Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.4, Aug. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.4.645

개인식별화된 SMS 발송을 통한 스팸식별 및 스미싱 예방(금융권중심)

주 춘 경,† 윤 지 원‡
고려대학교 정보보호대학원

Discrimination of SPAM and prevention of smishing by sending personally identified SMS(For financial sector)

Choon Kyong Joo,† Ji Won Yoon‡
Center for Information Security Technologies(CIST), Korea University

요 약

본 논문은 최근 휴대전화 사용 급증에 따라 계속 이슈가 되고 있는 스팸 문자 및 스미싱(Smishing)과 관련해서 금융기관에서 고객들에게 발송되는 SMS(Short Message Service)문자의 진위여부를 저비용, 고효율 측면에서 효율적으로 식별할 수 있는 방안을 제시하고자 한다.

먼저 본 논문에서는 스팸문자를 차단하기 위한 기존의 노력 및 대책에 대한 문제점 및 한계를 언급하고 그 한계를 효과적으로 극복할 수 있는 방안을 제시한다. 또한 제시된 개선방법에 대해 다양한 계층의 고객들에 대한 설문조사와 직접 구현 및 적용을 통해 그 효과성을 증명하려고 한다.

ABSTRACT

The purpose of this study is to provide low-cost and highly effective methods for customers to pick out SMS(Short Message Service) messages sent by financial institutions among SPAM messages and Smishing, which have rapidly spread recently and have caused critical issues.

Above all, the study aims to list problems and limitations of the past efforts and measures to block SPAM messages and provide one method to overcome those limitations. Also, the study aims to verify the effectiveness of the method by implementation of them and conducting surveys of a broad range of customers.

Keywords: Personally identified SMS, Personal identification code(PI Code)

I. 서 론

최근 '스미싱' 범죄가 다시 기승을 부리고 있는 가운데 이를 통해 개인정보유출 및 소액결제를 유도하는 범죄가 계속하여 발생하고 있다. 2014년 상반기 국민은행 콜센터 직원 및 SMS발송 담당직원들이 고객들로부터 수신된 SMS 문자의 진위여부를 묻는 전화를 직원 1인당 하루 평균 8통, 전체 32통 이상 받고 있으며 고객들은 수신된 발신처 전화번호와 메시지만으로는 수신된 메시지의 진위여부를 파악하는데 많은 어려움을 겪고 있는 게 현실이다.(현재 관련업무 담당). 또한 전화를 통하여 SMS 문자에 대한 진위 여부를 고객들에게 알려 주어도 통화에 대한 진실성을 의심하는 경우가 많은 것이 금융권의 현실이다. 특

접수일(2014년 6월 2일), 수정일(2014년 7월 22일), 게재확정일(2014년 7월 25일)
† 주저자, choonkyong.joo@kbfg.com
‡ 교신저자, jiwon_yoon@korea.ac.kr(Corresponding author)

히 동일 금융기관에서 발송되는 발신처 전화번호를 보면 은행 대표번호만이 아닌 업무별로 다양한 번호가 발신됨으로써 메시지를 받는 고객들이 발신처 전화번호로 문자메시지의 진위여부 판단에 별로 도움을 주지 못하고 있다.

현재 금융권에서 고객을 대상으로 제공하는 SMS 메시지 건수는 계속 증가하고 있으며 각 금융기관을 사칭하는 SMS 또한 그 수법이 날로 교묘해 지며 그

유형 또한 다양해지는 추세이다. 따라서 본 연구는 각 금융기관에서 발송하는 SMS 메시지를 고객이 사전에 거래에는 금융기관에 등록한 "개인식별코드"를 통해 수신된 메시지의 진위여부를 식별하게 하고, 더

나아가 스미싱과 같은 피해를 최소화 시키는 방안을 제안한다.

발송매체를 SMS(Short Message Service)와 LMS(Long Message Service)에 대한 문자 메시지로만 국한하며 발송기관 또한 그 중요성을 감안하여 금융기관만으로 한정하여 개선방안을 제시한다. 현재 각종 스팸등을 차단시켜주는 웹이나 통신사를 통한 기존의 각종 규제 방법이 아닌 고객이 보다 신뢰할 수 있는 방안을 제시하고 그 효과성을 입증함으로써 스팸식별 및 스미싱 예방에 크게 기여할 수 있을 것이라 본다.

