

2020

한국정보보호학회 하계학술대회

CISC- S'20

Conference on Information Security
and Cryptography - Summer 2020

07.15^{WED}

온라인 컨퍼런스

<http://www.cisc.or.kr/>

주최
주관



후원



과학기술정보통신부



한국인터넷진흥원



적대적 공격에 견고한 Perceptual Ad-Blocking 디자인	김민재 · 김보민 · 허준범 / 381
--	-----------------------

AI보안

DNN 모델 취약점 적대적 예제 생성 기법과 방어기법에 대한 분석	서성관 · 문현준 · 윤주범 / 387
딥러닝 시스템 커버리지 기반 퍼징 프레임워크 최적화 연구	유지현 · 문현준 · 윤주범 / 392
Variant AutoEncoder 기반 모바일 맬웨어 클러스터링 기법	고은별 · 김진성 · 반영훈 · 이정현 / 396
딥러닝을 활용한 CCTV 내 폭력 탐지 시스템 개발	김태옥 · 박현아 · 임다연 · 최은정 / 400
머신러닝 기반 네트워크 트래픽 분석 기법 성능 비교	황종배 · 하재철 / 404
금융데이터를 활용한 연합학습 평가	장진혁 · 최대선 / 409
CNN을 이용한 스마트 폰 부채널 공격	김동현 · 김지은 · 유건우 · 이승대 · 백유진 / 413
K-means Clustering을 이용한 kNN 속도개선에 관한 연구	김도연 · 이용수 · 윤재현 · 이태진 / 417

신원/인증시스템

분산 ID 기반 비대면 데이터 공유 접근 시스템	이정륜 · 윤태연 · 이우기 / 423
차세대 주민등록정보시스템 구축에 관한 연구	이현철 · 김대영 · 김현수 / 427
탈 중앙화된 분산 ID 시스템의 특징 및 한계에 대한 동향 조사	이길희 · 김석현 · 김은수 · 전소원 · 김봉곤 · 조영섭 / 431
열 기반 슬라이싱을 이용한 폐기 가능한 홍채 템플릿 생성 방법	신영아 · 정재열 · 정익래 / 436
안면인식을 통한 USB 파일 복호화 시스템	송경주 · 강혜진 · 백민진 · 김현지 · 서화정 / 440
스마트폰과 스마트워치를 활용한 2차 사용자 인증 방식 제안	심민주 · 엄시우 · 김현지 · 서화정 / 444

암호화폐/양자암호

암호화폐 금전가치 분석 동향	박재훈 · 최승주 · 서화정 / 451
암호화폐 거래 믹싱을 통한 익명화기술 동향조사	장철아 · 이경현 / 455
스마트 컨트랙트의 동적 모니터링을 지원하는 이더리움 가상머신	김지수 · 이수연 · 조은선 / 459
NIST 양자내성암호 공모전 부호 기반 암호 구현 동향	최승주 · 김현지 · 심민주 · 서화정 / 463
양자 컴퓨팅 환경에서 안전한 다중 서명 기법	이영경 · 박종환 · 이광수 · 이동훈 / 467
μ -Hope: 오류 정정 부호를 사용한 RLWE 기반 KEM	이주엽 · 김수리 · 홍석희 / 471

데이터식별/추적

저작권 침해 의심 사이트의 생애주기 단계 자동 탐지 기법	정해선 · 곽진 / 477
링크분석 기반 영상 저작권 침해 스트리밍 사이트 탐지 방안	이희승 · 곽진 / 481
스팸 리뷰 판별을 위한 텍스트 분석 관련 기술 동향	임세진 · 김현지 · 서화정 / 485
음란물 유포 경로 추적을 위한 Tumblr 애플리케이션 메모리 포렌식 분석	박진성 · 공성현 · 이창훈 / 489
안드로이드 어플리케이션의 DRM 기술 현황 분석 : 카카오멜론, 카카오톡	이나연 · 김도연 · 양승욱 · 김희석 / 493
메시지 시그니처 분석을 통한 송신자 식별 방안	김동현 · 곽진 / 497

