전자서명을 이용한 스미싱 공격 방어 기법1)

최병환*
*고려대학교 컴퓨터.정보통신공학과
e-mail : rapture@korea.ac.kr

Defense Techniques of Smishing Attacks Using Electronic signature on Network Environment

Byung-Hwan Choi*
*Dept. of Information and Communication Engineering, Korea University

요 약

본 논문에서는 스미싱 공격에 대해서 Host기반에 의한 탐지가 아닌 네트워크 기반에서 전자서명을 이용한 모델을 제안한다. 본 모델은 네트워크 기반에서 유입된 트래픽 중 문자 메시지를 분석하여, 문자메시지 중에서 URL이 포함된 경우 트래픽을 우회하여 라우팅을 전환시켜 URL을 포함한 문자메시지 트래픽에 대해서 별도의 망구간으로 분리를 시킨다. 별도 분리된 URL이 포함된 트래픽에 대해서 apk파일 다운로드가 없는 경우에는 통과를 시키고, apk 파일 다운로드를 시도하는 트래픽에 대해서는 전자서명을 검사후, 등록이 안되어 있는 경우 차단을 한다. 이는 기본적으로 전자서명이 되지 않은 apk파일에 대한 다운로드를 원천적으로 봉쇄함으로써 스미싱 공격에 대한 근복적인 방어를 하는 방식이다. 본 모델은 Host기반에서 발생할 수 있는 우회공격을 방지하여 스미싱 위협을 해소할 수 있다. 기존 Host기반 스미싱 방지 모델의 동작 방식과 설계를 통해 장점과 단점을 언급하고 네트워크 기반에서 전자서명을 이용한 스미싱 방어의 타당성을 증명하도록 한다.

1. 서론

스마트폰 환경이 확산됨에 따라 기존에 PC에서 행해지던 금융사기가 스마트폰 환경에서도 확산이 되고 점점 고도화 되고 있다.

스마트폰의 사용이 급증함에 따라 다양한 유형의 보안 위협 요소들이 증가하고 있는 추세이며, 특히 안드로이드 환경에서 이슈화 되고 있는 취약점들과 위협요소에 대한 방어 기법에 대해서 많은 연구가 되고 있다[1].

본 논문에서는 스마트폰 위협 요소 중에서 스미싱 공격에 대한 대응방법에 대해 살펴보고자 한다. 스미싱이란 '문자메시지(SMS)와 피싱(Phishing)의 합성어'로 기본적으로 발신자의 신원을 속인 문자 메시지를 통해 악의적인 사용자가 첨부한 링크에 접속하게 한 후, 악성 어플리케이션(이하 앱)을 설치하여 스마트폰 내의 개인 정보 또는 금융정보를 탈취하는 사기 수법이다. 국내에서는 악성 앱 설치후 휴대폰 결제 인증 SMS를 탈취하여, 피해자가 인지하지 못한 상태에서 휴대폰 결제를 완료시키는 수법으로 사용되고 있다. 또한, 기존에는 발신자의 신원을 무작위 익명으로 진행하였으나, 현재는 웹하드, 커뮤니티등에서 특정 계정 정보를 탈취한 후 지인 또는 정상 기관으로 사칭하여 해당 계정과 관계가 있는 지인들에게 문자메시지를 보내는 고도화된 수법도 진행되고 있다.

스미싱 공격은 감염시킬 스마트 폰에서 동작할 악성 앱을 반드시 설치해야 하기 때문에 기본적으로 문자 메시지 안에 악성 앱을 다운로드하기 위한 URL 또는 단축 URL이 포함되어 있다. 대부분의 스미싱 공격 사례를 분석해 보면 정상 URL보다는 사용자가 알아 볼 수 없는 단축 URL로 공격하는 사례가 높다.

