JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 18, No. 12 : 2878~2884 Dec. 2014

Smishing 사고에 대한 Mobile Forensic 분석

박대우*

Analysis on Mobile Forensic of Smishing Hacking Attack

Dea-Woo Park*

Department of Conversing Technology, Hoseo Graduate School of Venture, Seoul 137-867, South Korea

요 약

2013년도부터 스마트폰을 이용한 Smishing(스미싱) 공격으로 인하여 피해가 발생하고 있다. 2014년 카드 3사의 1억4백만건 개인정보유출로 인하여 Smishing을 이용한 해킹 공격은 증가하고 있다. Smishing 해킹 공격과 연계된 개인정보의 탈취와 직접적인 금융 피해가 발생하고 있다. 본 논문에서는 Smishing 사고에 대한 실제 사례를 실험실에서 연구 분석하고 Mobile Forensic 분석을 실행한다. Smishing 해킹 공격의 기술적인 원리와 실제적인 사례 분석을 하고, Mobile Forensic 분석을 통하여 Smishing을 이용한 해킹 공격의 기술적인 증거자료의 입증과 모바일 포렌식 보고서를 작성한다. 본 논문을 통해 모바일 포렌식의 기술 발전과 Smishing 사고로부터 법정증거의 추출을 연구하여, 안전하고 편리하게 스마트폰을 사용 할 수 있는 안전한 국민생활을 위한 연구가 될 것이다.

ABSTRACT

The Smishing attacks are caused using smartphone since 2013. Smishing hacking attacks are increasing due to the approximately 104 million private information leakage incidents by the 3 domestic credit card companies occurred in January 2014. The Smishing attack occurred in conjunction with hacking illegal leakage of personal information and direct financial damage. In this paper, i am analyze real-world case studies in the lab and study accident on Smishing Mobile Forensic analysis. I am study of a real case Smishing hacking attacks. And studying evidence for a Mobile Forensic analysis of the technical principles of Smishing attacks. The study for the Mobile Forensic evidence proved the Smishing hacking attacks using Mobile Forensic technic and create Mobile Forensic reports. Through this paper, the research will be safe for the people living in the smartphone can be used safely and conveniently, with the development of Mobile Forensic technology, to study the extraction of Smishing accident evidences from the court.

키워드 : 스미싱, SMS, 모바일 포렌식, 해킹, 공격분석

Key word : Smishing, Short Message Service, Mobile Forensic, Hacking, Attack Analysis

접수일자 : 2014. 10. 06 심사완료일자 : 2014. 11. 12 게재확정일자 : 2014. 11. 27

* **Corresponding Author** Dea-Woo Park(E-mail:prof_pdw@naver.com, Tel:+80-10-8299-4455)
Department of Conversing Technology, Hoseo Graduate School of Venture, Seoul 137-867, South Korea

Open Access http://dx.doi.org/10.6109/jkiice.2014.18.12.2878 print ISSN: 2234-4772 online ISSN: 2288-4165

ⓒThis is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(http://creativecommons.org/li-censes/by-nc/3.0/) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.
Copyright Ⓒ The Korea Institute of Information and Communication Engineering.

Ⅰ. 서 론

2013년 1월부터 8월까지 통신, 인터넷을 통한 보이스 피싱(Voice Phishing), Smishing 등의 사기피해 건수가 2만8827건이고 피해액은 439억원에 달하는 것[1]으로 나타났다. 그림 1처럼 2014년 1월에는 고객의 개인정보의 유출 사건은 KB카드 5천300만건, 롯데카드 2천600만건, NH카드 2천500만건으로 총 유출은 1억4백만건이나 되는 수치의 개인정보 유출사고가 발생했다[2].

