안드로이드 웹 환경에서의 딥 링크를 통한 간편결제 비밀번호 탈취 예방 방안에 대한 연구

고형민, 이승호, 김기천*

건국대학교

{jerrytoy77, phg0726, *kckim}@konkuk.ac.kr

Deep link based Anti key-logging solution for Android smartphone

Heoungmin Ko, Seung-ho Lee,, Keecheon Kim*

Konkuk Univ.

요 약

본 논문은 최근 증가하고있는 간편결제 시스템의 비밀번호가 악성 애플리케이션을 통해 탈취되는 시나리오를 구상하고, 실제 결재를 진행해봄으로서 일반 웹 환경에서 가상 키패드를 이용한 간편결제 비밀번호 입력 방식은 제시한 시나리오대로 탈취가 가능함을 실험하였다. 그에 대한 해결방안으로 안드로이드의 어플리케이션 호출 기능인 DeepLink를 이용하여 비밀번호 입력 페이지를 다른 어플리케이션에서 진행 함으로서, 악성 어플리케이션을 통한 간편결제 비밀번호 탈취를 예방 하는 방안을 제안한다.

Ⅰ. 서 론

스마트폰이 등장한 이후, e-commerce 시장은 기존 휴대전화보다 강력한 스마트폰의 인터넷 브라우저와 , 각종 e-commerce 애플리케이션에 힘입어 더욱 빠르게 발전하게 되었다.

스마트폰을 이용한 각종 e-commerce 시장 팽창에 따라, 스마트폰 사용자들의 ID와 비밀번호를 탈취 하기 위한 key-logging 시도나, 악성코드가 포함된 어플리케이션 등을 설치하도록 유도하는 스미싱 등의 공격 사례가 아직까지도 자주 보고 되고 있으며,

key-logging을 막기 위해 웹 브라우저 화면에 가상 키보드로 비밀번호를 입력하거나, 악성 어플리케이션을 탐지하는 백신 어플리케이션이 출시되는등 이러한 피해를 막기 위해 다양한 연구가 진행 되고 있다.[1]

그러나 다양한 안전한 어플리케이션으로 위장한 악성 어플리케이션들은 당시의 이슈와 키워드 등만 변형하여 유포되고 있으며, 누적 피해사례는 계속하여 증가[2] 하고 있다.

특히 기존 공인인증서 등을 사용하기 힘든 모바일 환경의 문제점과, 결제 간편화 경쟁 등과 맞물려, 웹 브라우저나 쇼핑몰 어플리케이션 으로 위장한 악성 어플리케이션을 통한 간편인증 암호 유출 등이 우려된다.

이러한 위협으로, 간편결제 미 사용자의 대부분은 이러한 보안 문제를 인식하고 있으며, 사용률에 부정적인 영향을 미치게 된다.[3]

본 논문은 브라우저 상에서 입력되는 간편인증 암호 유출을 방지 하기 위해, Android 환경에서 간편인증 암호 입력시 DeepLink를 활용하여 암호를 안전한 브라우저 상에서 입력하도록 유도하는 방법을 제시한다.

Ⅱ. 문제 정의

본 논문에서는 스미싱 피해 사례[4]를 토대로 (그림1)과 같은 공격 시나리오를 구성하였다.

1. 화제가 되는 키워드를 포함한 문자 등으로, 피해자가 악성 어플리케이션을 설치하도록 유도한다.

2.이후 피해자는 웹 브라우저로 위장한 악성 어플리케이션으로, 쇼핑몰에 접속해 물건을 구매한다.

3.공격자는 이때 악성 어플리케이션으로 피해자가 접속한 URL과 터치 좌표를 전송받아 간편인증 비밀번호를 탈취한다.

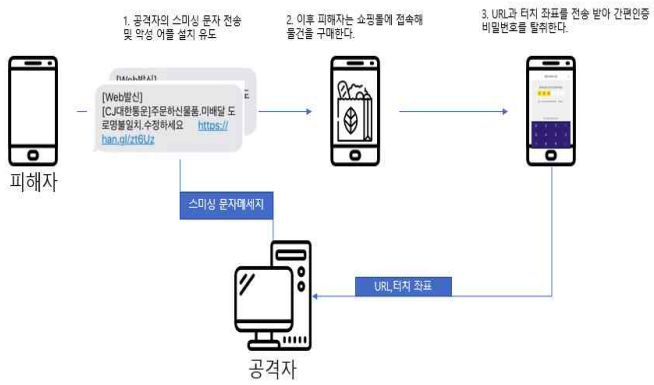

그림 1. 시나리오 그림

해당 공격 시나리오 대로 악성 어플리케이션을 설치 하였을 경우, (그림2)에서 확인할수 있는 바와 같이 국내 'A'사 등 브라우저 상에 웹으로 구현한 가상 키패드를 사용하는 경우, 좌표 등을 탈취 할 수 있음이 보여지며, 설험을 진행한 환경은 다음과 같다.(표1)

