Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.23, NO.6, Dec. 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.6.1007

휴대전화 소액결제 시스템의 구조적 취약점 및 이용자 보호를 위한 표준결제창의 개선방안

박 광 선,[1†] 이 상 진[2†]
[1]서울지방경찰청 사이버범죄수사대, [2]고려대학교 정보보호대학원

A Study on Structural Vulnerability of MobilePhone Micropayment System And Improvement of Standard Payment Module for User Protection

Kwang Sun Park,[1†] Sang-jin Lee[2‡]
[1]Seoul Metropolitan Police Agency,
[2]Center for Information Security Technologies, Korea University

요 약

휴대전화 소액결제 시스템은 자동결제 처리 시 이용자의 점유인증을 관리하지 않는다. 콘텐츠제공사업자가 이점을 악용하면 허위 결제정보를 생성하여 이용자에게 부당한 요금을 부과할 수 있다. 이와 같은 휴대전화 소액결제 시스템의 구조적 취약점은 소액결제 이용자의 피해로 이어졌다. 이를 해결하기 위해 2012. 8. 이후 이용자의 결제 인증 강화를 위한 표준결제창이 적용되었다. 그러나 표준결제창도 부당한 이용자 피해가 발생할 수 있는 취약점이 존재하는 바 이용자 보호를 위한 개선방안을 제안하고자 한다.

ABSTRACT

The automatic payment process of mobile phone micropayment system has not checked user's authentication. That is the structural vulnerability of mobile phone micropayment system. The malicious contents provider can cheat users and payment gateway through abusing the structural vulnerability. The payment gateway applies standard payment module after August, 2012 in order to solve the problem. But the standard payment module also has the vulnerability that makes damage of users. So the purpose of this paper is to suggest efficient improvement of standard payment module for user protection.

Keywords: Mobile Phone Micropayment System, Standard Payment Module, Vulnerability

I. 서 론

휴대전화 소액결제는 온라인에서 콘텐츠를 구매할 때 휴대전화 번호와 주민등록번호를 통해 본인 인증 후 이용 요금을 결제하면 익월 통신 요금에 해당 구매 비용이 청구되는 결제방식이다 [1].

길고 복잡한 카드번호와 계좌번호를 일일이 입력할 필요가 없어 다른 결제 수단에 비해 편리하고, 휴대전화를 사용하는 대부분의 사람이 이용할 수 있어 2000년 7월 상용화 이후 시장 규모가 매년 성장하고 있다 [2].

2013. 3. 방송통신위원회의 발표에 따르면 휴대전화 소액결제의 연간 이용자는 약 1,200만명에 달하며 온라인 콘텐츠 구매, 전자상거래 등 다양한 분야에서 보편적인 결제수단으로 자리 잡았다 [3].

그러나 휴대전화 소액결제의 유용성과 편리성의 이

접수일(2013년 8월 9일), 수정일(2013년 10월 7일), 게재확정일(2013년 10월 23일)
† 주저자, kwangsun@police.go.kr
† 교신저자, sangjin@korea.ac.kr(Corresponding author)

면에는 전화결제로 인한 소비자 피해사례가 지속적으로 발생하여 사회 문제로 부각되었다[1].

그간 휴대전화 소액결제 확산에 수반되는 문제를 해결하기 위하여 관련 기관의 연구와 법 제도개선 노력이 계속되었지만[1][4][5], 이용자 피해를 막는 근본 대책은 될 수 없었다. 그 이유는 휴대전화 소액결제 시스템이 가지고 있는 구조적 취약점에 대한 분석적 접근과 취약점 개선 노력이 미흡했기 때문이다.

본 논문에서는 휴대전화 소액결제 시스템의 처리구조와 구조적 취약점을 짚어보고, 경찰 수사 사례를 통해 악성 콘텐츠제공사업자의 취약점 악용방법을 살펴본다. 또한 최근 휴대전화 소액결제의 이용자 보호 대책으로 떠오른 표준결제창을 검증하여 잠재된 사고 위험과 그 개선방안을 제시하고자 한다.

II. 휴대전화 소액결제 시스템의 개요

휴대전화 소액결제 시스템은 콘텐츠제공사업자, 결제대행사업자, 이동통신사 및 이용자의 상호 작용으로 이루어진다.

콘텐츠 구매 비용 납부방식에 따라 단건결제와 자동결제로 구분할 수 있다.

2.1 단건결제의 시스템 처리구조

단건결제는 온라인 콘텐츠의 구매를 1회 결제로 마무리 하는 결제방식으로, 보통 이용자가 이해하고 있는 휴대전화 소액결제 시스템은 단건결제 방식이다.

