Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.5, Oct. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.5.1189

스미싱 제도와 소액결제 제도의 현황 조사 및 소액결제 피해를 줄이기 위한 법·제도 연구

박 한 진,†‡ 김 인 중
ETRI 부설연구소

A Survey of Regulations on Smishing and Mobile Micropayment and a Research of Regulations and Laws for Reducing Monetary Damages in Mobile Micropayment

Hanjin Park,†‡ Injung Kim
The Affiliated Institute of ETRI

요 약

스마트폰의 보급으로 인하여 문자메세지를 활용하는 스미싱이 급증하고 있으며, 그로 인한 금전적 피해가 크게 증가하고 있다. 본 논문에서는 이러한 피해를 줄이기 위하여, 스미싱 및 스미싱과 관련된 모바일 소액결제에 관련된 제도들의 현황을 살펴본다. 현황 조사 결과 제도적인 노력을 통해서 스미싱 억제는 잘 되고 있지만, 소액결제의 피해는 증가하고 있다는 점을 파악하여 모바일 소액결제 시스템의 보안 강화에 대한 의무 제도의 부재, 소액결제 피해 발생 시 소액결제 참여자(이동통신사, 콘텐츠제공자, 결제대행사) 간 피해보상 주체에 대한 모호성 등과 같은 한계점을 식별하였다. 이러한 한계점을 해결하기 위해서 소액결제 시스템의 보안을 강화하고 의무화 할 수 있도록 소액결제 사업자에 대한 정보보안 평가제도, 소액결제 피해 발생 시 손해배상 책임자에 대한 구체적 명시 제도 및 법안을 제안한다.

ABSTRACT

With the rapid increase in mobile device users, there are many cyber attacks using SMS messages to infect the mobile device. The monetary demage from those attacks are also increasing. Since those demage are generally related to mobile micropayement systems, we study the details of the incidents on smishing and mobile micropayment. We have identified several limitations of current regulations and laws of them. Thus, we propose new regulations and laws to reduce the financial demage from simishing and to strengthen the security and responsibility of the mobile network operator, payment gateway, and content providers who are participating in the structure of a mobile micropayment systems, such as a regulation for information security evaluation system, several laws for compensation of financial demage within mobile micropayement system.

Keywords: Smishing scams, SMS payment system, Regulations and laws on Smishing, Smartphone, Mobile device

Received(06. 26. 2017), Modified(09. 19. 2017), Accepted(10. 06. 2017)

† 주저자, hjpark001@nsr.re.kr
‡ 교신저자, hjpark001@nsr.re.kr (Corresponding author)

I. 서 론

정보통신 기술의 발전으로 인하여 모바일 기기의 보급률이 크게 증가하였다. KT 경제연구소가 발표한 2016년 3월 자료에 따르면 한국의 스마트폰 보급률은 약 91%로 인구 10명 중 9명이 스마트폰을 사용하고 있다고 한다[1]. 이와 함께 모바일 기기를 대상으로 하는 사이버 공격들이 증가하고 있다. 이러한 사이버 공격 방법은 해킹 E-mail 전송, 사설앱 마켓 등록 등 여러 가지가 있으며[1], 이 중에 문자 메시지를 활용하는 원격 공격인 스미싱이 2012년도 이후로 활발히 일어나고 있다[2][2]. 스미싱을 이용하는 해커들의 목적은 주로 정보탈취 또는 금전적 이득에 있다.

스미싱으로 인한 피해가 많이 발생하자 이를 해결하기 위해서 스미싱 문자 탐지앱 개발(예, T가드, 알스미싱가드, 알약 안드로이드 등[7])과 같은 기술적으로 많은 노력이 있어왔다. 이와 동시에 제도 및 법률적(예, 인터넷으로 발신되는 문자 메시지에 웹발신이라는 문구를 포함하도록 하는 제도[8])인 노력들도 있어왔다.

본 논문에서는 현 스미싱 제도에 대한 현황과 함께 스미싱의 금전적 피해와 관련이 있는 소액결제 관련 현황을 살펴본다. 스미싱 관련 사이버 사고를 해결하기 위한 기술적, 법률적, 제도적인 노력으로 스미싱 탐지 건수가 감소함(스미싱 건수 2014년 4천917건에서 2015년 1천120건으로 피해건수가 대폭 감소 [9])에도 불구하고 같은 기간 스미싱 사고로 인한 피해금액이 증가(스미싱 피해금액 2014년 3억4천만 원에서 17억 4천만 원으로 5배 이상 증가[9])하고 있는 문제점을 파악하고 이를 해결하기 위한 해결방안을 제시한다.

이러한 문제점의 원인으로 소액결제 시스템의 보안 의무화 제도의 부재 및 모바일 소액결제 피해 발생 시 손해배상 책임 주체의 모호함을 꼽을 수 있다. 관련하여 2016년 12월~2017년 2월까지 걸쳐서 발생한 쿠팡-LG U+의 스미싱 사고 사례를 중심으로 살펴보았다. 이 사고는 이통통신사(LG U+), 홈페이지의 취약점 존재 및 콘텐츠제공사(쿠팡) 홈페이지의 환불 절차상 현금화 가능 취약점 등에 의하여 발생하였다.

따라서 본 논문에서는 스미싱으로 인한 소액결제 피해를 막기 위해 소액결제지불구조 상 취약점을 보안할 수 있는 새로운 제도 및 법을 제안한다. 제안하는 제도는 소액결제 지불구조를 고려하여 통신과금서비스제공자(이동통신사, 결제대행사) 및 콘텐츠제공자들에게 스미싱으로 인한 소액결제 피해 사고 예방 및 피해발생 시 손해배상 책임을 구체화하는 법안과 제도를 제안한다. 소액결제 구조의 보안을 강화하여 스미싱으로 인한 금전적 피해를 최소화하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 스미싱 및 소액결제와 관련된 배경지식을 살펴보고, 3장에서는 최근 스미싱 탐지 건수를 바탕으로 스미싱 및 소액결제 관련 제도의 현황을 살펴본다. 4장에서는 스미싱 및 소액결제 관련 제도에 대한 한계점을 살펴보고 5장에서는 이러한 한계점을 해결할 수 있는 방법을 제안한다. 제안하는 방안은 크게 사업자 간 시스템의 보안성을 강화할 수 있는 제도와 소액결제 피해 발생 시 피해자 혹은 사업자 간 책임을 명확히 하는 제도 및 법안으로 구성된다. 그리고 마지막으로 6장에서는 결론을 제시한다.

