JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 19, No. 11 : 2615~2622 Nov. 2015

Mobile Smishing 해킹 동향 분석 및 보안대책

박대우*

Analysis of Mobile Smishing Hacking Trends and Security Measures

Dea-Woo Park*

Department of Conversing Technology, Hoseo Graduate School of Venture, Seoul 06711, South Korea

요 약

스마트폰 태블릿 PC와 같은 모바일 장치를 이용하여 인터넷뱅킹과 전자상거래는 물론 본인의 업무까지 처리하고 있다. 모바일 기기의 가용성과 편리성은 높아가고 있지만, SNS나 문자 이메일을 이용한 Smishing 금융사기사건과 개인정보유출 등 범죄사건도 많이 발생하고 있다. 스마트폰에서 Smishing 사고는 2013년부터 급격하게 증가되어 MERS 감염 사건, 지뢰도발 사건, 추석의 택배 등의 사회공학적 방법을 이용하여 교묘하게 발생하고 있다. 본 논문에서는 2014년 이후의 모바일 장치에서의 Smishing 해킹 동향을 분석한다. 사회적 이슈와 관련하여, 모바일 사용자들에게 금융사기로 이어지는 Smishing 해킹 공격의 프로세스를 분석한다. 그리고, Mobile Smishing 해킹에 대한 보안 방법과 금융 피해의 대책을 제시한다.

ABSTRACT

Using the mobile device, such as Smartphones tablet PC, online banking and e-commerce, as well as process and to their work. While going to high availability and convenience of mobile devices castle, SNS, letters, using an email Smishing financial fraud and leakage of personal information such as crime has occurred many. Smishing smartphone accidents increased sharply from 2013, MERS infection cases, landmine provocative events, such as the delivery of Thanksgiving has occurred cleverly using social engineering techniques. In this paper, i analyze the trends in Smishing hacking attacks on mobile devices since 2014. With regard to social issues, it analyzes the process of hacking attacks Smishing leading to financial fraud to mobile users. And, in this paper, i propose a secure way and measures of financial damage for mobile Smishing hacking.

키워드 : 모바일 해킹, 스마트폰, 범죄, 스미싱, 보안 대책

Key word : Mobile Hacking, Smartphone, Crime, Smishing, Security Measures

Received 02 October 2015, **Revised** 30 October 2015, **Accepted** 09 November 2015

*** Corresponding Author** Dea-Woo, Park(E-mail:prof_pdw@naver.com, Tel:+82-2-2059-2352)
Department of Conversing Technology, Hoseo Graduate School of Venture, Seoul 06711, South Korea

Open Access http://dx.doi.org/10.6109/jkiice.2015.19.11.2615 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

Smishing(스미싱) 사고는 2013년도부터 한국에서 급속한 사회문제가 되기 시작하였다. Smishing 사고는 스마트폰 태블릿 PC와 같은 모바일 장치에서 사용하는 단문자 서비스(SMS;Short Message Service)와 피싱(Phishing)의 합성어로, ① '무료쿠폰 제공'등의 문자메시지 내 인터넷주소를 클릭하면, ② 악성코드가 스마트폰에 설치되어 ③ 피해자가 모르는 사이에 소액결제 피해 발생 또는 개인의 금융정보를 탈취[1]한다.

최근 스마트폰, 태블릿 PC, 노트 북과 같은 Mobile 단말기를 이용하여 인터넷뱅킹과 전자상거래를 하고 있다. 발견된 Smishing 공격 문자는 스마트폰의 보안 강화, 예비군, 민방위 훈련, 유머를 활용하는 등 지인이나, 공공기관을 사칭하여 정치적, 사회적 이슈를 가장해 악성코드의 설치를 유도하는 '사회공학적 기법'이 주를 이루고 있다[2].

따라서 사회적 이슈가 되는 스마트폰, 태블릿 PC,에서의 Mobile Smishing 해킹에 대한 공격 트렌드를 분석하고 기술내용을 파악한다면, Mobile Smishing 해킹에 대한 보안 방법과 보안 대책이 생성 될 수 있다.

본 논문에서는 2014년 이후의 모바일 장치에서의 Smishing 해킹 공격에 대한 동향을 분석한다. 사회적 이슈와 관련하여, 모바일 사용자들에게 금융사기로 이어지는 Smishing 해킹 공격의 프로세스를 분석한다. 해킹 공격에 대한 분석 자료를 토대로 방어적인 보안 방법과 적극적인 예방적 보안대책에 대해 연구한다.

