https://doi.org/10.14400/JDC.2017.15.4.285

스미싱 공격 방지를 위한 클라우드 메시징 서비스

박효민*, 김완석**, 강소정**, 신상욱**
부경대학교 대학원 정보보호학협동과정*, 부경대학교 IT융합응용공학과**

Cloud Messaging Service for Preventing Smishing Attack

Hyo-Min Park*, Wan-Seok Kim, So-Jeong Kang**, Sang Uk Shin****
Interdisciplinary Program of Information Security, Graduate School, Pukyong National University*
Dept. of IT Convergence and Application Eng., Pukyong National University**

요 약 스마트 디바이스에 대한 악의적인 공격들이 빠르게 진화하고 있고, 이들 공격에 대해 스마트 디바이스를 적절하게 보호하는 것은 매우 중요한 이슈로 부각되고 있다. 특히, 스미싱 공격은 스마트 폰에서 가장 중요한 위협들 중의 하나로 주목되고 있다. 이 논문에서는 스미싱 공격의 위험으로부터 사용자를 근본적으로 보호할 수 있는 클라우드 서비스를 제안한다. 제안된 클라우드 메시징 서비스는 사용자 스마트 디바이스에서 URL을 포함한 텍스트 메시지들을 필터링하여 클라우드 서버에 의해 제공되는 가상 머신을 통해 필터링된 메시지들을 확인하고 관리할 수 있는 클라우드 서비스를 제공한다. 기존의 스미싱 방지 기법들이 이미 알려진 패턴의 악성코드에 대해서만 보호하거나, 오탐(FP) 또는 미탐(FN) 등의 오류 가능성을 내포하고 있지만, 제안 기법은 URL을 포함하고 있는 모든 문자 메시지들을 자동적으로 필터링하여 클라우드 서버 상의 저장공간에 저장하고 확인 및 관리하기 때문에 스마트 디바이스에서 스미싱 공격에 의한 멀웨어(악성코드)의 설치를 완벽하게 차단할 수 있다.

주제어 : 스미싱 공격, 스마트 디바이스, 클라우드 컴퓨팅, 가상 머신, 피싱, 멀웨어

Abstract They are rapidly evolving malicious attacks on smart devices, and to timely protect the smart devices from these attacks has become a very important issue. In particular, smishing attack has emerged as one of the most important threats on the smartphone. In this paper, we propose the cloud service that can fundamentally protect the user from the risk of smishing attack. The proposed scheme provides cloud messaging service that can filter text messages including URLs in the user's smart device, view and manage them through a virtual machine provided by a cloud server. The existing techniques for preventing smshing attacks protect only malicious code of a known pattern and there is the possibility of error such as FP(False Positive) or FN(False Negative). However, since the proposed method automatically filters all text messages including URLs, storing, viewing, and managing them in their own storage space on the cloud server, it can completely block the installation of malwares(malicious codes) on the user's smart device through smishing attacks.

Key Words : Smishing attack, Smart device, Cloud computing, Virtual machine, Phishing, Malware

* 이 논문은 부경대학교 자율창의학술연구비(2016년)에 의하여 연구되었음.
Received 2 March 2017, Revised 3 April 2017
Accepted 20 April 2017, Published 28 April 2017
Corresponding Author: Sang Uk Shin
(Pukyong National University)
Email: shinsu@pknu.ac.kr

ISSN: 1738-1916

1. 서론

오늘날 스마트폰, 태블릿과 같은 스마트 디바이스의 발달에 따른 보급이 확산되면서 사용자 수가 급속히 증가함에 따라 스마트 디바이스는 모바일 오피스, 스마트 뱅킹, 주식 거래, 전자 정부와 같은 민원 처리, 영화 예약 등의 각종 생활 편의 서비스, 모바일 인스턴트 메신저 서비스와 SNS(social networking service) 등에 폭넓게 활용되고 있다. 이에 따라 사용자의 개인정보나 업무에 활용할 기업의 중요 정보가 스마트 디바이스에 저장되고 폭넓게 이용되고 있다[6].

그 중에서도 활용 빈도가 상대적으로 매우 높은 서비스는 모바일 인스턴스 메신저 서비스나 SNS이다. 이 서비스들은 단지 문자만을 보내고 받는 것이 아니라 URL(Uniform Resource Locator)을 문자 메시지에 넣어 전송할 수도 있고, 수신자는 스마트 다비이스에서 수신한 문자 메시지에 표시된 URL을 클릭하여 동영상, 이미지, 웹페이지 등을 확인할 수 있다. 또한 모바일 전자 금융 거래의 편리함과 스마트 디바이스의 발달 때문에 스마트폰 등을 활용한 금융거래의 양이 매년 빠른 속도로 증가하고 있다[3,4]. 이와 같은 스마트 디바이스의 편리함으로 인해 최근에는 스마트 디바이스의 사용 시간이 기존 PC(Personal Computer)의 사용 시간을 추월하고 있는 추세이다. 이러한 현상은 스마트 디바이스의 디스플레이가 점점 커지고 성능도 크게 향상되고 있기 때문에 더욱 심화될 것으로 예상된다.

