정 보 보 호 학 회 지
제23권 제6호, 2013. 12

인증 및 사전 권한 검증을 통한 스미싱 방지 시스템 제안

박 상 호*, 이 준 형**

요 약

본 논문은 최근 가장 이슈화 되고 있는 스미싱 위협의 방지에 대해 다루며, 단순히 스미싱 방지뿐만 아니라 탐지율 향상, 오탐률 감소를 위해 새로운 모델을 제안한다. 첫 번째 모델은 문자메시지 송/수신 시 특정 인증 값을 첨부/확인하여 정상 기관 인증을 수행하는 모델이며, 두 번째 모델은 문자메시지에 첨부된 URL을 사용자가 메시지 수신을 확인하기 전에 사전 검증하여 악성 유무를 판별하는 모델이다. 두 모델의 기본 동작 방식 제안과 설계를 통해 장점과 단점을 언급한다.

Ⅰ. 서 론

스마트폰 및 스마트 뱅킹에 의해 사용자들의 생활은 더욱 더 편리해졌지만, 안타깝게도 보안 위협은 여전히 존재한다. 기존에 PC 환경에서 행해지던 금융사기는 스마트 폰을 겨냥한 고도화된 기법으로 바뀌고 있다. 대표적으로 소액결제, 금융피싱을 유도하기 위해 제작되는 악성 어플리케이션(이하 악성 앱)의 증가를 예로 들 수 있다. 아래 그림 1은 2013년 3월까지 진행된 스마트폰에서 악성 앱을 이용한 금융사기에 대한 통계이다.

[1] 악성 앱 발생 건수 (당월기준)

시기	'12.1	'12.10	'12.12	'13.1	'13.3
발행	1건	3건	8건	55건	207건

[2] 악성 앱 행위 유형

구분	소액결제	금융피싱	DDos
현황	223 (85%)	21 (8%)	18 (7%)

〔그림 1〕 스마트폰 금융 사기 통계

이들 악성 앱의 주요 특징은 수신된 문자 메시지를 탈취하여 해커에게 전송하도록 설계되어 있는 점이며, 해커는 이러한 문자로 전달되는 정보를 가로채어 소액결제 사기라는 2차 공격에 악용한다.

본 논문은 이러한 스마트 뱅킹 사용자 증가에 따른 고도화된 금융사기 피해 방지를 위한 모델 중에서 문자메시지를 통해 악성 앱을 유포하는 스미싱 기법을 방지하기 위한 시스템을 제안한다. 단순히 피해 방지뿐만 아니라 탐지율 향상, 오탐률 감소를 고려한 새로운 모델을 제안하며, 이를 통해 금융사기 피해를 줄이고 스마트 폰 사용자의 스미싱 위협을 해소할 수 있도록 기여할 것이다.

본 논문의 2장에서는 스미싱과 기존에 존재하는 방지 모델에 대해 살펴보며, 3장에서는 기존 방지 모델의 한계를 지적한다. 4장에서는 정상 기관 인증 및 악성 어플리케이션 사전 검증 시스템 제안을 하며, 5장의 결론으로 끝을 맺는다.

Ⅱ. 관련연구

2.1. 스미싱

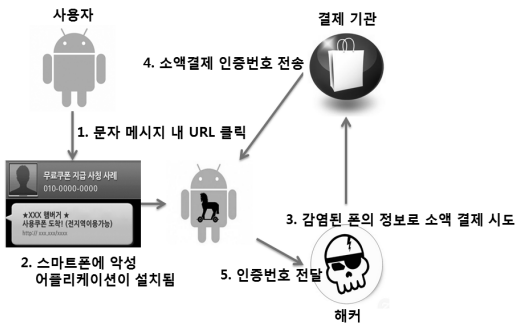
스미싱이란 '문자메시지(SMS)를 이용해 개인정보 또는 금융정보를 낚는다(Phishing)'는 의미의 합성어이

* 라온시큐어 보안기술연구팀 (ddeok9@gmail.com)
** 건양대학교 정보보호학과 (saiwnsgud@gmail.com)

다. 기본적으로 발신자의 신원을 속인 문자메시지를 통해 악의적인 사용자가 첨부한 링크에 접속하게 한 후, 악성 앱을 설치하여 스마트폰 내의 개인정보 또는 금융정보를 탈취하는 사기 수법이다. 국내에서는 악성 앱 설치 후 휴대폰 결제 인증 SMS를 탈취하여, 피해자가 인지하지 못한 상태에서 휴대폰 결제를 완료시키는 수법으로 사용되고 있다. 또한, 기존에는 발신자의 신원을 무작위 익명으로 진행하였으나, 현재는 웹하드, 커뮤니티 등에서 특정 계정 정보를 탈취한 후 지인 또는 정상 기관으로 사칭하여 해당 계정과 관계가 있는 지인들에게 문자메시지를 보내는 고도화 된 수법도 진행되고 있다.