Ⅱ. 관련 연구

2.1. Smishing

SMS와 Phishing의 결합어로 Smishing은 스마트폰 태블리PC에서 문자메시지에 연결된 URL 링크 수단을 이용하여 피싱하는 방법을 말한다. 공격자는 스마트폰과 같은 (이동)통신단말기에서 사회공학적 문자메시지에 포함된 URL을 클릭하게 하여, 소액 결제, 자동 결제, 금액 이체 등 해킹 침해사고를 발생시켜서 금융 피해를 발생시킨다. 또한 Smishing 문자메시지에 포함된 URL 링크를 클릭하면, 악성 코드를 자동으로 다운로드하면서, 사용자의 의도를 회피하면서, 트로이목마 등 해킹 공격 툴을 이용하여 스마트폰을 통제하고, 침해사고를 일으켜, 금융피해를 발생시키게 된다[3].

2.2. 사회 공학(Social engineering)적 기법

사회공학은 정보보안 측면에서 기술적인 방법이 아닌 사람들 간의 기본적인 신뢰성을 이용하여 목표시스템에 관여하는 관리자(사람)을 속여 비밀 정보를 획득하는 인적 보안의 취약성을 이용하는 기법이다. 컴퓨터 통신보안에서 정보에 접근 권한이 있는 담당자의 지인처럼 가장하여 이메일, 스마트폰의 SNS수단을 통해 공격대상자의 정치적, 사회적 이슈를 가장해 경계심을 약하게 하거나, 권한을 도용하기 위해 속이는 방법의 하나이다[4].

2.3. 개인정보보호(Personal Information Protection)

개인정보보호란 생존하는 개인에 관한 중요 정보를 보호하는 것으로서 성명, 주민등록번호, 여권번호, 운전면허번호, 주소, 전화번호, 생년월일 등으로 개인을 식별할 수 있는 부호, 문장, 음성 및 영상 등의 정보를 보호하는 것을 말한다. 현재 개인정보보호법이 시행중에 있다[5].

Ⅲ. Mobile Smishing 해킹 동향 분석

3.1. 2014년 Mobile Smishing 해킹 동향 분석

예비군/민방위 훈련 문자는 2014년 2월에 가장 많이 유포된 Smishing 문자 유형으로, 2월에 국방부가 주의를 발표한 이래, 3월 첫째 주에 발견된 Smishing 악성코드의 약 66%를 차지하였다.

또한, 봄철을 맞아 결혼과 건강에 화두를 두고, '웨딩'과 '건강 암 검진 대상' Smishing 도 등장 하고 있다. "[청첩장] 저희 두 사람 하나가 되기를 약속하려 합니다. 청첩장보기 w*w.c**.do/Y**, "고객님은 2014년 암 검진 대상이오니, 꼭 암 검진 받으십시오. H**p://goo.**/M3a**u" 등의 시즌 별 문구가 발견되기도 했다.

Fig. 1, Fig. 2, Fig. 3, Fig. 5, Fig. 6은 경찰청에서 증거 수집하여 분석한 스마트폰에서 사이버 범죄와 Smishing에 관한 내용[5]이다.

Fig. 1 Smishing issue in 2014

개인정보 유출과 스마트폰 뱅킹 보안에 대한 관심이 사회적 이슈가 되고 있어서, 스마트폰 사용자들은 무심코 URL을 클릭하기 쉽다. Smishing 문자 내 URL클릭 시 금융정보와 같은 민감한 개인정보 유출이나 소액결제, SMS[문자메시지]와 주소록 유출 및 전화송수신 감시 등 피해[6]가 발생할 수 있다.

Fig. 2 Smising using X-mas, End of the year in 2014

Fig. 2처럼 2014년 연말과 성탄절 시즌을 악용한 Smishing 공격이 연말연시 분위기를 악용한 사회공학적 내용을 이용하여, Smishing 공격이 있었다.

3.2. 2015년 Mobile Smishing 해킹 동향 분석

2015년 연초의 휴일과 연말에서 연초로 이어지는 이동 중에 분실물 관련하여 스마트폰에서 Smishing 해킹 공격이 발생하였으며, 2015년 1월 역시 국민들에게 화두가 되었던, 연말정산 관련하여 Smishing 해킹 공격이 발생하여 많은 피해를 입었다.