이와 같이 스마트 디바이스의 사용 시간이 점점 늘어나고 신규 서비스를 제공하는 앱(App)들이 많이 등장하고 있지만, 보안 위협에 대한 대응과 사용자 보호를 위한 보안 기술의 발전은 그에 미치지 못하고 있어서 사용자의 피해와 우려가 커지고 있는 실정이다. 피싱(phishing)에서부터 멀웨어(malware)까지 스마트 디바이스에 대한 악의적인 공격들이 끊임없이 행해지고 있다. 악의적인 공격, 특히 스마트 디바이스에서 금융 사기 시도는 최근 수년간 만연해지고 있다. 스마트 디바이스에서의 악의적인 공격들은 빠르게 진화하고 있으며, 이러한 공격들로부터 스마트 디바이스를 시기적절하게 보호하는 것은 매우 중요한 이슈가 되었다[7,8,9,10]. 특히, 스미싱(smishing) 공격은 스마트 폰에서 가장 중요한 위협 중의 하나로 부각되고 있다. 스미싱은 문자 메시지(SMS, short message service)와 피싱(phising)의 합성어로서, 문자 메시지 내에 URL을 포함시켜 전송하면 사용자가 이를 클릭하여 원치 않은 멀웨어(악성 코드)가 스마트 디바이스에 설치됨으로써 사용자의 개인 정보를 빼내어 가거나 소액 결제가 자동으로 이루어지도록 하는 사기 기법을 말한다[1,2]. 이에 대응하기 위해 스미싱 공격을 탐지하고 차단하기 위한 보안 앱들이 개발되어 앱 스토어 등을 통해 배포되고 있고, 또한 출처가 명확하게 확인되지 않은 URL을 클릭하지 않도록 여러 언론매체 등을 통해 직간접적으로 교육과 홍보가 이루어지고 있다. 하지만, 대부분의 스미싱 공격 대응 보안 앱들은 기존에 이미 알려진 패턴들의 악성 코드에만 유효하게 작동하기 때문에 완벽한 방지 및 대응책이 되지 못한다. 또한 매우 다양한 형태의 새로운 스미싱 수법들이 계속 등장하고 있기 때문에 사용자가 조심한다고 하더라도 부지불식간에 URL를 클릭하는 경우가 많이 발생하고 있다.

본 논문에서는 위와 같은 기존의 문제점을 해결하기 위해 스미싱 공격의 피해로부터 사용자를 원천적으로 보호할 수 있는 클라우드 메시징 서비스 시스템을 제안한다. 제안 기법은 URL이 포함된 문자 메시지를 사용자의 스마트 디바이스에서 자동적으로 필터링하여 클라우드 서버의 사용자 메시징 저장공간에 전송하고 클라우드 서버 상에서 제공되는 가상머신을 통해 메시지들을 확인 및 관리할 수 있는 클라우드 메시징 서비스를 제안한다. 기존의 스미싱 방지 기법들이 기존에 알려진 정형화된 패턴의 악성코드에 대해서만 보호하거나, 미검출 또는 오탐 등의 오류 가능성을 내포하고 있는 단점을 가지고 있으며, 또한 사용자 보안 교육이나 스마트 디바이스의 보안 설정 등을 요구하는 것에 비해, 제안 기법은 URL을 포함하고 있는 모든 문자 메시지들을 자동적으로 필터링하여 클라우드 서버 상의 저장공간에 저장하고 확인 및 관리하기 때문에 스마트 디바이스에서 스미싱 공격에 의한 멀웨어(악성코드)의 설치를 완벽하게 차단할 수 있다.

본 논문의 2장에서는 스미싱과 기존의 방지 기법들을 간단히 살펴보고, 3장에서 클라우드 서비스를 이용한 스미싱 방지 기법을 제안하며, 4장의 결론으로 끝을 맺는다.

2. 관련 연구

2.1 스미싱 공격(smishing attack)

스미싱(Smishing)은 문자 메시지(SMS)와 피싱(Phishing)을 합성한 신조어로, 스마트 디바이스에서 문자 메시지에 연결된 URL 링크 수단을 이용하여 피싱하는 공격을 말한다[5]. 공격자는 스마트 디바이스에서 사회공학적 문자 메시지에 포함된 URL을 클릭하게 하여, 사용자가 알지 못하게 자동 결제, 금액 이체, 소액 결제 등을 유발시켜서 금융 피해를 발생시킨다. 또한 URL 링크를 포함하고 있는 Smishing 문자 메시지에서 URL을 클릭하게 되면, 멀웨어(악성 코드)를 자동적으로 다운로드되어 설치되며 사용자가 알지 못하게 트로이목마 등의 해킹 공격 툴을 이용하여 사용자의 스마트 디바이스를 제어하여 침해사고를 일으켜 금융피해를 유발하게 된다[1,2].

스미싱 공격의 동작 과정은 [Fig. 1]과 같이 악의적인 공격자가 URL 링크를 클릭하도록 유도하는 문자 메시지를 피해자에게 발송한다. 사용자가 확인을 위해 URL을 클릭하게 되면, 악성코드가 포함된 앱이 다운로드된다. 그리고 특별한 의심 없이 사용자가 설치를 진행하게 되고, 설치된 후에는 사용자의 개인정보가 무단으로 유출되며, 사용자가 알지 못하게 소액결제가 진행되어 금전적 피해를 발생시킨다[3].