II. 배경지식

2.1 스미싱

스미싱은 문자 메시지(SMS)와 Phising의 합성어로 문자 메시지를 활용한 사이버 사기 중 하나이다[10].

스미싱 문자 메시지는 스미싱 문구와 악성앱이 다운될 수 있는 URL로 구성되어 있다. 스미싱 문구는 주로 사회공학적인 방법을 활용하여 작성되며, 대표유형으로 무료쿠폰을 나눠주는 쿠폰형, 청첩장으로 대표되는 관혼상제형, 불안감 조성형, 택배 사칭형, 호기심 유도형 등이 있다[11]. 스미싱 과정은 다음과 같다. ① 해커가 피해자에게 악성앱(코드) 설치 URL이 담긴 문자 메시지를 전송한다. ② 피해자가

1) 스마트폰을 원격에서 해킹하는 방법에는 무선 통신 기술(3G, LTE, Wi-Fi)을 이용한 해킹, 인터넷에 악성 웹사이트 구축 후 접속 시 공격하는 Drive by Download 해킹, 사회공학적인 방법 해킹(예, 해킹 E-mail, 문자 메시지) 등 다양한 방법이 있을 수 있다. 본 논문에서는 문자 메시지를 이용하여 악성앱에 감염시키는 스미싱에 대해서만 주로 다루도록 한다.

2) 2014년 스미싱 악성코드 10,777개 발견, 이는 2013년 5,206개 대비 약 2배, 2012년 29개 대비 371배 증가한 수치[3]. 2014년 초 개인정보 유출사고(2014년 1월 KB국민카드, 롯데카드, NH 농협카드 약 2,000만 건)[4], 같은 해 3월 KT 1,200만 건[5], SKT, LG U+등 약 1,230만 건 유출)로 스미싱이 급증하였다[6].

(부주의하게) URL 클릭하여 악성앱 다운로드한다. ③ 피해자가 다운로드한 악성앱을 (부주의하게) 설치하여 스마트폰 감염된다. 스마트폰이 감염되고 나서는 해커는 자신이 원하는 바를 마음대로 수행할 수 있게 된다. 해커들의 대표적인 목적은 스마트폰의 정보 탈취[3] 또는 소액결제를 통한 금전적 이득 취득 등이 될 수 있다. 본 논문에서는 금전적 이득을 목적으로 하는 경우를 주로 다룬다. 금전적 이득을 목적으로 하는 경우에는 스미싱 공격을 활용하여 피해자 스마트폰을 감염시킨 후 모바일 소액결제를 활용하는 수법이 널리 사용된다[14].

2.2 스미싱과 모바일 소액결제

해커는 스미싱을 통해서 피해자의 단말을 감염시키고, 미리 탈취한 피해자의 개인정보를 바탕으로 피해자를 사칭하여 콘텐츠제공자에게 소액결제를 요청한다. 관련 절차는 다음과 같다(Fig. 1. 참고).

① 해커가 피해자를 사칭하여 문자 메시지를 이용한 소액결제를 선택하면 ② 콘텐츠제공자(Content Provider, CP)는 결제대행사(Payment Gateway, PG)에게 결제요청을 하고 ③ 결제대행사는 이동통신사(Mobile Network Operator, MNO)에게 인증번호를 생성하여 보내준다. ④ 이동통신사는 사용자에게 인증번호를 문자 메시지의 형태로 보내준다. ⑤ 해커가 피해자의 문자 메시지를 가로채어 인증문자의 번호를 콘텐츠제공자에게 입력 전송한다. ⑥ 인증문자 확인이 되면 콘텐츠제공자는 해커에게 콘텐츠를 제공해주며 ⑦ 요금은 피해자에게 이동통신사의 통신요금으로 추가되어 청구된다. ⑧ 이동통신사는 결제대행업체에게 결제요금정산을 하고 ⑨ 결제대행업체가 다시 콘텐츠제공자에게 결제요금을 정산한다. 마지막으로 해커는 다양한 경로를 통해서 획득한 콘텐츠를 현금화를 통해 금전적 이득을 얻는다.

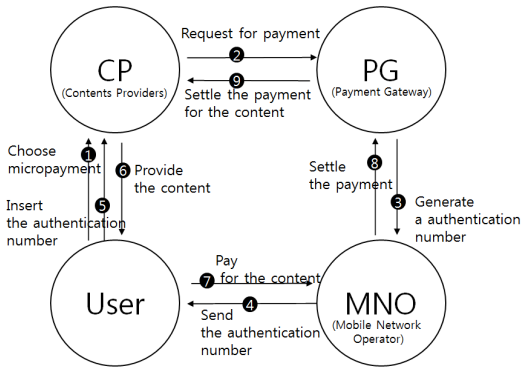

Fig. 1. A process of SMS payment using SMS message verification

3) 대표적인 사례로서 2015년 3월 17일 청와대 교육문화수석 스마트폰이 스미싱 당한 사례[12], 2016년 3월 8일 외교부 및 군의 주요인사들 40여명이 스미싱에 감염된 사례[13]이 있다.

III. 관련연구 및 현황

스미싱 문제를 해결하기 위해서 새로운 기술을 개발 방법과 제도적인 방법이 있을 수 있다. 본 장에서는 스미싱과 소액결제의 제도 현황과 관련연구를 살펴본다.

3.1 스미싱 제도 현황 및 관련연구

본 절에서는 최근 2년간(2014년~2015년) 월별 스미싱 탐지 건수[15]를 참고하여 시기별 스미싱 제도와 법 현황을 살펴본다(Table 1. 및 Fig. 2. 참고).