Fig. 3 Smishing using MERS issue in 2015

Fig. 3은 2015년 6월 국가적인 메르스(MERS-coV) 감염으로 국민과 국가 경제에 큰 영향을 미치고, 국내분만 아니라, 외국인의 방문객의 감소로 인한 경제적 타격을 입었다. 이를 이용한 메르스 Smishing 해킹 공격이 발생하여 많은 피해를 입었다.

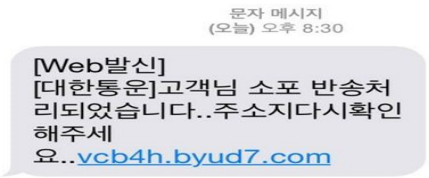

Fig. 4 Contents of Thanksgiving Delivery Service Smishing attack

Fig. 4는 2015년 9월 추석을 즈음하여 급격히 증가한 택배서비스를 이용한 사회공학적 Smishing 해킹이 발생하였다. 2015년 추석을 전후해서 '택배 반송처리 주소지 재확인' 문구를 사용해 유명 택배업체를 사칭한 Smishing이 다량 발견되고 있다.

3.3. Mobile Smishing 해킹 기술 분석

스마트폰에서 Smishing 사고가 발생하면, 경찰청 사이버수사대, KISA, 융감독원에 신고를 하고, Smishing 공격을 당한 스마트폰에서 Smishing 공격 기술적 분석을 한다. 스마트폰에서 Smishing 사고를 분석해 보면, Smishing 사고를 발생시키는 악성코드는 정보의 탈취와 정보의 삭제 등 사이버공격을 목적으로 컴퓨터 사용자의 중요정보를 빼가는 프로그램이다. 해킹 기능을 가지고 있어 인터넷을 통해 감염된 컴퓨터의 정보를 외부로 유출하는 것이 특징이다. 그러나 바이러스처럼 다른 파일을 전염시키지 않으므로 해당 파일만 삭제하면 치료가 가능하다. 트로이 목마는 인터넷에서 다운로드 파일을 통해 전파되는데, 사용자가 입력한 자판 정보를 외부에 알려주기 때문에 신용카드번호나 비밀번호 등이 유출될 수 있다.

Fig. 5 Method of use to detect smishing

일반인들은 Fig. 5처럼 스마트폰에서 경창청에서 배포한 경찰청 사이버캅 애플리케이션(앱)을 온라인으로 다운로드 하고 설치하면 Smishing 탐지가 가능하다.

Ⅳ. Mobile Smishing 해킹 보안 대책

스마트폰 태블릿PC에서 Smishing 피해발생의 원리와 Smishing 내용 분석을 통해 Smishing 피해 예방을 위하여 Fig. 6과 같이 사용자에 대한 보안 방법과 보안 대책을 작성한다.

Fig. 6 Menu of category in prevention strategies on Cyber Cop Application

4.1. Smishing 사고에 대한 보안 인식과 사회적 대응 방법

- 온라인에서 재 발급되지 않는 공인인증서를 사용한다 (개인정보 탈취로 공인인증서 유출 피해가 발생할 수 있기 때문에, 금융기관에서 본인 신분 확인 후 인증서를 발급받아 사용하는 것이 안전하다.).
- 공인인증서를 보안토큰에 보관한다(보안토큰은 비밀 정보가 장치 외부로 복사 또는 재생성 되지 않아 공인인증서의 유출을 막는다.).
- 소셜 네트워크 사이트에 자신에 대한 너무 많은 정보를 게재하지 않는다.
- 개인이 온라인으로 서명한 모든 자료는 우편을 통하여 받을 수 있도록 조치한다.
- 출처가 미확인 문자메시지의 링크주소(숫자 열 포함) 클릭을 주의한다(지인에게서 온 문자도 인터넷 주소가 포함된 경우 클릭 전에 확인한다.).