메시지 시그니처 분석을 통한 송신자 식별 방안

김동현¹, 곽진²

^{1,2}아주대학교 사이버보안학과

Message Signature Analysis based Sender Identification Method

Dong-Hyun Kim¹, Jin Kwak²

^{1,2}Department of Cyber Security, Ajou University

요약

최근 개인정보 유출이 잇따르고 SNS가 발달함에 따라 획득한 개인정보를 정교하게 획득하는 것이 가능해졌고 이를 바탕으로 특정 인물을 사칭하여 지인을 상대로 금전적 요구를 하는 메신저 피싱 사건이 연이어 발생하고 있다. 이러한 사고를 막기 위한 노력을 기울이고 있지만 치밀한 계획을 세워 접근하는 악의적인 송신자를 특정 수신자가 직접 확인하지 않는 이상 명확히 판단하기에는 많은 어려움이 따른다. 따라서 본 논문에서는 기존의 특정 인물이 송신한 메시지의 패턴을 분석하고 추출한 특징을 활용하여 새로운 메시지와 비교 분석함으로써 악의적인 송신자의 접근을 판단하는 방안을 제안한다.

I. 서론

최근 개인정보 유출 사고가 연이어 발생하고 있다. 습득한 개인정보를 통해 SNS 내의 방대한 정보를 추가로 활용하여 특정 인물에 대해 더 정교한 개인정보를 수집하고 활용할 수 있게 됐다[1]. 그중, 수집했던 정보를 바탕으로 카카오톡, 네이버, 페이스북 등 타인의 메신저 아이디를 도용하여 로그인한 뒤 등록된 지인에게 메시지를 보내 금전을 탈취하는 신종 범죄 수법인 메신저 피싱(Phishing)이 많이 발생하고 있다[1]. 이러한 피싱을 방지하기 위해 특정 메신저에서는 친구로 등록되지 않은 사용자, 금전을 요구하는 메시지, 해외 IP를 사용하는 사용자 등을 인식하여 사용자에게 피해 예방을 위한 안내와 같은 예방책을 시행하고 있다[2]. 하지만 악의적인 송신자가 방대한 데이터를

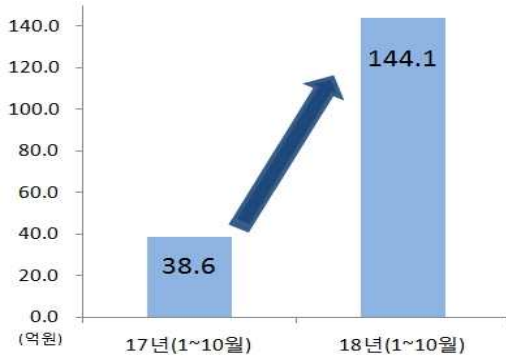
통해 개인정보를 포함한 지인의 정보, 호칭, 말투, 어감, 만난 시간과 장소 등과 같은 둘만이 알 수 있는 정보를 직접 혹은 유추하여 습득할 수 있다. 이렇게 습득한 정보를 바탕으로 치밀한 계획을 세워 수신자에게 접근하는 경우 정상 송신자와 악의적인 목적으로 접근하는 송신자를 식별하는 것이 매우 어렵다.

본 논문에서는 악의적인 목적으로 접근하는 송신자를 식별하기 위해서 특정 수신자에게 전송되는 메시지의 패턴을 분석하고 그 분석을 바탕으로 시그니처를 생성하여 통계적 분석을 통해 특정 인물을 사칭하는 메시지를 수신하였을 경우 저장하고 있는 시그니처와 비교하여 악의적인 송신자를 식별하는 방안을 제안한다.

이 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2017R1E1A1A01075110)

II. 관련 연구

2.1 메신저 피싱 피해사건 동향

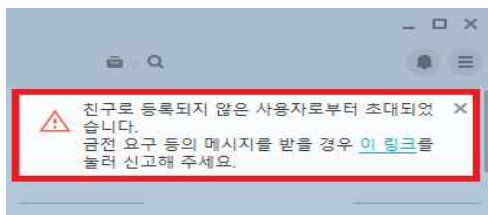


(Fig. 1) Monetary Damage By Messenger Phishing



(Fig. 2) Status of Monthly Cases

금융감독원의 조사에 따르면 메신저 피싱 피해 건수는 2017년 915건에서 2018년 6,764건으로 큰 증가세를 보였으며 피해액 또한 38.6억 원에서 144.1억 원으로 큰 증가를 나타내고 있다[1].