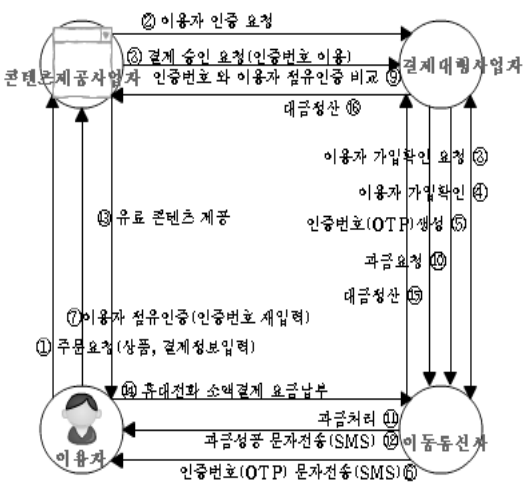

Fig.1. The Service flow chart of a single payment system

① 이용자는 구매할 콘텐츠를 선택하고, 콘텐츠제공사업자의 결제창에 휴대전화번호, 주민번호, 이동통신사 정보(이하 이용자 결제정보)를 입력한다.

② 콘텐츠제공사업자는 이용자 결제정보를 결제대행사업자에게 전송한다.

③ 결제대행사업자는 이용자 결제정보를 이동통신사로 전송하여 이용자의 이동통신사 가입여부 확인을 요청한다.

④ 이동통신사는 이용자의 가입내역을 확인하고 그 결과를 결제대행사업자에게 회신한다.

⑤ 결제대행사업자는 6자리의 인증번호(OTP)를 생성하여 이동통신사에 전달한다.

⑥ 이동통신사는 결제대행사업자가 생성한 인증번호(OTP)를 이용자의 휴대전화에 문자(SMS) 발송한다.

⑦ 이용자는 휴대전화로 수신된 인증번호(OTP)를 콘텐츠제공 사업자의 결제창에 입력함으로써 이용자가 소액결제에 사용하는 휴대전화를 소유하고 있다는 사실을 인증한다. 이를 점유인증이라고 한다.

⑧ 콘텐츠제공사업자는 결제대행사업자에게 이용자 결제정보와 점유인증 번호를 전송하고, 이용자가 주문한 콘텐츠의 결제승인을 요청한다.

⑨ 결제대행사업자는 자신이 생성한 인증번호(OTP)와 사용자가 입력한 인증번호(점유인증)를 비교한다.

⑩ 이용자의 점유인증 확인 후 결제대행사업자는 이동통신사에 과금을 요청한다.

⑪ 이동통신사는 이용자가 구매한 콘텐츠에 대한 과금을 처리한다.

⑫ 이동통신사는 이용자에게 구매한 콘텐츠에 대한 과금이 처리되었음을 문자(SMS)로 통보한다.

⑬ 콘텐츠제공사업자는 이용자에게 이용자가 구매한 유료 콘텐츠를 제공한다.

⑭ 이용자는 익월 이동통신사에 휴대전화 이용요금과 함께 휴대전화 소액결제 이용 요금을 납부한다.

⑮ 이동통신사는 결제대행사업자에게 휴대전화 결제대금을 정산한다.

⑯ 결제대행사업자는 콘텐츠제공사업자에게 결제대금을 정산한다.

2.2 자동결제의 시스템 처리구조

자동결제란 이용자가 인터넷 및 기타 정액 서비스 이용 시 결제에 동의한 경우 매월 또는 일정기간마다 자동으로 결제가 이루어지는 휴대전화 결제방식이다.

사용자 편의를 고려하여 개발되었으나 부정한 요금 청구 등 부작용이 많다.

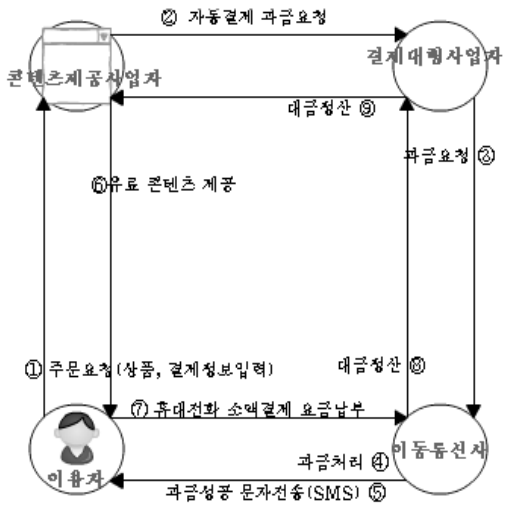

Fig.2. The service flow chart of an automatic payment system

① 이용자는 구매할 서비스를 선택하고, 콘텐츠제공사업자의 결제창에 이용자 결제정보를 입력한다.