- 백신프로그램 설치하고, 업데이트 및 실시간 감시 상태 유지한다(이동통신사・보안업체가 제공하는 Smishing 방지앱을 설치한다.).
- 보안승급 명목으로 요구하는 보안카드번호 입력을 금지한다(스마트폰 등 정보저장장치에 보안카드 사진·비밀번호 등 저장을 하지 않는다.).
- 예방서비스를 사용한다(공인인증서 PC지정, SMS 사전인증 등 금융회사 제공 보안강화 서비스 사용한다.). Smishing 사고에 대한 사회적 대응은 보안에 대한 기본적인 인식의 강화, Smishing 사고에 대한 정보공유, 대응방안 협력과 시행을 통해 이루어진다.
- 제3자에게 개인정보를 제공하는 것을 신중히 검토하고, 금지를 권고한다.
- 스마트폰 제조사와 협조하여 해킹 피해 축소 및 개인정보보호를 위한 대책 마련한다.
- 스마트폰 발신처가 명확하지 않은 곳으로부터 전달되는 문자메시지의 단축 URL은 클릭하지 않고, 클릭을 하였더라도 애플리케이션을 설치하라고 하는 경우에는 설치하지 않는다.
- 인식의 강화는 Smishing 으로 인한 개인정보의 탈취를 예방하기 위한 금융권, 정보보호관련 기관의 인식제고를 강화함과 동시에 예방 활동을 포함한다.
- 관련 공공 기관은 Smishing 에 대한 일반적인 정보를 고객에게 신속히 전달하고, 가짜 사이트에 유도되더라도 사용자가 직접 사이트의 유무를 판단할 수 있도록 적극적으로 대처하는 전략이 필요하다.
- 정보공유는 위험 요소의 확산을 방지하고 피해를 최소화하기 위한 정책의 수립 및 계몽이 필요하다. 관련기관은 일괄성 있는 보안 알림 기능을 수립하여 이용자에게 전파하고, 최신 보안 패치를 적용 할 수 있도록 지속적으로 관리해야 한다.
- 대응방안은 사고 발생 시 신속한 대처 방법을 통하여 피해를 최소화 하는데 있다. 이를 위해 적절한 대응을 위한 관련 기관의 자율적인 협의체 구성 및 정보를 공유하며, 신속한 신고를 할 수 있도록 단일 창구 방법을 제공한다.
- 기타 사항으로는 금융 회사와 같은 금융 기관은 고객들이 유의할 사항 등을 홈페이지에 게시하고, 이메일 발송, SNS 안내 등 홍보 활동을 강화한다.

4.2. Smishing 사고에 대한 기술적 보안

- 공인인증서는 가급적 외부 저장소에 저장한다.
- 금융기관에서 발급한 보안카드를 안전하게 관리한다(보안카드를 사진을 찍어 보관하거나 복사해서 가지고 다니지 않고, 보안카드 번호 전체를 입력하라는 요구에는 응하지 않는다.).
- 의심되는 이메일이나 게시판의 글은 열어보지 말고, 첨부 파일은 열람 또는 저장하기 전에 백신 검사한다.
- 스마트폰 애플리케이션을 설치할 때는 해당 업체의 운영체제(OS)에서 제공하는 공식 스토어에서 검증된 애플리케이션만을 사용한다.
- 안드로이드 스마트폰에서 루팅이나 아이폰에서 탈옥을 사용하여 관리자 권한을 변경하지 않아야 상대적으로 보안성이 강화된다.
- iPhone 스마트폰의 탈옥을 금지한다.
- iPhone 스마트폰의 경우 애플리케이션 인증을 받고 애플스토어로 등록하고, 다운 받을 시, 앱스토어에서 바이러스 검사를 한다.
- iPhone은 폐쇄적 운영체제로, 애플리케이션 설치가 앱스토어를 통한 설치만 가능하다.
- Fig. 7처럼 스마트폰 사용자들은 본인의 스마트폰의 보안 설정을 강화한다. 환경설정> 보안> 디바이스 관리> 알 수 없는 출처에 체크가 되어 있을 경우 해제 ; 애플리케이션 설치 전 확인> 체크 ; 일반-URL에 연결 허용> 체크 해제).