3.1.1 '[Web발신]' 문구 입력 제도(2014. 7)

미래창조과학부(이하 미래부)에서는 인터넷 발신 문자인 경우 '[Web발신]' 문구를 자동 입력하는 알림서비스를 실시하였다[8]. 이 제도의 효과는 Fig. 2.의 2014년 월별 스미싱 탐지 건수(파란색)에 대한 그래프를 보면 알 수 있다. 2014년 6월 약 901,250건 탐지되던 스미싱 문자들이 8월 약 486,669건으로 약 46%가 감소하였다.

3.1.2 스미싱 차단앱 의무 탑재 제도(2014. 9.)

미래부와 한국인터넷진흥원(이하 KISA)에서는 2014년 9월 스미싱 차단앱을 의무적으로 탑재하도록 이동통신사 3사(SKT, KT, LG U+)와 협의하였다(SK텔레콤의 T가드, KT 알스미싱가드, LGU+ 알약안드로이드)[7]. Fig. 2.의 2014년 그래프(파란색)보다 2015년 그래프(붉은색)에서 스미싱 탐지 건 수가 크게 감소된 것을 알 수 있다.

3.1.3 인터넷발송문자서비스 사업자 등록 관리 및 발신번호조작 문자 차단에 관한 법 시행(2015. 4.)

2015년 4월 국회 전기통신사업법 일부개정 법률안이 실행되어 인터넷발송문자서비스 사업자 등록 관리되고, 발신번호가 변작된 문자 메시지 차단되는 등의 법률 제도가 시행되었다[16]. 이 효과는 2015년 4월 스미싱 탐지 건수(붉은색) 약 432,946건에서 5월 약 91,041건으로 약 79% 정도 탐지건수가 급감한 것을 통해 알 수 있다(Fig. 2. 참고).

3.1.4 모바일 응급 사이버 치료체계 관련 제도(2015. 10.)

2015년 10월 1일 미래부, KISA, 이동통신사 3사가 협력하여 모바일 응급 사이버 치료체계를 운영하였다[17]. 이 체계는 선제적으로 악성코드에 감염된 스마트폰 식별이 가능하며, 감염된 스마트폰이 발견 시 이용자에게 안내 문자 메시지를 발송하고, 해당 악성앱을 원격에서 삭제하는 기능을 포함하였다[17]. 이 제도의 효과로 탐지 건수가 눈에 띄게 감소하는 것을 확인할 수 있다(Fig. 2.의 2015년 탐지 건수(붉은색) 그래프 참고).

3.1.5 전자금융거래 기본약관 개정 스미싱 손해배상에 관한 제도(2017. 1.)

2017년 1월 20일 공정거래위원회에서 전자금융거래 기본약관을 개정하였다[18](공정거래위원회 표준약관 제10028호)[19] 개정된 내용 중에는 해킹, 스미싱, 피싱, 파밍에 대한 금융 사고의 피해 입증책임을 은행에게 부담한다는 점을 명시하였다[20]. 은행에게 사이버 사고에 대한 입증 책임을 부여함으로써 소극적인 보안 제도 및 시스템 운용에서 적극적인 행동을 보여줄 것을 주문한 것으로 판단된다[21].

3.1.6 스미싱 차단을 위한 연구

위의 제도적인 노력과 함께 스미싱 문자를 줄이기 위한 연구들이 많이 수행되었다. [22]에서는 안드로이드 플랫폼 상에서 자동으로 스미싱을 차단하는 연구를 수행하였고, [23]에서는 발송기관을 금융기관으로 한정하고, 금융기관에 등록한 개인식별코드를 통하여 문자 메시지의 진위여부를 식별할 수 있는 방안을 제안하였다. [24]에서는 클라우드 플랫폼을 활용하여 악성 URL 및 수정된 APK 파일을 검증할 수 있는 방안을 제안하였고, [25]에서는 스미싱을

Table 1. Number of Monthly Simishing Detection (2014~2015 Year)[15]

	Jan.	Feb.	Mar.	Apr.	May.	Jun.	Jul.	Aug.	Sep.	Oct.	Nov.	Dec.
2014	47,996	139,371	155,377	245,378	386,178	901,250	774,665	487,669	167,664	250,142	335,222	152,265
2015	120,597	570,291	13,293	432,946	91,041	35,335	31,416	15,946	8,797	12,031	5,391	

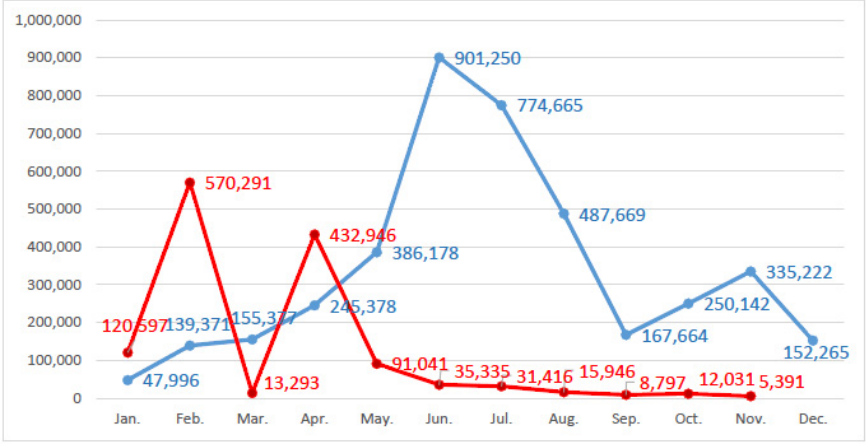

Fig. 2. Number of Monthly Smishing Detection (2014~2015 Year)[15]

통해 감염되는 악성 APK을 프로파일링하여 스미싱 범죄를 예방할 수 있는 모델을 제안하였다.

3.2 모바일 소액결제 제도 현황 및 관련연구

3.2.1 미래부 정보통신망법 개정 및 통신과금서비스 이용약관 개정안 시행(2014. 12.)