본 논문에서는 스미싱 공격에 대해서 Host기반에 의한 탐지가 아닌 네트워크 기반에서 전자서명을 이용한 모델을 제안한다. 본 모델은 네트워크 기반에서 유입된 트래픽 중 문자 메시지를 분석하여, 문자메시지 중에서 URL이 포함된 경우 트래픽을 우회하여 라우팅을 전환시켜 URL을 포함한 문자메시지 트래픽에 대해서 별도의 망구간으로 분리를 시킨다. 별도 분리된 URL이 포함된 트래픽에 대해서 apk파일 다운로드가 없는 경우에는 통과를 시키고, apk 파일 다운로드를 시도하는 트래픽에 대해서는 전자서명을 검사후, 등록이 안되어 있는 경우 차단을 한다. 이는 기본적으로 전자서명이 되지 않은 apk파일에 대한 다운로드를 원천적으로 봉쇄함으로써 스미싱 공격에 대한 근복적인 방어를 하는 방식이다. 본 모델을 사용함으로써 금융사기 감소 및 스미싱 위협을 해소할 수 있도록 기여할 것이다.

본 논문의 2장에서는 기존 Host기반 스미싱 방지 모델에 대해 살펴보고, 3장에서는 기존 Host기반 스미싱 방지

1) 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 정보통신·방송 연구 개발사업[공고번호:2014-044, 네트워크 위협 탐지규칙 생성·검증 자동화 및 관리기술개발]과 고려대학교 컴퓨터정보통신대학원 학위논문의 일환으로 수행하였음

모델의 단점과 한계점을 지적하고, 4장에서는 전자서명을 이용한 모델을 제안하며, 5장에서 결론으로 끝을 맺는다.

2. 관련 연구

스미싱 공격에 대해서 기존의 대응 방법으로는 대부분 Host 기반으로 한 앱이 제안되었다.

현재 안드로이드 스미싱 방지 앱의 탐지 모델은 표1과 같이 URL 검사 모델과 문자열 검사 모델 그리고, 설치된 악성 앱 권한 검사 모델, 정상 기관 인증 모델, 악성 앱 사전 검증 모델 로 크게 5가지로 분류할 수 있다.

탐지모델	동작방식
URL 검사 모델	URL 포함여부 및 'apk' 확장자 포함여부 검사.
문자열 검사 모델	특정 문자열에 대한 포함 여부 검사.
앱 권한 검사 모델	앱의 권한 범위 검사 및 악성 앱의 권한과의 유사도 검사.
정상 기관 인증 모델	정상 기관에서 메시지 발송시 해쉬값을 같이 발송하여, 사용자 인증메세지(PassPhrase)와 변형된 HMAC 알고리즘 이용하여 발신지 검증[2].
악성 앱 사전 검증 모델	통계를 기반하여 악성 앱 행동 탐지 및 악성 여부를 점수를 책정하여 악성 여부 판단[2].

표 1 기존 Host기반 스미싱 방지 모델

URL 검사 모델은 악의적인 스미싱 URL/단축URL이 존재하는 경우, URL에 포함된 'apk'확장자 유무를 검사하여 확장자가 존재하면 스미싱 문자로 간주하고 사용자에게 알려준다.

문자열 검사 모델은 악의적인 스미싱 관련 문자열이 존재하면 스미싱 문자로 간주하고 사용자에게 알려준다.

설치된 악성 앱 권한 검사모델은 일반적인 앱에 필요 없는 권한이 설정되어 있거나 스미싱 피해를 유발한 악성 앱의 권한과 유사한 권한 설정이 되어 있는 경우 사용자에게 알려준다.

정상 기관 인증 모델은 사용자 등록 과정을 통하여 사용자 고유 PassPhrase를 이용해 금융기관과 사용자간의 일대일 신뢰 관계를 형성 후에 금융기관에서 메시지 발송시에 변형된 HMAC 알고리즘을 이용하여 생성한 해쉬값과 발송메시지를 함께 발송하고, 사용자가 메시지를 수신하면 수신된 메시지의 해쉬값과 사용자 PassPhrase를 금융기관에 전송하여 재인증을 함으로써 발신지를 검증하여 스미싱 문자열를 판단하고 사용자에게 알려준다[2].