(Fig. 3) Warning Sign of Messenger

이러한 피해를 막기 위해서 메신저에서는 (Fig. 3)과 같이 안내 메시지를 채팅창 상단에 보여주고 있으며 금융감독원에서는 지인으로 사칭한 메신저 피싱에 대한 주의를 당부하는 보도자료[1]를 배포하는 등과 같은 노력을 기울이고 있다.

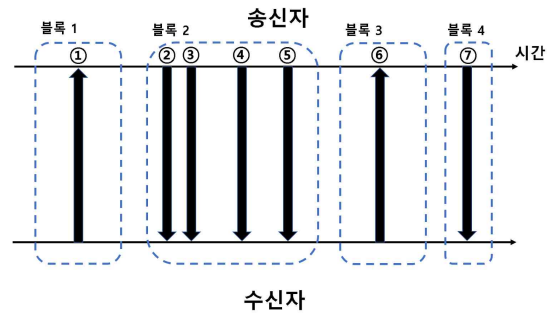
2.2 기존 예방책의 한계점

KISA는 이상거래탐지시스템(FDS) 적용이나 로그인시 이중인증을 통한 해킹 이용 방지 등 공조체계에 대한 필요성을 강조하고 있다[3]. 하지만 메신저 사업자들이 사용자의 환경 침해에 따른 가입자 불만 증가를 우려하기 때문에 주저하고 있어 그에 따른 피해가 지속해서 증가하고 있다[3]. 따라서 악의적인 송신자가 전송한 메시지를 판단하고 선제적인 차단을 수행하는 기술의 개발이 필요하다.

III. 메시지 특징 분석

□ 메시지 블록

메시지 전송 간 시간, 단일 자음 사용 횟수, 이모티콘 사용 횟수, 답장까지 걸린 시간, 답장의 개수 각 항목에 대해 정의하도록 한다.



(Fig. 4) Example of Message Block

정의에 앞서 (Fig. 4)는 송수신 메시지의 한 예시를 나타낸 그림이다. 수신자가 보낸 1번 메시지와 6번 메시지 사이의 송신자가 보낸 2~5번 메시지를 하나의 메시지 블록이라고 정의한다.

□ 메시지 전송 간 시간

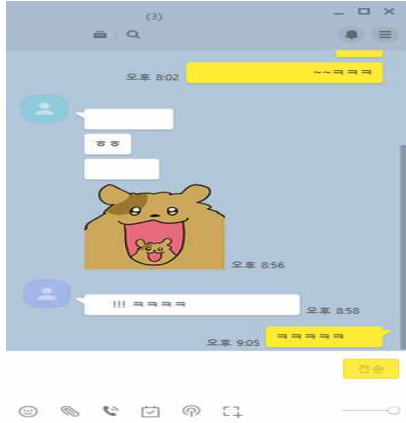
앞에서 정의한 한 메시지 블록 내에서 송신자가 보낸 메시지 블록 내의 총 n 개의 메시지를 전송할 경우, m 번 메시지 전송 이후 $m+1$ 번

(단, $0 < m < n$, m 과 n 은 1보다 큰 자연수)

메시지를 전송할 때까지의 시간을 모두 합한 값을 메시지 전송 간 시간으로 정의한다. 단, 송신자가 보낸 메시지가 1개뿐 이라면 0이라고 한다.

□ 단일 자음 사용 횟수

정의한 메시지 블록 내에서 (Fig. 5)에서의 ‘ㅋㅋㅋ’, ‘ㅎㅎ’, ‘ㅋㅋㅋㅋㅋ’과 같이 하나의 메시지 안에서의 단일 자음 개수를 단일 자음 사용 횟수로 정의한다.



(Fig. 5) Usage Example of Single Consonant

□ 이모티콘 사용 횟수

앞서 정의한 메시지 블록 내 이모티콘 사용 횟수를 이모티콘 사용 횟수로 정의한다.