2014년 12월 미래부는 통신과금서비스 이용환경 조성을 위해 표준결제창 도입, 스마트폰소액결제의 이용한도 증액 시 미리 사용자 동의 필요, 문자 메시지 인증방식 이외에 사용자가 미리 설정한 개인비밀번호를 입력해야만 결제가 가능한 안전결제서비스 등을 도입하였다[26].

3.2.2 휴대폰 소액결제 피해를 줄이기 위한 연구

소액결제의 피해를 줄이기 위해서 [27]에서 소액결제 시스템이 가진 구조적 취약점을 분석하고 이를 해결할 수 있도록 기존 표준결제창 개선 방안을 연구하였다. 또한 [28]에서는 휴대폰 결제 서비스와 관련된 제도적 문제점을 분석하였다. 주로 콘텐츠제공자의 문제점(온라인 사이트의 약관 표시 실태의 문제 등등)에 대해서 다루었다. 이를 해결하기 위해서 콘텐츠사업자를 규제 및 관리 감독을 강화하여, 불법·부당행위를 하지 못하도록 강제하였다. 또한 소액결제 관련 요금 청구 시 세부내역 표시 방법을 개선하여 사용자의 의식 및 인지를 강화하고자 하였다.

3.2.3 소액결제 피해 시 손해배상 책임에 대한 연구

[29]는 모바일 소액결제 피해 발생 시 소비자와 다수의 사업자(콘텐츠제공자, 결제대행사, 이동통신사)가 참여하고 있어 소액결제 피해 발생 시 책임 부담의 주체가 불명확하다고 언급하고 있다. 소비자의 과실에 의해 피해가 발생한 경우를 제외하고는 통신과금서비스제공자 측에게 무과실책임을 부과하도록 하는 법률 개정안을 제안하였다. 하지만 [29]에서 제안하는 방법에도 불구하고 통신과금서비스제공자는 이동통신사와 결제대행사 두 사업자를 모두 함께 지칭하는 단어로 여전히 피해 발생 시 두 사업자 간 손해배상에 대한 책임 주체가 불명확한 문제점이 남아 있다.

IV. 현 스미싱 제도과 모바일 소액결제 제도의 한계점

4.1 소액결제 제도의 한계: 소액결제 피해금액 증가

3.1절에서 알 수 있듯이 스미싱 억제 제도를 통해 스미싱 탐지 건수가 크게 줄어들었다(2014년 4,917건에서 2015년 1,120건으로 대폭 감소[9]). 하지만, 2014년에서 2015년까지 스미싱으로 인한 피해금액은 3억 4천만 원에서 17억 4천만 원으로 5배 이상 증가하였으며, 건 당 피해액도 2014년 10만원에서 2015년 160만원으로 크게 증가하였다[9]. 스미싱으로 인한 금전적인 피해는 주로 소액결제로 인한 피해가 많았다[9].

4.2 소액결제 참여 사업자들의 시스템 보안성 의무 및 강화에 대한 제도의 부재

스미싱 공격이 이미 발생한 경우에 금전적 피해를 최소화하기 위해서 모바일 소액결제 시스템의 보안적 조치가 잘 되어 있어야 한다. 특히 모바일 소액결제의 경우에는 이동통신사, 콘텐츠 제공자, 결제 대행사 3자의 시스템이 사용되기 때문에 각각의 시스템에 대한 취약점이 없도록 보안성을 의무화하는 것이 필요하다. 하지만 지금까지는 시스템의 보안 조치를 의무화하는 제도는 없었다. 보안 조치를 의무화하기 위해서는 정기적으로 해당 사업자의 홈페이지에 대한 취약점을 점검하고 평가할 수 있는 제도가 필요하다.

이와 관련해서 아래의 사례를 살펴보자.

4.2.1 사례분석: 이동통신사 및 콘텐츠제공자의 소액결제 관련 시스템에 대한 보안성 미비로 인한 사고 사례

2016년 12월에서 2017년 1월 사이에 신종 스미싱 사고[4]가 발생하였다[30]. 이 사건은 이동통신사 LG U+와 온라인쇼핑몰 쿠팡에 집중 발생하였으며, 다음의 문제점들로 인하여 발생하였다[30].

(1) LG U+(이동통신사) 홈페이지의 취약점: 개인당 2개 이상의 아이디를 생성할 수 있는 취약점이 있었다. 이에, 공격자들은 해킹을 통해 개인정보(이

4) 휴대폰소액결제를 사전 차단한 이용자도 스미싱으로 인한 휴대폰소액결제 피해가 발생하였다는 점에서 신종 스미싱 사건으로 분류가 되고 있다[30].

름, 생년월일, 주민등록번호 등)를 활용[5]하여 피해자의 아이디를 추가 생성하였다. ② 공격자가 새롭게 생성한 LG U+ 아이디를 활용하여 휴대폰소액결제 차단을 해제하고 휴대폰소액결제 한도를 최대치인 50만원으로 상향 조정하였다. LG U+와 달리 SKT와 KT의 경우에는 개인당 하나의 아이디만을 생성할 수 있기 때문에 이러한 문제점은 발견되지 않았다[30].

(2) 쿠팡(콘텐츠제공자)의 취약한 시스템: ① 가짜 아이디 무한대 생성할 수 있는 문제점이 있었으며, ② 환불 시 타명의의 계좌로 환불할 수 있는 취약점이 존재하였다. 해커들은 피해자의 명의로 소액결제를 진행 후 쿠팡의 환불 절차를 악용하여 대포통장을 활용한 현금화를 시도하였다.

이렇듯, 스미싱으로 인한 금전적 피해를 줄이기 위해 소액결제 구조상의 이동통신사, 콘텐츠 제공자, 결제대행사 간의 발생할 수 있는 보안상 취약점들을 해결해야하며 이를 의무화할 수 있는 제도적 보완 및 설계가 필요한 시점이다.

4.3 모바일 소액결제 피해 발생 시 사업자 간 손해배상 책임에 대한 한계

스미싱으로 인한 소액결제 피해사고가 발생할 경우 〈정보통신망 이용촉진 및 정보보호 등에 관한 법률〉 제58조 ③항에 의거하여, 결제대행사와 콘텐츠 제공자가 협의하여 "결제금 청구 취소 여부"를 결정하고, 스미싱으로 인한 소액결제 사기로 판단된 경우에는 요금 결제 전에는 이동통신사에서 과금을 취소하고, 요금 결제 후에는 콘텐츠제공자가 결제금을 환불하는 방식으로 피해를 구제해주었다[32].

