모바일 하이퍼바이저를 이용한 신종 금융사기 예방에 관한 연구

서길원* · 문일영*

*한국기술교육대학교

A study of new type of financial fraud prevention using mobile hypervisor

Gil won Seo* · Il-young Moon*

Korea University of Technology and Education

E-mail : sgw4401@kut.ac.kr

요 약

2009년 이후부터 현재에 이르기까지 스마트폰 사용자는 꾸준히 증가하고 있다. 그리고 스마트폰의 애플리케이션을 사용하여 언제 어디서나 원하는 작업을 손쉽게 수행할 수 있게 되었다.

그러나 이러한 장점을 악용한 피싱, 파밍, 스미싱과 같은 신종 금융사기가 나타나게 되었고, 이로 인해 스마트폰을 사용하는 많은 사용자들이 금전적 피해를 입고 있다. 이에 본 논문에서는 모바일 하이퍼바이저를 이용하여 최근 사회적으로 이슈가 되고 있는 피싱, 파밍, 스미싱 피해를 예방할 수 있는 기술적 방안을 제안한다.

ABSTRACT

From 2009 to the present, smart phone users has been steadily increasing. And through the use of smart phone applications, smart phone user can perform easily what they want to do whenever and wherever.

However, new types of financial fraud such as phishing, pharming and smishing are appeared exploiting these advantages. Accordingly in this paper, I propose to prevent social issues like phishing, pharming and smishing for the technical way using mobile hypervisor.

모바일, 하이퍼바이저, 피싱, 파밍, 스미싱

Mobile, Hypervisor, Phishing, Pharming, Smishing

Ⅰ. 서 론

2009년 이후 스마트폰 사용자가 눈에 띄게 증가하였고, 2013년에는 약 26억 명이 스마트폰을 사용할 것으로 예상된다.

<그림 1> 전 세계 스마트폰 이용자 수 추이

스마트폰을 사용하는 가장 큰 이유는 스마트폰의 애플리케이션을 이용하여 언제 어디서나 원하는 작업을 손쉽게 수행할 수 있다는 장점 때문일 것이다. 그리고 무엇보다 스마트폰에서 가동되는 애플리케이션은 누구나 개발이 가능하며, 이를 마켓이라 하는 곳에 등록함으로써 애플리케이션을 몇 번의 터치로 쉽게 설치 및 사용할 수 있다.

그러나 "폰"이라는 휴대성과 "스마트"라는 편의성과 개방성으로 많은 사용자들의 삶의 패턴까지도 바꾸고 있는 스마트폰도 기계일 뿐이고 누군가에 의해 만들어진 프로그램을 사용하기에, 스마트폰 자체의 결함, 설치된 애플리케이션의 버그, SMS/MMS나 SNS 등을 통해 자신도 모르게 설치된 악성코드가 삽입된 애플리케이션으로 인한 해킹 및 정보유출 등 다양한 보안 취약점들이

존재할 수 있다.

특히 신종 금융사기라 불리는 피싱과 파밍, 그리고 스미싱으로 인해 많은 스마트폰 사용자가 금전적 피해를 보고 있다.

이에 본 논문에서는 모바일 하이퍼바이저를 이용하여 최근 사회적으로 이슈가 되고 있는 피싱, 파밍, 스미싱 피해를 예방할 수 있는 기술적 방안을 제안한다.

본 논문의 구성은 다음과 같다. 본 논문의 2장에서는 피싱과 파밍, 그리고 스미싱에 대해 설명하고, 3장 에서는 하이퍼바이저를 이용하여 앞에서 설명한 피싱과 파밍, 그리고 스미싱을 예방할 수 있는 기술적 방안을 제안한다. 마지막 4장에서 결론을 맺는다.

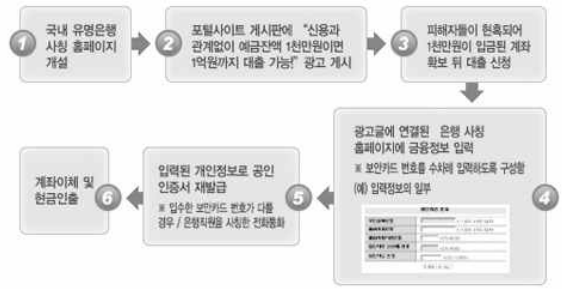
II. 신종 금융사기의 종류 및 방법

1. 피싱(Pshishing)

피싱(Pshishing)은 개인정보(Private Data)와 낚시(Fishing)를 합성한 신조어로, 인터넷을 통해 국내외 유명기관을 사칭하여 개인정보나 금융정보를 수집한 뒤 이를 악용하여 금전적인 피해를 일으키는 사기 유형이다.