본 논문의 2장에서는 스팸식별 및 스미싱 예방에 대한 기존의 대책 및 한계를 살펴보며, 3장에서는 기존 대책에 대한 문제점 및 한계를 극복할 수 있는 개선방안을 제시하고, 제시된 개선방안을 실제적으로 구현 및 적용을 통해 그 효과성을 실제 고객을 통해 입증할 것이다. 또한 다양한 계층의 고객 설문조사를 통해 얻어낸 결과를 통해 그 기대효과를 입증하려고 한다. 마지막으로 4장에서는 본 논문의 결론으로 끝을 맺는다.

II. 관련연구

2.1 이론적 배경 및 현황

2.1.1 스미싱의 정의 및 그 유형

스미싱이란 휴대전화 문자를 의미하는 문자메시지(SMS)와 인터넷,이메일 등으로 개인정보를 알아내 사기를 벌이는 피싱(Phishing)의 합성이다. 기본적으로 발신자의 신원을 속인 문자메시지를 통해 악의적인 사용자가 첨부한 링크에 접속한 후, 악성 앱을 설치하여 스마트폰내의 개인정보 또는 금융정보를 탈취하는 사기수법이다. 국내에서는 악성 앱 설치 후 휴대폰 결재인증 SMS를 탈취하여 피해자가 인지하지 못한 상태에서 휴대폰 결재를 완료시키는 수법으로 사용되고 있다[1].

최근 가장 많이 사용되는 스미싱 유형으로는 택배 부재, 사이버경찰청 출석 요구, 등기물 정보 확인, 카드결재, 알뜰폰 출시 등 이용자가 쉽게 속을 수 있는 문구로 사용자를 노리는 6가지 유형으로 발견 되었다. 이는 모두 사회공학적 수법으로 이용자들의 관심을 끌만한 내용과 사회적 이슈 등의 문구를 이용하여 문자메시지에 포함된 URL을 클릭하도록 유도하고 있다. 이러한 스미싱 유형은 그 해의 사회적 이슈와 맞물려 개인정보와 결합된 지능화된 형태로 진화하고 있다.

2.1.2 스미싱에 이용되는 국내SMS발송경로 및 방법

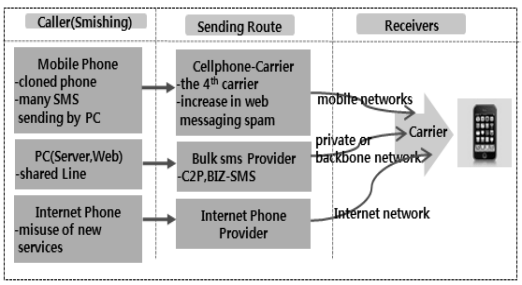


Fig. 1. SMS sending domestic route

스팸 및 스미싱에 이용되는 SMS발송경로 유형으로는 Fig.1과 같이 통신사에서 제공하는 웹페이지를 통해 개별 및 대량전송을 하는 SMS Web서비스, 고객 자체 서버 및 DB프로그램을 이용하여 실시간으로 개별 및 대량 전송을 하는 SMS서버연동서비스, 통신사에서 제공하는 메신저 프로그램을 이용하여 전송하는 SMS 메신저 서비스, 이통사 휴대전화를 이용하여 개인이 직접 발송하는 유형이 있다.

SMS Web서비스에는 웹메시징서비스, SMS서버연동서비스에는 C2P나 BIZ-SMS가 있으며 앞에서 언급했듯이 이중 C2P(대량문자발송서비스)를 가장 많이 이용되는 것으로 조사 되었다[2].

2.1.3 스팸방지를 위한 그 동안의 대책

KISA, 방통위 그리고 정부에서 지금까지 계획 및 추진 중인 스팸방지를 위한 대책[3]을 보면 전체적으

로 휴대전화 스팸방지, 신종 스팸방지, 스팸지수 발표/스팸대응 기반 고도화 및 국제협력 확대, 이용자 스팸방지 인식제고의 4개영역으로 구성되어 있으며 그 아래에 총 13개의 세부 추진과제를 담고 있다.