스미싱 공격은 감염시킬 스마트 폰에서 동작할 악성 앱을 반드시 설치해야 하는 문제점 때문에 공통적으로 문자메시지 안에 악성 앱 다운로드를 위한 URL링크가 포함되어 있는 특징이 있다. 대부분 실제 URL이 아닌 단축 URL 서비스를 거친 사용자가 알아볼 수 없는 URL로 변환하여 문자 메시지를 발신한다.

아래 그림 2는 국내에서 가장 많이 사용되는 스미싱 공격인 소액결제 공격의 동작 방식을 간략하게 나타낸 그림이다.



〔그림 2〕 스미싱 공격 방식(소액결제)

두 번째 단계인 ‘스마트폰에 악성 앱 설치’가 진행되면 악성 앱은 해커에게 전화번호부, 문자메시지, 사진(보안카드가 포함될 수 있음) 등과 같은 개인정보를 수집하여 메일 또는 문자메시지를 자동으로 전송한다. 이를 통해 해커는 감염된 폰에서 소액 결제에 필요한 모든 정보를 획득할 수 있으며, 결제기관에 결제 요청을 할 수 있다.

그리고, 다섯 번째 단계인 ‘인증번호 전달’ 단계에서는 악성 앱이 브로드캐스트로 뿌려지는 문자 메시지를 가장 먼저 가로채어 사용자에게는 소액결제 인증번호가 포함된 문자메시지를 보여주지 않고, 해커가 운영하고 있는 서버에만 해당 정보를 전송한다. 또한, 소액 결제가 완료 되었다는 문자도 사용자에게 보여주지 않는 방식을 사용한다. 결국 사용자는 자신의 폰에 온 문자메시지를 전혀 모른 상태로 청구서를 받고 나서야 소액결제 피해를 입은 것을 알 수 있다.

2.2. 기존 스미싱 방지 모델

스미싱 피해가 심각해짐에 따라 각 통신사 및 보안업체에서는 스미싱 방지를 위해 어플리케이션(이하 앱)을 배포하고 있다. 현재 안드로이드 스미싱 방지 어플리케이션(이하 스미싱 방지 앱)은 총 16개가 등록되어 있으며, 아래 표 1은 스미싱 방지 앱의 탐지 모델을 크게 URL/문자열 검사와 설치된 악성 앱 권한 검사로 나눈 표이다.

〔표 1〕 스미싱 방지 앱 탐지 모델별 분류

탐지 모델	스미싱 방지 앱 이름
URL/문자열 검사	S-GUARD
	SMS 피싱
	피싱캅
	링크스캔
	뭐야 이 문자
	피싱제로
	Smishing Defender
	유후
	엠엔 메시지 통
설치된 앱 권한 검사	올레 스미싱 차단
	뭐야 이 문자
	앱 보안관
	라인 백신
	알약 안드로이드
	스파이 수사대
	스마트 안티스파이

URL/문자열 검사 모델은 악의적인 URL 링크 또는 스미싱 관련 문자열이 존재하면 스미싱 문자로 간주하고 사용자에게 알림을 준다. URL 세부 검사를 지원할 경우 단순히 URL에 포함된 ‘.apk’ 확장자 유무 검사를 하여, 확장자가 존재하면 사용자에게 알림을 준다. 설치된 앱 권한 검사 모델은 일반적인 앱의 경우 필요가 없는 권한 또는 스미싱 피해를 유발하는 악성 앱의 권한과 유사한 앱을 실시간으로 탐지하여 사용자에게 알린다.

각 탐지 모델 별로 탐지율 및 오탐률이 차이가 나며, 설치된 앱 권한 검사의 경우 URL/문자열 검사 방식에 비해 오탐률이 낮은 장점이 있다. 이와 같은 이유로 높은 탐지율 및 오탐률을 자랑하는 앱은 모두 해당 방식을 사용하고 있다.