② 콘텐츠제공사업자는 결제대행사업자에게 이용자의 결제정보를 전송하여 자동결제 과금을 요청한다.

③ 결제대행사업자는 이동통신사에 자동결제 이용자의 과금을 요청한다.

④ 이동통신사는 이용자 구매 서비스에 대한 자동결제 과금을 처리한다.

⑤ 이동통신사는 이용자에게 구매한 서비스에 대한 과금이 처리되었음을 문자(SMS)로 통보한다.

⑥ 콘텐츠제공사업자는 이용자에게 이용자가 구매한 유료 서비스를 제공한다.

⑦ 이용자는 익월 이동통신사에 휴대전화 이용요금과 함께 휴대전화 소액결제 이용 요금을 납부한다.

⑧ 이동통신사는 결제대행사업자에게 휴대전화 결제대금을 정산한다.

⑨ 결제대행사업자는 콘텐츠제공사업자에게 결제대금을 정산한다.

III. 휴대전화 소액결제의 구조적 취약점

3.1 콘텐츠제공사업자의 결제창 구성 권한

휴대전화 소액결제는 결제창에 결제정보를 입력함으로써 주문을 요청하는 이용자 행위로부터 시작한다. 결제창이란 이용자가 입력한 결제정보를 바탕으로 이용자 인증 및 결제 승인을 요청하는 페이지로, 이용자가 소액결제 시스템과 소통하는 창구로서 중요한 역할을 담당한다.

콘텐츠제공사업자는 결제대행사업자가 제공한 결제모듈을 사용하여 자유롭게 결제 페이지를 구성할 수 있다. 하지만 콘텐츠제공사업자가 결제창 구성 권한을 악용하면 유료 컨텐츠를 판매하는 결제창을 무료회원가입 또는 무료 서비스 제공 페이지로 위장할 수 있다.

때문에, 콘텐츠제공사업자의 결제창 구성 권한은 악성 콘텐츠제공사업자가 이용자를 속일 수 있는 주요 취약점이다.

3.2 자동결제의 점유인증 검증 부재

단건결제 시스템은 이용자가 요청한 결제정보에 대하여 점유인증을 확인함으로써 거래의 진정성을 검증한다.

반면 자동결제 시스템은 콘텐츠제공사업자가 승인을 요청하는 결제정보에 대하여 거래안전을 담보할 인증절차가 없다. 자동결제는 이용자가 피해사실을 인지하지 못할 경우 매월 그 피해가 반복될 수 있다. 이 때문에 자동결제는 단건결제보다 더욱 높은 안전성이 요구되고, 이에 대한 이용자의 기대치 역시 높다.

하지만 결제대행사업자는 콘텐츠제공사업자가 자동결제 승인을 요청하면 점유인증 확인 없이 이용자의 휴대전화 요금에 콘텐츠 이용요금을 부과하였다. 이와 같은 자동결제 처리방법은 이용자의 신뢰에 반한 것으로 휴대전화 소액결제의 구조적 취약점으로 작용하였다.

3.3 휴대전화 소액결제 이용자 피해분석

선행연구를 통해 확인된 휴대전화 소액결제 이용자

의 대표적인 피해유형은 ① 무료라고 표시광고 하였으나 요금이 결제된 경우, ② 무료사용기간 만료 후 자동으로 유료로 전환된 경우가 있다[1][2][4][5]. 이와 같은 이용자 피해의 대부분은 콘텐츠제공사업자의 불법 부당 행위에서 비롯되며, 휴대전화 소액결제의 구조적 취약점에서 원인을 찾을 수 있다.

①의 피해유형은 악성 콘텐츠제공사업자가 결제창 구성 권한을 악용하여 유료서비스를 무료인 것처럼 꾸밈으로써 이용자를 기망한 것이다.

②의 피해유형은 악성 콘텐츠제공사업자가 자동결제의 점유인증 검증 부재를 악용한 것이다. 악성 콘텐츠제공사업자는 무료서비스 제공을 빙자하여 이용자의 개인정보를 수집한다. 그리고 일정 기간이 지나면 이용자의 개인정보를 사용하여 결제정보를 만들고 결제대행사업자에게 자동결제 승인을 요청한다. 결제대행사업자는 자동결제를 처리할 때 이용자의 점유인증을 확인하지 않기 때문에, 악성콘텐츠제공사업자는 이용자 모르게 유료 전환하여 부당한 요금을 부과할 수 있는 것이다.