□ 답장까지 걸린 시간

앞서 정의한 메시지 블록 간의 시간을 답장까지 걸린 시간으로 정의한다.

□ 답장의 개수

앞서 정의한 메시지 블록 내의 메시지 개수를 답장의 개수라고 정의한다.

IV. 시그니처 기반 송신자 식별

4.1 개요

메시지가 서버를 통해 특정 수신자에게 전송될 때 서버에서 특정 송신자가 보낸 메시지의 전송 간 시간, 단일 자음 사용 횟수, 이모티콘 사용 횟수, 답장까지 걸린 시간, 답장의 개수 등의 특징을 분석하여 추출하고 시그니처를 생성한다.

기존의 수신한 메시지에 대한 시그니처를 생성하여 저장하고, 새로운 메시지에 수신되었을 경우 새로운 메시지에 대한 시그니처를 생성하여 비교분석 후 송신자를 식별한다.

4.2 메시지 시그니처 정의

시그니처의 사전적 정의는 서명, 특징을

뜻하는 말로써 어떠한 대상이 갖는 고유한 특징을 통해 특정 대상을 한정 짓는 경우(예를 들어, JPEG 파일의 경우에 “FF D8 FF E0”를 시그니처로 갖는 경우)에 활용되고 있다.

본 논문에서는 메시지 시그니처를 특정 송신자에게 메시지를 전송하는 한 명의 송신자의 메시지가 가지는 고유한 특징을 메시지 시그니처라고 정의한다.

4.3 송신자 식별 단계

<Table 1> Identification Steps

Step 1	Step 2	Step 3	Step 4
메시지 블록 특징 벡터 생성	메시지 시그니처 생성	신규 수신 메시지 분석	송신자 식별

Step 1. 메시지 블록의 특징 벡터 생성

송신자의 메시지 중 30개의 메시지 블록을 완전 무작위로 추출하여 각각 표본을 만든다. 메시지 블록이 가지는 특징들을 성분으로 갖는 벡터를 특징 벡터라고 하고 $MB_1, MB_2 \dots MB_{29}, MB_{30}$ 와 같이 나타낸다. 30개의 표본으로부터 앞서 정의한 5가지의 특징을 추출하여 각각의 특징 벡터를 만든다. 특징들 각각의 평균값들을 성분으로 가지는 벡터를 MB_m 이라고 하자. 위 과정을 복원추출을 통하여 K회 실행한 후 그 값들을 통해 전체 메시지 블록의 MB_m 을 추정한다. 이때 K는 충분히 큰 추출횟수로서 시스템의 특성과 메시지 블록 특성에 맞는 적절한 값을 채택한다.

$$MB_1 = (x_1, y_1, z_1, w_1, p_1)$$

⋮

$$MB_{30} = (x_{30}, y_{30}, z_{30}, w_{30}, p_{30})$$

(x,y,z,w,p는 5개의 특징을 값을 저장하는 변수)

$$MB_m = \frac{1}{30} \sum_{i=1}^{30} (x_i, y_i, z_i, w_i, p_i)$$

표본의 크기가 30인 샘플을 K번 복원추출하여 특징 벡터 각각의 성분의 평균을 계산하고 이 표본들 각각의 성분들의 분포를 통해 전체 메시지 블록을 대상으로 한 특징 벡터의 각 성분을 추정할 수 있다. 이 방식은 중심극한정리를 이용한 방식으로 충분히 큰 표본의 크기(30 이상)를 충분히 많은 복원추출을 하였을 경우 모집단이 어떤 분포를

가졌는지에 관계없이 표본들의 평균 분포가 정규분포로 수렴한다는 점을 바탕으로 하고 있다.

Step 2. 메시지 시그니처 생성

앞서 정의한 MB_m 에 가중치 벡터 $W = (w_1, w_2, w_3, w_4, w_5)$ (단, $w_n \geq 0$, $1 \leq n \leq 5$ 인 정수, $\sum_{i=1}^5 w_i = 1$)를 내적하여 시그니처 값을 생성한다. 이때, 가중치 벡터의 각 성분은 나이, 학업, 직업, 성격 등과 같은 여러 환경 요소에 따라 메시지 블록 내의 특징값들의 가중치를 나타낸 것이다.