Ⅲ. 기존 모델의 문제점

3.1. 발신지 검증의 부재

기존 스미싱 방지 모델은 문자메시지의 발신지 검증을 하지 않고, 문자 메시지의 내용 및 설치되는 악성 앱에 초점을 맞추어 설계되어 있다. 그러나 사람들의 낮은 보안 인식에 따른 피해 가능성을 고려하면, 발신자 검증의 부재는 심각한 문제이다. 지인 또는 금융권을 사칭한 스미싱 문자메시지 경우 사용자는 자신이 평소에 자주 접하던 곳에서 보냈기 때문에 안전하다고 생각하여 별다른 검사를 수행하지 않으며, 심지어 검사 결과가 악성 또는 위험으로 나오더라도 잘못된 탐지로 여기고 악성 앱을 설치한다. 이와 같이 사용자가 익히 알고 있는 발신지라 하더라도, 검증을 수행하지 않으면 스미싱 문자메시지 내용 및 설치되는 악성 앱 검증을 충분히 무력화 시킬 수 있다. 금융권 및 공기업의 정상 발신지 인증을 통해 가장 먼저 해당 문제점이 보안되어야 한다.

3.2 부적절한 검사 방식

스미싱 방지 앱 중 URL/문자열 검사 방식을 사용하는 ‘S-GUARD‘, ‘피싱제로’를 테스트 스마트 폰에 설치한 후 스미싱 문자와 일반 문자를 전송할 경우를 테스트하면 아래 내용과 같은 결과를 확인 가능하다.

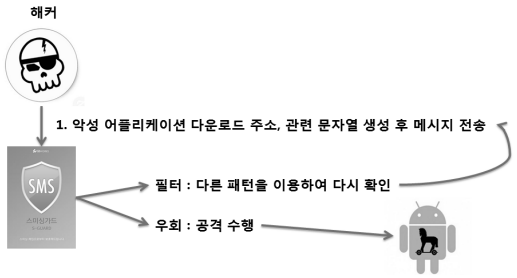
‘S-GUARD’는 현재 배포되고 있는 스미싱 해킹용 주소를 실시간 수집하여 탐지하는 방식을 사용한다. 테스트를 위해 10개의 악성코드 다운로드 주소를 신규 생성하여 문자메시지를 전송했으나 아무런 반응이 없으며, 악성코드를 다운로드한 후 설치를 하여도 아무런 반응이 없다.

‘피싱제로’는 스마트폰으로 수신되는 문자메시지를 자동 감지 후 URL 분석 기능을 통해 스미싱으로 예상되는 파일이 존재할 경우 사용자에게 위험을 알린다. 그러나 테스트 결과 실제 악성 앱 다운로드를 유발하는 URL을 첨부하였음에도 불구하고, 제대로 된 탐지를 하지 못하는 것으로 확인된다.

두 스미싱 방지 앱 모두 블랙 리스트에 등록된 URL을 기반으로 위험성을 판별하는 방식을 사용하기 때문에 이러한 문제가 발생한다. 아래 그림 3은 ‘피싱제로’에서 악성 URL을 첨부하였음에도 불구하고, 스미싱 문자메시지를 탐지하지 못한 화면이다.

〔그림 3〕 스미싱 문자메시지를 탐지하지 못한 화면

해커는 ‘S-GUARD’, ‘피싱제로’와 같이 URL이 기존에 악성으로 등록되었는지 여부를 확인하는 스미싱 방지 앱일 경우 테스트를 통하여 손쉽게 우회 가능하다. 가능한 시나리오를 도식화 하면 아래 그림 4와 같다.



〔그림 4〕 URL/문자열 검사 방식 우회 시나리오

우선 악성 앱 다운로드를 유도하기 위한 IP 또는 도메인 주소를 구매한 후 다운로드 주소를 생성한다. 그 후, 실제 스미싱 문자메시지를 배포하기 전에 스미싱 방지 앱이 설치된 스마트폰으로 문자메시지를 보내어 필터 여부를 확인한다. 만약 필터가 된다면, 다른 패턴 및 주소를 이용하여 다시 반복 확인을 수행하고, 우회된다면 사용자들에게 스미싱 문자메시지를 보낸다.

대부분의 사용자들은 스미싱 방지 앱을 중복해서 설치하고 있지 않기 때문에 ‘S-GUARD’, ‘피싱제로’와 같은 동작방식의 스미싱 방지 앱을 설치한 사용자의 경우 위 그림 4의 추가 방어책이 없어 그대로 스미싱 피해를 입을 가능성이 높다.