Fig. 7 Smartphone Settings > Unknown sources> Disable

- 스마트폰에 설치된 애플리케이션이 위험한 작동을 할 수 있는지에 대해 경고해 주는 기능을 가지는 통신사가 추천하는 모니터 애플리케이션을 설치한다.
- 자체 보안시스템 바운서(Bouncer : 새로운 애플리케이션이 등록되면 이를 분석해 악성 코드, 스파이웨어, 트로이목마 등이 애플리케이션에 포함돼 있는지를 확인한다)를 도입, 애플리케이션 마켓에 등록된 애플리케이션을 검색해 악성 소프트웨어를 찾아내는 시스템을 작동한다.
- 애플리케이션과 달리 사전검증 없이 애플리케이션을 올릴 경우 바운서를 미작동한다(애플리케이션이 아닌 다이렉트 설치의 경우 보안 효과가 적다.).
- 신뢰할 수 있는 보안업체에서 제공하는 그림 17과 같은 모바일 백신을 스마트폰에 설치하고 실시간 감시 기능을 활성화하며 정기적으로 업데이트 후 검사를 실시한다.

4.3. Smishing 사고에 대한 금전피해 보안 대책

- 평소에 스마트폰을 통한 소액 결제를 자주 이용하지 않는다면, 자신이 사용하는 통신사 고객센터나 공식 홈페이지를 통해 Fig. 8처럼 “휴대폰 소액 결제 서비스”를 미리 차단 해두거나 통신사 홈페이지에서 소액 결제 한도를 0원으로 변경한다.

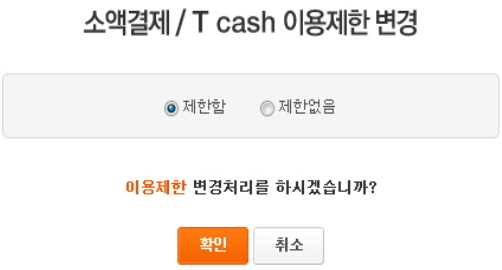

Fig. 8 Change of micro payment limit

- 국내 각 통신사 고객센터 또는 통신사 인터넷홈페이지를 이용하여 휴대폰 소액 결제를 원천적으로 차단을 함으로써 해커에게 Smishing 공격을 당했더라도 금융사고에 대한 예방이 가능하다.
- 스마트폰 내 Smishing 문자발송 차단 : 문자메시지로 들어가서 ‘설정 > 스팸 메시지 설정 > 스팸 문구로 등록’을 클릭한다.
- 스마트폰용 백신 프로그램을 설치하여 악성 코드 설치를 차단한다.
- 스마트폰의 보안설정 강화방법 : 환경설정 > 보안 > 디바이스 관리 > ‘알 수 없는 출처’에 V체크가 되어 있다면 해제한다.
- T스토어 – 올레마켓 – U+애플리케이션 마켓 등 공인된 오픈 마켓을 통해 애플리케이션을 설치한다.

【금전피해가 발생한 경우】

<악성파일 삭제> 스마트폰 내 ‘다운로드’ 앱 실행 → 문자를 클릭한 시점 이후, 확장자명이 apk인 파일 저장 여부 확인 → 해당 apk파일 삭제한다.

<악성파일이 삭제되지 않는 경우>

휴대전화 서비스센터 방문, 스마트폰 초기화한다.

<피해 구제> 경찰서에서 발급받은 ‘사건사고 사실 확인원’을 이통사, 게임사, 결제대행사 등 관련 사업자에게 제출한다.

【금전피해가 발생하지 않은 경우】

<악성파일 삭제> 서비스 센터를 방문하여 스마트폰에 설치된 악성파일 삭제한다.

<사용자 예방 조치> 사용자 예방 관리 지침에 수록된 내용을 수행한다.

4.4. Smishing 사고에 대한 금전피해 법적 대응

【전기통신 금융사기 피해 방지 및 피해금 환급에 관한 특별법 시행령】

스마트폰 사용자들이 전자거래로 인한 피해가 발생함에 따라 2011.09.30. 에 “전자금융사기 피해금 환급에 관한 특별법”이 지정되었다. 그러나 최근 들어 방법과 수단이 더 교묘해지고 피해자가 다양해짐에 따라 2014.07.22. “전기통신 금융사기 피해 방지 및 피해금 환급에 관한 특별법 시행령” 개정안이 국무회의를 통과하였다.

동 시행령은 “전기통신 금융사기 피해방지 및 피해금 환급에 관한 특별법 제정”(’14.01,27 개정, ’14.07.29 시행)의 후속 조치로, 개정법률 시행일과 동일하게 ’14.07.29부터 시행 되었다.

이 개정안에 보이스 피싱, 파밍(Pharming), 대출사기 등이 포함되었으며, 전기통신사기 관련 금융위원회의 적극적 대응의무 부여, 사기 이용 우려가 있는 금융거

래의 확인절차 강화 등으로 국민의 금융자산 보호가 한층 강화 되었다.