하지만, 쿠팡과 LG U+의 신종 스미싱 사고의 경우에는 해커가 이미 쿠팡에서 타명의의 대포통장을 이용한 환불 절차를 통하여 소액결제 현금화를 수행하였기 때문에, 결제대행사와 콘텐츠제공자 간 결제금 청구 취소로 피해금액을 회수하기 어렵다. 또한 콘텐츠제공자와 이동통신사가 모두 소액결제 피해에 대한 책임이 있는 상황이기 때문에 어느 사업자에게 손해배상에 대한 책임을 얼마나 물어야 하는지 명확하지 않다[6]. 따라서 스미싱으로 인한 소액결제 피해사고 발생 시 피해자의 고의 또는 중대한 과실이 없는 경우 사업자 간 손해배상의 책임 여부 및 범위에 대한 구체적인 가이드를 제시할 수 있는 제도 및 법안이 필요한 시점이다.

V. 모바일 소액결제에 대한 제도적 개선방안

5.1 소액결제 시스템 보안성 강화를 위한 제도 제안

소액결제 피해액을 줄이기 위해서는 스미싱 억제하는 노력뿐만 아니라, 소액결제 참여 사업자들의 시스템 취약점으로 인한 문제를 해결해야하므로 사업자의 소액결제 관련 시스템에 대한 보안성을 의무 및 강화할 수 있는 제도를 제안한다. 또한 보안성 강화의 의무를 좀 더 강하게 부여하고, 피해자를 구제하기 위해서, 소액결제 피해사고 발생 시 사업자 간 책임소지를 명확히 할 수 있는 제도/법안을 제안한다.

5.1.1 소액결제 관련 사업자들의 시스템에 대한 보안취약점 점검 수행 및 평가제도 제안

2014년 미래창조과학부에서는 이동통신사, 인터넷 포털, 웹하드 등 3개 분야에 대해서 시범적으로 홈페이지 보안취약점 점검을 수행하고 그 결과를 언론에 발표한 적이 있다[33]. 이러한 시범적 점검을 넘어서 정기적으로 제도화하여 취약점을 점검하는 방안을 제안한다. 정부가 정기적으로 소액결제와 관련된 사업자들(통신과금서비스제공자 및 콘텐츠제공자)에 대한 홈페이지 보안취약점 점검을 수행하고 평가하여 그 결과에 따라 징벌적 벌금 혹은 상금을 주는 제도를 제안한다. 이는 공공기관에 대한 정보보호실태평가[2]와 유사한 제도이다.[7] 이러한 평가 제도를 통해 소액결제 관련 사업자들의 시스템을 보안강화할 수 있는 계기가 될 수 있다.[8]

---

5) 공격자들이 피해자의 개인정보를 얻기 위해서 LG U+나 쿠팡의 고객센터 등을 해킹했을 가능성이 있다[31].

6) 2017년 1월에 발표된 공정거래위원회의 전자금융거래 기본 약관은 스미싱 피해로 인한 손해배상 책임을 은행에 있다고 명시하고 있는데 이는 은행 거래 시 사고에 대한 손해배상에 대한 부분을 포함하지, 스미싱으로 인한 소액결제 사기에 대한 손해배상을 포함하기 어렵다. 왜냐하면, 소액결제는 결제대행사를 거쳐 피해자의 이동통신사 통신요금으로 청구가 되기 때문이다.

7) 공공기관의 정보보호실태평가 평가점수는 경영평가에 일부 반영되어 기관에서 긴밀하게 대응하고 준비하고 있다. 이러한 것은 공공기관의 보안성을 강화할 수 있는 강력한 방안이다[2].

8) 미래부에서는 KISA와 함께 정보보호실태조사를 수행하여 민간 기업에 대한 보안 실태를 조사하고 있지만 조사 차원일 뿐 평가결과에 대한 책임을 부여하지 않아 강제성

5.1.2 소액결제 사업자에 대한 보안 가이드라인 제시

이동통신사, 콘텐츠제공자, 결제대행사와 같은 소액결제에 관련된 사업자들에 대한 보안 가이드라인을 제시하고 이를 지킬 수 있도록 제도화 한다.

다음은 이동통신사 홈페이지의 보안 가이드라인에 대한 예시이다.

① 휴대폰소액결제 시 SMS 인증보다 한층 강화된 휴대폰소액결제 안심결제서비스(사용자가 사전에 설정한 비밀번호를 입력해야만 결제가 되는 서비스)를 이용 의무화를 한다.

② 홈페이지에서 다중 아이디 발급 시 문자 메시지 인증보다 한층 강화된 본인 인증(전화인증, 안심결제서비스 등) 절차를 통과하여 발급이 가능하도록 한다. ③ 소액결제 한도금액 변경 시에 이용자에게 문자 이외에 전화와 E-mail을 통해서 변경 사항을 확인하고 안내해준다.

다음은 콘텐츠제공자의 홈페이지 보안 가이드라인에 대한 예시이다.

① 가짜 아이디를 생성할 수 없도록 아이디 생성 시에 인증과정을 강화한다. ② 환불 시 계좌 아이디 인증 절차를 강화하며, 타인의 명의로 된 계좌로 환불이 불가능하도록 한다.

5.2 모바일 소액결제 손해배상 관련 법 개선(안)

모바일 소액결제로 인한 피해는 일차적으로 사용자의 단말의 해킹을 통해서 발생하기 때문에 사용자에게 대한 부주의 및 과실에 대한 일차적인 책임이 있다.

하지만 앞선 사례에서도 보았듯이 이동통신사 혹은 콘텐츠제공자의 시스템 보안 취약점으로 피해가 발생할 수 있으며 이 경우 사업자들에 대한 책임도 함께 존재한다. 하지만 다수의 사업자가 연관되어 있기 때문에 어느 사업자가 얼마의 피해를 보상해야하는 지 불분명한 부분이 있다.