이와 같이 URL/문자열 검사를 통한 스미싱 방지 모델에서 부적절한 검사 방식을 적용할 경우 다양한 우회 시나리오와 높은 오탐률 등의 문제점이 존재한다. 때문에 최근에 출시되는 스미싱 방지 앱은 설치되는 악성 앱의 권한/상태를 검사하여 사용자들에게 위험을 알리는 방식을 사용하고 있다.

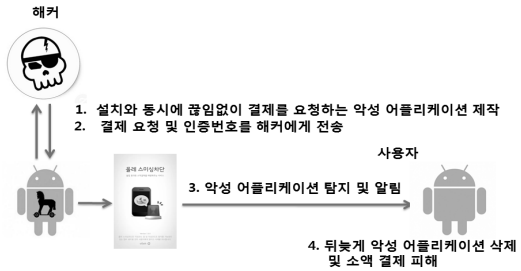
3.3 검사 시기의 부적절

최근 스미싱 방지 앱은 3.1절의 URL/문자열 검사 모델에서 나타나는 다양한 문제점들 때문에 설치된 앱의 권한검사를 하는 모델을 채택하고 있다. 그러나 이러한 방법에도 검사 시기의 부적절함에 따른 문제점이 존재한다. ‘올레 스미싱 차단’을 통해 해당 문제점을 확인하면 아래와 같다.

‘올레 스미싱 차단’은 이미 알려진 스미싱 URL 및 앱을 차단하는 기존 방식과는 달리 설치된 앱이 가지고 있는 기능을 파악하여 스미싱 동작 감염 여부를 알려주는 스미싱 방지 앱이다. 아래 그림 5는 악성 앱 탐지 결과 화면이다.

〔그림 5〕 악성 여부 탐지

사용자가 앱 설치를 하면, ‘올레 스미싱 차단’은 악성 앱이 소액결제 사기 행위를 하기 위해 필요한 권한인 ‘사용자의 SMS/MMS 내용 확인’, ‘인터넷 접속’등의 권한이 설치된 앱에 존재하는지 확인한다. 권한이 존재할 경우 사용자에게 악성 앱일 수 있다는 알림을 준다. 이와 같이 설치 후에 검사를 하기 때문에 악성 앱의 공격 수행 시기에 따라 피해를 입을 수 있는 위험이 존재한다. 아래 그림 6은 설치 후 앱의 권한을 확인하는 모델의 우회 시나리오 이다.



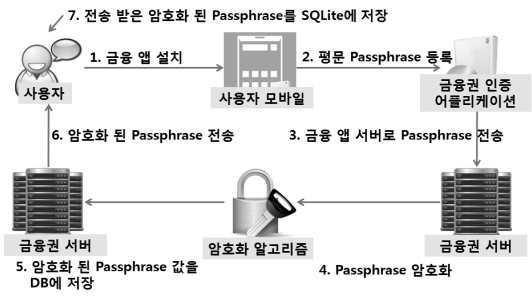
〔그림 6〕 설치된 앱 권한 검사 방식 우회 시나리오

악성 앱은 ‘올레 스미싱 차단’이 사용자에게 위험을 알리기 전에 결제 요청 및 인증번호 전송을 끊임없이 수행하여 사용자가 악성 앱을 삭제하기 전에 피해를 입게 만들 수 있다. 이와 같이 검사 시기의 부적절함으로 인해 사용자들에게 스미싱 피해 위험이 존재한다.

Ⅳ 정상 기관 인증 및 사전 검증 시스템 제안

4.1 정상 기관 인증 모델

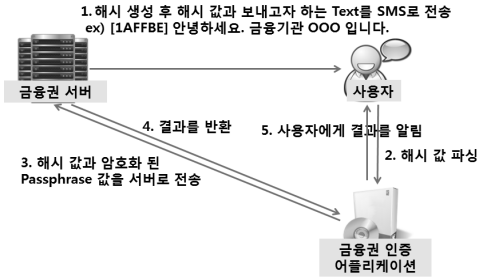
해당 모델은 ‘사용자 고유의 Passphrase를 이용 해 금융권 기관과 사용자 간의 일대일 신뢰관계를 형성’을 기본 아이디어로 삼고 있다. 사용자 등록 과정과 사용자 인증과정으로 나뉘게 되며, 그림 7은 사용자 등록 과정을 도식화한 그림이다.



