Journal of KIIT. Vol. 17, No. 10, pp. 93-99, Oct. 31, 2019. pISSN 1598-8619, eISSN 2093-7571 93
http://dx.doi.org/10.14801/jkiit.2019.17.10.93

스미싱 예방을 위한 악성문자훈련시스템 설계 및 구현

최학규*, 김황래**

Design and Implementation of a Malicious SMS Training System for Preventing Smishing

Hark-Kyu Choi*, Hwang-Rae Kim**

요 약

IT 기술 발전과 스마트폰 보급률의 증가로 인해 사이버범죄는 공공기관과 기업뿐만 아니라 일반 국민에게까지 막대한 피해를 주고 있다. 그 중 스미싱(Smishing) 공격으로 인한 피해는 노년계층, 초·중·고 학생계층, 20대 사회 초반 계층에서 두드러지게 나타나고 있다. 스미싱 공격을 차단하기 위한 다양한 기술들이 연구 및 개발되어 보급되고 있으나 이들 기술은 스미싱 공격 차단에만 집중되어 개발되었기에 사회공학 기법을 이용한 스미싱 공격을 예방하기에는 한계가 있다. 본 논문에서는 스미싱 공격 예방을 위한 보안교육 도구로써 악성문자훈련시스템(MSTS)을 설계 및 구현하였고 MSTS 시스템을 통한 스미싱 훈련과 보안교육으로 스미싱 공격에 대한 예방효과를 확인하였다.

Abstract

Due to the development of IT technology and the increasing penetration of smartphone, cybercrimes have caused enormous damage not only to public institutions and corporations but also to ordinary people. In particular, the damage caused by Smishing attacks is prominent in the elderly, elementary, middle and high school students, and those in their early 20s. Various techniques for blocking Smishing attacks have been researched, developed, and spread. However, since these techniques are developed only for blocking Smishing attacks, there is a limit to prevent Smishing attacks using social engineering techniques. This study designed and implemented a malicious SMS training system(MSTS) as a security training tool for preventing Smishing attacks, and confirmed the prevention effect on Smishing attacks as Smishing training and security training through the MSTS system.

Keywords
smishing, sms training system, malicious sms, information security

* 공주대학교 컴퓨터공학과
- ORCID: https://orcid.org/0000-0002-3124-8485
** 공주대학교 컴퓨터공학과(교신저자)
- ORCID: https://orcid.org/0000-0001-9378-4139

· Received: Jul. 22, 2019, Revised: Sep. 27, 2019, Accepted: Sep. 30, 2019
· Corresponding Author: Hwang-Rae Kim
Dept. of Computer Engineering, Kongju National University, 1223-24 Cheonan Daero, Seobuk Gu, Cheonan-Si, Chungnam, Korea,
Tel.: +82-41-521-9227, Email: plusone@kongju.ac.kr

Ⅰ. 서 론

IT 기술의 발전과 스마트폰의 보급률 증가로 인해 매년 사이버범죄는 증가하고 있다. 사이버 공격은 이제 공공기관뿐 아니라 민간기관 또는 일반 국민에게까지 막대한 피해를 주고 있다. 최근 스마트폰의 급격한 기술발전과 더불어 해킹 공격 또한 고도화되고 치밀해 지고 있으며 피해 또한 매년 증가하고 있다. 2018년 과학정보통신부는 표 1과 같이 스마트폰을 이용한 스미싱 발생 관련 통계를 발표했으며 ‘16년 대비 ’17년도 스미싱 문자는 61% 증가한 50만여 건이 탐지되었고 ‘18년 8월까지는 발생 건수가 일부 감소한 상태를 보이나 여전히 스미싱 공격은 계속되고 날로 고도화되고 있다.

표 1. 과학기술정보통신부 스미싱 발생 현황
Table 1. Smishing statistical data of “Ministry of Science and ICT”

Classification	2016	2017	2018(~Aug)
택배사칭	267,274	317,618	136,398
공공기관사칭	75	6,156	8,516
자인사칭	17,413	15,080	8,722
기타	27,149	163,173	7,476
Sum	311,911	502,027	161,112

스미싱은 단문자서비스(Short message service)와 피싱(Phishing)의 합성어로, 2013년부터 급속히 사회문제화되기 시작하여 금전적인 피해를 일으키고 있다. 스미싱 공격은 문자메시지와 스마트폰을 이용하여 피싱 사기를 유도하거나, 스마트폰 상에서 개인정보 등을 빼내고, 본인이 모르는 소액결제가 되는 등 신종 모바일 사기 수법의 일종이다[1][2].