이처럼 휴대전화 소액결제 시스템의 구조적 취약점은 악성 콘텐츠제공사업자들의 기만적인 영업방법으로 사용됐다.

IV. 사건 사례 분석

2013. 3 서울지방경찰청 사이버범죄수사대는 불법 수집한 개인정보를 이용해 휴대전화 소액결제 대금을 가로챈 성인 모바일 웹 사이트에 대한 수사결과를 발표하였다[6].

이 수사사례를 통해 휴대전화 소액결제 시스템이 지닌 구조적 취약점을 살펴보자.

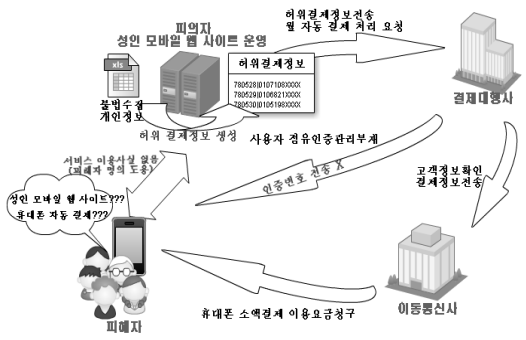

Fig.3. The summary of the accident using the vulnerability of the small amount of money charged on the cell phone system

4.1 사건개요

피의자는 성인 동영상 콘텐츠를 스마트폰으로 제공하는 모바일 웹 사이트를 운영하면서 타인의 개인정보를 불법 취득하여 허위결제정보를 생성하는 형태로 부당한 이익을 편취하였다. 불과 3주간 21,719건의 허위 결제정보를 생성하였고, 피해금액이 215,018,100원 이었다.

4.2 범행수법

4.2.1 결제창 구성권한을 악용한 이용자 기망

피의자는 무료 서비스를 빙자한 결제창을 만들어 이용자를 속였으며, 관련기관의 단속과 피해를 인식한 이용자 항의를 회피할 목적으로 점유인증을 위장하였다.

피의자는 성인 콘텐츠 무료 제공을 빙자하여 이용자의 호기심을 자극함으로써 이름, 주민번호, 휴대전화번호를 입력하게 하였다. 그리고 이용자가 무료입장 버튼을 클릭하였을 때 6자리의 인증번호가 표시된 팝업 페이지를 띄웠다. 정상적인 점유인증은 결제대행사업자가 만든 인증번호(OTP)를 이용자의 휴대전화로 전송하고 이 번호를 이용자에게 확인하는 방법으로 처리된다.

그러나 피의자의 결제창에 표시된 인증번호는 자바스크립트의 RAND 함수로 생성된 무의미한 숫자일 뿐 이용자 인증에 아무런 효과가 없다.


```
if($result != '0') {
        echoScript('alert("본인명의의 핸드폰번호를 입력해주세요.");','exit');
        exit;
} else {
        $certno = rand(111111,999999);

        $msg = "".$_conf['corp']." 인증번호는 [".$certno."]입니다.";
        $sql = "INSERT INTO msgDB.uds_msg (MSG_TYPE, CHID, REQUEST_TIME, SEND_TIME, DEST_PHONE, SEND_PHONE, MSG_BODY)
                VALUES (0, now()+0, now(), now(), '".$member['userid']."', '".$_conf['corptel']."', '".$msg."')";
        sql_query($sql);
```

Fig.4. User fraud with pretence of free entrance and OTP

피의자는 자신이 구성한 결제창에 “이용약관 및 월 자동결제에 동의하면 월 9,900원이 결제됩니다”라는 문구를 표시하였다. 하지만 무료입장에 현혹된 이용자는 이상의 절차를 무료 회원 가입절차로 오인하여 이 ‘월 자동결제 동의’의 의미를 유료 결제로 인식하지 못하였다.

4.2.2 자동결제의 점유인증 검증 부재를 악용한 개인정보도용

피의자는 이용자 점유인증을 확인하지 않는 자동결제 시스템의 구조적 취약점에 주목하였다. 피의자는 불법 취득한 타인의 이름, 주민번호, 휴대전화번호, 통신사 정보 등 개인정보를 도용하여 과금요청을 위한 허위결제정보로 변환하였다. 그리고 이 정보를 결제대행사업자의 결제처리시스템으로 전송함으로써 피해자들이 사용하지 않은 서비스 요금을 부과하여 부당한 이득을 취득하였다.