이러한 문제점을 해결하기 위해서 소액결제로 인한 피해 발생 시 각 사업자에게 자신의 시스템의 보안 문제로 인한 피해가 아님을 입증할 책임을 부여하고, 입증 가능한 경우에만 손해배상 책임이 없도록 하는 방안을 제안한다. 만약 소액결제와 관련된 모든 사업자가 자신의 시스템으로 인한 피해 사례가 아님을 입증할 수 있다면 최종 책임은 사용자에게 있으며, 이때는 사용자가 피해보상을 받을 수 없도록 한다.

이 부족한 한계점이 있다.

5.2.1 통신과금서비스 기본 약관 개정(안)

소액결제 결제지불구조를 고려하여 통신과금서비스제공자(이동통신사, 결제대행사)의 책임 발생 시 이에 대한 손해배상 책임을 부여한다. 다만 통신과금서비스제공자의 문제가 아닌 이용자의 고의나 중대한 과실에 의해서만 이용자의 피해가 발생한 경우에는 그 책임을 면하도록 한다.

예를 들어 휴대폰소액결제 결제 지불구조에서 본인인증 문제로 발생한 스미싱 사고로 인한 금전적 피해가 발생했을 시에는 담당 이동통신사나 혹은 결제대행사에게 그 책임을 묻도록 한다. 통신과금서비스제공자에 대한 손해배상 책임을 촉구하여 통신과금서비스 제공자들이 관련 시스템을 보안할 수 있도록 유도한다.[9)]

이를 위해, 통신과금서비스 기본약관[10)]을 개정한다. 이에 대한 예시로 결제대행업체 다날의 통신과금서비스 이용약관 참조하여 아래와 같이 제안한다.

제10조 (회사의 권리와 의무) 부분 수정안

개정(전)	개정(안)
제 10조 2항 회사가 접근매체의 발급주체가 아닌 경우에는 접근매체의 위조나 변조로 발생한 사고로 인하여 이용자에게 발생한 손해에 대하여 배상책임이 없습니다.	(삭제)
제 10조 3항 회사가 접근매체의 발급주체이거나 사용, 관리주체인 경우에는 접근매체의 위조나 변조로 발생 한 사고로 인하여 이용자에게 발생한 손해에 대하여 배상책임이 있습니다.	(삭제)
제 10조 4항 회사는 다음 각 호의 어느 하나에 해당하는 사고로 인하여	제 10조 2항 회사는 다음 각 호의 어느 하나에 해당하는 사고로 인하여

9) 제안하는 제도를 원활하게 수행하기 위해서는 소액결제 시장 참여자인 계약당사자(콘텐츠제공업체, 소비자)와 통신과금서비스제공자(결제대행업체, 이동통신사)의 적극적인 협조가 필요하다.

10) 공정거래위원회 전자금융거래 기본약관 개정안(2017. 1. 16.)의 제20조(손해배상 및 면책)를 참고

이용자에게 손해가 발생한 경우에는 그 손해를 배상할 책임이 있습니다. 다만, 본조 제2항에 해당하거나 법인('중소기업기본법' 제2 조 제2항에 의한 소기업을 제외한다)인 이용자에게 손해가 발생한 경우로서 회사가 사고를 방지하기 위하여 보안절차를 수립하고 이를 철저히 준수하는 등 합리적으로 요구되는 충분한 주의의무를 다한 경우에는 그러하지 아니합니다. ① 접근매체의 위조나 변조로 발생한 사고 ② 계약체결 또는 거래지시의 전자적 전송이나 처리 과정에서 발생한 사고 ③ 전자금융거래를 위한 전자적 장치 또는 "정보통신망 이용촉진 및 정보보호 등에 관한 법률" 제2조 제1항 제1호에 따른 정보통신망에 침입하여 거짓이나 그 밖의 부정한 방법으로 획득한 접근매체의 이용으로 발생한 사고	이용자에게 손해가 발생한 경우에는 그 손해를 배상할 책임이 있습니다. 다만, 회사가 사고를 방지하고 이를 철저히 준수하는 등 합리적으로 요구되는 충분한 주의의무를 다한 경우에는 그러하지 아니합니다. ① 접근매체의 위조나 변조로 발생한 사고 ② 계약체결 또는 거래지시의 전자적 전송이나 처리 과정에서 발생한 사고 ③ 전자금융거래를 위한 전자적 장치 또는 "정보통신망 이용촉진 및 정보보호 등에 관한 법률" 제2조 제1항 제1호에 따른 정보통신망에 침입하여 거짓이나 그 밖의 부정한 방법으로 획득한 접근매체의 이용으로 발생한 사고

또한, 이동통신사에 대한 책임을 부여하기 위해서 통신과금서비스이용약관 LG U+예시를 참고하여 수정된 약관을 아래와 같은 예시로 제안한다.

제6조 (회사의 권리와 의무)

개정(전)	개정(안)
제 6조 1항 회사가 접근매체의 발급주체가 아닌 경우에는 접근매체의 위조나 변조로 발생한 사고로 인하여 이용자에게 발생한 손해에 대하여 배상책임이 없습니다.	(삭제)
제 6조 2항 회사가 접근매체의 발급주체이거나 사용, 관리주체인 경우에는 접근매체의 위조나 변조로 발생 한 사고로 인하여 이용자에게 발생한 손해에 대하여 배상책임이 있습니다.	제 6조 1항 접근매체의 위조나 변조로 발생 한 사고로 인하여 이용자에게 발생한 손해에 대하여 배상책임이 있습니다.

5.2.2 정보통신망법 개정(안)

4.2.1 절에서 언급한 바와 같이 통신과금서비스 기본약관을 개정하는 것만으로는 통신과금서비스제공자에게 스미싱으로 인한 소액결제 피해에 대한 법적인 과실 책임을 부여하는데 부족하기 때문에 관련 법안을 개정도 함께 제안한다.

본 논문에서는 정보통신망법 제60조(손해배상 등)에 4항을 신설하여 통신과금서비스제공자에게 손해배상에 책임을 묻도록 한다. 아래는 제안하는 예시이다.