그림 1. 2014년 카드 3사 개인정보유출 사고 건수
Fig. 1 Number of accidents in personal information leakage from 3 cards in 2014(source : SBS News)

2014년 금융카드 3사 개인정보 유출로 인하여 Smishing사고의 위험이 증대되었다. Smishing 사고는 단문자서비스(SMS:Short Message Service)와 피싱(Phishing)의 합성어로, 2013년도부터 급속하게 사회문제화가 되기 시작하였다[3]. 스마트폰을 이용하여 Smishing 공격자는 피싱 사기를 유도하고, 스마트폰상으로 개인정보를 빼내거나, 본인도 모르게 소액결제를 하게하는 신종 휴대폰 사기 수법이다[4].

Smishing 사고는 휴대폰 또는 스마트폰에서 사회공학적인 SMS서비스가 URL(Uniform Resource Locator)을 포함하여 전송되며, 스마트폰 사용자가 웹사이트 링크인 URL을 누르게 되면, 바이러스 퇴치를 위한 애플리케이션 등을 무료로 다운받을 것을 권고[5] 받게 되나, 이 파일에는 트로이 목마 바이러스가 포함되어, 다운로드 즉시 해커의 조종으로 피싱 사이트로 이동 후[6] 클릭을 유도하여 스마트폰에서 개인정보가 유출되거나, 금융결제가 이루어지게 된다.

따라서 Smishing 사고에서 개인정보 유출과 금융피해가 발생함에 따라, Smishing 사고에 대한 해킹공격을 분석하고, 모바일 포렌식을 연구하여, 안전한 국민 생활을 위하여, 스마트폰 스미싱 공격 기술 분석과 책임소재 판단을 위한 증거추출에 관한 연구가 필요하다.

Ⅱ. 관련연구

2.1. 개인정보보호법

개인정보보호법은 2011년 3월 29일 제정을 하여 2012년 3월 30일부터 시행이 되었다. 이 법은 개인정보의 수집·유출·오용·남용으로부터 사생활의 비밀 등을 보호함으로써 국민의 권리와 이익을 증진하고, 나아가 개인의 존엄과 가치를 구현하기 위하여 개인정보 처리에 관한 사항을 규정함을 목적으로 한다.

개인정보보호법에 따르면 개인정보처리자는 개인정보의 안전환 관리를 위한 기술적·관리적·물리적 보호조치 등을 철저하게 수행해야 한다.

개인정보보호법의 내용의 일부 중 개인정보처리자가 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다.

개인정보처리자는 법 제21조에 따라 개인정보를 파기할 때에는 다음 각 호의 구분에 따른 방법으로 하여야 한다. 1) 전자적 파일 형태인 경우: 복원이 불가능한 방법으로 영구 삭제 2) 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우: 파쇄 또는 소각하여야 한다.

2.2. 최근 스미싱 사고 동향

2013년도부터 사회문제화 되기 시작한 Smishing 공격은 여러 이슈별로 국내에서 피해가 급증하였다.

특히 2014년 1월 금융권에서 발생한 대규모 개인정보 유출 사건 이후 '카드사 정보유출' 관련 Smishing이 새롭게 등장하여 2주 동안 173건의 신고를 기록하고 있다. 또 새해를 맞아 직장인의 관심을 끄는 '연말정산', '공인인증서 갱신'과 관련된 Smishing의 신고 건수도 2014년 1월부터 증가하는 추세다.

이러한 Smishing 공격은 실시간으로 이슈를 모니터링하고, 문자에 반영하여 사용자를 손쉽게 속이는 등 그 수법이 더욱 지능화되고 있다. 기존에는 문자 내 URL을 클릭하면 바로 악성 애플리케이션이 다운로드 되었으나, 피싱 사이트로 이동 후 클릭을 유도하는 수법도 최근 발견되고 있다.

Ⅲ. Smishing 공격 분석

Smishing 공격의 피해 원리를 알아보면, 해커는 SMS/MMS 등과 같이 메시지를 공격목표 사용자에게 보내고, 공격목표 사용자가 첨부된 링크를 클릭하게 되면, 악성코드가 포함된 애플리케이션을 다운로드 된다.