Fig.5. A generation program of false payment information

다년간의 해킹사고로 수많은 개인정보가 외부로 유출되었다. 이렇게 유출된 개인정보가 휴대전화 소액결제 시스템의 구조적 취약점에 악용되어 막대한 이용자 피해가 발생하였다.

V. 표준결제창의 개요 및 개선방안

5.1 표준결제창의 개요

5.1.1 표준결제창의 도입배경

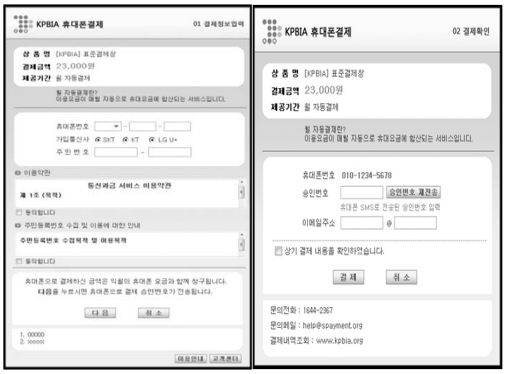

Fig.6. The example of the standard payment screen of mobile small amount of money payment

표준결제창은 결제대행사업자에서 제공하는 웹 방식의 결제 페이지이다.

표준결제창은 2012. 8. 7. 국무회의에서 의결된 전자상거래 등에서의 소비자보호에 관한 법률 시행령 개정안에 따라 전자적 대금 지급 시 그 도입이 의무화 되었다[7].

표준결제창은 이용자에게 ‘결제’에 대한 명확한 인식을 제공하여 콘텐츠제공사업자가 편법적인 방법으로 소비자의 착오나 미인지를 유발할 여지를 제거할 수 있게 한다.

5.1.2 표준결제창의 결제 처리구조

표준결제창은 이용자로 하여금 결제대행사업자가 제공하는 결제창을 사용토록 함으로써 악성 콘텐츠제공사업자의 기망적 영업을 막고 이용자 인증을 강화하였다.

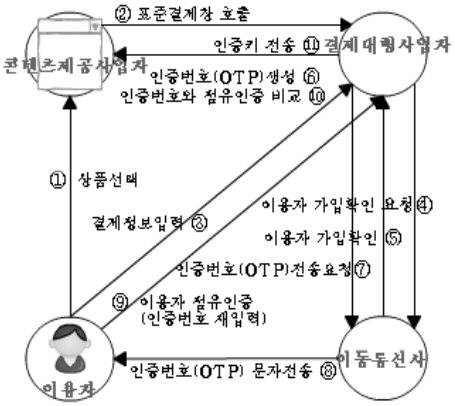

Fig.7. The certification process of a user on the standard payment screen

또한 자동결제처리 과정에 이용자의 점유인증 확인 절차를 확립하였다. 특히 악성 콘텐츠제공사업자가 생성한 허위 결제정보가 이용자와 결제처리시스템을 기망할 수 없도록 개선되었다.

이용자가 표준결제창에 휴대전화번호, 주민번호, 통신사정보 등 결제정보를 입력하고 자동결제를 신청하면 결제처리시스템은 OTP를 사용하여 이용자의 점유인증을 확인한다. 이용자의 점유인증 결과가 정상으로 확인되면 이용자가 신청한 자동결제의 첫 번째 과금 처리를 완료한다.

그리고 이용자의 결제정보를 바탕으로 새로운 인증키를 발급하여 콘텐츠제공사업자에게 전송한다.

이후 콘텐츠제공사업자는 이용자의 결제정보에 인증키를 결합하여 결제처리시스템으로 전송함으로써 이용자의 두 번째 자동결제 과금 처리를 요청 할 수 있다. 이때 결제처리시스템은 콘텐츠제공사업자가 전송한 인증키와 결제대행사업자가 보관중인 인증키를 비교하여 자동결제 이용자의 첫 회 결제 시 점유인증을 검증한다.

이로써, 표준결제창 환경의 결제처리시스템은 악성 콘텐츠제공사업자가 타인의 개인정보를 도용하여 허위 결제정보를 생성하는 행위를 예방할 수 있다.

5.2 표준결제창의 잔존 위험과 개선방안

표준결제창 역시 이용자 피해를 유발할 수 있는 취약점을 가지고 있어 이용자 보호를 위한 개선이 필요하다.

악성 콘텐츠제공사업자는 부정한 과금 처리를 위하여 ① 중복결제와 ②가짜 표준결제창을 사용한 이용자의 결제정보 가로채기를 시도할 수 있다.

