번호 6자리는 신용카드별 식별 번호로써 이를 가지고 해당카드가 어떤 카드를 구별하는 용도로 사용한다. 따라서 신용카드번호를 가상카드번호로 변환시킬 때, 신용카드 유형에 따른 가상카드번호를 구분할 목적으로 가상카드빈번호를 구성한다. 줄리안데이트는 가상카드번호의 생성일에 대한 정보를 갖는다. 즉, 줄리안 데이트는 가상카드번호 생성 날짜를 의미한다. 가상카드번호는 6개의 디지털(digit)로 구성된 난수이다. 000001~999999 사이에 해당하는 숫자 중 규칙에 의하여 가상카드번호 생성시에 하나를 추출해서 사용한다. 체크디지트는 카드번호가 유효한지를 점검하기 위해 만든다. 15자리의 카드번호를 일정 식에 대입해서 결과가 같아야 유효한 것으로 판단한다.

3-4 가상카드번호 생성 알고리즘

가상카드번호를 생성하는 핵심 알고리즘을 의사 코드(Pseudo Code)로 표현하면 각각 다음과 같다.

1) 가상카드빈번호 생성

```

GET INPUT 실카드번호 FROM 안심클릭
CASE 카드 빈 번호 OF
    0 : "신용카드" -> 가상 빈 번호(신용카드)적용
    1 : "체크카드" -> 가상 빈 번호(체크카드)적용
    2 : "선불카드" -> 가상 빈 번호(선불카드)적용
    6 : "기타" -> 가상 빈 번호(기타)적용
END CASE
SET 가상빈번호 TO 임시변수1
    
```

가상카드빈번호는 안심클릭 시스템으로부터 실카드번호를 넘겨받아 카드종류에 따라 정해진 번호 6 자리를 생성한다. 이는 카드사마다 다르며, 카드의 종류에 따라 다르게 정해놓은 번호를 사용하면된다.

2) 줄리안데이트 생성

```

char* get_julian()
{
//가상카드번호에 포함시킬 julian date 변수 설정
    char julian_date[4];
// julian date 구하기
    strftime(julian_date, 4, "%j", localtime(&now));
    return julian_date;
}
SET 줄리안데이트 함수 실행 TO 임시변수2
    
```

줄리안데이트는 기존의 함수를 활용하며, 가상카드번호의 생성일을 알기 위함이다.

3) 가상카드번호 생성

```

SELECT 시드값, 누적값, 시드값, 시드값카운트, 전체카운트 FROM DB WHERE 빈 번호 별
SET 누적값, 시드값카운트, 전체카운트 TO 1 증가
SET 누적값 + 시드값카운트x시드값 TO 가상번호인덱스
SELECT 가상번호 FROM 가상번호pool WHERE 가상번호인덱스
SET 가상번호 TO 임시변수3
    
```

여기서, 시드값은 임의로 생성한 디지털로 가상번호의 풀(Pool)에서 번호를 뽑아오기 위한 값이다.

4) 체크디지트 생성

```

SET 임시변수1+임시변수2+임시변수3 TO digit[15]
FOR( i=0; i<15; i++)
{
    IF ( i%2 == 0 ) {
        digit[i] = digit[i]*2/10 + digit[i]*2%10;
    }

    digit_sum = digit_sum + digit[i];
}
SET digit_sum TO 임시변수4
    
```

5) 가상카드번호 조합

```

SET 임시변수1+임시변수2+임시변수3+임시변수4 TO 가상카드번호
RETURN 가상카드번호 TO 안심클릭
    
```

이 과정을 통해 가상카드번호를 조합하고 다시 안심클릭시스템으로 생성된 가상카드번호를 전송한다.

결국, 이 알고리즘은 가상카드번호 16자리를 생성하는 과정이며, 각각 가상카드빈번호 6자리, 줄리안데이트 3자리, 가상카드번호 6자리 그리고 체크디지트 1자리를 생성하여 조합하는 과정이다.

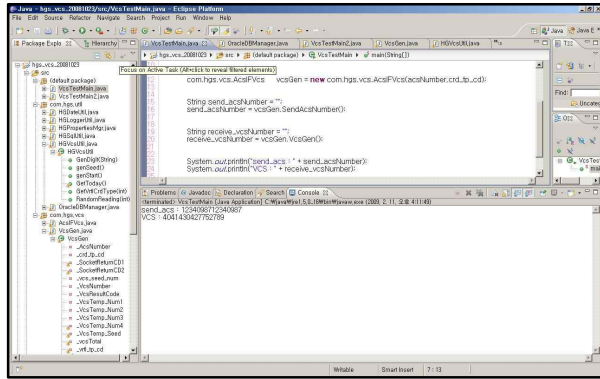
IV. 실험 및 결과

먼저, 개발환경을 표로 요약하면 다음과 같다.