[Fig. 1] Process of smishing attack[3,5]

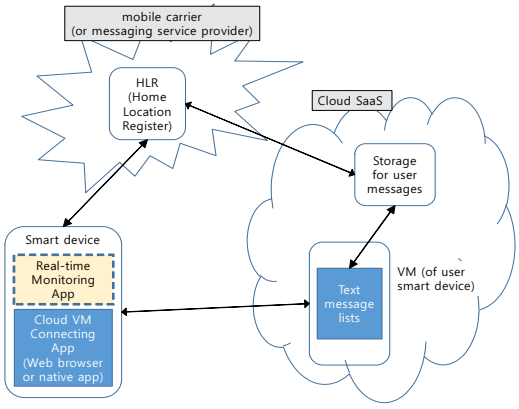
2.2 스미싱 방지 기법

스마트 디바이스, 특히, 스마트폰에 대한 스미싱 공격 방지를 위한 여러 기법들이 제안되었다. 이들 기법들을 특성에 따라 분류하면, 다음과 같이 크게 3가지로 분류할 수 있다[11,12].

- 컨텐츠 기반 필터링(content-based filtering): 이 기법은 의심스러운 URL에 대해 콘텐츠가 조사되고 URL의 콘텐츠와 일치하는지를 검사한다[14,15]. 이 기법은 전통적인 스팸 필터링 기법을 보완하며, 규칙 기반과 통계적 기반으로 분류될 수 있다[13].
- 블랙리스트(blacklist): 블랙리스트는 검증에 인간을 필요로 하는 방법이다. 웹 사이트 집합이 알려진 피싱 URL들로 명시적으로 리스팅된다[16]. 이 기법은 매우 낮은 긍정 오류(false positive)를 가지기 때문에 산업체에서 피싱에 대응하기 위해 광범위하게 적용되고 있다. 블랙리스트 URL 정보를 얻기 위해 신뢰 서버와 통신하는 방법으로 다양한 브라우저에서 지원되고 있다.
- 화이트리스트(whitelist): 이 기법은 사용자가 자신이 신뢰하고 자주 접근하는 웹사이트를 명시한다. 이 리스트에 명시되지 않은 사이트들은 의심스러운 URL로 조사된다. 이 기법은 가짜 웹 주소를 포함한 SMS를 수신하지 않도록 스미싱 검출을 위해 사용될 수 있다[15].

3. 제안 기법

3.1 클라우드 서비스를 이용한 스미싱 방지 기법



[Fig. 2] System model

제안 기법은 스마트폰에 대한 스미싱 공격으로부터 사용자를 보호하는 것을 목표로 한다. 제안 기법은 [Fig. 2]와 같이 사용자 스마트 디바이스, 이동통신 사업자(또는 메시징 서비스 제공자), 클라우드 서버로 구성된다. 여

기서 이동통신 사업자는 서비스 가입자의 식별 번호, 위치 정보 등의 기본 정보와 부가 서비스 정보들을 저장하는 HLR(Home Location Register) 시스템을 관리하며, 서비스 가입자에게 전송되는 메시지들을 전달한다. 이동통신 사업자의 부가 서비스 제공 여부에 따라 URL이 포함된 문자 메시지들을 직접 필터링하여 클라우드 서버로 전달할 수 있다. 클라우드 서버는 사용자의 메시지를 저장하기 위한 저장 공간과 DaaS(Desktop as a Service)[17]와 같은 가상 데스크탑을 제공하는 클라우드 서비스를 적용하여 사용자 스마트폰 환경과 동일한 가상의 스마트폰 VM(Virtual Machine)을 사용자에게 제공한다. 그리고, 사용자는 자신의 스마트폰을 이용하여 전용 프로그램 또는 웹 브라우져를 통해 스마트폰 VM에 접속한다. 이동통신 사업자가 URL 포함 메시지에 대한 직접 필터링을 제공하지 않는 경우에는 사용자 스마트 디바이스에 실시간 모니터링 앱이 설치되어야 한다. 이 모니터링 앱은 자동적으로 URL 포함 문자 메시지들을 필터링하여 클라우드 서버에 전달하여 개인별 저장 공간에 저장한다.

제안하는 스미싱 방지 서비스는 문자 메시지를 수신하는 단계와 문자 메시지를 확인하는 단계로 구성된다.