악성 앱 사전 검증 모델은 최근 유포되고 있는 악성 앱들에서 사용되는 권한을 선별하여 권한별 점수를 책정하고, URL/PK시그니쳐를 파악하여 행동별 점수를 책정하여 합산한 점수가 일정 점수 이상인 경우 스미싱 문자로 간주하고 사용자에게 알려준다[2].

각 Host 기반의 탐지 모델의 경우, 스마트폰에 앱으로 설치되어 검사하는 방식으로, URL/문자열 검사 모델이 비해 탐지율이 높고 오탐율이 적으며, 정상 기관 인증 모델에 비해 구현이 용이한, 앱 권한 검사 모델을 많이 사용한다.

3. 기존 스미싱 방지 모델의 단점과 한계점

기존 Host기반 스미싱 방지 모델 중 URL/문자열 검사 모델의 경우에는 그림1에서와 같이 블랙리스트에 등록된 URL 또는 문자열의 존재여부에 따라 위험성을 판별하는 방식으로, 블랙리스트에 등록된 URL 또는 문자열이 아닌 다른 URL이나 다른 문자열을 삽입하여 스미싱 문자메시지를 발송하는 경우 URL/문자열 검사 모델을 우회하여

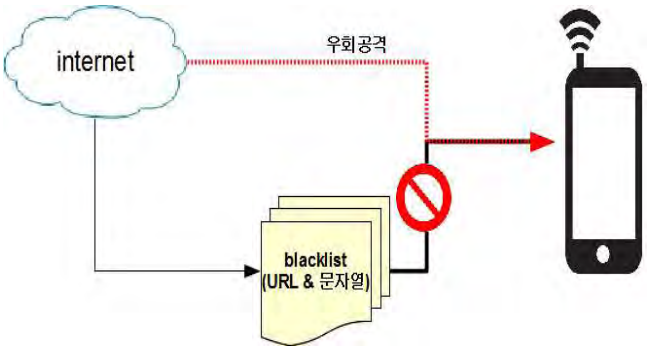

그림 1 URL/문자열 검사 모델 우회공격 시나리오

공격이 가능하다.

기존 Host기반 스미싱 방지 모델 중 앱 권한 검사 모델의 경우에는 그림2에서와 같이 스마트폰에 앱으로 설치된 후 권한 검사를 수행되는 방식이기 때문에, 설치된 후 권한 검사를 수행하기까지의 공백시간이 발생한다. 이 공백시간안에 악성 앱이 동작하여 악성코드를 수행하거나 금융정보, 개인정보 등을 해커에 전달할 가능성이 존재한다.

그림 2 앱 권한 검사 우회 공격 시나리오

기존 Host기반 스미싱 방지 모델 중 정상 기관 인증 모델의 경우에는 그림3과 같이 사용자 환경이 루팅(Rooting)

된 경우에는 사용자 인증 과정에서 악성 앱 고유 경로에 존재하는 PassPhrase를 루트 권한으로 탈취하여 인증앱을 사칭, 인증과정에 사용할 가능성이 있다. 이러한 이유로 정상 기관 인증 모델의 경우에는 루팅 시 무력화된다[2].

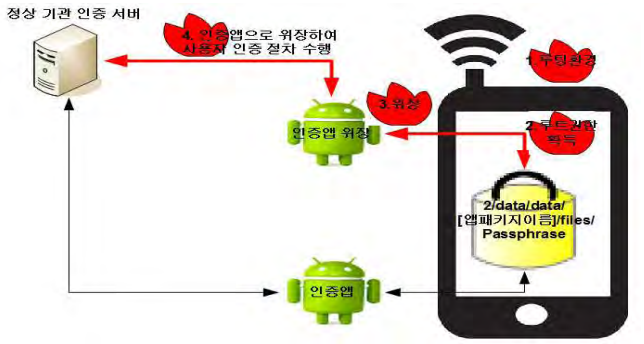

그림 3 정상 기관 인증 모델 우회 공격 시나리오

또한, 인증 앱이 구현되어야 하며, 인증 기관 서버 측의 보안성이 중요하기 때문에 인증 앱 개발 비용과 서버의 보안 비용이 증가하고, 암호화에 사용되는 키관리의 비용이 발생한다[2].