Smishing에 대한 다양한 법제도적 대응을 준비하고 있지만 법적 대응에는 온라인 범죄자들의 색출의 어려움, 재판권 획득의 어려움, 판결내용 증명의 어려움, 범죄증거 소멸의 용이 등 해결 과제가 많다. 특히 신종 해킹 기술의 발전으로 인한 새로운 범죄의 출현은 이를 더 힘들게 하고 있다. 이를 해결하기 위해서는 범정부 차원의 대응책이 마련되어야 하며, 피해 요소에 대한 Risk를 평가하고, 위험을 감소시키기 위한 정책이 수립되어야 한다.

【경찰서 민원실과 경찰청 사이버수사대】

스마트폰에서 Smishing 피해를 입은 사용자는 경찰서 민원실과 경찰청 사이버수사대를 통하여, 아래와 같은 절차를 통해 법적 대응을 할 수 있다.

- 가까운 경찰서 민원실을 방문하고, 스마트폰에서 Smishing 피해 내용을 접수하여, 법적 구제를 통해 금전적 피해를 보상 받는 방법이다.
- 경찰청 사이버범죄 신고 방법은 범죄신고 시스템을 이용, Smishing 금전적 피해를 접수하는 방법이다.
- 사이버 범죄 신고 시스템은 처리 기간이 14일 이내이고, 관할 경찰관서 직접 방문하는 경우는 즉시 처리해준다.
- 범죄 신고 시 담당관서 지정까지 일정 기간이 소요되며, 담당 수사관이 지정되면 형사사건 여부를 검토 후 정식 사건 접수 시 수사가 진행한다.
- 경찰청 사이버안전국 대표 전화 : 1566 – 0112.
- Smishing 피해 확인 증명서를 발급받아 올 경우, 모든 피해 금원을 환불 받을 수 있다.

V. 결 론

본 논문에선 2014년 발생한 예비군/민방위 훈련 관련 문자로 출발하여, 봄철에는 '웨딩'과 '건강 암 검진 대상' Smishing 공격, 청첩장보기, 스마트폰 뱅킹 보안 관련, 성탄절, 연말연시 분위기를 악용한 Smishing 공격을 조사 분석 하였다. 2015년에 발생한 Smishing 공격분실물 관련, 연말정산 관련, 메르스 감염 관련, 추석 택배서비스에 관련한 Smishing 해킹 공격의 동향을 분석하였다. 그리고, Mobile Smishing 해킹에 대한 보안 방법과 금융피해를 입은 대책을 제시하였다.

ACKNOWLEDGMENTS

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) Funded by the Ministry of Education in 2015 (No. 2013R1A1A 2010118).

REFERENCES

[1] 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.

[2] Dea-Woo, Park. Sung-Young Yang, "Hacking Aattack Trends Analysis of Mobile Smishing and Security Measures," in *Proceeding of the Conference on Information and Communication Engineering*, Busan: South Korea, pp. 154, Oct. 2015.

[3] Dea-Woo, Park, Analysis on Mobile Forensic of Smishing Hacking Attack, *Journal of the Korean Institute of Information and Communication Engineering*, vol. 8, no. 12, pp. 2878-2883, Dec. 2014.

[4] Dea-woo Park, "Guideline for Countermeasures against Smishing Incident", CJK IT Standards Meeting, South Korea, April, 2014.

[5] Telecommunications fraud (Phishing, Pharming, Smishing, hacking memory, etc.), cybercrime reporting/consultation Crime Information Network, [Internet]. Available: http://cyberbureau.police.go.kr, Oct, 2015.

[6] Korean National Police Agency Cyber Bureau,"Coping with smishing", [Internet]. Available: http://www.netan.go.kr/, the National Police Agency, Jun, 2015.

박대우(Dea-Woo Park)

2004년 : 숭실대학교 컴퓨터학과(공학박사)
2004년 : 숭실대학교 겸임교수
2006년 : 정보보호진흥원(KISA) 선임연구원
2007년 ~ 현재 : 호서대학교 벤처대학원 교수
※관심분야 : Hacking, Forensic, CERT/CC, 침해사고대응, e-Discovery, 국가사이버안보, Cybersecurity, 정보보호, 이동통신보안, 융합보안, IT융합