스미싱을 탐지 및 차단하기 위한 다양한 기술개발과 시도에도 불구하고 스미싱 피해사례가 증가하는 이유는 스미싱 공격이 실시간 이슈 사항이나 사회공학 기법을 이용해 문자를 전송하기 때문이다.

스미싱 피해는 사회생활을 하는 남성보다 주로 노년계층, 초·중·고 학생계층, 20대 사회 초반 계층, 여성계층 등에서 많이 발생하고 있다. 이는 사회생활을 하는 남성들이 각종 매체나 조직 등을 통해 이미 보안교육을 지속해서 받아 오거나 보안지식을 습득하는 환경에 더 많이 노출되었기 때문이다[1][3].

본 논문에서는 스미싱 공격을 차단기술로 예방하는 것이 아닌 보안교육을 통해 더 효과적으로 예방할 수 있음을 증명하기 위해 악성문자훈련시스템(MSTS)을 설계 및 구현하고 실험을 통하여 예방효과를 확인하였다.

Ⅱ. 관련 연구

2.1 스미싱 피해사례 연구

우리나라에서는 정보통신망 이용촉진 및 정보보호 등에 관한 법률 48조 2항에 따라 악성 프로그램의 유포행위를 불법적으로 규정하고 있다.

최근 남자 143명, 여자 16명 기준으로 스미싱 피해사례 연구를 한 결과 스미싱 피해는 남성보다 여성이 통계적으로 유의하게 높은 수준으로 많이 발생한 결과를 얻었다. 스미싱 문자를 받고 URL을 클릭하는 연구를 한 결과 남성의 1.51에 비해 여성이 1.88로 통계적으로 유의하게 많은 스미싱 문자 내 URL을 클릭하고 있었다. 이 연구에서는 스마트폰을 오래 사용할수록 스미싱 공격에 노출될 위험이 더 크다는 결론을 내렸다[1].

2.2 단축 URL의 행위분석 연구

스미싱 관련 범죄의 수사 및 예방을 위한 차단 행위들은 피해자가 수사기관이나 통신회사에 신고 후 확보된 악성코드를 분석하거나 해당 악성코드의 유포지 주소로 확인된 URL을 차단하는 방식으로 문자메시지가 피해자들에게 발송된 이후의 사후 대처 방식에만 초점이 맞춰져 있다. 일반적으로 스미싱은 피의자들이 악성코드를 생성한 후 무료 혹은 유료로 임대한 서버나 해킹된 서버에 악성코드를 업로드 한다[4]-[6]. 그 후 해당 주소를 단축 URL 서비스를 통해 단축한 뒤 해당 링크를 문자메시지에 포함해 보내는 수법을 사용한다. 단축 URL은 인터넷상의 긴 URL을 짧게 만들어 주는 기술로 인터넷에 사용될 수 있는 주소의 크기가 수백 바이트라 해도 단축 URL 서비스를 이용하여 30바이트 수준을 넘지 않는 크기의 주소를 생성하여 주소 자원을

절약하고 타인의 관심을 끌 수 있게 해주는 서비스를 말한다. 이러한 단축 URL은 글쓰기 자수의 제한이 있는 SNS 서비스에서 널리 사용되는 등 인기를 얻고 있다[7]-[9]. 그림 1은 단축 URL을 사용한 메시지와 사용하지 않은 메시지를 보여주고 있다.