개정(전)	개정(안)
(신설)	제60조(손해배상) 4항 통신과금서비스제공자는 다음 각 호의 1의 사고로 인하여 이용자에게 손해가 발생한 경우 그 손해를 배상한다. 1. 접근매체의 위조나 변조로 발생한 사고 2. 계약체결 또는 거리지시의 전자적 전송이나 처리과정에서 발생한 사고 3. 전자금융거래를 위한 전자적 장치 또는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조 제1항 제1호에 따른 통신과금서비스제공자의 정보통신망에 침입하여 거짓이나 그 밖의 부정한 방법으로 획득한 접근매체의 이용으로 발생한 사고

이와 함께, 정보통신망 이용촉진 및 정보보호법 제 72조 4항을 개정하여 통신과금서비스를 이용해 자금을 융통하는 행위(소액결제 현금화)가 가능하도록 콘텐츠제공자의 시스템 혹은 홈페이지를 방치하는 경우에 대한 책임을 묻도록 한다.

즉, 콘텐츠제공자의 의무를 다하지 않을 경우에 손해배상에 대한 책임을 묻는다. 특히 타명의의 계좌로 환불이 불가능하도록 하여 해커가 쉽게 현금화할 수 없도록 한다. 제안하는 개정안은 다음과 같다.

개정(전)	개정(안)
제 72조 4항 다음 각 목의 어느 하나에 해당하는 행위를 통하여 자금을 융통하여 준 자 또는 이를 알선·중개·권유·광고한 자 가. 재화 등의 판매·제공을 가장하거나 실제 매출금액을 초과하여 통신과금서비스에 의한 거래를 하거나 이를 대	제 72조 4항 다음 각 목의 어느 하나에 해당하는 행위를 통하여 자금을 융통하여 준 자 또는 이를 알선·중개·권유·광고한 자 또는 자금 융통이 가능하도록 시스템 방치한 자 가. 재화 등의 판매·제공을 가장하거나 실제 매출금액을

행하게 하는 행위 나. 통신과금서비스이용자로 하여금 통신과금서비스에 의하여 재화 등을 구매·이용하도록 한 후 통신과금서비스이용자가 구매·이용한 재화등을 할인하여 매입하는 행위	초과하여 통신과금서비스에 의한 거래를 하거나 이를 대행하게 하는 행위 나. 통신과금서비스이용자로 하여금 통신과금서비스에 의하여 재화 등을 구매·이용하도록 한 후 통신과금서비스이용자가 구매·이용한 재화 등을 할인하여 매입하는 행위

위와 같은 개정안을 통해 콘텐츠제공자가 홈페이지 운용에 있어서 통신과금서비스를 이용한 자금 융통행위가 쉽도록 시스템을 방치하지 못하도록 한다.

또한 콘텐츠제공자로 인한 피해 사실이 입증되면, 이에 대한 강력한 책임을 물어 콘텐츠제공자가 스스로 자체 시스템에 대한 시스템 보안 및 운용상 보안 점검을 철저하게 하도록 유도한다.

VI. 결 론

스마트폰의 보급과 함께, 모바일을 대상으로 하는 사이버 공격이 활발하게 일어나고 있으며, 특히 스미싱을 이용한 피해가 많이 발생하고 있다. 이를 해결하기 위해여 여러 제도 및 법안들이 제안되었고, 이를 통하여 상당 부분의 스미싱 건수가 줄어드는 효과를 보았다. 본 논문에서는 현 스미싱 제도를 분석하고, 그 한계점을 살펴보았다. 스미싱 피해건수 감소에도 불구하고, 스미싱 피해액이 증가하는 문제점을 인식하고, 이를 해결하기 위해서 소액결제와 관련된 문제점을 살펴보았다. 스미싱으로 인한 소액결제 피해를 예방하고, 피해액을 줄이고자, 본 논문에서는 소액결제 시스템의 보안을 강화하고, 의무화할 수 있는 소액결제 사업자에 대한 정보보안 평가제도, 소액결제 피해 발생 시 손해배상 책임자 구체적 명시의 제도 및 법안을 제안한다. 이를 통해 향후 소액결제로 인한 피해금액을 줄이고 피해구제가 쉬워지기를 기대한다.

References

〔1〕 Etoday News, “Smartphone penetration rate 91% ‘Finance in the hand’,” http://www.etoday.co.kr/news/section/newsview.php?idxno=1441840, Jan. 2017

〔2〕 National Information Security White Paper, http://isis.kisa.or.kr/ebook/download_pdf/2016.pdf, Apr. 2016

〔3〕 Ahnlab, “Major issues on cyber security,” http://www.ahnlab.com/kr/site/securityinfo/asec/asecView.do?groupCode=VNI001&seq=23587, Ahnlab ASEC Report, 26, Feb. 2015

〔4〕 https://ko.wikipedia.org/wiki/2014%EB%85%84_%EB%8C%80%ED%95%9C%EB%AF%BC%EA%B5%AD_%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4_%EB%8C%80%EB%9F%89%EC%9C%A0%EC%B6%9C_%EC%82%AC%EA%B1%B4

〔5〕 Yonhap News, “KT homepage hacking… 12 million personal information leaked,” http://www.yonhapnews.co.kr/society/2014/03/06/0702000000AKR20140306149651065.HTML, Mar. 2014

〔6〕 MoneyToday News, “12.3 million personal information leaked from mobile network operator such as LG U+ and SKT,” http://news.mt.co.kr/mtview.php?no=2014031111001655436, Mar. 2014

〔7〕 Yonhap News, “Smartphone released after next month should have a built-in anti-smishing app,” http://www.yonhapnews.co.kr/economy/2014/08/28/0303000000AKR20140828063100017.HTML Aug. 2014

〔8〕 Electronic News, “From today, displaying the 〔Web〕 on a SMS message when the message is sent from Internet,” http://www.etnews.com/20140720000011, Jul, 2014