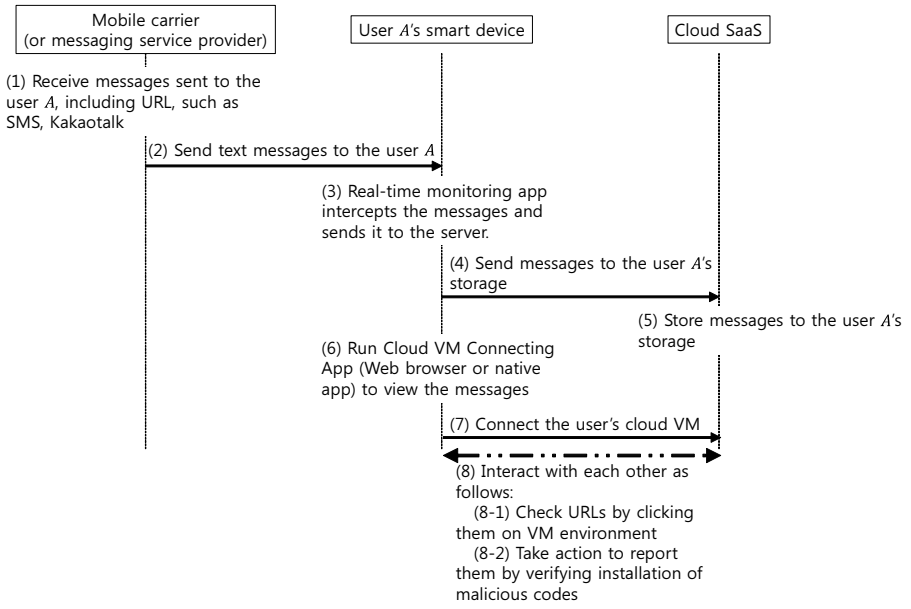
- 문자 메시지를 수신하는 단계: 스마트폰에서 모니터링 앱이 설치되어 동작하는 형태와 이동통신 사업자가 직접 서비스를 제공하는 형태로 동작할 수 있다.
  - 첫 번째 형태의 경우, 스마트폰의 커널 레벨에서 문자 메시지를 실시간으로 모니터링한 후, 탐지된 인터넷 주소 URL 포함 문자 메시지를 클라우드 상의 사용자 계정의 문자 메시지 저장 공간으로 전달하는 과정으로 동작한다.
  - 두 번째 동작 형태의 경우, 이동통신 사업자 쪽에서 사용자에게 수신되는 인터넷 주소 URL 포함 문자 메시지를 직접 클라우드 상의 사용자 계정의 문자 메시지 저장 공간으로 전달하는 과정으로 동작한다.
- 문자 메시지를 확인하는 단계 : 사용자가 스마트폰을 이용하여 클라우드 서비스를 통해 스마트폰 VM에 접속하여 문자 메시지를 확인하는 단계, 스마트폰 VM 환경에서 문자 메시지에 포함된 인터넷 주소 URL을 클릭하여 확인하는 단계, 악성 코드 설치 등의 문제가 발생하면 이를 신고하는 단계를 포함하여 구성된다.

제안 기법인 클라우드 메시징 서비스를 활용한 스미싱 방지 기법의 구체적인 동작 과정을 [Fig. 3]과 [Fig. 4]에서 보여준다. 문자 메시지를 수신하는 단계는 이동 통신 사업자의 서비스 제공 여부에 따라 두 가지 형태로 구현될 수 있다. 사용자의 스마트폰에 실시간 모니터링 앱이 직접 설치되어 동작하는 형태와 이동통신 사업자가 직접 서비스를 제공하는 형태로, 두 가지 방법으로 동작할 수 있다.

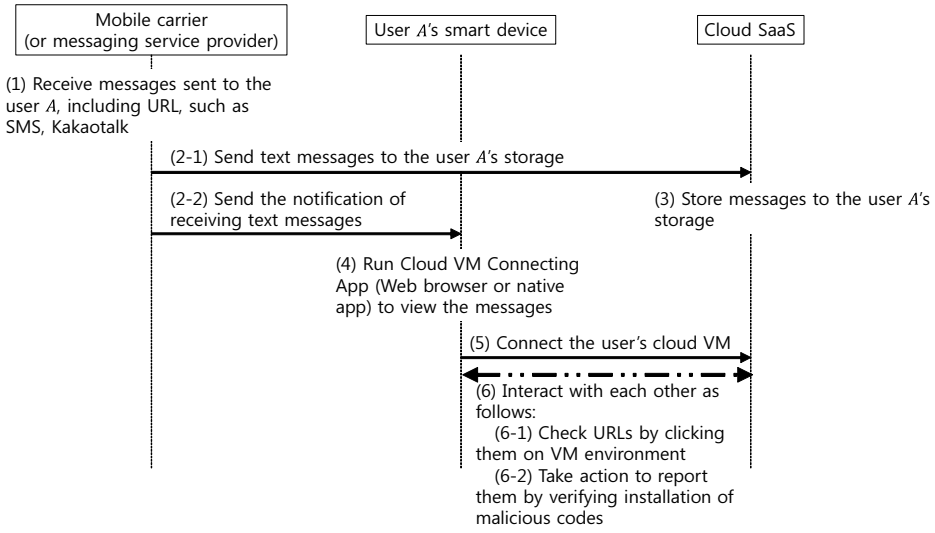
첫 번째로 앱이 설치되어 동작하는 형태의 경우, [Fig. 3]에서 보듯이 SMS, 카카오톡과 같이 스미싱 공격 위협이 있는 메시지들을 실시간 모니터링하는 앱이 사용자의 스마트폰에 직접 설치된다. 이 앱은 스마트폰의 커널 레벨에서 동작할 수도 있고, 또는 메모리 상주 프로세스로 동작할 수도 있다. 실시간 모니터링 앱이 스마트폰에 수신되는 SMS, 카카오톡 등의 인터넷 주소 URL이 포함된 문자 메시지를 실시간으로 탐지한다. 서비스 사용을 위해 사용자는 클라우드 컴퓨팅 서비스에 가입하여, 자신의 스마트폰 환경과 동일한 가상의 스마트폰 VM을 생성하여 할당받는다. 할당받은 VM은 스마트폰에 설치된 전용 앱 또는 웹 브라우져를 통하여 접속할 수 있다. 이는 현재 클라우드 컴퓨팅 서비스로 제공되는 DaaS와 같은 가상 데스크톱 서비스의 형태로 사용자에게 제공될 수 있다. 클라우드 컴퓨팅 서비스 제공자는 스마트폰 운영체제가 설치된 가상의 VM을 사용자들에게 할당하고, 문자 메시지를 저장할 수 있는 저장 공간을 할당한 후, DaaS와 같은 클라우드 서비스 형태로 사용자에게 서비스할 수 있다.