해외에서는 유명 기관을 사칭하여 이메일을 발송하고, 메일 본문의 인터넷 주소로 접속하여 개인정보 및 금융정보를 입력하도록 하는 방법이 주로 이용되고 있다.

국내에서는 이런 방법 외에도 경품 이벤트나 신용대출, 게임 아이템 충전 등을 미끼로 방문자가 많은 사이트의 게시판에 광고 글을 게시하거나 포탈의 쪽지를 보내는 방법이 주로 이용되고 있다.[1]



<그림 2> 은행 사이트 피싱 사례

특히 스마트폰 사용자가 늘어남에 따라 앱스토어에는 유명 기관의 애플리케이션을 사칭한 가짜 애플리케이션이 늘어났고, 사용자의 부주의로 이를 다운로드 받아 설치 및 실행하는 경우가 늘고 있다.

2. 파밍(Pharming)

파밍은 합법적으로 소유하고 있던 사용자의 도메인을 탈취하거나 도메인네임시스템(DNS) 이름을 속여 사용자들이 진짜 사이트로 오인하도록 유도하고, 가짜 사이트로 접속한 사용자의 개인정보를 훔치는 금융사기 방법이다.[2]

즉, 파밍 공격을 통해 공격자는 사용자의 의지와 관계없이 가짜 사이트로 접속하게 함으로써 개인정보 및 금융정보를 공격자에게 제공하여 사용자의 금전적 피해를 유발시킬 수 있다.[3]

<그림 3> 파밍 흐름도

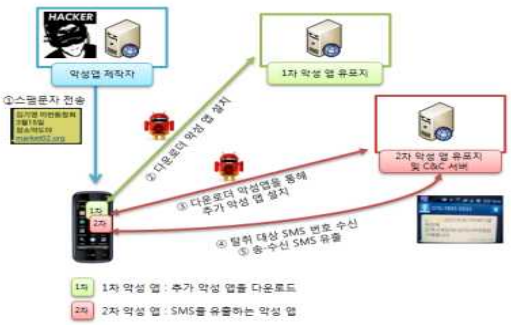
3. 스미싱(Smishing)

스미싱(Smishing)은 SMS와 낚시(Fishing)을 합성한 신조어로, 최근 가장 성행하는 금융사기수법이다.

스미싱은 악성코드를 이용하며 피싱과 달리 악성코드가 삽입된 악성 애플리케이션이 유출 행위를 일으키므로, 사용자는 정보유출 및 금전적 피해 뿐 아니라 악성 애플리케이션이 실행되는 것조차 모르는 경우가 대부분이다.

악의적인 목적을 가진 공격자가 공격 대상에게 이벤트, 무료쿠폰, 대출, 사진송부 등과 같이 관심을 끌만한 메시지를 SMS/MMS로 전송한다. 이때 이를 수신한 스마트폰 사용자가 흥미를 느껴 해당 메시지에 포함된 링크나 이미지를 클릭하게 되면, 사용자의 의지와 관계없이 사용자의 스마트폰에 악성코드가 포함된 악성 애플리케이션이 설치되고, 이를 이용하여 사용자의 인증정보를 확보해 사용자 모르게 소액 결제를 할 수 있다.[4]

또한 스미싱 공격에 사용되는 애플리케이션도 점점 진화하여 근래에는 공격용 애플리케이션 외에 다운로더 애플리케이션이 추가되어 어떠한 애플리케이션이 실질적으로 활동하고 있는지 조차 알 수 없도록 설계되고 있다. 결과적으로 다운로더 애플리케이션을 제거하더라도 최종적으로 악성 행위를 수행하는 애플리케이션은 제거되지 않고 그대로 남아서 사용자 몰래 계속 활동하는 것이다.[5]



<그림 4> 스미싱 공격 개요

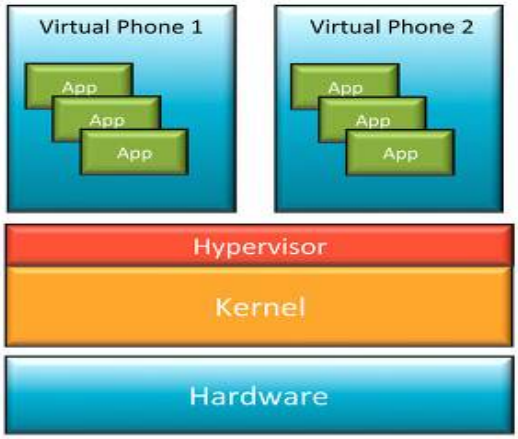
III. 금융 사기의 기술적 대응방안

스마트폰의 특성 상 악성코드가 삽입된 악성 애플리케이션을 이용하여, 공격자는 쉽게 사용자의 개인정보 및 금융정보를 획득할 수 있다.