휴대전화 스팸방지 대책에는 다량의 스팸을 유발하는 대량문자발송 서비스(BIZ-SMS, C2P) 사업자에 대해 전송속도를 축소하고 사업자간 스팸 전송자 정

보를 공유(KISA통합 DB구축)하여 서비스 이용을 제한하는 등 사업자 책임의식 강화를 통한 스팸발송 억제, 휴대전화 이용자들의 이통사 지능형 스팸차단 서비스 가입 단계적확대 등 전송수신단계의 취약요인 개선을 통한 스팸차단 효율성 제고, 지인을 가장한 사기성 스팸전송을 통해 부당하게 정보이용료를 편취하는 성인컨텐츠 제공업체 대한 규제강화 등 스팸 전송자 규제 강화, 스팸 과태료 부과대상자의 범위 및 징수 방법의 다각화 검토 등 스팸과태료 징수율 제고 등으로 구성되어 있다.

스팸지수 발표/스팸대응 기반 고도화 및 국제협력 대책에는 정보 통신망을 통해 전송되는 스팸현황을 실시간으로 파악하여 선제적으로 대응할 수 있는 "종합 모니터링 및 분석체계 구축", 휴대전화 서비스 제공자의 스팸유통량을 정기적으로 공표함으로써 사업자간 자발적인 스팸감축 노력제고 등으로 구성되어 있다.

이용자 스팸방지 인식제고 대책으로는 스팸차단 및 신고요령을 이용자들이 보다 쉽게 접하고 이해할 수 있도록 "스팸방지 SMART 5대 수칙" (차단서비스, 차단 기능, 번호관리, 스팸이용금지, 118신고센터 활용) 등 다각적 홍보활동 전개를 그 내용으로 하고 있다.

2.1.4 스미싱방지를 위한 그 동안의 대책

지금까지 스미싱방지를 위한 주요 권고사항 및 대책 등을 살펴보면 스미싱/스팸 차단어플 설치 및 핸드폰용 백신어플 설치, 스미싱/스팸 어플을 항상 최근 버전으로 업데이트 유지, 확인되지 않은 앱이 함부로 설치되지 않도록 자신이 보유한 스마트폰의 보안설정 강화, 통신사 고객센터에 전화하거나 통신사 인터넷 홈페이지를 이용하여 소액결제를 원천적으로 차단하거나 결제금액 제한, 쿠폰/상품권/무료/조회/공짜 등으로 스팸문구를 미리 등록하여 스팸메시지 차단, 출처가 확인되지 않은 링크가 설정된 문자메시지 클릭주의, 웹에서 휴대전화로 보내는 '웹투폰(web to phone)'문자 앞에 '웹발신' 이란 식별문구 삽입해 주의 촉구(미래과학창조부) 등이 있다.

2.1.5 그 동안의 대책에 대한 문제점 및 한계

① 스팸차단 측정결과를 통한 한계분석

Table 1에 나와 있듯이 2013년6월 3대 통신사에서는 지능형 스팸차단 서비스에 가입되어 이통3사 단말기에 스팸 및 비 스팸 메시지를 2,900개를 발송하여 스팸차단율과 오차단율을 측정하였다[4]. 측정결과 Table 2의 측정 결과표를 보면 알 수 있듯이 측정한 스팸차단율이 각 통신사별로 50%가 안 되는 것을 볼 수 있다. 기존의 방지대책으로는 계속 진화하는 스팸 및 스미싱을 차단할 수 없다는 것을 알 수 있다.

Table 1. Spam protection factor Measurement of Intelligent anti-spam service

division	Measurement of intelligent anti-spam service accuracy
target	SKT, KT, LGU+
period	06. 2013
measurement	Spam protection rate and non-blocking spam rate measurement by sending each spam and non-spam message to 3 cellphone-carrier's cellphones which is joined to an intelligent anti-spam service. ※ (The number of the blocked messages / The number of the total messages) × 100
The number of samples	spam and non-spam message 2,900
Sampling error	within error ± 2%

Table 2. Measurement results

division	KT	SKT	LGU+
blocking rate	43%	37%	7%

② 발신처 전화번호의 한계

현재 정부와 통신사, 경찰청이 협동하여 발신처전화번호 도용 방지를 통해 스팸을 차단하려고 하고 있으나 현재 금융기관에서는 금융기관별, 업무별로 발신처 전화번호를 여러 가지로 사용하고 있는 현 시점에서 그것 또한 한계가 있다. 예를 들어 각 은행에서 고객에게 나가는 발신처 전화번호는 은행에서 사용하는 대표전화가 있고, 다시 은행 업무별/직원 개인별로 고객에게 발신처 전화번호를 다르게 보내고 있다.