5.2.1 표준결제창의 중복결제 취약점

자동결제는 매월 또는 일정기간마다 자동으로 결제가 이루어지는 휴대전화 결제방식으로, 정해진 결제주기에 한 번 결제가 이뤄져야 한다.

하지만, 현재 표준결제창의 결제처리시스템 역시 자동결제 주기 안에 발생한 중복 결제를 탐지하고 차단할 수 있는 예방책이 구현되어 있지 않다.

악성 콘텐츠제공사업자가 자동 결제고객 인증키를 이용하여 자동결제정보를 만들고, 이를 결제처리시스템에 반복 전송하면, 표준결제창 환경의 결제처리시스템은 이를 탐지하지 못하고 이용자에게 중복된 과금을 청구하게 된다. 이러한 표준결제창의 중복결제 취약점은 결국 이용자 피해로 발현될 위험이 크다.

5.2.2 표준결제창의 중복결제 취약점 개선방안

표준결제창의 중복 결제 취약점은 결제대행사업자의 자동결제 유형정의와 부정결제 탐지 절차를 추가하여 개선할 수 있다.

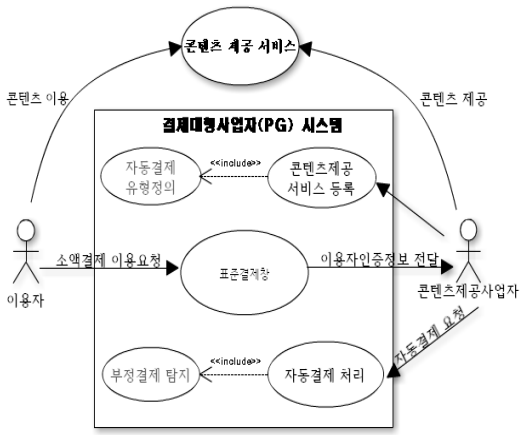

Fig.8. The improvement plan of the vulnerability of duplicated payment on the standard payment screen

콘텐츠제공사업자가 발생시키는 부당한 중복결제를 탐지하려면 결제대행사업자가 자동결제 서비스 별 결제 주기를 정확히 알고 있어야 한다. 그러나 현 시스템에서 결제대행사업자는 콘텐츠제공사업자가 요금 결제를 위탁한 자동결제 서비스에 대하여 결제 주기를 관리하지 않는다.

결제대행사업자는 결제처리시스템에 자동결제 유형정의 절차를 추가하여 콘텐츠제공사업자로 하여금 그들이 이용자에게 제공하는 모든 자동결제 서비스에 결제 주기를 등록하게 해야 한다.

이로써 결제대행사업자는 콘텐츠제공사업자의 자동결제서비스에 대한 결제 주기를 관리할 수 있다.

결제대행사업자는 표준결제창의 중복결제 취약점을 개선하기 위하여 결제처리시스템에 부정결제 탐지절차를 가동할 수 있다.

부정결제 탐지절차는 자동결제 유형정의에서 정의한 자동결제 서비스별 결제 주기에 기반을 둔다.

콘텐츠제공사업자가 결제처리시스템에 이용자의 자동결제 과금 처리를 요청할 때, 결제처리시스템은 현

재 날짜와 해당 이용자의 마지막 결제일의 차이를 확인하고 이를 서비스 결제 주기와 비교한다.

만약 한 달 주기의 자동결제 서비스에 대하여 마지막 결제일 이후 한 달이 지나지 않은 시점에 자동결제 처리가 요청되었다면, 부정결제 탐지절차는 이를 중복결제로 분류하여 결제처리를 보류한다. 처리를 보류한 자동결제정보는 이용자에게 통보하여 결제 승인을 위한 새로운 인증을 받거나, 결제처리를 거절하여 이용자 피해를 예방할 수 있다.

또한 부정결제로 탐지되지 않은 자동결제는 과금처리 후 그 사실을 이용자에게 통지해야 한다. 이미 SMS를 사용한 이용자 통지절차가 마련되어 있으나 이 역시 콘텐츠제공사업자가 통지내용을 구성함으로써 이용자 기망의 한 방법으로 오용할 수 있다. 이제 과금성공 통지 역시 이용자에게 '결제'에 대한 명확한 인식을 제공하기 위해 결제대행사업자 또는 이동통신사 주도의 표준 통지 방법을 개발하고 적용해야 한다.

이처럼 자동결제의 결제주기를 관리하고 부정결제 탐지 절차를 운영하면 표준결제창에 내재된 중복 결제 취약점의 개선이 가능하다.