〔그림 7〕 사용자 등록 과정

사용자는 금융권에서 제공하는 인증 어플리케이션(이하 인증 앱)을 정상적인 경로를 통해 다운로드 받아 자신의 모바일에 설치한다. 그 후, 사용자는 인증 앱에 8~16글자 사이의 문자열을 등록하고, 인증 앱은 사용자가 등록한 Passphrase 문자열을 서버로 전송한다. 서버는 사용자의 Passphrase 문자열을 AES 암호 알고리즘으로 암호화 한 후 데이터베이스에 사용자 식별번호와 암호화 된 Passphrase를 저장한다. 다음으로 서버는 사용자 인증 앱에게 암호화 된 Passphrase를 전송하고, 인증 앱은 전달 받은 암호화 된 Passphrase 값을 사용자 모바일에 /data/data/[앱의 패키지 이름]/files/과 같은 경로에 SQLite 파일 형태로 저장한다.

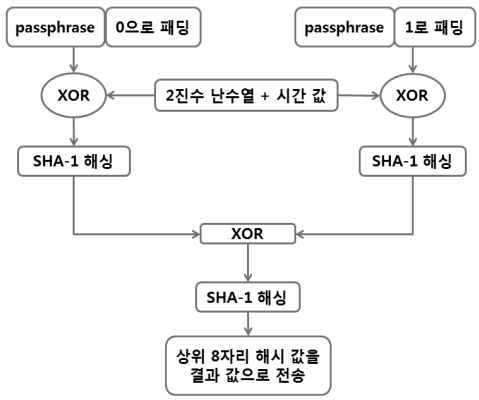
사용자 등록을 완료하면 사용자와 금융권 기관간의 1차 신뢰관계가 형성 된다. 완전한 신뢰 관계를 형성하기 위해서는 사용자 인증 과정이 진행되어야 한다. 사용자 인증 과정은 아래 그림 8과 같다.



〔그림 8〕 사용자 인증 과정

금융권 서버는 서버에 등록된 사용자의 Passphrase를 복호화 하여 평문 Passphrase를 획득 후 해시 값을 생성한다. 추후 검증을 위해 해시 알고리즘에서 사용되었던 난수 값과 해시 값을 사용자 별로 금융권 서버에서 저장하고, 생성한 해시 값은 사용자에게 보내고자 하는 Text와 함께 사용자에게 전송 된다. 그 후, 사용자 스마트 폰의 인증 앱이 금융권에서 특정 형태로 전송 된 문자메시지를 감지하고 해당 문자메시지에 포함되어 있는 해시 값을 파싱한다. 다음으로 인증 앱이 파싱한 해시 값과 SQLite에 저장된 사용자의 암호화된 Passphrase를 금융권 서버로 전송하며, 금융권 서버에서 사용자가 보낸 암호화된 Passphrase를 데이터베이스에서 검색하고, 검색한 Passphrase 값을 복호화 한다. 그 후 복호화 된 Passphrase와 첫 번째 단계에서 사용자 별 Passphrase와 함께 저장되어 있던 난수를 이용 해 해시 값을 생성한 후 인증 앱이 보낸 해시 값과 금융권 서버가 생성한 해시 값이 일치한지 확인한다. 일치한다면 인증 앱에게 이 사실을 알리고, 결과 값을 인증 앱에게 보냄과 동시에 저장하고 있던 난수와 해시 값을 삭제한다. 마지막으로 인증 앱이 금융권 서버로부터 받은 결과를 사용자에게 알려준다. 만약 인증 앱이 금융권 서버로부터 일치하다는 결과를 받았다면 현재 검증을 시도한 문자메시지는 금융권에서 전송한 정상 문자메시지라고 할 수 있다.

사용자 인증 과정에서 사용되는 해시 알고리즘은 HMAC 알고리즘을 변형한 알고리즘으로, 난수열과 Passphrase가 사용 된다. 아래 그림 9는 해시 알고리즘을 도식화 한 그림이다.



〔그림 9〕 해시 알고리즘 순서도

해시 알고리즘에서는 XOR 연산에 사용되는 Passphrase 문자열의 길이를 16으로 맞추기 위해 패딩(Padding)을 수행하고, 생성 된 난수열 16자리와 함께 XOR 연산을 수행한다. 수행 된 XOR 연산 결과 값은 SHA-1 해시 알고리즘으로 해시 연산하고 연산 된 두 Passphrase 해시 값을 다시 XOR 연산과 SHA-1 해시 연산을 수행한다. 그 후 마지막으로 생성 된 해시 값 상위 8자리를 문자 메시지와 함께 사용자에게 보낼 해시 값으로 사용한다.