스마트폰에 설치된 실시간 모니터링 앱이 인터넷 주소 URL이 포함된 문자 메시지를 탐지하면, 이 문자 메시지를 클라우드 상의 사용자 계정의 문자 메시지 저장 공간으로 전달한다. 사용자에게는 인터넷 주소 URL이 포함된 문자 메시지가 수신되어 클라우드 VM에 전달되었다는 것을 알려줄 수 있다.

두 번째 동작 형태의 경우, [Fig. 4]에서 보듯이 이동통신 사업자나 메시징 서비스 사업자 쪽에서 사용자에게 수신되는 인터넷 주소 URL 포함 문자 메시지를 직접 클라우드 상의 사용자 계정의 문자 메시지 저장 공간으로 전달하는 과정으로 동작한다. 이동통신 사업자의 경우, 사용자 스마트폰의 전화번호로 수신되는 문자 메시지를 필터링하여 인터넷 주소 URL을 포함하는 문자 메시지를 클라우드 상의 사용자 계정의 문자 메시지 저장 공간으



[Fig. 3] Cloud message service for preventing smishing attack through real-time monitoring app



[Fig. 4] Cloud message service for preventing smishing attack through mobile carrier

로 전달한다. 사용자 스마트폰에는 문자 메시지가 클라우드로 전달되었다는 것을 알려준다. 메시징 서비스 사업자 역시 유사하게 사용자 계정으로 전달되는 메시지들 중에서 인터넷 주소 URL을 포함하는 문자 메시지들을 필터링하여 클라우드 상의 사용자 계정의 문자 메시지 저장 공간으로 전달하고, 사용자에게 이를 알려준다.

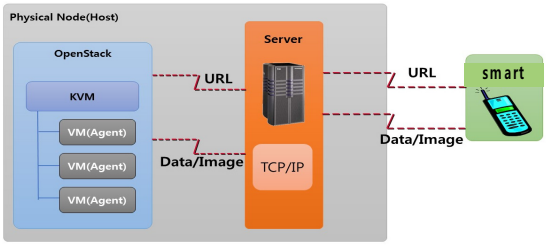
두 번째 단계인 문자 메시지 확인 단계는 앞의 두 가지 메시지 수신 단계의 동작 방법들에 대해 동일하게 동

작한다. 사용자가 클라우드 메시징 서비스를 사용하여 인터넷 주소 URL이 포함된 문자 메시지를 확인하기 위해서는 전용 앱이나 웹 브라우져를 사용하여 자신의 VM에 접속한다. 이때 사용자 로그인 과정을 통해 사용자 확인을 수행한다. 자신의 VM에 접속한 후, 문자 메시지 저장 공간에 저장된 문자 메시지들을 읽어 온 후, 문자 메시지를 확인할 수 있다. 이때 문자 메시지에 포함된 인터넷 주소 URL을 클릭하여 확인할 수 있다.

만약 스미싱 공격의 문자 메시지인 경우 URL을 확인하게 되면, VM에 악성 코드가 설치될 것이다. 이는 가상의 VM 환경이기 때문에 사용자에게 어떤 손실도 발생하지 않을 것이며, 또한 공격이 발생한 것을 쉽게 확인할 수 있게 된다. 이를 사용자가 바로 신고할 수 있을 것이다.

3.2 간단한 테스트 모델 구현 결과

제안 기법의 동작 가능성을 보여주기 위해, 간단한 테스트 모델을 아래 [Fig. 5]와 같이 구성하여 구현 결과를 제시한다. 오픈스택을 이용한 클라우드 서비스 기반 스미싱 공격 방지 시스템과 GoogleSafeBrowsing API를 활용하여 가상의 인스턴스에서 사용자가 스마트폰에서 클릭한 URL의 악성코드 유무를 판별하고 실행결과의 화면의 이미지와 판별결과 값을 사용자에게 알려주어 스미싱 공격을 방지하도록 구현하였다.