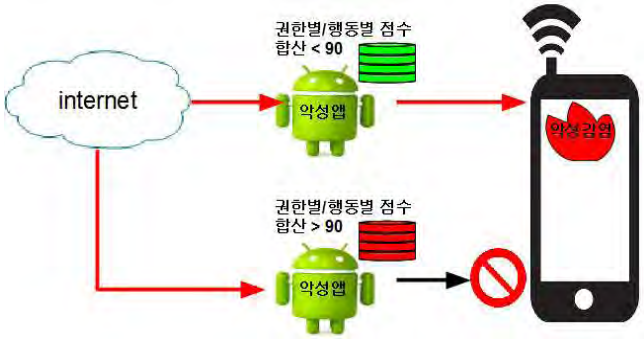

그림 4 악성 앱 사전 검증 모델 우회 공격 시나리오

기존 Host기반 스미싱 방지 모델 중 악성 앱 사전 검증 모델의 경우에는 다른 모델에 비해 오탐율이 낮은 모델이나 완전히 오탐률을 제거할 수 없을 뿐만 아니라, 차단 선택권을 사용자에 제공함으로써 이로 인한 피해 가능성이 존재한다[2]. 또한, 악성 앱 사전 검증 모델은 그림4와 같이 악성 여부를 점수기반으로 하기 때문에 일정 점수이하인 앱에 대해서 악성앱을 정상이라고 오판할 가능성이 존재한다.

기존 Host 기반의 탐지 모델뿐만 아니라 서명되지 않은 앱에 대한 다운로드 및 설치에는 문제가 있다.

4. 전자서명을 이용한 모델 제안

본 모델은 Network환경에서 전자서명을 이용한 스미싱 방어 모델로, 스미싱 공격이 마켓에 등록되지 않은 앱이 검증이 없이 설치 되는 것을 막는 것을 아이디어로 출발한다.

본 모델은 네트워크 기반에서 유입된 트래픽 중 문자 메시지를 분석하여, 문자메시지 중에서 URL이 포함된 경우 트래픽을 우회하여 라우팅을 전환시켜 URL을 포함한 문자메시지 트래픽에 대해서 별도의 망구간으로 분리를 시킨다. 별도 분리된 URL이 포함된 트래픽에 대해서 apk파일 다운로드가 없는 경우에는 통과를 시키고, apk 파일 다운로드를 시도하는 트래픽에 대해서는 전자서명을 검사후, 서명이 안되어 있는 경우 차단을 한다. 이는 기본적으로 전자서명이 되지 않은 apk파일에 대한 다운로드를 원천적으로 봉쇄함으로써 스미싱 공격에 대한 근복적인 방어를 하는 방식이다.

제안 모델의 동작 방식은 다음과 같다.

1. 미러링 장치를 통한 문자 메시지 트래픽을 센서부에 유입한다.

2. 센서부에서는 유입된 문자 메시지 트래픽에 대하여 분석하여 URL 포함여부를 판단한다.

3. URL이 포함되어 있는 경우, 센서부에서는 단축 URL 또는 일반 URL에 대해서 스미싱 서버의 IP를 추출하는 작업과 클라이언트 IP를 추출하는 작업을 수행하고, 추출된 스미싱 서버 IP와 클라이언트 IP에 대한 트래픽 우회 전환을 위한 동작을 수행한다.