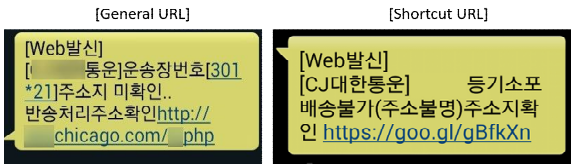


그림 1. 단축 URL 사용의 예
Fig. 1. Example of shortened URL usage

최근 단축 URL 내 악성코드가 포함되어 있는지 판별하는 연구는 활발히 진행되고 있다. 일반적으로 단축 URL을 포함한 문자메시지가 스마트폰 사용자에게 전달되었다면 우선 단축 URL을 정상적인 URL로 변환하고 그 URL 내에 APK라는 텍스트가 포함되어 있는지 판별하여 메시지를 차단하거나, 또는 악성 URL 정보를 제공하는 웹사이트 DB 검색을 통해 판별하여 메시지를 차단할 수 있다. 하지만 이런 차단방식에는 치명적인 단점이 존재한다. 스미싱은 단순히 스마트폰에 악성코드를 설치하는 행위뿐만 아니라 계좌번호 등 이용자의 중요정보를 입력하게 하여 정보를 탈취하거나 이용자의 심리를 이용하여 범죄자에게 전화를 걸게 하는 보이스 피싱 범죄로 그 범위가 확대될 수 있기 때문이다. 단순히 메시지를 필터링하는 방법만으로는 스미싱을 근본적으로 막을 수는 없다.

2.3 보안교육이 조직에 미치는 영향

실험을 통해 보안교육이나 보안서비스 제공이 조직구성원의 보안정책 준수 행동에 어떤 영향을 미치는지 알아보는 연구는 아래와 같은 결론을 얻었다. 첫 번째 실험에서는 국내 대기업 임직원을 대상으로 스팸 이메일 대응 교육을 한 후 교육 효과를 알아보기 위해 스팸 이메일 열람 여부를 측정했고, 3개월이 지난 후에도 효과가 지속하는지 알아보았다. 두 번째 실험에서는 보안서비스의 효과를 알아보기 위해 보안경고 알림 메시지를 제공한 후 그 효과를 측정하였다. 실험 결과, 보안교육은 보안정책 준수 행동에 긍정적인 영향을 미치는 것으로 나타났다. 보안교육 직후 교육 이수 집단이 미이수 집단보다 스팸 이메일 열람률이 낮았다. 또한 보안위험 경고 알림 메시지는 스팸 이메일을 낮추는 데 효과가 큰 것으로 나타나 보안정책 준수 행동에 긍정적인 영향을 미쳤다[10].

위의 연구결과와 같이 기술적 보안대책만으로는 사이버범죄를 막는 데 한계가 있고 보안교육과 보안서비스 활용이 병행되어야 효과적인 사이버범죄를 예방할 수 있음을 확인할 수 있었다.

III. 악성문자훈련시스템 설계 및 구현

본 연구에서 제안한 MSTS는 AWS(Amazon Web Service) 환경에 Ubuntu 리눅스와 PHP, Maria DB, Tomcat을 이용하여 시스템을 구현하였다. MSTS의 기본 구성은 훈련양식 등록, 문자훈련 실행, 훈련결과 이렇게 3가지 부분으로 나누어지며 단축 URL 변환을 위해서는 NAVER 단축 URL 서비스를 연동하였고 SMS 문자발송을 위해서는 비즈 뿌리오 상용 문자서비스를 이용하였다.

3.1 MSTS 훈련 프로세스

MSTS는 그림 2와 같이 4단계 훈련 프로세스를 통해 악성 문자 모의훈련을 한다. 첫 번째 단계는 훈련대상자 등록과 훈련에 사용할 악성 문자 템플릿을 생성하는 단계이다. 두 번째 단계는 모의훈련 관리자가 MSTS를 통해 이미 등록한 훈련대상자와 훈련문자 템플릿을 조합하여 문자훈련을 등록하는 단계로 단축 URL이 생성되고 훈련문자가 발송된다. 세 번째 단계는 열람자 DB 기록 단계로 문자가 발송된 대상자 정보와 등록된 훈련 명을 기초로 훈련결과를 DB화하는 단계이다. 네 번째 단계는 훈련결과 생성단계로 훈련문자를 받은 대상자가 단축 URL을 클릭하면 MSTS는 훈련 명에 맞는 스미싱 웹페이지를 보여주고 훈련대상자 정보를 훈련 DB에 기록한다. 모든 훈련이 종료되면 모의훈련 관리자는 MSTS에서 훈련결과를 확인할 수 있다.