3.1. 2014년 카드 유출 사고 Smishing 사고 사례

2014년 1월, 금융카드 3사 개인정보 유출 사고가 발생했다. KB 카드 5천300만건, 롯데카드 2천600만건, NH카드 2천500만건이 사고 발생 건수[7]이다.

그림 2와 같이 개인정보유출에 따른 고객의 불안심리를 악용하여 개인의 금융거래정보를 빼돌린 후 금전을 가로채는 전형적인 Smishing 사기가 기승을 부리고 있다.

그림 2. 정보유출 사고를 가장한 Smishing 공격
Fig. 2 Smishing attacks of masquerade in Information leakage incidents

서울 검찰청 직원이라고 하면서 “최근 정보유출 사고에 당신이 연루됐으니 수사를 위해 요청하는 정보를 알려달라”며 계좌비밀번호와 보안카드 등을 빼내 5,000만원을 가로챈 사례가 있다.

최근 개인정보를 유출한 3개 카드사와 신용정보사가 보낸 것처럼 가장하면서 악성코드가 포함된 문자메시지를 발송해, 스마트폰을 감염시켜 카드사 직원이라고 하면서, “기존 고금리 대출을 저금리로 전환해 줄 테니 당신의 채무정보를 알려 달라”고 하고 또한 일부 채무는 우선 변제돼야 한다고 속여 가상계좌로 이체할 것을 요청해 500만원을 가로챈 사례이다.

3.2. Smishing 공격을 통한 무단 정보수집

해커가 Smishing 공격을 위해 사용자에게 보낸 SMS를 통하여 설치한 악성 애플리케이션을 실행시키면 “점검시간입니다. 불편을 드려서 죄송합니다”라는 문구로 가장하여 사용자를 안심시키고 실제로는 악성코드가 설치되어 SMS 탈취 서비스가 동작하고 있다.

Smishing 공격의 피해 원리는 해커는 SMS/MMS 등과 같이 메시지를 공격목표 사용자에게 보내고, 공격목표 사용자가 첨부된 링크를 클릭하게 되면, 악성코드가 포함된 애플리케이션을 다운로드 된다.

Smishing 공격자인 해커는 사용자가 눈치 채지 못하게, 스마트폰에 트로이목마와 같은 악성코드를 배포하여, 악성코드나 악성애플리케이션을 통해 사용자 스마트폰의 문자, 수신알람, 카메라, 전화번호, 금융정보, 개인정보 등과 같은 스마트폰의 기능을 제어하면서 정보를 절취하게 된다.

3.3. Smishing 공격으로 금융결제 사기

Smishing 공격을 위해 공격자 해커는 스마트폰 사용자들에게 악성 애플리케이션 설치용 단축 URL을 클릭적용 문자 메시지를 지인을 가장하여 사회공학적 방법으로 발송한다.

스마트폰 사용자가 문자메시지에 흥미를 느껴서 단축 URL을 클릭하면 악성 애플리케이션을 설치함과 동시에 스마트폰 단말기를 감염시킨다.

Smishing 공격자인 해커는 그림 3처럼 사용자가 눈치 채지 못하게, 스마트폰에 트로이목마와 같은 악성코드를 배포하여, 악성코드나 악성애플리케이션을 통해 사용자 스마트폰의 문자, 수신알람, 카메라, 전화번호, 금융정보, 개인정보 등과 같은 스마트폰의 기능을 제어하면서 정보를 절취하여 (해외)서버로 전송하게 된다. Smishing 공격자인 해커는 수집한 정보를 바탕으로 게임 사이트, 온라인 쇼핑몰 등 각종 인터넷 구매 사이트에서 소액 결제 서비스를 진행한다.