〔9〕 Kyeonggi ilbo news, “In Smishing·Pharming·Phishing area, 1,395 billion financial damages for three years,” http://www.kyeonggi.com/?mod=news&act=articleView&idxno=1230305, Aug. 2016

〔10〕 KISA, “A guide book for preventing and responding to the Smishing attack,” https://www.boho.or.kr/download.do?path=temp&name=smishing.pdf&orgName=%EC%8A%A4%EB%AF%B8%EC%8B%B1%EC%98%88%EB%B0%A9%EB%

B0%8F%EB%8C%80%EC%9D%91%EA%B0%80%EC%9D%B4%EB%93%9C.pdf, Mar. 2015

〔11〕 Yongdae Kim (Ahnlab), "Cyber Security Threats and responses for Mobilephone," Proceedings of the Mobile Infomation Security Conference (MISCON) 2015, Feb. 2015

〔12〕 YTN News, "Kim Sang-ryul, the senior secretary to the President for educational affair, was subjected to smishing attacks," http://ytn.co.kr/_ln/0101_201503171658263049, Mar. 2015

〔13〕 CNN News, "North Korea hacked government officials' smartphones, South Korea says," http://edition.cnn.com/2016/03/08/asia/south-korea-smartphone-hack/index.html, Mar. 2016

〔14〕 https://en.wikipedia.org/wiki/SMS_phishing

〔15〕 iNews News, "The number of smishing attack is decreasing," http://news.inews24.com/php/news_view.php?g_serial=934649&g_menu=020200, Dec. 2015

〔16〕 Boannews News, "Starting from the 16th, blocking the phone number change for smishing," http://www.boannews.com/media/view.asp?idx=45948, Apr. 2015

〔17〕 Boannews News, "Emergency response system for malicious app infections on smartphone," http://www.boannews.com/media/view.asp?idx=48006&kind=2, Sep. 2015

〔18〕 Newsis News, "Banks should pay damages from hacking, phishing, smishing,,, the revised e-commercial terms and conditions of the Fair Trade Commission," http://www.newsis.com/view/?id=NISX20170124_0014661503, Jan. 2017

〔19〕 Free Trade Commissions, "Agreement on using electronic financial transactions," 10028, Jan. 2017

〔20〕 The DigitalTimes News, "Electronic financial hacking damage compensation becomes easy… The bank's responsibility for proving," http://www.dt.co.kr/contents.html?article_no=2017032902100151800001, Mar. 2017

〔21〕 Chosun Biz News, "Hacking, phising, pharming demage from 'bank account'…," http://biz.chosun.com/site/data/html_dir/2017/03/13/2017031300984.html, Mar. 2017

〔22〕 Si-young Lee, Hee-Soo Kang, and Jong-Sub Moon, "A Study on Smishing Block of Android Platform Environment," Jounal of The Korea Institute of Information Security & Cryptology, 24(5), pp. 975-985, Oct. 2014

〔23〕 Choon Kyoung Joo and Ji Won Yoon, "Discrimination of SPAM and prevention of smishing by sending personally identified SMS(For financial sector)," Journal of The Korea Institute of Information Security & Cryptology, 24(4), pp. 645-653, Aug, 2014

〔24〕 Seolah Je, Vu Long Nguyen, and Souhwan Jung, "Design and Implementation of Verification System for Malicious URL and Modified APK File on Clould Platform," Journal of The Korea Institute of Information Security & Cryptology, 26(4), pp. 921-928, Aug, 2016

〔25〕 Youngho Jeong, Kukheon Lee, and Sangjin Lee, "Designing SMS Phishing Profiling Model," Journal of The Korea Institute of Information Security & Cryptology, 25(2), pp. 293-302, Apr. 2015

〔26〕 ZDNet Korea News, "Blocking Micropayment illegal fraud," http://www.zdnet.co.kr/news/news_view.asp?artice_id=20141125110622, Nov. 2014

〔27〕 Kwang Sun Park and Sang-jin Lee, "A Study on Structural Vulnerability of MobilePhone Micropayment System And Improvement of Standard Payment Module for User Protection," Journal of the Korea Institute of Information

Security & Cryptology, 23(6), pp. 1007-1015, Dec. 2013
〔28〕 Seok-il Ryu, "A research for the problem of mobile micropayment and improvement plan," Korea Consumer Agency, Report 11-09, pp. 1-50, Sep. 2011
〔29〕 Min-a Kim and Hee-ju Park, "A study on consumer protection measures of mobile micropayments," Report 13-14, Korea Consumer Agency, Dec. 2013
〔30〕 IT Chosun News, "It's your fault"...Coupang vs LG U+, shifting responsibility to others," http://it.chosun.com/news/article.html?no=2830545, Feb. 2017
〔31〕 Edaily News, smishing incident damege, why was there a lot of LG-U+ user's micro payment cases?," http://www.edaily.co.kr/news/NewsRead.edy?SCD=JE41&newsid=04546086615828880&DCD=A00504, Feb. 2017
〔32〕 Korean National Police Agency Cyber Bureau, "Telecommunications fraud (Smishing) damage remedies," http://cyber.go.kr/mobile/sub/sub_08_g.jsp
〔33〕 Hankyung News, "Ministry of Science, ICT, and Future Planning, A Report for Homepage Vulnerability of Mobile Network Operators, Web-portal, and Web-hard," http://news.hankyung.com/article/201401081788g, Jan. 2014

〈저자소개〉

박 한 진 (Hanjin Park) 정회원
2007년 2월: 연세대학교 컴퓨터.산업공학과(컴퓨터과학 전공) 학사
2015년 2월: KAIST 전산학과 박사
2015년 1월~현재: ETRI 부설연구소 선임연구원
〈관심분야〉 사이버보안, 정보보호, 네트워크 보안, 모바일 보안

김 인 중 (Injung Kim) 종신회원
2006년: 성균관대학교 전기전자 및 컴퓨터공학부 박사
1992년~1999년: 국방과학연구소 선임연구원
2000년~현재: ETRI 부설연구소 책임연구원, 충남대학교 전자공학과 겸임교수, 한국사이버안보법정책학회 부회장
〈관심분야〉 사이버보안, 개인정보보호