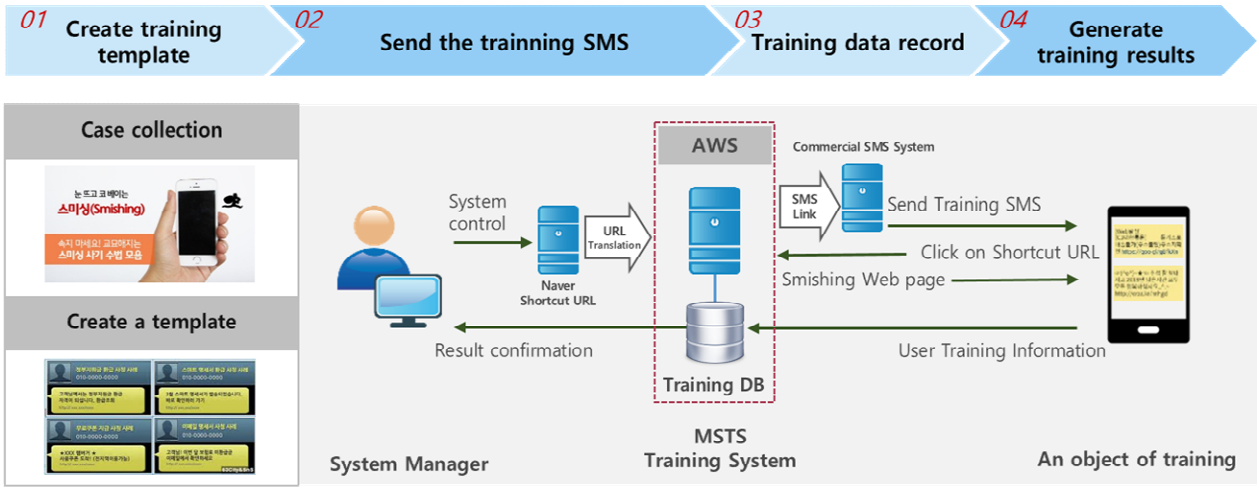


그림 2. 악성문자훈련시스템 훈련프로세스
Fig. 2. MSTS training process

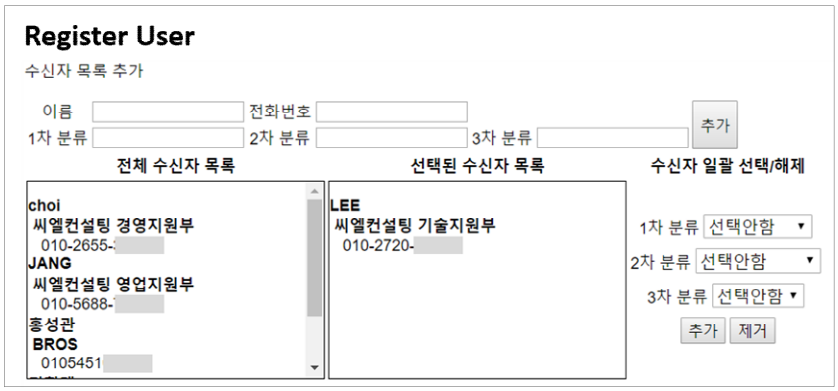


그림 3. 사용자 등록 화면
Fig. 3. Input screen of user data

3.2 MSTS 주요 기능

"훈련양식 등록" 기능은 사용자 등록, 문자훈련 템플릿 등록, 문자훈련 등록으로 나누어져 있다. 사용자 등록은 그림 3과 같이 훈련대상자의 조직 구분을 위해 3차까지 구분하여 등록할 수 있게 하였다.

문자훈련 템플릿은 단문자 발송을 위해 문자의 크기가 URL을 포함해 80바이트를 넘지 않게 하였고 문자메시지 내 URL 링크를 삽입하기 위해 그림 4와 같이 {링크}라는 치환단어를 문자메시지에 포함하였다. 문자훈련 템플릿은 단순히 URL클릭을 유도하는 문자와 사용자 정보를 입력하게 하는 문자 템플릿으로 구성된다. 훈련대상자와 문자템플릿 생성이 완료되면 마지막으로 훈련명을 입력하여 훈련 목록을 생성한다.