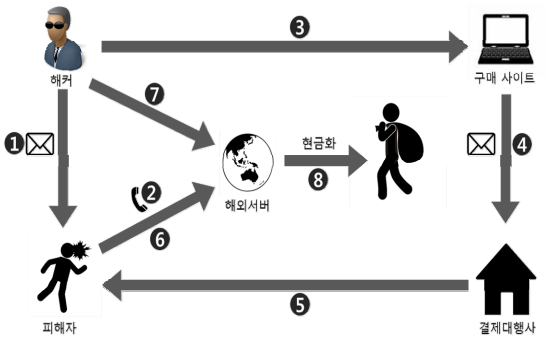


그림 3. Smishing 공격의 금융사기 원리
Fig. 3 Principle of Smishing attack for financial fraud

인터넷 구매 사이트에서 결제 대행사 등을 통해 본인 인증용 승인 문자 번호를 사용자 스마트폰으로 발송하게 되는데, 이때 악성 애플리케이션이 설치가 되어 있어 스마트폰에서 수신된 승인 문자 번호가 보이지 않게 조작하여, 스마트폰 사용자는 승인 문자가 온지도 모르고 그냥 넘어가게 된다[8].

공격자인 해커는 수신된 승인번호를 (해외) 서버로 몰래 전송을 시켜, 승인 번호를 가로 채어 정상적 인터넷 전자상거래 등 금융거래 절차를 수행한다.

Smishing 공격자인 해커는 적립된 사이버머니를 현금화하거나, 물건 등을 불법적으로 취득하여 금융 이득을 취한다. 스마트폰 사용자는 나중에 피해 금액을 청구 받게 되고 나서야, Smishing 공격을 당한 사실을 인지한다.

Ⅳ. Mobile Forensic 분석 및 보고서

4.1. 스마트폰에서 Smishing 증거 수집

Smishing 공격자인 해커와 공격 목표가 될 스마트폰을 실험실 환경에서 설정하고, 스미싱 공격 문자서비스와 URL이 포함된 공격을 목표 스마트폰으로 발송한다.

목표 스마트폰 사용자는 사회공학적 내용의 URL을 클릭하고 악성코드를 다운 받게 하여 스마트폰을 감염시킨다. 감염된 스마트폰을 PC와의 동기화를 통해 스마트폰에서 증거자료를 백업 받은 PC에 저장된 자료에 대한분석은 표 1과 같다.

표 1. 스마트폰의 증거 자료 분석
Table. 1 Evidence analysis of the smartphone data

	안드로이드	분석가능 프로그램	윈도우 모바일	분석가능 프로그램
전화 번호부	.spb	kies	.vcf	MITs
문자 메시지	.sme	kies	.sms	MITs, 메모장
일정	.ssc	kies	.csv	MITs, Excel
멀티 미디어	.mp3, .avi 등 (원본파일 형식)	windows media player, 곰플레이어	.skm	windows media player, 곰플레이어

스마트폰의 증거자료를 실험용 PC로 백업을 실행하고, 증거자료는 복사본을 만들어 분석을 실시한다.

다음은 Mobile Forensic을 위한 실험 스펙이다.

- Desktop 스펙 – Forensic 자료 추출용
  CPU : Inter(R)Core(TM) i3 @ 2.93GHz
  메모리 : 4.0GB RAM
  운영체제 : Windows 7 Home Premium K SP 1 32비트
- Laptop 스펙 – 분석용
  CPU : Inter(R)Core(TM) i7-2630QM @ 2.00GHz
  메모리 : 4.0GB RAM
  운영체제 : Windows 7 Ultimate K SP1 64비트
- Laptop 스펙 – 공격용
  CPU : Inter(R)Core(TM)i5-3230M @ 2.60GHz
  메모리 : 4.0GB RAM
  운영체제 : Windows 8.1 K 64비트
- WiBro 에그 스펙
  모델명 : KWI-B2200
  무선랜 : 802.11 b/g
  보안 : WEP, WPA, WPA2
- 스마트폰 Galaxy S IV 스펙
  모델명 : 삼성전자 SHV-E300S
  CPU : S5PC111 1GHz
  메모리 : 2G RAM, 32GB Storage
  운영체제 : Android Platform ver 4.4.2
  통신규격 : LTE(850/1800), WCDMA(1900/2100), GSM(900/1800/1900)
- AirPcap NX : 802.11 무선 네트워크 패킷 캡처

분석용 Laptop에는 스마트폰인 Galaxy S에서 데이터를 백업 받기위해 삼성모바일에서 제공해주는 Kies 3을 설치하였다. 패킷 분석을 위해 패킷 Wireshark와 Cain & Abel를 설치하였고, Forensic 자료 추출을 하기 위해 Forensic 프로그램인 Digital Evidence Analysis System(DEAS) 2와 Oxygen Forensic Suite 2014를 설치하였다.