사용자 등록 과정과 사용자 인증 과정이 모두 정상적으로 수행 될 경우 사용자와 금융권 정상 기관은 사용자의 Passphrase와 Passphrase에 대한 서버의 해시 값으로 인해 최종적으로 서로 일대일 신뢰관계를 형성하게 된다.

4.2 악성 앱 사전 검증 모델

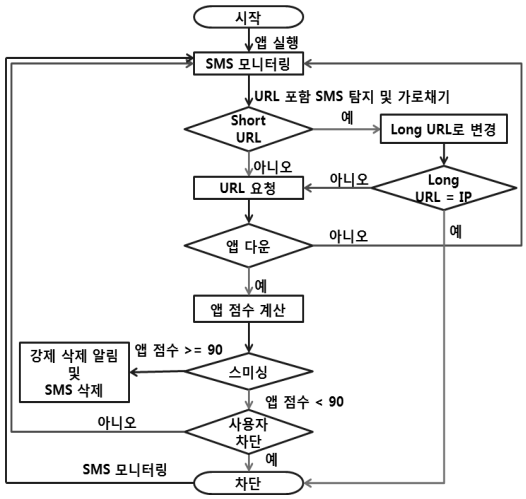
해당 모델은 ‘악성 앱 행동 탐지 및 악성 여부 점수 책정’을 핵심 아이디어로 하는 모델이다. 기존에 알려진 악성 앱들의 행동에 대한 통계를 통해 산출한 행동 패턴을 기반으로 검사를 진행하며, 최근 유포 되고 있는 4000여 종류의 악성 앱 행동 패턴을 확인한 결과 악성 앱에서는 많이 사용하고, 정상 앱에서는 자주 사용하지 않는 권한이 아래 표 2와 같이 나타난다.

〔표 2〕 악성 앱에서 사용하는 권한 선별

권한	설명
INTERNET	인터넷 기능
ACCESS_COARSE_LOCATION	데이터 네트워크를 이용한 위치 확인 기능
ACCESS_FINE_LOCATION	Wi-Fi를 이용한 위치 확인 기능
READ_PHONE_STATE	단말기의 상태 읽기 기능
READ_SMS	SMS 읽기 기능
SEND_SMS	SMS 전송 기능
READ_CONTACTS	주소록 읽어오기
RECEIVE_BOOT_COMPLETED	부팅 완료 후 서비스로서 실행되는 기능
RECEIVE_SMS	SMS 수신 기능
WRITE_SETTINGS	환경 설정 변경
RECORD_AUDIO	오디오 수신

해당 통계에서 산출 된 권한 별로 점수를 부여하여 스미싱 문자에 포함된 URL에서 다운로드하는 앱의 점수를 계산 한다. 일정 점수 이상인 앱은 사용자에게 강제 차단 알림을 알리며, 일정 점수 이하인 앱은 사용자 차단 여부를 알리는 메시지 창을 띄어 사용자가 미리 알고 있는 앱인지 확인한 후 차단 여부를 결정한다. 아래 그림 10은 관련 모델의 순서도 이다.

해당 모델의 기능을 가지는 탐지 어플리케이션(이하 탐지 앱)이 실행되면 모바일 플랫폼 백그라운드에서 사용자 모바일로 도착하는 문자메시지의 내용을 모니터링 한다. 그 후, 모니터링 중 URL을 포함한 문자메시지가 도착 할 경우 탐지 및 차단 여부 확정을 위한 동작이 진행 되는 동안 사용자에게 문자메시지를 보여주지 않기 위해 문자메시지를 가로채고, 문자메시지에 포함되어 있는 URL이 단축 URL인지 원본 URL인지 파악하며,