"문자훈련 실행" 기능은 훈련양식 등록기능에서 생성된 훈련목록을 선택해서 문자메시지를 발송하는 단계로 문자메시지 내 {링크}라는 치환문자를 훈련 URL로 변환하고 다시 네이버 단축 URL 서비스를 이용하여 단축 URL을 생성하는 단계이다. 이렇게 생성된 문자메시지는 상용 SMS 서비스를 통해 훈련대상자에게 문자가 발송된다.

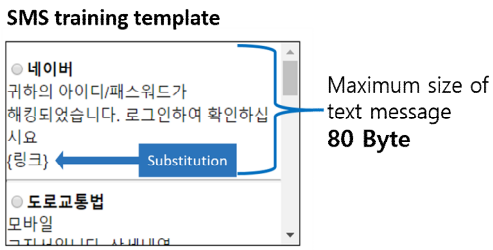
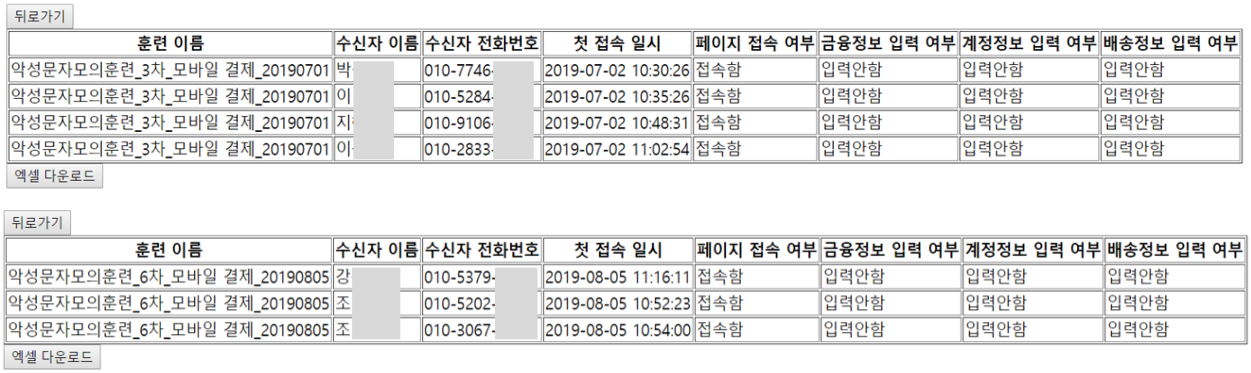


그림 4. 문자훈련 템플릿
Fig. 4. Short message service(SMS) template



뒤로가기

훈련 이름	수신자 이름	수신자 전화번호	첫 접속 일시	페이지 접속 여부	금융정보 입력 여부	계정정보 입력 여부	배송정보 입력 여부
악성문자모의훈련_3차_모바일 결제_20190701	박	010-7746-	2019-07-02 10:30:26	접속함	입력안함	입력안함	입력안함
악성문자모의훈련_3차_모바일 결제_20190701	이	010-5284-	2019-07-02 10:35:26	접속함	입력안함	입력안함	입력안함
악성문자모의훈련_3차_모바일 결제_20190701	지	010-9106-	2019-07-02 10:48:31	접속함	입력안함	입력안함	입력안함
악성문자모의훈련_3차_모바일 결제_20190701	이	010-2833-	2019-07-02 11:02:54	접속함	입력안함	입력안함	입력안함

엑셀 다운로드

뒤로가기

훈련 이름	수신자 이름	수신자 전화번호	첫 접속 일시	페이지 접속 여부	금융정보 입력 여부	계정정보 입력 여부	배송정보 입력 여부
악성문자모의훈련_6차_모바일 결제_20190805	강	010-5379-	2019-08-05 11:16:11	접속함	입력안함	입력안함	입력안함
악성문자모의훈련_6차_모바일 결제_20190805	조	010-5202-	2019-08-05 10:52:23	접속함	입력안함	입력안함	입력안함
악성문자모의훈련_6차_모바일 결제_20190805	조	010-3067-	2019-08-05 10:54:00	접속함	입력안함	입력안함	입력안함

엑셀 다운로드

그림 5. 훈련결과
Fig. 5. Training results

"훈련 결과" 기능은 훈련문자를 받은 훈련대상자가 문자메시지 내 단축 URL을 클릭했을 경우 생성된 데이터를 확인하는 단계로 그림 5와 같이 8가지 정보(훈련 이름, 수신자 이름, 수신자 전화번호, 첫 접속 일시, 페이지 접속 여부, 금융정보 입력 여부, 계정정보 입력 여부, 배송정보 입력 여부)를 확인하고 결과값을 내려받을 수 있다.