[Fig. 5] Simplified test model of the proposed scheme

안드로이드 앱은 문자메시지의 URL을 클라우드에 전달, 접속하기 위한 매개체 역할을 한다. 또한, TCP/IP를 통하여 서버와 통신을 하여 악성코드 포함의 유무와 URL이 실행된 캡쳐 화면을 서버를 통해 전달 받는다. 실행했던 URL을 SQLlite를 이용하여 DB에 저장하여 사용자가 눌렀던 URL목록들을 볼 수 있다. 그리고 이 목록들을 통해 내가 눌렀던 URL들 중 어떠한 URL이 악성코드가 포함된 것인지 알 수 있다.

클라우드의 VM(agent)는 클라우드에서 생성된 가상의 운영체제로써 클라우드 서버에서 넘겨받은 URL을 Jsoup과 Google Safe Browsing API를 통해 악성코드의 유무를 판별한다. 또한 캡쳐한 실행화면과 악성코드의 판별유무를 다시 서버에게 보내준다.

[Fig. 6]는 테스트 모델의 실행 결과를 보여준다. 사용자의 스마트폰에서 URL이 포함된 스팸 메시지에서 URL을 클릭한다. URL을 클릭 하였을 때 실행가능 한 앱 목록에 개발한 앱이 나타난다. 앱을 실행하면 클라우드와 연결이 되고 클라우드는 다시 가상의 운영체제인 인스턴스로 접속을 하게 된다. 인스턴스에서 넘겨 받은 URL의 악성코드 유무를 판별하고 그 URL을 실행한다. 실행 된 화면을 이미지로 캡쳐하여 서버로 보내주고 서버는 다시 사용자에게 악성코드 판별 유무와 실행화면을 보내준다.

[Fig. 6] Execution result of the proposed model

3.3 고찰

제안 서비스를 사용하면, 사용자는 스미싱 공격의 위협에 대해 신경쓸 필요없이 문자 메시지에 포함된 인터넷 주소 URL을 확인할 수 있다. 만약 스미싱 공격을 위한 문자 메시지인 경우에도 가상의 스마트폰 VM에 악성코드가 설치되므로 사용자의 실제 스마트폰은 손상을 입지 않는다. 이는 기존의 스미싱 공격의 위협에 대한 대처 방안이나 예방 방법이 사용자 보안 교육을 통해 대처하거나, 또는 기존에 알려진 스미싱 공격 문자 메시지의 패턴을 탐지하여 사용자에게 경고하는 보안 앱을 통한 차단 방법들이 있지만, 여전히 이러한 방법들은 모든 스미

싱 공격들을 효과적으로 방지할 수가 없다. 본질적으로 사용자가 100% 신뢰성 있게 행동하는 것을 기대할 수 없다.

피싱이나 스미싱 방지 기법의 평가 척도 관점에서 가장 중요한 척도는 오류율이며, 특히 오탐(FP, False Positive)와 미탐(FN, False Negative) 오류율이 중요하다.

- 오탐(FP) : 정상적인 메시지를 공격 메시지로 잘못 판단하는 오류
- 미탐(FN) : 공격 메시지를 공격이 아닌 정상적인 메시지로 잘못 판단하는 오류

URL을 포함한 메시지를 수신하는 사용자 입장에서 보면, 오탐은 정상적인 문자 메시지를 스미싱 공격 메시지로 판단하여 차단시킴으로써 사용자가 문자 메시지를 수신하지 못하는 문제가 발생한다. 반대로 미탐의 경우에는 정상적인 메시지로 판단하여 URL을 클릭했는데 스미싱 공격이 실행되어 피해를 입게 되는 문제가 발생한다. 두 가지 모두 사용자 입장에는 손해/손실이 발생하게 된다. 기존의 기법들은 모두 비교적 높은 오탐(FP) 또는 미탐(FN) 오류가 발생한다. 이 오류들을 동시에 모두 줄이는 것은 기존 기법의 경우 매우 어렵다. 구현된 방식에 따라 조금씩 다르지만 대체적으로 기존 기법들의 경우, 0.1%~17%의 FP 오류율, 또는 0.1%~30%의 FN 오류율을 보인다[18]. 하지만, 제안 기법의 경우, URL을 포함한 모든 메시지들은 사용자의 클라우드 메시지 저장 공간에 저장되고, 사용자가 이들 메시지를 VM 상에서 확인할 수 있기 때문에 정상적인 메시지를 수신하지 못하는 문제(오탐의 문제)는 발생하지 않는다. 또한 VM 상에서 모든 메시지를 확인할 수 있기 때문에 미탐의 경우 역시 문제가 되지 않는다. VM 상에서 확인한 메시지가 스미싱 공격 메시지인 경우에도 VM에 악성 코드가 설치되므로, 사용자의 스마트 디바이스는 아무런 영향을 받지 않는다. 따라서 미탐으로 문자 메시지를 확인하는 경우에도 공격으로부터의 손실이 전혀 발생하지 않는 장점이 있다.