즉 고객 입장에서 보면 동일 금융기관에서 여러 가지로 수신되는 발신처 전화번호 가지고는 각 금융기관으로부터 보내온 메시지내용의 진위를 판별하기는 쉽지 않은 게 현실이다.

디지털타임즈 2013년 9월9일자를 보면 '개인정보 보호캠페인 등 스미싱 예방대책도 강구하고 있지만 수법이 날로 고도화돼 사실상 한계가 있다는 게 업계의 중론이다' 라고 보도 하고 있다.

III. 개선방안 및 기대 효과

3.1 개선된 SMS 발송방법 및 순서

개선된 발송프로세스는 금융기관이 고객으로부터 SMS 수신 동의 접수 시 "개인식별코드" 를 함께 접수받아 SMS전송 시 고객이 설정한 "개인식별코드"를 메시지 끝에 붙여 함께 전송하는 방식이다. 동시에 통신사는 각 금융기관으로부터 요청된 SMS에 대해 각 금융기관별로 사전에 정의된 금융기관명을 메시지 앞에 함께 붙여 최종적으로 고객에게 전송하게 된다. 세부적인 SMS 발송 프로세스(Fig.2)는 다음과 같다.

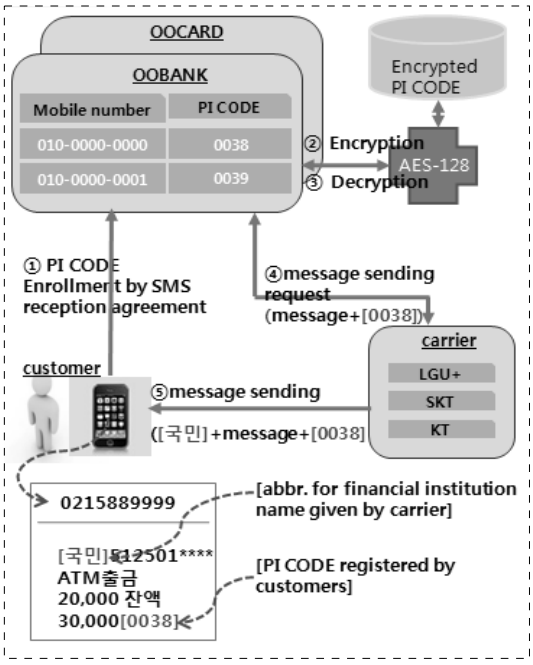


Fig. 2. The process of the sending SMS by PI Code

고객이 금융기관 내점 시 고객으로 부터 SMS 수신동의 여부 및 "개인식별코드"를 추가적으로 접수 받아 고객원장 정보에 등록한다. "개인식별코드"는 4 Byte(숫자 또는 영문자,특수문자)로 구성한다.

고객이 지정한 "개인식별코드"가 금융기관에서 사용하는 고객의 비밀번호와 유사하거나 동일하게 지정되지 못 하도록 유효성 체크 후 고객원장에 등록 한다. 금융기관은 "개인식별코드"를 DB에 저장 시 개인정보 유출에 대비하여 AES-128 bit 암호화 알고리즘을 이용하여 암호화하여 저장하며 SMS발송 시에는 암호화된 "개인식별코드"를 복호화하여 전송한다. 이때 금융기관는 메시지내용+"개인식별코드" 형태로 발송 요청하고 통신사는 사전에 정의된 통신사 지정 금융기관명(예:우리,국민,신한)+메시지내용+"개인식별코드" 형태로 다시 고객에게 전송한다.

고객은 메시지 본문 끝에 사전에 등록한 "개인식별코드"와 통신사에 의해 붙여진 본문 앞 금융기관명을 통해 메시지 진위 여부(스팸)를 판단하게 된다. 고객의 성향에 따라 금융기관별로 다르게 구성 할 수도 있고 모두 동일하게 구성할 수도 있다. 또한 고객이 인터넷뱅킹이나 스마트뱅킹(휴대폰)을 통해 언제든지 "개인식별코드"를 변경할 수 있게 하여 편리성을 제공해야 한다.