IV. 실험 및 성능 평가

스미싱 실험에 참여한 참가자는 총 52명이며, 이 중 남자는 40명 여자는 12명이다. 모집단의 연령대는 19~23세이다. 실험은 2개의 모집단으로 나누고 각각 4주씩 진행되었고, 개인정보보법에 의거 실험 모집단에게 개인정보 동의를 받은 후 실험 정보는 제공하지 않았다. 각 모집단의 실험방법은 동일하며 먼저 1차 스미싱 문자를 전송한 후 1주 이내 보안교육을 했고, 보안교육 후 1주 이내에 2차 스미싱 문자를 전송하였다. 3차 스미싱 문자는 2차 스미싱 문자발송 후 2주 후에 발송하였다. 스미싱 문자는 표 2와 같이 A~C 그룹을 먼저 실험하고 4주 후 D~F 그룹을 3가지 종류의 훈련문자를 준비하여 실험하였다.

실험대상자에게 실험정보를 제공하지 않고 보안교육도 하지 않은 상태에서 스미싱 문자를 발송한 1차 실험 결과 스미싱 앱이 설치되어 있거나 단축 URL 클릭 시 경고문이 발생해도 표 3과 같이 52명 중 15명(28.8%)이 단축 URL을 클릭하였다.

표 2. 실험 방법
Table 2. Test methods

Group	User	1st test	2nd test	3rd test
A	10	네이버 아이디	모바일 결제	KT 명세서
B	10	KT 명세서	네이버 아이디	모바일 결제
C	8	모바일 결제	KT 명세서	네이버아이디
D	8	네이버 아이디	모바일 결제	KT 명세서
E	8	KT 명세서	네이버아이디	모바일 결제
F	8	모바일 결제	KT 명세서	네이버 아이디

표 3. 실험 결과
Table 3. Test results

Classification	1st test	2nd test	3rd test
모바일 결제	7 (13.5%)	3 (5.8%)	3 (5.8%)
KT 명세서	3 (5.8%)	0 (0.0%)	0 (0.0%)
네이버 아이디	5 (9.6%)	1 (1.9%)	2 (3.8%)
Sum (rate%)	**15 (28.8%)**	**4 (7.7%)**	**5 (9.6%)**

이 중 7명이(13.5%) 모바일 결제 스미싱 문자메시지에 가장 많은 반응을 보였고, 네이버 아이디 해킹 스미싱 문자는 5명(9.6%), KT 명세서 도착 스미싱 문자는 3명(5.8%)이 스미싱 문자 내 단축 URL을 클릭하였다.

2차 실험은 1차 실험이 종료된 후 보안교육을 하고 1주 이내 실시하였으며 52명 중 4명(7.7%) 만이 스미싱 문자메시지 내 단축 URL을 클릭하였다. 3차 실험은 2차 실험이 종료된 후 2주 이내 실시하였고 2차 실험보다는 다소 높은 단축 URL 클릭률을 보였으나 2차 실험 결과와는 크게 다르지 않았다. 따라서 MSTS 시스템을 통한 스미싱 보안교육이 스미싱 공격을 예방하는 데 효과가 있음을 확인할 수 있었다.

Ⅴ. 결론 및 향후 과제

스미싱 사이버범죄를 예방 및 차단하기 위한 기존 기술들은 단순히 스미싱 문자메시지 내 단축 URL을 기초로 악성코드가 삽입되었는지 아니면 URL 자체가 블랙리스트에 포함되었는지만을 판단하여 스미싱을 예방 및 차단하려 했다. 본 논문에서 제안한 MSTS 시스템은 기존의 예방 및 차단 기술 방식과는 다른 보안교육과 악성문자모의훈련으로 스미싱 공격를 예방하고자 했다. MSTS 시스템을 구현하고 모집단을 통해 실험한 결과 보안교육 및 훈련을 하기 전 약 28%의 스미싱 공격 성공률이 훈련 후 약 10% 이내로 줄어들어 MSTS 시스템이 스미싱을 예방하는 데 효과가 있음을 확인하였다.