- Samsung Mobile Kies v.1.0
- The Wireshark Network Analyzer v.1.8.2
- Cain & Abel v4.9.43 released
- Digital Evidence Analysis System 2
- Oxygen Forensic® Suite 2014 v.6.1

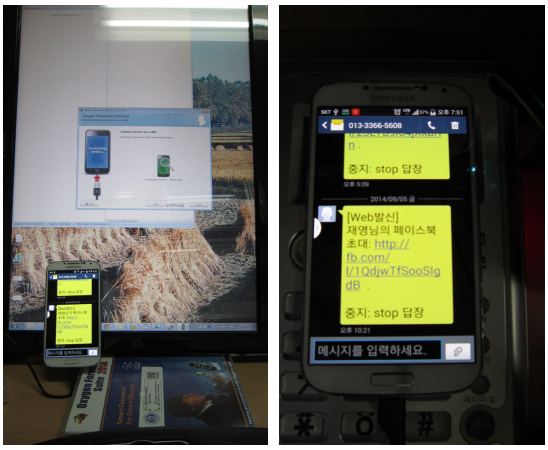


그림 4. Smishing 공격당한 스마트폰 포렌식
Fig. 4 Smartphone forensics attacked Smishing

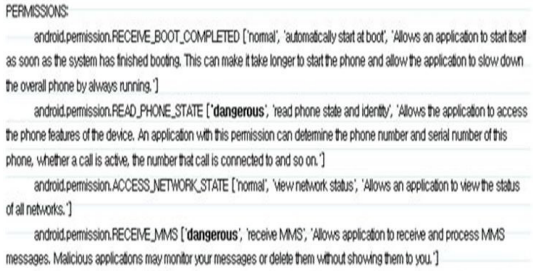
4.2. Mobile Forensic 증거자료 분석

그림 4처럼 Smishing 공격당한 스마트폰 포렌식을 위한 실험용 갤럭시 S IV는 안드로이드 운영체제를 탑재하고 있어, 삼성전자에서 제공하는 Kies 프로그램만 설치하면 PC에서 스마트폰의 증거 자료를 백업 및 수집할 수 있다. Kies 3 프로그램을 사용하여 갤럭시 S IV에서 SMS 증거자료를 백업받아 PC의 폴더에서 저장된 파일을 수집 및 확인해야 한다.

백업된 증거 자료를 살펴보면, SMS의 경우 .SME 파일로 압축되어 저장이 되고, 전화번호부인 폰북의 경우에는 .SPB 파일로 압축되어 저장 되고, 일정의 경우 .SSC로 압축되어 저장이 되어 진다. 그리고 멀티미디어 증거 자료들은 원형 그대로 저장되는 것을 볼 수 있다. Mobile Forensic 분석도구인 Oxygen 2014 Suit와 자바 decompiler을 통해 실험용 감염 스마트폰에서 추출한 증거자료의 백업본을 Forensic한다. Oxygen Forensic Suite 2014는 심비안, 윈도우 모바일, 안드로이드, iOS의 운영체제를 분석가능하며, 복사본 생성에는 MD5, SHA-1 알고리즘을 적용하여 복제 할 수 있다.

Smishing 공격에 감염된 스마트폰의 경우, 기본 정보, 전화번호부, 메시지, 통화기록, 캘린더, 파일브라우저를 통해 타임라인, 애플리케이션과 사전을 분석한다.