이와 같은 악성 애플리케이션으로 인한 피해를 예방하고자 하이퍼바이저를 이용하여 스마트폰에 설치되어 있는 애플리케이션이 외부와 통신하는 것은 가상의 보안 영역에서 대신 실행하고, 가상의 보안 영역에서 키 값 비교 및 URL 검사를 통해 신종 금융사기를 예방하는 기법을 제안한다.

1. 제안 환경

스마트폰의 특성 상 제한된 자원을 효율적으로 사용해야 하므로 하이퍼바이저 Type I 방식을 적용한다.[6]



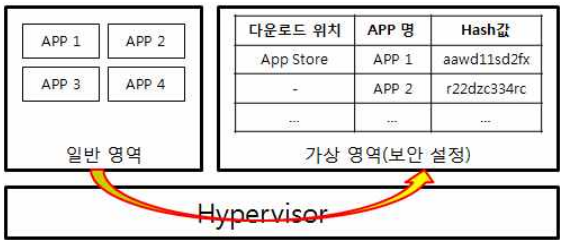
<그림 5> 하이퍼바이저 Type I

하이퍼바이저 위에 Virtual Phone 1 환경과 Virtual Phone 2 환경이 존재하며, Virtual Phone 1은 통화/문자/사용자가 설치한 일반적인 애플리케이션이 가동된다. Virtual Phone 2에는 외부와의 통신을 관장하고 검증하는 보안 로직이 포함되어 있는 가상 OS를 탑재하고 이상 여부를 탐지토록 한다.[7~9]

2. 구현 방법

일반적인 애플리케이션의 통신은 모두 가상의 보안 영역에서 이루어지도록 하며, 스마트폰을 켜면 일반 영역과 가상 영역 모두가 활성화 되도록 한다.

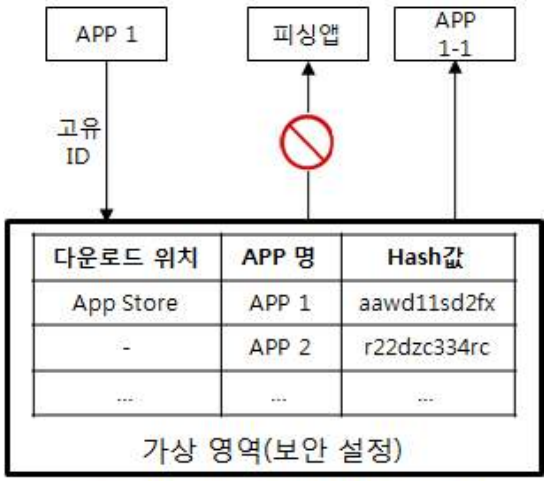
사용자가 최초로 애플리케이션을 설치할 때는 애플리케이션의 고유한 ID 값을 암호화하여 가상의 보안 영역에 저장한다. 본 논문에서는 애플리케이션명과 고유 ID 값을 식별 정보라 칭하며, 한 번 저장한 식별 정보는 애플리케이션을 삭제하더라도 지속적으로 유지토록 한다.



<그림 6> 구현 개요

이 식별 정보를 이용하면 보유한 애플리케이션의 업데이트본이 출시되어 업데이트를 진행하거나 혹은 애플리케이션을 재설치할 경우 해당 애플리케이션의 고유 ID에 대한 해시값 비교를 통해 애플리케이션의 안전성을 검증할 수 있다.

만약 스마트폰에 악성코드가 삽입되어 일반 사용자 영역의 DNS 정보가 변조되더라도 외부와의 실질적인 통신은 가상의 보안 영역에서 주관하고 있으므로 파밍 공격에도 안전하다.



<그림 7> 피싱 및 파밍 대응

SNS 링크나 SMS/MMS를 이용한 사기 방법인 스미싱은 단축 URL이 삽입된 경우가 대부분이다. 혹은 단축 URL을 이미지나 동영상에 숨긴 경우도 있으며, 문자 개봉과 동시에 바로 악성 애플리케이션을 다운로드할 수도 있다.