본 연구는 52명의 모집단을 통해 검증하였으나 더 다양한 남·여 비율과 연령대 비율의 모집단 실험 검증이 필요하다. MSTS 시스템은 현재 단문자 발송 기능만을 구현하였으므로 향후 장문자나 메신저 등을 활용한 기술구현과 다양한 훈련문자 템플릿이 포함된 시스템을 구현할 계획이다.

References

[1] Tae-Jong You and Jong-Hyun Kim, "Prevention Measures and Forecasting Model Through the Analysis on the Causes of Smishing", Journal of KNOM, Vol. 21, No. 1, pp. 27-37, Jun. 2018.

[2] Nam-i An, "Design and Implementation of Spam Protection System for Text Messages based on Machine Learning", Master's Thesis, Hanyang University, Feb. 2012.

[3] Han-Jin Park and In-Jung Kim "A Survey of Regulations on Smishing and Mobile Micropayment and a Research of Regulations and Laws for Reducing Monetary Damages in Mobile Micropayment", Journal of The Korea Institute of Information Security & Cryptology, Vol. 27, No. 5, pp. 1189-1199, Oct. 2017.

[4] Mi-Suk Kwak, Ah-bin Kim, and Yoonhee Kim, "Design and implementation an integrated malicious code collection and monitoring system", Journal of KIIT, Vol. 8, No. 2, pp. 117-125, Feb. 2010.

[5] Donghyeok Lee and Namje Park, "Hacking Training Plan for Cyber Security in Industry 4.0", Journal of KIIT, Vol. 15, No. 5, pp. 47-56, May 2017.

[6] Sung-Min Byun and Jin Kim, "Spam Message Filtering System using Message Digest Algorithm", Proceedings of KIIT Conference, 120-123, May 2014.

[7] Ankit Kumar Jain and B. B. Gupta, "Rule-Based Framework for Detection of Smishing Messages in Mobile Environment", Procedia Computer Science, Vol. 125, pp. 617-623, Jan. 2018.

[8] Gunikhan Sonowal and K. S. Kuppusamy, "SmiDCA: An Anti-Smishing Model with Machine Learning Approach", Security in Computer Systems and Networks The Computer Journal, Vol. 61, No. 8, pp. 1143-1157, Aug. 2018.

[9] Yong-Bum Cha, Won-Yong Choi, and Gang-Seok Lee, "Proactive Response Against Smishing Using Shorten URL", Journal of Digital Forensics, Vol. 9, No. 1, pp. 19-32, Jun. 2015.

[10] Bo-Ra Kim, Jong-Won Lee, and Beom-Soo Kim "Effect of Information Security Training and Services on Employees' Compliance to Security Policies", Journal of National Information Society Agency, Vol. 25, No. 1, pp. 99-114, Feb. 2018.

저자소개

최 학 규 (Hark-Kyu Choi)

2002년 2월 : 배재대학교 컴퓨터공학(공학사)
2018년 3월 : 공주대학교 컴퓨터공학과(석사과정)
2013년 4월 ~ 현재 : 대·중소기업·농어업협력재단 기술보호 전문가
2019년 1월 ~ 현재 : (주)씨엘컨설팅 대표
관심분야 : 정보보안, 네트워크 보안, 보안 컨설팅, 클라우드 보안

김 황 래 (Hwang-Rae Kim)

1982년 8월 : 중앙대학교 전자계산학과 (이학사)
1991년 2월 : 중앙대학교 대학원 컴퓨터공학과 (공학석사)
2007년 8월 : 대전대학교 대학원 컴퓨터공학과 (공학박사)
1983년 3월 ~ 1994년 2월 : 한국전자통신연구원 책임연구원
1994년 3월 ~ 현재 : 공주대학교 컴퓨터공학부 교수
관심분야 : 컴퓨터 네트워크, 네트워크 보안, 네트워크 생존성 관리, 스마트 제어