5.2.3 가짜 표준결제창을 사용한 이용자 결제정보 가로채기

표준결제창은 이용자로 하여금 더 이상 콘텐츠제공사업자가 구성한 결제페이지에 결제정보를 입력하지 않도록 설계되었다.

표준결제창의 결제 처리구조에서 이용자가 구매할 상품을 선택하면, 콘텐츠제공사업자는 결제대행사업자의 표준결제창을 호출하여 이용자에게 제공한다.

하지만, Fig.9.와 같이 악의적인 콘텐츠제공사업자는 결제대행사업자의 표준결제창 대신 표준결제창을 모방한 가짜 결제 페이지를 이용자에게 제공하여 결제정보를 가로챌 수 있다.

콘텐츠제공사업자는 결제대행사업자의 결제시스템에 10만원의 결제요금이 청구되는 서비스를 등록한 후, 표준결제창을 모방한 가짜 결제페이지에 이용요금을 9천원으로 표시하여 이용자를 기망한다. 이용자는 콘텐츠제공사업자의 가짜 결제페이지에 9천원의 결제를 요청하지만, 콘텐츠제공사업자는 이용자가 가짜 표준결제창에 입력한 결제정보를 가로채어 결제대행사업자의 표준결제창에 입력함으로써 10만원의 부당한 결제금액을 청구할 수 있다.

5.2.4 양방향 인증을 통한 표준결제창 개선방안

이와 같은 문제는 이용자와 표준결제창의 양방향 인증을 통해 해결 할 수 있다.

결제대행사업자는 표준결제창에 SSL(Secure Socket Layer)을 적용하여 인증과 전송 메시지의 보호를 담보하고 있지만, 대다수의 이용자는 결제 페이지의 겉모습만으로 그 진정성을 판단한다.

때문에 SSL은 가짜 표준결제창으로 인한 이용자 피해 예방 대책으로 충분하지 않다. 표준결제창의 양방향 인증을 위한 시스템 개선이 필요한 이유이다.

Fig.10.과 같이 결제대행사업자는 표준결제창 생

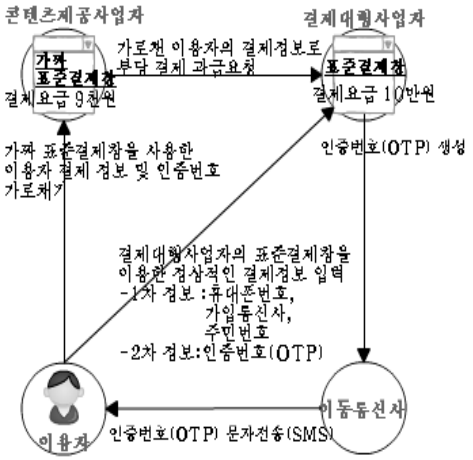

Fig.9. Snatch of a user information using a fake standard payment screen

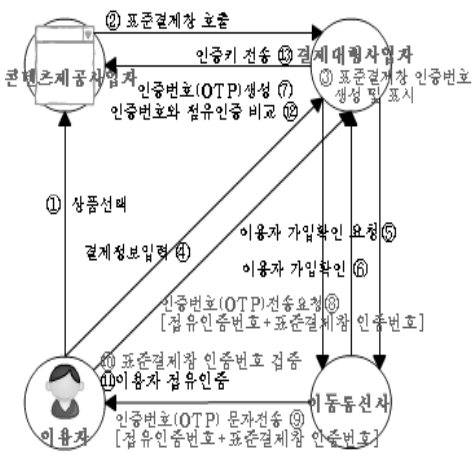

Fig.10. The improvement plan of the standard payment screen through two-way certification

성 시 해당 페이지에 진정성을 입증할 임의의 인증번호(OTP)를 생성한다. 이를 사용자 점유인증을 위한 인증번호와 구분하여 표준결제창 인증번호로 칭한다.

결제대행사업자는 이용자가 표준결제창 인증번호를 확인 할 수 있도록 표준결제창 화면에 표준결제창 인증번호를 표시한다.

그리고, 사용자 점유인증을 위한 인증번호와 함께 표준결제창 인증번호를 이동통신사에 전달하여, 이용자로 하여금 표준결제창 인증번호와 이용자 점유인증을 위한 인증번호를 전송받도록 한다.

이용자는 이동통신사로부터 전달받은 표준결제창 인증번호와 표준결제창 화면에 표시된 인증번호를 비교하여 표준결제창의 진정성을 확인 할 수 있다.