2.2절에 기술된 스미싱 공격 방지를 위해 제시된 기존의 기법들과 비교해 보면<Table 1>, 컨텐츠 기반 필터링 기법 자체는 스마트 디바이스에서 스미싱 검출을 위해 구현되기에는 비효율적이라는 문제점이 있다[11,12]. 블랙리스트는 DB 갱신과 검증 관점에서 비효율적이며, 다른 기법들에 비해 사용자 보호 관점에서 더 적은 능력을 가지고 있다[16]. 화이트리스트 기법은 모든 정당한 URL을 포함할 수 없다는 제한 사항을 가진다. 또한 알려진 URL, 즉, 사용자가 알고 있는 지인으로부터의 공격 또는 지인을 사칭/위장한 공격들은 검출할 수 없다는 문제점을 가지고 있다. 기존의 스미싱 방지 기법들과 스미싱 차단 보안 앱들은 공통적으로 기존에 알려진 특정 패턴들만을 차단하므로, 새로운 형태의 스미싱 공격은 방지할 수가 없다는 한계점을 가지고 있다. 하지만 제안 기법은 기존의 이러한 문제점들을 해결할 수 있다.

〈Table 1〉 Comparison of methods for preventing Smishing attack

Method	Advantage	Disadvantage
Blacklist based	• Effective in detecting known patterns	• Only can detect attacks from the known senders (attackers) • Cannot detect new attacks • Less efficiency in updating and verify the attack in database
Whitelist based	• Have list of trusted senders	• Cannot detect attacks from the known senders (or attacker disguised as a trusted sender) • Need to collect the list of trusted senders
Content Based	• Flexible	• Less efficient • Highly dependent on the rules or statistics applied.
Proposed method	• No need to worry about missing legitimate messages • No need to worry about whether it is smishing message or not • The user's device is not affected by the attack.	• Require individual VM • Require the installation of the real-time monitoring app as needed

일단 URL이 포함된 문자 메시지는 클라우드 메시지 저장 공간에 저장되고, 사용자는 VM에 접속하여 이를 확인함으로써, 알려지지 않은 새로운 형태의 스미싱 공격 패턴에 대해 대처할 수 있으며, 또한 스미싱 공격 메시지인지에 대해 걱정할 필요없이 메시지의 URL을 마음놓고 확인할 수 있다. 또한 기존 기법들의 경우 공격이

아닌 정상적인 URL을 포함한 메시지들이 오탐에 의해 필터링되는 경우가 발생하지만, 제안 기법의 경우 이러한 오류없이 모든 메시지를 놓치지 않고 확인할 수 있다. 또한 공격에 대한 대응을 위해 사용자들에게 보안 교육을 하거나 보안 설정 등의 대처를 사용자에게 요구할 필요가 없이 안전하게 동작가능하다.

4. 결론

스마트 디바이스가 전자금융거래, SNS 등의 다양한 서비스에 사용 빈도가 높아짐에 따라, 스마트 디바이스에 대한 악의적인 공격들 역시 빠르게 진화하고 있으며, 이러한 공격들로부터 스마트 디바이스를 시기적절하게 보호하는 것은 매우 중요한 이슈가 되고 있다. 특히, 스미싱 공격은 스마트 폰에서 가장 중요한 위협 중의 하나로 부각되고 있다.

본 논문에서는 클라우드 서비스를 활용한 스미싱 공격 방지 기법을 제안하였다. 제안 기법은 URL이 포함된 문자 메시지를 사용자의 스마트 디바이스에서 자동적으로 필터링하여 클라우드 서버의 사용자 메시징 저장공간에 전송하고 클라우드 서버 상에서 제공되는 가상머신을 통해 메시지들을 확인 및 관리할 수 있는 클라우드 메시징 서비스를 제안하였다. 기존의 스미싱 방지 기법들이 이미 알려진 패턴의 악성코드에 대해서만 보호하거나, 미검출 또는 오탐 등의 오류 가능성을 내포하고 있으며, 또한 사용자 보안 교육이나 스마트 디바이스의 보안 설정 등을 요구하는 것에 비해, 제안 기법은 URL을 포함하고 있는 모든 문자 메시지를 자동적으로 필터링하여 클라우드 서버 상의 저장공간에 저장하고 확인 및 관리하기 때문에 사용자의 스마트 디바이스에서 스미싱 공격에 의한 멀웨어(악성코드)의 설치를 완벽하게 차단할 수 있다. 제안 기법의 한 가지 제약 사항은 사용자별로 개별적인 클라우드 저장 공간과 VM의 할당을 요구하며, 필요에 따라 실시간 모니터링 앱의 설치가 필요하다는 것이다. 향후 연구로 사용자 스마트폰에 대한 클라우드 VM 서비스를 Smartphone as a service 형태의 클라우드 서비스로 진화시켜, 인증 등의 좀더 다양한 서비스로 발전시키는 방안에 관해 계속 연구할 계획이다.

ACKNOWLEDGMENTS

This work was supported by a Research Grant of Pukyong National University(2016 year).

REFERENCES

[1] D.W. 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, 2014.

[2] D.W. Park, “Analysis of Mobile Smishing Hacking Trends and Security Measures,” Journal of the Korea Institute of Information and Communication Engineering, Vol. 19, No. 11, pp. 2615-2622, 2015.