〔그림 10〕 점수 책정 모델 순서도

만약 단축 URL이라면 원본 URL로 변환하는 과정을 거친다. 이때 원본 URL이 도메인이 아닌 IP 형태로 되어 있다면, 이는 공격자의 서버로 의심하고 바로 차단한다. 원본 URL이 도메인 형태라면 일반 기업의 URL일 수도 있으므로 해당 URL을 통해 서버에 통신을 요청하고 요청 응답의 내용에서 ‘PK’ 시그니쳐(Signature)가 있는지 확인한다. ‘PK’시그니쳐가 있다면 어플리케이션 파일일 가능성이 높다. 또한 ‘*.apk’ 확장자가 응답 내용에 포함되어 있는지도 확인 한다. 이러한 경우 해당 어플리케이션은 악성 앱 혹은 악성 앱의 동작을 수행할 가능성이 높으므로, 다운로드 되는 앱에게 다른 앱이 접근하지 못하도록 탐지 앱의 고유 경로에 다운로드 된 앱을 격리 한 후 어플리케이션을 검증하기 위해 압축을 해제하고 AndroidManifest.xml 파일에 명시되어 있는 권한을 확인 하여 아래 표 3에서 명시한 대로 점수를 계산한다.

점수 계산이 끝나면 해당 앱의 점수가 90점을 넘는지 확인한다. 90점 이상이면 악성 앱이 하는 대부분의 행동을 하는 앱으로 판단하며, 해당 앱의 다운로드를 유도한 문자메시지를 강제 삭제한다는 알림을 사용자에게 알린 후 문자메시지를 삭제한다. 해당 앱의 점수가 90점 미만이라면 악성 앱의 행동을 가지고 있지만, 그 행동이 정상 앱의 기능을 위한 행동일 수 있으므로 사용자에게 앱의 행동과 악성 앱 여부의 점수를 알리며 허용 및 차단의 선택권을 부여한다. 사용자가 차단을 선택하면 문자메시지를 가로챈 상태에서 문자메시지 및 격

〔표 3〕 점수 계산 표

점수 부여 항목	점수
다운로드 되는 파일이 'PK' 시그니처를 가지고 있는 경우	35
응답 내용에 '.apk' 확장자가 포함되어 있을 경우	5
압축 해제 후 AndroidManifest.xml 파일이 존재 하는 경우	5
INTERNET 권한	8
ACCESS_COARSE_LOCATION 권한	5
ACCESS_FINE_LOCATION 권한	5
READ_PHONE_STATE 권한	3
READ_SMS 권한	8
SEND_SMS 권한	6
READ_CONTACTS 권한	3
RECEIVE_BOOT_COMPLETED 권한	5
RECEIVE_SMS 권한	6
WRITE_SETTINGS 권한	3
RECORD_AUDIO 권한	3

〔표 4〕 정상 기관 인증 모델의 장점과 단점

		내용
장점	일회성	악성 앱은 금융권 정상 메시지를 사칭하기 위해 해시 값을 알아야 한다. 해시 값을 생성하기 위해서는 사용자의 Passphrase와 난수를 알아야 한다. 하지만 해당 값을 구하는데 큰 시간이 소모되는 반면, 해시 값의 수명은 10분이 되지 않기 때문에 해시 값을 역으로 해독 해 유효한 해시 값을 구현하는 것은 불가능하다.
	기술응용	해당 모델은 인증이라는 것에 초점을 두어 고안되었기 때문에 인증을 필요로 하는 모든 단체, 기관 등에 적용 이 가능하다.
	구현용이	해당 모델은 서버와 클라이언트의 네트워크 통신만 필요하기 때문에 인증 시스템 구축이 용이하다.
단점	루팅 시 무력화	해당 모델은 일반 사용자 환경에서는 Passphrase 문자열이 저장되어 있는 인증 앱 고유 경로에 인증 앱만 접근 할 수 있어 강력한 인증 능력을 발휘하지만, 루팅(Rooting) 환경에서는 사용자 인증 과정에서 악성 앱이 인증 앱 고유 경로에 존재하고 있는 Passphrase를 루트 권한으로 탈취하여 인증 앱을 사칭, 인증 과정에 참여 할 수 있다.
	비용증가	해당 모델은 인증 앱이 구현되어야 하며, 서버 측의 보안성이 중요하기 때문에 인증 앱 개발 비용과 서버의 보안비용이 증가하고, 암호화에 사용 되는 키 관리의 비용이 발생한다.

리 된 앱을 삭제하고, 허용을 선택하면 격리된 앱은 삭제 하되, 사용자 모바일의 문자메시지 저장소에 문자메시지를 저장한다.

모든 과정이 끝나면 탐지 앱은 다시 문자 메시지 모니터링을 수행함으로 사용자 스마트폰을 스미싱 위협으로부터 보호한다.