다음은 현재 금융기관에 적용된 유사적용 사례이다.

① 인터넷뱅킹에서 사용하는 개인화이미지
로그인시 본인이 사전에 등록한 문구 및 이미지로 금융기관 홈페이지 진위여부를 판별한다.

② 안심클릭의 개인 확인메시지
온라인 상품결재 시 사전에 등록한 문구를 통해 카드사에서 제공하는 안심클릭창 진위여부를 판별한다.

3.2 개인식별코드 노출에 대한 안전성

① 메시지 구성

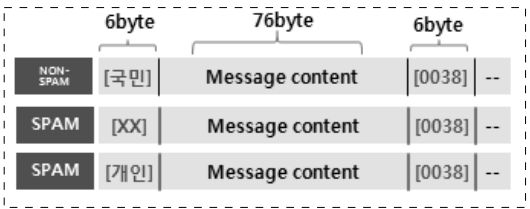


Fig. 3. Comparison of Spam and non-spam message format

전문 구성은 기존 80 Byte와 대량문자발송서비스(BIZ-SMS, C2P)인 경우만 가능한 예비 8 Byte를 포함하여 총 88 Byte를 사용한다.

88 Byte는 메시지내용 76 Byte, 구분자 4 Byte, 고객이 지정한 "개인식별코드" 4 Byte, 통신사가 지정한 금융기관명 4 Byte로 구성된다.

② "개인식별코드" 노출에 대한 안정성

Table 3. Message Sending Type

type		sending msg.	received msg.	origin
1	normal	msg+〔0038〕	〔국민〕+msg+〔0038〕	institution
2	the forged PI Code	msg+〔0038〕	〔xx〕+msg+〔0038〕	sending compay
3	the forged institution name & PI Code	〔국민〕+msg+〔0038〕	〔xx〕+〔국민〕msg+〔0038〕	sending compay
4	the forged PI Code	msg+〔0038〕	〔개인〕+msg+〔0038〕	individual
5	the forged institution name & PI Code	〔국민〕+msg+〔0038〕	〔개인〕+〔국민〕msg+〔0038〕	individual

고객에게 전송된 SMS내용과 함께 전송 된 "개인식별코드"가 악의적인 해커들에 의해 노출될 경우 통신사에서 SMS전송 시 마다 새로이 붙이게 되는 금융기관명을 통해 노출에 대한 위험을 방지 할 수 있다.

예를 들어 악의적인 해커들에 의해 "0038" 이라는 "개인식별코드" 및 금융기관명 "국민" 이 노출되었다고 하자. 해커들은 Table 3. 과 같이 스팸문자와 함께 위조된 "국민", "0038"를 메시지와 함께 고객들에게 보내게 될 것이다. 이때 통신사는 메시지가 요청된 업체가 국민은행이 아니므로 "국민" 대신 "XX"(발송업체명)를 붙이게 됨으로 즉 "XX", "0038"라고 고객은 메시지를 받게 되거나 발송업체가 아닌 직접 해커 개인이 핸드폰으로 발송하는 경우는 "개인", "0038" 이라고 받게 될 것이다. 즉 개인이 등록한 4자리숫자 뿐만 아니라 통신사에서 지정한 한글2자(또는 영문 4 Byte)를 통해 고객은 메시지 진위여부를 판별하게 된다.

결론적으로 말하면 고객입장에서는 금융기관별로 본인이 지정한 "개인식별코드" 와 통신사가 인증한 금융기관명 2개의 인증을 통해 더욱더 메시지에 대한 신뢰성 및 안정성을 확보할 수 있다.

3.3 개인식별코드 암호화 방법

고객정보원장 유출시 발생될 위험을 줄이기 위해 암호화하여 DB에 저장하고 전송 시 복호화 하여 전송한다. AES-128 bit 암호화 알고리즘을 이용하여 개인식별코드를 암호화 한다. 암호화 시 사용되는 Key는 암호화된 주민번호를 입력 값으로 하여 PBKDF2 (Password-Based Key Derivation Function 2)를 사용한다. PBKDF2는 아주 가볍고 구현하기 쉬우며 SHA와 같이 검증된 해쉬함수만을 사용한다. PBKDF2 구성은 다음과 같이 구성한다〔5〕.