Smishing은 정상 애플리케이션을 가장하여 문자메시지 전송 후 설치되어 피해자의 문자를 가로채는 행위의 분서을 위해서는 소스파일 패킹, 언패킹 하는 'Apk tools', jar 파일 추출하는 'dex2jar'등을 시행한다.


PERMISSIONS:

android.permission.RECEIVE_BOOT_COMPLETED ['normal', 'automatically start at boot', 'Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.']

android.permission.READ_PHONE_STATE ['**dangerous**', 'read phone state and identity', 'Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.']

android.permission.ACCESS_NETWORK_STATE ['normal', 'view network status', 'Allows an application to view the status of all networks.']

android.permission.RECEIVE_MMS ['**dangerous**', 'receive MMS', 'Allows application to receive and process MMS messages. Malicious applications may monitor your messages or delete them without showing them to you.']

그림 5. 안드로이드 사용자 API 퍼미션
Fig. 5 User API permission in Android

그림 5처럼 안드로이드 스마트폰 사용자 API 퍼미션을 생성하고, 압축이 되어 있는 Apk 파일을 풀면 classes.dex 파일이 생성되된다. 'dex2jar'을 이용하여 dex 파일을 jar로 변환하고니서, Java Decompiler를 이용하여 Smishing 해킹 공격의 애플리케이션에 대한 기술적 구조를 분석 한다.

따라서 Smishing 분석 시스템인 'dex2jar'과 자바 decompiler를 이용하여 개인정보 유출 Smishing.apk 파일을 실험실에서 분석을 해본 결과, 그림 6처럼 공격자인 해커에게 안드로이드 스마트폰의 개인, 금융정보를 전송하여, Smishing 해킹공격이 일어나는 것을 확인하였다. 소스를 분석하여 설치 될 때 http://cn.zz.mu/Android_SMS/installing.php, Http Post 방식으로 스마트폰 번호를 전송하는 것을 확인할 수 있다.

패킷 분석 툴 Wireshark을 통하여 패킷을 분석한 결과, 해커의 서버로 스마트폰 사용자의 개인정보가 전송되는 것을 확인함으로써 Smishing 사고를 분석할 수 있다.

```
package com.example.adt;

import android.content.BroadcastReceiver;

public class BootBroadcastReceiver extends BroadcastReceiver
{
  static final String action_boot = "android.intent.action.BOOT_COMPLETED";
  static final String action_unlock = "android.intent.action.USER_PRESENT";

  public void onReceive(Context paramContext, Intent paramIntent)
  {
    if ((paramIntent.getAction().equals("android.intent.action.BOOT_COMPLETED"))
    {
      Intent localIntent = new Intent();
      localIntent.setClass(paramContext, CoreService.class);
      paramContext.startService(localIntent);
    }
```

그림 6. 스마트폰에서 정보유출 Smishing 공격
Fig. 6 Information leakage Smishing attack on smartphone

4.3. Mobile Forensic 보고서 작성

Smishing 공격으로 감염된 스마트폰에서 포렌식 증거 자료를 확인하였을 경우, 증거를 수집하여 수사보고서인 포렌식 보고서 형태로 작성한 다음 법정에 증거기록으로 사용한다.

스마트폰에서 포렌식 증거 자료는 법정에서 인정하는 수사관이 인증된 포렌식 툴과 포렌식 기술과 공공의 장소나, 현장에서, 포렌식 증거 자료를 생성하고, 백업 프로그램을 통해 추출할 수 있는 증거 자료의 원본성과 무결성을 입증하기 위해 Hash 함수 값을 비교하여, 무결성을 입증한 자료를 표 2와 같이 포렌식 보고서를 작성하여 검사나 법정에 제출한다.

Smishing 사고에 대한 법정 증거 자료를 문서화 작업으로서 포렌식 분석 보고서를 프린트하거나, pdf파일로 변환하여, 법정 증거자료로서 제출한다.