4.3 제안 모델의 장단점 분석

제안 모델인 정상 기관 인증 모델과 악성 앱 사전 검증 모델의 장점과 단점은 아래와 같다. 기존의 스미싱 방지 모델에 비해 많은 점이 개선되며, 두 모델을 함께 수행할 경우 기존에 연구한 문제점을 벗어나, 더욱 높은 스미싱 방지 효과를 낼 수 있다. 정상 기관 인증 모델이 구현되고 운용됨으로써 발생 할 수 있는 장점과 단점은 표 4와 같다.

악성 앱 사전 검증 모델이 구현되고 운용됨으로써 발생 할 수 있는 장점과 단점은 아래 표 5와 같다.

〔표 5〕 악성 앱 사전 검증 모델의 장점과 단점

		내용
장점	높은 효율	모바일 플랫폼이라는 제한된 환경에서 사용 할 수 있는 자원을 최대로 사용하며, 플랫폼 자체에 부담을 적게 주는 모델이다.
	높은 탐지 낮은 오탐	기존 모델 중 URL/문자열 검사 모델은 블랙 리스트를 기반으로 해 수집되지 않은 새로운 악성 URL을 탐지해 내지 못하는 반면, 해당 모델은 URL을 대상으로 탐지하는 것이 아닌 URL을 통해 다운로드 되는 앱의 행동 패턴을 기반으로 정상 문자메시지와 악성 문자메시지를 탐지/구분하여 정상 문자메시지와 악성 문자메시지의 판별력이 다른 모델들에 비해 월등하다.
	우회 가능성 감소	기존 모델 중 설치 후 앱 권한을 체크할 경우 앱의 동작 방식에 따라 피해를 입을 가능성이 존재하는 반면, 해당 모델은 사전 탐지를 진행하기 때문에 이와 같은 우회 가능성을 줄일 수 있다.
단점	오탐률 제거불가	다른 모델들에 비해 오탐률이 낮은 모델이나, 완전한 오탐률 제거는 되지 않는다.
	사용자 선택	다른 모델들이 해결하지 못한 사용자에게 차단 선택권을 제공한다는 점으로 인해 피해 가능성이 존재한다.

V. 결 론

본 논문에서는 기존 스미싱 방지 어플리케이션 모델의 부적절한 기술을 분석하고, 우회 가능한 시나리오 제시를 통해 한계를 확인하였다. 이러한 한계점을 극복하기 위해 정상 기관 인증 수행 모델과 악성 어플리케이션 사전 검증 모델을 제안 하고 설계 및 장/단점을 언급하였다. 제안 모델은 모두 다른 분야에도 확장 가능한 모델로 금융권뿐만 아니라 사용자 인증이 필요한 모든 곳에서 사용할 수 있고, 악성 어플리케이션 검사 시에도 기존과는 다른 새로운 탐지 방법으로 사용할 수 있다. 향후 본 논문에서 제시한 설계를 기반으로 도구 구현을 할 시 첫 번째 모델이 구축되어 서비스됨으로써 해당 모델을 사용하는 사용자는 악의적인 해커의 금융기관 사칭 위험으로부터 벗어나며, 만약 사용자의 실수로 인하여 해커가 유도한 서버로 접속하였을 때 두 번째 모델을 적용함으로써 사용자의 악성 앱 감염을 탐지 및 차단할 수 있다. 이로 인해 기존 스미싱 방지 어플리케이션보다 높은 탐지율과 안전성을 제공하여 사용자들의 스마트 폰 사용에 도움이 될 것으로 예상된다.

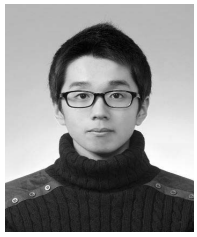
참고문헌

[1] 심재홍, “금융 소비자를 위협하는 악성코드 위협사례 분석”, *한국인터넷진흥원*. pp. 8-10, 2013.05

[2] 권용주. “최근 발생한 신종금융사기 수법에 대한 조치사항 및 이용자 유의사항”, *금융감독원*, pp. 2-4, 2013.07

〈저자소개〉

박 상 호 (Park Sangho)
2011년 12월~현재 : 라온시큐어 보안기술연구팀 주임연구원
<관심분야> 디지털 포렌식, 정보보호, 취약점 분석



이 준 형 (Lee Jun Hyeong)
2009년 3월~현재 : 건양대학교 정보보호학과 재학
<관심분야> 디지털 포렌식, 정보보호, 취약점 분석