① 용어 정의

PK: 개인식별코드 암호화 키
PIC: 개인식별코드
EPIC: 암호화된 개인식별코드
PRF: 의사난수 발생기, SHA1을 이용한 HMAC 사용
MK: 전용 하드웨어 어플라이언스 형태의 키 관리 솔루션에서 관리하는 마스터 키
ESSN: 암호화된 고객의 주민번호
Salt: ESSN을 사용
c: 카운터. 안전성과 속도를 고려하여 설정. 국내 PKI환경에서는 일반적으로 10000을 사용함
dklen: 출력값의 길이. AES-128의 키로 사용되므로 128비트
hlen: PRF의 출력 길이. SHA1을 이용한 HMAC을 PRF로 사용할 경우 160비트

② 개인식별코드 암호화 키(PK) 생성

$PK = PBKDF2(PRF, MK, ESSN, c, dklen)$

$PK = T_1 \| T_2 \| ... \| T_{dken/hlen}$, T의 인덱스로 사용되는 dklen/hlen = 128/160의 최대값은 1 이므로

$PK = T_1 = F(MK, ESSN, c, 1)$

$F(MK, ESSN, c, 1) = U_1 \oplus U_2 \oplus ... \oplus U_c$

$U1 = PRF(MK, ESSN \| INT(1))$

$U_2 = PRF(MK, U_1)$

...

$U_c = PRF(MK, U_{C-1})$

③ 개인식별코드(PIC) 암복호화

$EPIC = E_{PK}(PIC)$: 개인식별코드 암호화

$PIC = D_{PK}(EPIC)$: 개인식별코드 복호화

3.4 개인식별코드를 저장하는 시스템의 안전성

다음과 같은 환경 구성으로 "개인식별코드"를 저장하는 시스템을 해커로 부터의 외부공격이나 내부공격으로 부터 안전성을 확보할 수 있다. 여기서는 안전성에 대한 수학적 증명등과 같은 자세한 내용기술은 향후 연구과제로 남기고 간략히 안전성에 대해 언급하겠다.

① 고객의 암호화된 주민번호(ESSN)는 고객신규등록 시 고객주민번호 관리 원장과 분리되어 저장된다.

② 마스터 키(MK)는 고객정보가 저장되어 있는 서버와 분리된 별도의 서버에서 서버 외부로 이동(EXPORT)하지 않으면서 DB서버에서 암복호화 작업이 가능한 전용 하드웨어 어플라이언스 형태의 키 관리 솔루션에서 관리하고 있다.

③ 개인식별코드(PIC)는 고객정보 원장과 분리된 별도 SMS발송원장에 암호화 되어 저장된다.

④ 마스터 키 DB관리자와 계정관리자의 권한이 분리되어 관리 된다.

3.5 실제적용 및 설문조사

3.5.1 적용방법

본 적용은 실제 OO은행 고객 중 2014년7월 SMS 발송 대상고객 533,107 중 사전 전화를 통하여 본 연구의 취지를 충분히 설명한 후 동의를 한 고객 12명을 대상으로 적용을 해보았다. 발송대상고객 선정은 SMS발송 대상 고객 533,107명을 연령, 학력, 직업군별로 분류하여 98명을 1차적으로 선정한 후 동의를 한 12명을 최종으로 선정하였다.

사전에 동의를 구한 고객에게 동일 메시지에 대해 실제 발송될 SMS 1건, 본 논문에서 제시한 개선방안을 이용한 SMS 1건 총 고객별 2건을 Fig.4와 같은 SMS전문 형식으로 실제 OO은행 SMS발송시스템을 이용하여 발송하였다. 고객별 "개인식별코드"는 사전 전화를 통하여 수보 받아 사용하였고 금융기관명은 테스트를 위해 통신사가 아닌 SMS발송시스템에서 직접 붙여 발송하였다.

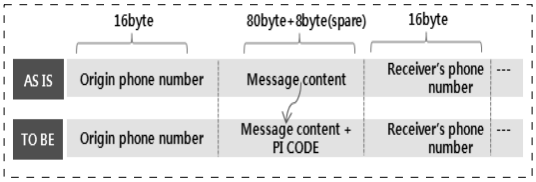


Fig. 4. Comparison of SMS sending text format

3.5.2 적용결과

SMS 발송 후 사전 동의를 구한 12명의 고객에게 변경 전 SMS와 개선방안 대한 비교 의견조사를 실시하였다.