4. 센서부에서 트래픽 우회 전환 동작이 수행되게 되면

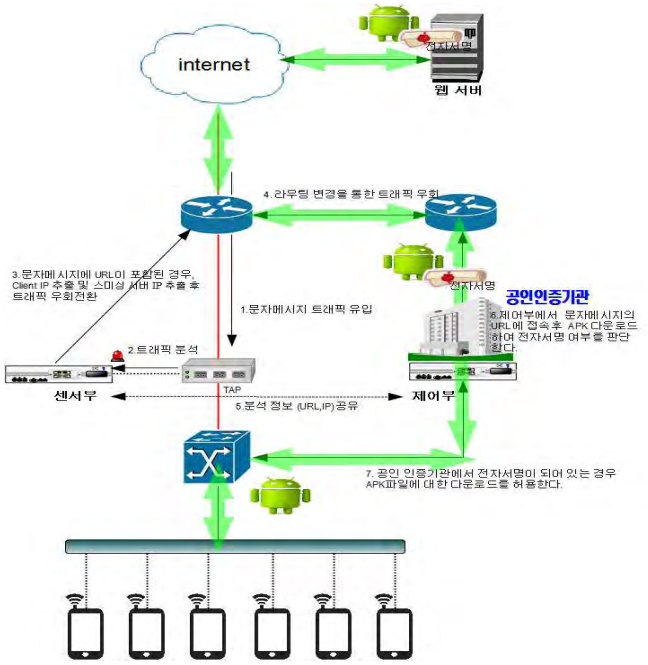

그림 5 제안된 모델 동작 방식-1

라우팅 변경을 통하여 그림5과 같이 트래픽을 제어부로 우회 시킨다.

4-1. 트래픽이 우회된 이후부터 추출된 스미싱 서버 IP를 목적지 IP로 하는 클라이언트에 대한 모든 트래픽은 제어부를 통하여 통신을 하게 된다.

4-2. 또한, 클라이언트 IP를 목적지 IP로 하는 트래픽 유입에 대해서도 제어부를 통하여 통신하게 된다.

5. 센서부에서 분석된 단축 URL 또는 일반 URL 정보와 스미싱 서버 IP정보를 제어부와 공유한다.

6. 제어부는 공유 받은 정보를 기반하여 URL에 접속한 후 실행앱(apk)을 다운로드하여 전자서명여부를 판단한다.

7. 제어부에서 분석한 결과에 대해 그림5과 같이 전자서명이 되지 않은 경우에는 차단을 하도록 한다. 이후 클라이언트가 동일한 실행 앱을 다운로드하려는 경우 차단되게 된다.

8. 제어부에서는 전자서명 뿐만이 아니라 스미싱 서버 IP를 목적지 IP로 하는 통신 트래픽에 대해서 감시를 함으로써 이미 스미싱 공격이 이루어진 클라이언트에 대해서

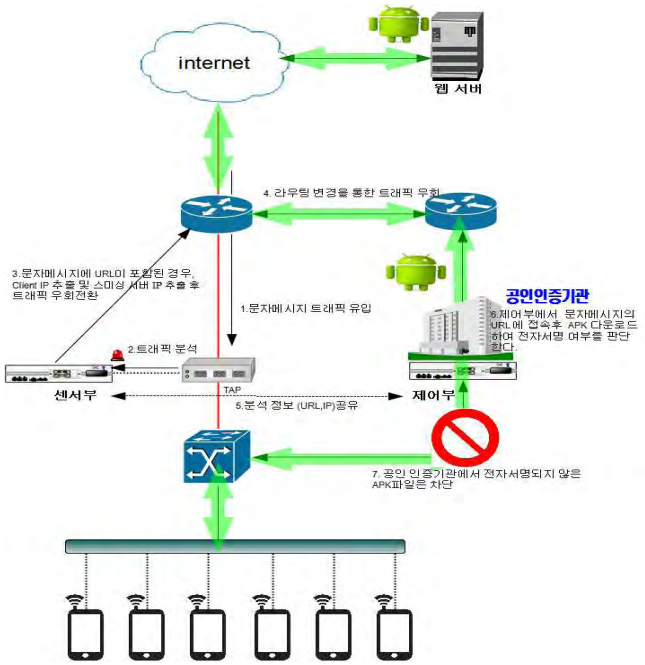

그림 6 제안된 모델 동작 방식-2

도 제어가 가능하다.

9. 제어부는 그림6과 같이 전자서명이 되어 있는 앱의 경우에는 다운로드를 허용한다..

기존에 Host 기반 탐지 모델의 한계점을 극복하고, Host 기반 탐지의 단점을 Network 기반으로 전환함으로써 스미싱 방어에 대한 효율성을 높였다.