위의 과정을 통해 계산된 시그니처 값은 각각의 설명변수인 가중치 벡터의 성분 값들이 특징 벡터의 성분에 얼마나 영향력을 갖는지 고려하여 계산한 한 값으로써 하나의 값으로 살펴볼 수 있기에 특징 벡터와 가중치 벡터를 내적한 값을 시그니처라고 하였다. 이러한 과정을 거쳐 생성한 메시지 블록 각각의 시그니처들은 정규분포를 이룬다.

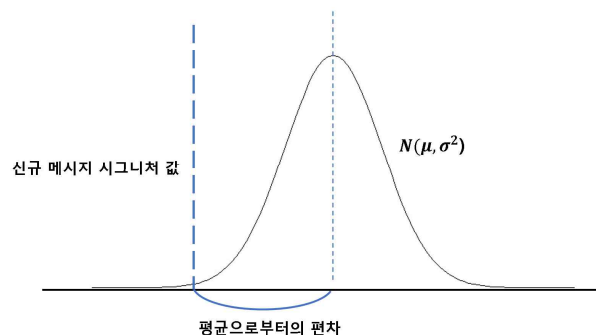
($\because E(x+y) \times w = E(wx) + E(wy)$, w 는 상수)

Step 3. 신규 수신 메시지 분석

신규 수신 메시지 블록들로 하나의 샘플 추출을 통해 특징 벡터를 생성하고 이를 기반으로 신규 메시지의 시그니처를 생성한다.

Step 4. 송신자 식별

신규 메시지에서 추출한 시그니처를 기존의 시그니처와 통계적 분석을 통하여 송신자를 식별한다. 신규 메시지의 시그니처가 기존의 시그니처의 평균에서 얼마만큼의 편차를 보이는지를 통해 송신자를 식별해내는 하나의 지표가 될 수 있다.



(Fig. 6) Judging New Message Signature

V. 프라이버시 침해 방지

메신저 피싱이 증가함에 따라 메신저 피싱을 예방하고자 하는 연구가 진행되었다[4]. 기존의 방법은 메시지를 분석하여 메신저 피싱에 자주 사용되는 단어와 그 단어의 연관도를 분석하여 피싱의 단계를 정의하고 단계별로 사용되는 단어를 분류를 통해 점수를 부여함으로써 메신저 피싱을 탐지하는 방안이다. 하지만 탐지하는 과정에서 분석한 메시지의 내용을 저장하여 관리하기 때문에 프라이버시 침해 문제가 발생할 수 있다. 따라서 프라이버시 침해 측면에서 분석한 메시지의 특징만을 수치화하여 관리함으로써 프라이버시 침해 이슈를 방지할 수 있다.

VI. 결론

메신저 피싱 방지를 위한 기술/사회적 노력이 이루어지고 있지만, 피싱 시도와 피해 발생 모두 증가세이기 때문에 이를 방지하기 위한 기술의 고도화가 필요하였다.

본 논문에서는 메시지 시그니처를 정의하고 관련 산출과정을 제안함으로써 악의적으로 접근하는 송신자를 식별해 낼 수 있는 기술의 기반을 마련하였다.

향후 추가적인 메시지 특징들의 상관관계 분석, 가중치 벡터 성분의 정교화 연구를 통해 시그니처 값을 통한 송신자 식별 기술 고도화 방안에 관한 연구를 진행할 예정이다.

[참고문헌]

- [1] 불법금융대응단, “181218_지인을 통한 메신저 피싱 주의 당부(19일 조간)”, 금융감독원, Dec. 2018.
- [2] 조은아, ““엄마, 돈 좀” 카톡 피싱에 안 속계... 경고문구 띄워준다”, 동아닷컴, Dec. 2018.
- [3] 이재운, “급증하는 메신저 피싱, 대응체계 손질 없이는 계속 '구멍'”, 이데일리, Dec. 2018.
- [4] 배지효, 채수열, 송명준, 방경찬, “메신저 피싱 대화 분석을 통한 탐지 방안”, 한국통신학회 학술대회논문집, pp. 537-538, 2019