Table 4. The apply results of Improvement

division	positive	negative	No difference
improvement	11	0	1

Table 4에 나와 있듯이 적용결과를 보면, 개선방안에 대해서는 12명중 11명(약92%)이 현재 SMS표시 방식보다는 훨씬 스팸식별에 도움이 된다고 응답을 하였다. 그러나 실제발송을 통한 설문 진행은 고객동의를 얻는 것에 대한 한계가 있어 개선방안의 효과성을 입증하기에는 설문대상 고객 수가 너무 작았다. 따라서 실제발송이 아닌 설문지만으로 여러 계층의 고객들에 대한 설문조사를 별도로 진행하여 개선방안에 효과성을 다시 한 번 입증하였다

Fig. 5. SMS Message Capture of the actual results

Fig.5은 실제 발송한 SMS결과를 화면 캡처한 것이다.

3.5.3 설문조사

설문조사는 전체 125명을 대상으로 학력별, 나이대별, 성별, 직업군별로 조사를 실시하였다. 조사 후 상한 값과 하한 값 25명을 제거한 후 100명을 대상으로 설문결과를 작성하였다.

조사기간은 2014년7월2일부터 7월13일까지 전화 및 직접방문을 하는 방법으로 친구 및 가족, 선후배들이 알고 있는 지인들의 명단을 사전에 파악 후 나이, 직업군, 학력 등이 한쪽으로 치우치지 않도록 사전에 조정 후 조사를 실시하였다.

설문내용은 현재 금융회사로부터 받고 있는 SMS 문자 서비스에 대해 발신처 전화번호와 메시지내용만 가지고 해당 메시지의 진위여부 판단이 가능한지에 대한 2가지 질문과 개선된 방식으로 보냈을 때 어떠했는지에 대한 2가지 질문으로 설문지를 구성하였다.

Table 5. The results of the questionnaire survey about the discrimination of spam using existing SMS methods

	division	positive	negative	no diff.	total
academic background	college graduates	0	30	4	34
	high school diploma	15	36	0	51
	in college	2	13	0	15
age	20	0	15	0	15
	30	3	30	0	33
	40	10	17	3	30
	50	4	17	1	22
sex	man	10	58	0	68
	woman	7	21	4	32
occupational cluster	financial business	4	16	0	20
	student	2	13	0	15
	medium and small firm	0	11	4	15
	major firm	0	20	0	20
	housewife	4	6	0	10
	selfemployed	7	13	0	20
	total	17	79	4	100

조사결과를 분석해 보면 기존방식에 대해서는 Table 5에 나와 있듯이 발신처 전화번호와 메시지만으로는 해당 SMS메시지에 대한 진위여부 파악이 어렵다는 의견이 79%, 가능하다는 의견이 17%로 조사되었다. 특히 부정적 의견이 학력에서는 별 차이가 없었으나 연령은 20/30대가, 직업군은 금융업/대기업에서 부정적 의견이 높았다.

개선방식에 대해서는 Table 6에 나와 있듯이 사전에 등록한 "개인식별코드"와 통신사가 붙이는 금융기관명을 SMS전송 시 함께 전송하는 것에 대해서는 긍정 84%, 부정 11%, 모름 5%로 조사 되었다. 특히 학력은 대졸, 연령은 30대, 직업군은 금융업종사자에서 긍정적의견이 많았으며, 상대적으로 고졸, 30대, 주부에서는 다소 부정적의견이 높은 것으로 조사 되었다.

종합적으로 보면 Fig.6에서 볼 수 있듯이 스팸식별에 대해 긍정적인 의견이 기존방식 17%에서 개선방식 85%으로 68% 향상된 것으로 조사 되었다. 기존방식으로는 스팸식별이 힘들다는 것으로 조사 되었으며 개

Table 6. The results of the questionnaire survey about the discrimination of spam using improved SMS method

	division	positive	negative	no diff.	total
academic background	college graduates	31	1	2	34
	high school diploma	40	9	2	51
	in college	13	1	1	15
age	20	13	1	1	15
	30	29	2	2	33
	40	26	4	0	30
	50	16	4	2	22
sex	man	60	7	1	68
	woman	24	5	3	32
occupational cluster	financial business	20	0	0	20
	student	13	1	1	15
	medium and small firm	13	0	2	15
	major firm	19	0	1	20
	housewife	4	5	1	10
	selfemployed	15	5	0	20
	total	84	11	5	100

선된 방식이 기존방식보다는 월등히 스팸식별에 도움이 되는 것으로 조사 되었다.