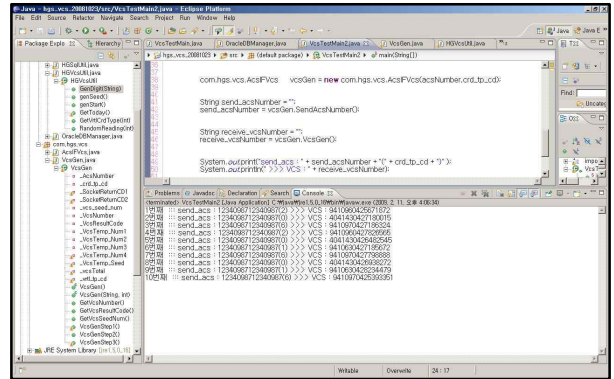
표 1. 개발환경
Table. 1 Development Environment

H/W	S/W
CPU : Intel Core Duo Memory : 2GB	OS : Windows XP DB : Oracle 8i Java : jdk 1.5 Development Tool : Eclipse

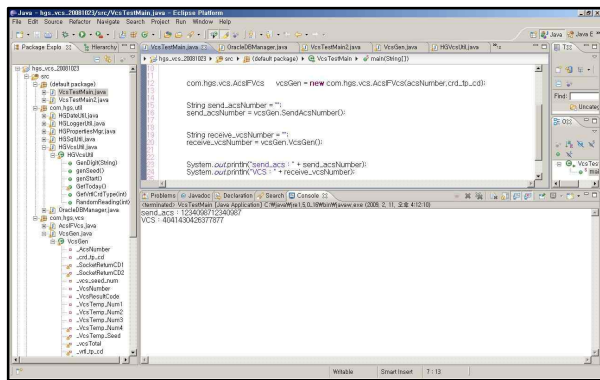
먼저 임의의 실카드번호(1234098712340987)를 기준으로 가상카드번호를 생성하였다. 이것은 실제카드번호 입력 시 가상카드번호가 생성 되는 지를 확인하기 위해서이다. 결과는 그림 6의 (a), (b)와 같다.



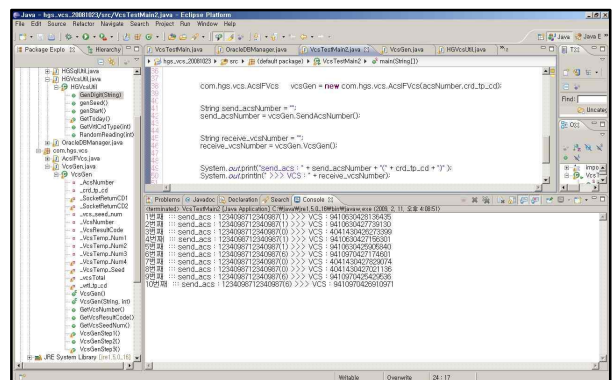
(a)



(a)



(b)



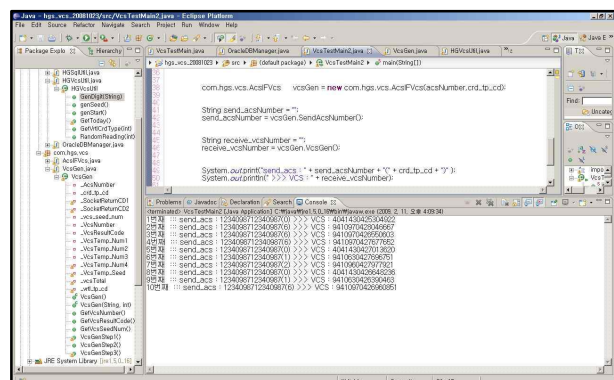
(b)

그림 6. 가상카드번호 생성 결과

Fig. 6 Generated Results of Virtual Card Number

위 그림에서 보여준 결과는 유형코드 즉, 신용카드 유형을 0으로 고정시켜 실험한 결과이다. 따라서, 유형코드 0에 대응되는 가상번호는 404143이므로 생성된 가상카드번호의 빈번호는 404143으로 나타나고, 2월11일 기준 줄리안 데이트는 042 며 따라서 실험을 통한 줄리안 데이트의 디지털트는 모두 042로 나타났다.