표 2. 모바일(스마트폰) 포렌식 보고서
Table. 2 Mobile(Smartphone) Forensic Report

(양식 제 4 호)

Forensic 보고서

접수일자 접수자 요청대상 관리번호	2014. 08 29. 박대우 호서대학교 벤처전문대학원 2014 제 09호	
분석일시 분석장소	2014. 07. 30. ~ 2014. 11. 29. 호서대학교 벤처전문대학원 HFITC Lab	
분석대상 제조사 일련번호 S / N 운영체제	Samsung Galaxy S IV (SHV-E300S) 삼성전자 0010447 R1AB555700 Android 4.4.2	
분석 System	CPU	Intel(R) Core(TM) i3 CPU
	RAM	4 GB
	OS	Microsoft Windows 7 - 32 bit
	HDD	Samsung HD502IH (500 GB)
Foresic Software	EnCase, Oxygen, Wireshark	
프로그래밍 언어	MicroSoft Visual C, Java	

호서대학교 벤처전문대학원 HOSEO GRADUATE SCHOOL OF VENTURE Page 1

Ⅴ. 결 론

최근 스마트폰 사용량의 증가와 함께, Smishing 해킹 공격과 연계된 개인정보의 탈취와 직접적인 금융 피해가 발생하고 있다.

본 논문에서는 스마트폰에서 Smishing 사고에 대한 실제 사례를 실험실에서 연구 분석하고, Mobile Forensic 분석을 실행한다. Smishing 해킹 공격의 기술적인 원리와 실제적인 사례 분석을 하였다. 또한 Mobile Forensic 분석을 통하여 Smishing을 이용한 해킹 공격의 기술적인 법정의 증거자료의 입증을 위한 모바일 포렌식 보고서를 연구하고 작성하였다.

향후 연구로는 스마트폰과 인터넷과 연계된 스미싱 공격에 의한 개인정보 유출과 금융거래 피해를 예방하는 보안 방법을 강구한다.

감사의 글

본 연구는 2014년도 호서대학교 교내학술비 지원에 의하여 이루어진 연구로서, 관계부처에 감사드립니다.

REFERENCES

[1] In-Woo Park, Dea-Woo Park, “A Study on the Analysis and Security Measures for Smishing Hacking Attacks”, *International Conference on Computing and Convergence Technology*, Oct, Korea, 2013.

[2] In-Woo Park, Dea-Woo Park,"A Study of Intrusion Security Research and Smishing Hacking Attack on a Smartphone", *Journal of the Korea Institute of Information and Communication Engineering*, vol. 17, no. 2, pp. 399-406, Mar, 2013.

[3] Korea Internet & Security Agency, “http://spam.kisa.or.kr/kor/smishing/smishingWay.jsp”, Korea, 2014.

[4] Korean National Police AgencyCyber Bureau,"Coping with smishing", Available: http://www.netan.go.kr/, the National Police Agency, 2013.

[5] Dea-woo Park, "Guideline for Countermeasures against Smishing Incident", CJK IT Standards Meeting, April,

Korea, 2014.

[6] Korea Internet & Security Agency,“Monthly analysis and trend of Internet incidents : March, May, June”, Korea Internet & Security Agency, Korea, March, May, June 2013.

[7] Jin Shin, Dea-Woo Park,"A User’s Guide for Counter-measures against Smishing Incident", *Information An International Interdisciplinary Journal*, vol. 17, no. 11(B), pp. 5683-5688, Nov, 2014.

[8] Dea-Woo Park,"Forensic Analysis of Smishing Hacking Attack in Smartphone", *Information An International Interdisciplinary Journal*, vol. 17, no. 11(B), pp. 5689-5694, Nov, 2014.

박대우(Dea-Woo Park)

2004년 : 숭실대학교 컴퓨터학과(공학박사)
2004년 : 숭실대학교 겸임교수
2006년 : 정보보호진흥원(KISA) 선임연구원
2007년 ~ 현재 : 호서대학교 벤처전문대학원 교수
※ 관심분야 : Hacking, Forensic, CERT/CC, 침해사고대응, E-Discovery, 정보보호, 이동통신보안, IT융합보안, 서비스보안 표준화, 국가사이버안보정책