또한, 점유인증을 위한 인증번호 발송 시 표준결제창 인증번호 외에도 이용자에게 과금될 콘텐츠 이용요금을 함께 전달한다면 악성 콘텐츠제공사업자의 이용자 기망을 막고 이용자의 주의를 환기시키는데 도움을 줄 수 있다.

악성 콘텐츠제공사업자가 결제대행사업자의 표준결제창을 모방하더라도, 콘텐츠제공사업자는 결제대행사업자가 생성한 이용자 점유 인증 번호를 알 수 없어 표준결제창 인증번호와 이용자 점유인증 번호를 이용자에게 전송할 수 없으므로, 이상의 방법을 통해 표준결제창의 양방향 인증을 효과적으로 처리할 수 있다.

VI. 결 론

앞서 살펴본 바와 같이 휴대전화 소액결제 시스템의 구조적 취약점은 악성 콘텐츠제공사업자에게 악용되었고 그로 인한 피해는 사용자의 몫으로 전가되었다. 또한, 피해자의 고통과 함께 사고 수습을 위한 관련 기관의 사후 처리는 막대한 사회비용의 지불을 불러왔다.

그간 전화결제 이용자 피해 분석과 대책 마련을 위한 선행연구들은 법 제도 개선을 통한 피해 예방에 집중하였다. 그러나 악성 콘텐츠 제공사업자는 타인명의로 사업을 운영하거나 이용자 기망을 통해 부당 수익을 거둬들이면 사업자를 변경하고 잠적하는 행태를 보이기 때문에 법 제도 개선을 통한 피해 예방의 한계는 명확하다.

이번 연구를 통해 휴대전화 소액결제 시스템의 구조적 취약점과 악용 사례를 확인하였다. 소액결제 피해 예방을 위한 근본대책은 현 시스템이 갖고 있는 구조적인 취약점을 보완하고, 과거의 실수를 교훈삼아 향후 예상되는 위험에 대비하는 것이다.

2012. 8. 이후 이용자의 결제 인증 강화를 위한 표준결제창이 도입되었다. 그러나, 표준결제창 역시 콘텐츠 제공사업자가 부당한 중복 결제를 발생시키고 표준결제창을 모방하여 이용자의 결제정보를 가로챌 수 있는 취약점이 존재한다.

본 논문을 통해 제시한 개선방안을 적용하여 소액결제로 인한 반복된 피해를 예방해야 한다. 안전한 휴대전화 소액결제 시스템을 만들기 위한 관련기관과 결제대행사업자의 노력을 기대해본다.

References

[1] Cho Yong Hyuk, Nam Kwang Woo, Jung Yun Hee, Yoon Doo Young, Kim Sun A, Korea Internet Law Society, Korea Communications Agency And Korea Communications Commision, A study on legal improvement for telecommunication-based payment service, Korea Communications Commission, Nov. 2010.

[2] Kim Boo Hyun, "An Analysis of the Use of Cellular-phone's micro payment - The Actural Condition and its Problems," Master Thesis, Seoul National University, Feb. 2007.

[3] Press release by Korea Communications Commission, "Korea Communications Commission, the announcement for the improvement plans of communication tariff service user protection," Mar 14. 2013.

[4] Advice by Anti-corruption & Civil Rights Commission, "Improvement of the system to prevent small-amount payment victim," May. 2010.

[5] Ryu Suk Il, A Study on Improvement for the Problem of Mobile Phone Micropayment System , Korea Consumer Agency, Sep. 2011.

[6] Press release by Seoul Metropolitan Police Agency, "Exposure of the swindlers of 200 millionKorean won using small-amount of payment through a mo-

bile phone without certification," Mar 18. 2013.
〔7〕 Press release by Fair Trade Commission, "Strengthen of consumers' payment security through compulsory verification of purchase safety service membership," Aug 7. 2012.
〔8〕 Press release by the Ministry of Science, ICT, and Future Planning, "Rapid increase of conflicts about small-amount payment using a mobile phone, such as downloading music and movies in 2012," May 16. 2013.

〈저자소개〉

박 광 선 (Kwang Sun Park) 정회원
1997년 1월~2001년 11월 : 삼성SDS 물산건설IS팀 CERT
2008년 7월~현재: 서울지방경찰청 사이버범죄수사대 수사관
2012년 9월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 사이버범죄수사, 디지털 포렌식

이 상 진 (Sang-jin Lee) 종신회원
1989년 2월~1999년 2월: 한국전자통신연구원 선임 연구원
1999년 2월~2001년 8월: 고려대학교 자연과학대학 조교수
2001년 9월~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 대칭키 암호, 정보은닉이론, 디지털 포렌식