따라서 본 논문에 제시되는 개선방안은 금융기관에서 보내는 SMS메시지에 대해서 상당한 신뢰성을 제공할 것으로 판단된다.

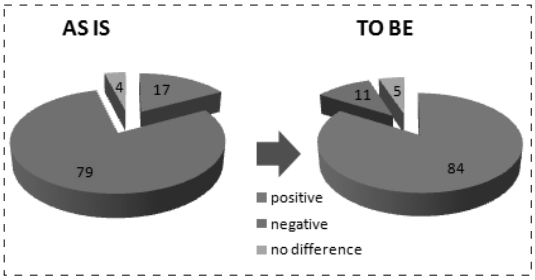


Fig. 6. Comparison Chart of the results of the questionnaire survey

3.5.4 기대 효과

개선방안의 적용 및 설문조사를 통해 알 수 있듯이 금융기관을 거래하는 고객들에게 SMS(LMS)발송시 개인이 등록한 "개인식별코드" 와 통신사가 인증한 금융기관명 2개의 인증을 통해 기존에 발송된 메시지에 대한 진위 여부판단의 문제점을 상당히 제거 할 것으로 보인다. 또한 금융기관으로부터 전송된 SMS메시지에 대한 안전성을 확보함으로써 스팸문자 식별 및 스미싱예방에도 큰 기여를 할 것으로 본다.

IV. 결 론

본 논문에서는 기존 스팸 및 스미싱 예방을 위해 각종 예방책을 사용했지만 계속해서 스팸 및 스미싱이 진화하여 발생하는 것을 알아보았다. 또한 통신사들의 스팸 차단 실험을 통해 기존 방식으로는 한계가 있다는 것을 알 수 있었다. 이 논문을 통해 제안한 방식을 직접 적용 및 설문조사를 통해 그 효과성을 입증하였다. 비용은 최소화하면서 스팸식별에는 효과적이 개선방안을 통해 스팸식별 및 스미싱을 예방하는데 크게 기여할 것으로 본다.

References

[1] Sang-ho Park, Jun-Hyeong Lee, "The smishing protection system proposal through Certification and pre-authorization," Journal of The Korea Institute of Information Security and Cryptology, pp. 1-2, 12. 2013

[2] "Spam distribution status analysis in the first half of 2013," KISA, pp. 2, Sept. 2013

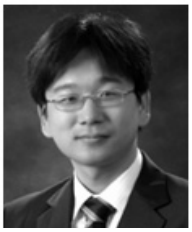
[3] "Anti-spam comprehensive measures," The Korea Communications Commission, pp. 11-12, Jan. 2011

[4] "Spam distribution status analysis in the first half of 2013," KISA, pp. 10, Sept. 2013

[5] "PKCS#5 v2.1: Password-Based Cryptography Standard," 1999. RSA Laboratories, pp. 8-10, Oct. 2006

〈저자소개〉

주 춘 경 (Choon Kyong Joo) 학생회원
1998년 2월: 강원대학교 전자계산학과 졸업
1998년 2월~현재: KB국민은행 전산정보본부
2013년 2월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 금융정보보안, 보안개발방법론



윤 지 원 (Ji Won Yoon) 정회원
2003년 2월: 성균관대학교 정보공학사 졸업
2005년 2월: University of Edinburgh. 정보학과 석사 졸업
2008년 11월: University of Cambridge 전자공학과 박사 졸업
2008년 2월~2009년 5월: University of Oxford. 로봇연구소 박사후과정
2009년 5월~2011년 5월.: University of Dublin 통계학과 연구원 및 강사
2011년 7월~2012년 8월.: IBM 연구소 정규 연구원
2012년 9월~현재: 고려대학교 정보보호대학원 조교수
〈관심분야〉 신호정보처리, 응용통계, 빅데이타 분석 기술, 도감청 탐지기술