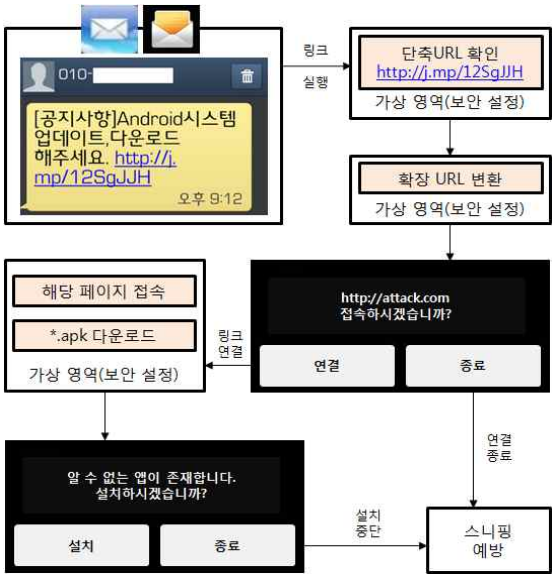
이와 같은 경우에도 통신 자체를 가상 영역에서 주관하므로 추가적인 동의를 구하는 등 사용자가 인지할 수 있는 방법을 제공하여 스미싱 공격을 일정 부분 예방할 수 있다.

다음은 본 논문에서 제안하는 스미싱 공격에 대한 대응 절차이다.

가상의 보안 영역에서 단축 URL로의 접속 요청이 확인되면 이를 바로 접속하는 것이 아니라 단축 URL을 확장하여 원래의 URL을 파악한 후, 원래의 URL을 사용자에게 팝업의 형태로 알려준다. 사용자는 이를 보고 일차적으로 해당 링크로 접속할지 여부를 판단할 수 있다. 또한 접속을 진

행하더라도 접근한 사이트에서 ○○.apk 형태의 애플리케이션을 다운로드 받는다면 사용자에게 "알 수 없는 앱" 설치가 될 수 있다고 다시 한 번 경고를 주어 설치 진행 여부를 결정한다.

이를 통해 사용자가 자신의 스마트폰에 무엇인가 설치될 수 있음을 인지하여 스미싱을 상당 부분 예방할 수 있다.



<그림 8> 스미싱 대응 흐름도

Ⅳ. 결 론

본 논문에서는 스마트폰 사용자의 실수 혹은 인지조차 못한 상태에서 발생할 수 있는 신종 금융사기에 대해 기술적으로 우회할 수 있는 방법을 제안하였다.

아직 스마트폰의 OS 별 차이와 애플리케이션 개발 표준 및 관련 제도의 미흡으로 인해 완벽한 차단을 위한 추가적인 연구 및 보완이 필요하다.

그러나 금번 논문에서 제안하는 방법을 사용하는 경우, 스마트폰 사용자의 금전적 피해를 어느 정도 예방하고, 안심하며 스마트폰을 사용할 수 있는 기반을 마련할 수 있을 것으로 기대한다.

참고문헌

[1] KISA 보호나라, 피싱, http://boho.or.kr
[2] 정완, 인터넷사기의 신종유형과 법제도적 대응방안, 경희법학 40권 1호, 1229-2478, 61p, 2005
[3] 금융감독원, 파밍으로 인한 이용자 피해 예방 당부, http://www.fss.or.kr
[4] 이훈재, 스마트폰 신종범죄의 유형 및 경찰 대응방안에 관한 연구, 한국경찰연구 제 11권 제 4호, 330p, 2013
[5] KISA 보호나라, 갈수록 지능화 돼 가는 스미싱 유포 악성 앱!, http://boho.or.kr, 2013
[6] 유재성, 이광우, 김승주, 원동호 Hypervisor를 이용한 스마트폰 사용자 프라이버시 보호, 한국컴퓨터정보학회 동계학술대회 논문집 제 19권 제 1호, 30p, 2011
[7] 김정한, 김지홍, 신은환, 엄영익, 가상화를 이용한 모바일 플랫폼 보안성 향상 기술, 정보보호학회논문지 제 21권 제 1호, 1598-3978, 205p, 2011
[8] 이재익, 스마트폰 보안 위협 및 하드웨어 보안 기술 동향, 금융보안연구원, 6p, 2012
[9] 김정한, 김인혁, 민창우, 엄영익, 모바일 가상화 기술 동향, 정보과학회논문지 제 28권 제6호 통권 제 253호, 1738-6322, 39p, 2010