다음은 임의의 실제카드번호(1234098712340987)를 가지고 유형코드 즉, 카드유형 값(0,1,2,6)에 따른 가상카드번호를 연속으로 생성하였다. 여기서, 카드 유형 값 0은 신용카드, 1은 체크카드, 2는 선불카드 그리고 6은 기타카드들을 의미한다. 가상카드번호를 동시에 10회 생성하여 그 결과 값이 옹게 생성되었는지를 알아보았다. 결과는 그림 7의 (a), (b), (c)와 같다.



(c)

그림 7. 각 유형에 따른 가상카드번호 생성 결과
Fig. 7 Generated Results of Virtual Card Number by Each Card Type

실험을 통하여 실카드번호에 대응되는 가상카드번호가 생성되었음을 확인하였다. 그리고, 각 카드 유형에 따른 가상카드번호도 생성되고 있음을 확인하였다.

V. 결 론

현재 전자상거래의 규모와 거래금액이 매년 급격히 증가하고 있다. 상대적으로 온라인상에서 이루어지는 범죄의 양도 늘어나고 있는 실정임은 분명하다. 특히, 개인 쇼핑몰 등 개인이 운영하는 전자상거래에서는 문제가 더욱 심각해지고 있다. 본 논문에서는 보다 안전한 전자상거래를 위한 방법을 제안하였다. 네트워크상에 중요한 개인정보인 카드번호가 노출될 위험이 있기 때문에, 가상카드번호로 변환 후 노출시키면 도용의 위험은 전혀 없다.

현 단계에서는 가상카드번호를 생성하는 알고리즘에 초점을 맞추어 연구를 진행하였지만, 향후 전체 시스템 상에서 다양한 각도로 검증단계를 거쳐야 할 것이다.

감사의 글

본 논문은 인덕대학 연구비에 의해 수행되었음.

참 고 문 헌

- [1] 김경자, "신용카드 상담사례를 통해 본 소비자문제의 유형과 개선 방안," *한국가정관리학회지*, 제19권 제1호, pp. 77, 2001.
- [2] 안익수, 황락훈, "신용카드 결제 시스템의 장애 처리에 관한 연구," *컴퓨터정보학회 논문지*, 제11권 제1호, pp. 237-242, 2006.
- [3] 김용수, 백승문, "국내 금융권 재해복구시스템의 문제점 분석," *컴퓨터정보학회 논문지*, 제10권 제2호, pp. 223-229, 2005.
- [4] 이만영외, 전자상거래보안 기술, 생능출판사, pp. 275 - 317, 1999.
- [5] 김용, 이태영, "디지털콘텐츠 유통을 위한 스마트카드기반의 다중인증처리방법설계 및 구현," *정보처리학회지*, 제8권 제5호, pp.23-46, 2002.
- [6] 장재빈, 김건아, 강병훈, 이중정, "금융보안서비스의 채택에 대한 개인사용자의 의식에 관한

요인분석," *한국산업정보학회 추계 공동 국제 학술대회*, pp.91-95, 2008.

- [7] 김민철, 노규성, "전자상거래에 있어서 보안성의 가치추정에 관한 연구 전자상거래에 있어서 보안성의 가치추정에 관한 연구," *정보처리학회 논문지*, *The KIPS transactions*, Part C, v.8 no.5, pp.615-620, 2001.
- [8] 김현우, 이근수, 김세현, "전자상거래를 위한 웹사이트 보안 평가에 관한 연구 전자상거래를 위한 웹사이트 보안 평가에 관한 연구," *한국경영과학회 추계공동학술대회*, pp.340-347, 2005.

최 준 기(崔俊起)



1993년 순천향대학교 전산학과 공학사
1995년 순천향대학교 전산학과 공학석사
1999년 순천향대학교 전산학과 공학박사
1999년 ~ 현재 인덕대학 비서과 부교수
관심분야 : 네트워크 보안, 디지털 워터마킹, RFID

이 종 광(李宗光)



2002년 광운대학교 컴퓨터공학전공
2005년 고려대학교 공학대학원
전자컴퓨터공학전공 공학석사
현)(주)에이치기술루션 연구소 소장 /
인덕대학 겸임교수
관심분야 : E-Payment Ubiquitous

Computing Environment

강 영 창(康永昌)



1980년 광운대학교 전자공학과
1982년 광운대학교 전자통신공학과 공학석사
2001년8월: 순천향대학교 정보통신전공
공학박사
1993년2월~현재 가천의과학대학교 IT
학과 교수

관심분야: 정보보호, Digital Watermark 등