본 논문에서 제안된 모델의 경우에 사용자 스마트폰에 악성 앱에 대한 판단을 하기전에 네트워크상에서 URL이 포함된 경우, 트래픽을 우회하여, 정상 트래픽과 스미싱으로 의심되는 트패픽을 분리하여 격리를 시킨 상태에서, 격리된 트래픽에 대해서 전자서명 여부를 판단하도록 한다. 이렇게 함으로써 사용자 스마트폰에서 앱이 직접 실행되지 않고 스미싱 공격에 대한 대응이 가능하며, 스마트폰에서 악성앱이 실행될 가능성을 최소화하여 스미싱 공격 피해 가능성을 최소화할 수 있다.

또한, 앱 권한 검사 모델에서 앱 권한 검사 우회 공격 시나리오[그림2]에서 발생할 수 있는 공격 가능성에 대해서 본 논문에서 제안된 모델에서는 Host 단말에서 수행하는 것이 아니라 네트워크상에서 수행함으로써 앱 권한 검사 우회 공격에 발생할 수 있는 위협요소를 사전에 방지할 수 있다.

실험조건은 동일한 실험시나리오를 기준으로 각 10회의 공격시도 후 Host기반 앱 권한 검사 모델과 제안된 모델에서 각 방어 횟수를 비교 분석하였다.

공격에 대한 방어 여부는 개인정보(주소록)를 획득을 못하였을 경우 방어로 판정하였다. 이미 알려진 공격과 변형 공격의 비율은 50%: 50%로 하였다.

	실험 시나리오	시도 회수	Host 기반 앱	제안된 모델
조건 #1	URL/문자열 검사 모델 우회공격	10	10	10
조건 #2	앱 권한 검사 우회 공격	10	0	10
조건 #3	악성 앱 사전 검증 모델 우회 공격	10	10	10
조건 #4	Root권한 획득 후 개인정보유출	10	10	10
조건 #5	정상적인 앱 위장 (정상앱과 동일한 권한)	10	0	10

표 2 실험 조건-1

5. 결론

본 연구에서는 기존에 Host 기반 탐지 모델을 Network 기반에서 사용하게 되는 경우의 한계점을 극복하고, Host 기반 탐지시 발생할 수 있는 우회공격에 대해서 Network 기반으로 전환함으로써 스미싱 방어에 대한 효율성을 높였다. 또한 전자서명과 공격트래픽을 격리 시킴으로써 망에 대한 안정성을 보장하며, 격리된 트래픽 개인정보, 이메일, 주소록, 금융정보 등의 트래픽에 대해서 감시 및 제어 함으로써 이미 스미싱 공격이 이루어진 스마트폰에 대한 대응도 가능하였다.

그리고 실험을 통해서 동일한 조건의 스미싱 공격을 기존 Host기반의 모델과 Network기반의 제안된 모델을 비교하였을 때 제안된 모델이 기존 Host기반의 모델보다 스미싱 공격에 대한 방어가 더 효과적임을 확인 하였다.

본 논문에서는 전자서명을 이용한 스미싱 방어 모델을 제시하였지만, 제안된 모델을 우회하는 공격 시나리오의 존재 여부와 대응 방법에 대해서 연구를 수행할 예정이다.

참고문헌

[1] 장준혁, 환승환, 조유근, 최우진, 홍지만, “안드로이드 환경의 보안 위협과 보호 기법 연구 동향”, 『보안공학연구논문지』, 제11권 제 1호, pp.01-12, 2014년 2월.

[2] 박상호, 이준형, “인증 및 사전 권한 검증을 통한 스미싱 방지 시스템 제안”, 『정보보호학회지』, 제23권 제6호, pp.5-11, 2013년 12월.

[3] 이훈재, “스마트폰 신종범죄의 유형 및 경찰 대응방안에 관한 연구”, 『한국경찰연구 』, 제11권 제4호, pp.319-344, 2012년 12월.

[4] 김민철, 서태원, “안드로이드 플랫폼에서 네트워크 패킷 분석을 통한 스미싱 보안 사례 연구”, 『한국컴퓨터교육학회』, 제 17권 제2호, pp.325-329, 2010 6월.