[3] S.Y. Lee, H.S. Kang, and J.S. Moon, “A Study on Smishing Block of Android Platform Environment,” Journal of the Korea Institute of Information Security and Cryptology, Vol. 24, No. 5, pp. 975-985, 2014.

[4] Yun-Young Song, Kyung min Han, “A Study of Response and Plan of Banks for Mobile Payments of Non-financial Corporations”, Journal of IT Convergence Society for SMB, Vol. 5, No. 2, pp.7-13, 2015.

[5] Smishing(2008), http://www.police.go.kr/portal/main/contents.do?menuNo=200287 (accessed Jun., 24, 2016).

[6] D.C. Kim, and J.C. Ryou, “The blocking method for accessing toward malicious sites based on Android platform,” Journal of the Korea Institute of Information Security and Cryptology, Vol. 24, No. 3, pp. 499-505, 2014.

[7] W.J. Park, K.H. Lee, S.J. Kim, and W. Ryu, “A financial fraud protection platform on Android smartphones in real-time,” Information and Communication Technology Convergence (ICTC), 2015 International Conference on. IEEE, pp. 1246-1248, 2015.

[8] Sik-Wan Cho, Won-Jun Jang, Hyung-Woo Lee, “Development of User Oriented Vulnerability Analysis Application on Smart Phone”, Journal of the Korea Convergence Society, Vol. 3, No. 2, pp. 7-12, 2012.

[9] Byung-Seok Yu, Sung-Hyun Yun, "The Design and Implementation of Messenger Authentication Protocol to Prevent Smart Phone Phishing", Journal of the Korea Convergence Society, Vol. 2, No. 4, pp. 9-14, 2011.

[10] Sunghyuck Hong, "Cognitive Approach to Anti-Phishing and Anti-Pharming : Survey", Journal of IT Convergence Society for SMB, Vol. 3, No. 2, pp.33-39, 2013.

[11] H. Shahriar, T. Klintic, and V. Clincy, "Mobile Phishing Attacks and Mitigation Techniques," Journal of Information Security, Vol. 6 No. 3, pp. 206-212, 2015.

[12] C.F.M. Foozy, R. Ahmad, and M.F. Abdollah, "Phishing detection taxonomy for mobile device," International Journal of Computer Science, Vol. 10, No. 3,pp. 338-344, 2013.

[13] P. He, X. Wen, and W. Zheng, "A Novel Method for Filtering Group Sending Short Message Spam," Proceedings of the International Conference on Convergence and Hybrid Information Technology, 2008. ICHIT'08, International Conference on, pp. 60-65, 2008.

[14] J.W Yoon, H Kim, and J. H Huh, "Hybrid spam filtering for mobile communication," Computers & Security, Vol. 29, pp. 446-459, 2010.

[15] T.T. Mahmoud, and A.M. Mahfouz, "SMS Spam Filtering Technique Based on Artificial Immune System," International Journal of Computer Science, Vol. 9, pp. 589-597, 2012.

[16] S. Sheng, B. Wardman, G. Warner, L. Cranor, J. Hong, and C. Zhang, "An Empirical Analysis of Phishing Blacklists," 6th Annual Conference on Email and AntiSpam (CEAS), 2009.

[17] Desktop as a Service(2016), https://en.wikipedia.org/wiki/Desktop_virtualization#Desktop_as_a_Service (accessed Jun., 24, 2016).

[18] M. Khonji, Y. Iraqi, and A. Jones, "Phishing Detection: A Literature Survey," IEEE Communications Survey & Tutorials, Vol. 15, No. 4, pp. 2091-2121, 2013.

박 효 민(Park Hyo Min)

- 2016년 2월 : 부경대학교 IT융합응용공학과(공학사)
- 2016년 3월 ~ 현재 : 부경대학교 정보보호학협동과정
- 관심분야 : 암호 프로토콜, 네트워크 보안
- E-Mail : oxeak846@gmail.com

김 완 석(Kim, Wan Seok)

- 2017년 2월 : 부경대학교 IT융합응용공학과(학사)
- 2017년 3월 ~ 현재 : 포스코ICT
- 관심분야 : 빅데이터, 인공지능
- E-Mail : kws911004@gmail.com

강 소 정(Kang So Jeong)

- 2016년 8월 : 부경대학교 IT융합응용공학과(학사)
- 2016년 7월 ~ 현재 : 한국선재 전산팀 사원
- 관심분야 : 모바일 프로그래밍, 웹 프로그래밍, 네트워크 보안, 데이터베이스
- E-Mail : rkdthwjd1111@naver.com

신 상 욱(Sang Uk Shin)

- 1995년 2월 : 부경대학교 전자계산학과(학사)
- 1997년 2월 : 부경대학교 전자계산학과(석사)
- 2000년 2월 : 부경대학교 전자계산학과(박사)
- 2000년 4월 ~ 2003년 8월 : 한국전자통신연구원 선임연구원
- 2003년 9월 ~ 현재 : 부경대학교 IT융합응용공학과 교수
- 관심분야 : 암호 프로토콜, 모바일 네트워크 보안, 디지털 포렌식, E-Discovery
- E-Mail : shinsu@pknu.ac.kr