테스트 환경	
테스트 기종	Android Virtual Device
타겟 SDK	Target SDK ver 26(oreo)
OS버전	Android version 10 (sdk ver 29)
결제 테스트	인터넷 쇼핑몰 A사

표 1. 구현 및 테스트 사양

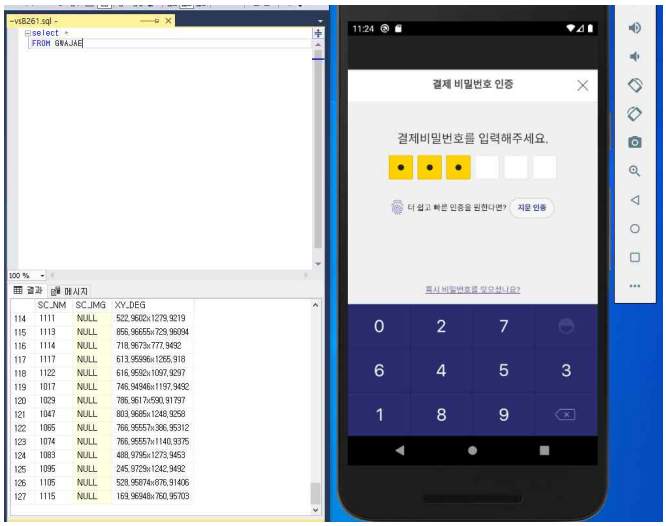

그림2 . 로컬 환경 테스트 화면

Ⅲ. 제안 기법

애플리케이션 DeepLink는 사용자를 앱의 특정 콘텐츠로 바로 연결하는 URL기능이다.

Android 6.0(API 레벨 23) 이상의 Android 기기에서 DeepLink를 호출하면 애플리케이션이 특정 유형의 링크에 적용되는 기본 핸들러로 애플리케이션 자체를 지정할 수 있다.

이런 특성을 가진 DeepLink 기능을 이용해 간편인증 비밀번호를 입력하는 페이지로 이동할 때, 어플리케이션을 호출하고 진행하도록 하는 방법을 제안한다.

DeepLink로 Android에 기본 설치된 크롬 브라우저나 해당 쇼핑몰의 어플리케이션을 호출하면, DeepLink호출 기능이 없는 악성 어플리케이션일 경우 그림(그림3) 과 같이 오류 페이지를 보이게 되며,

DeepLink호출 기능도 구현되있는 정밀한 악성 어플리케이션일 경우에도,쇼핑몰에서 링크한 어플리케이션이 호출되어 터치 좌표가 노출되면 쉽게 탈취 될수 있는 브라우저 상에 웹으로 구현한 가상 키패드를 악성 어플리케이션이 아닌 쇼핑몰이 지정한 어플리케이션에서 입력 하게 되므로, 공격자는 간편인증 비밀번호를 탈취 하기 어렵게 된다.

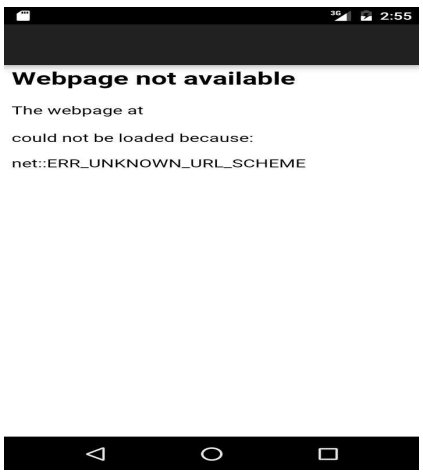

그림3 . 딥링크 미구현시 오류 메세지

Ⅳ. 결론

본 논문은 악성 어플리케이션이 Android 사용자의 간편결제 비밀번호를 탈취하는 시나리오와, 어플리케이션 링크 기능을 이용하여 비밀번호 입력 페이지 다른 어플리케이션으로 진행 하도록 유도함으로서 악성 어플리케이션으로 인한 간편결제 비밀번호 탈취를 예방하는 방법을 제안하였다. Android 환경의 특징인 통신사나 기기 제조사, 기타 세컨드 파티 애플리케이션 마켓을 허용하는 환경 특성상, 아직까지도 문자 스미싱, 유료 크랙 어플로 위장 하는 등의 방법으로 많은 악성 어플리케이션들이 설치 되고 있다. 이에 따라 결제 비밀번호를 입력하는 과정에서의 검증된 어플리케이션 사용이 무엇보다 중요하다. 하지만 본 논문에서 제안하는 과정은 사용자의 Android 버전이 낮으면 사용 할 수 없어 API 기준 6.0 이상 환경으로 전부 전환 되지 않은 현재 Android 환경 특성상 당장 적용하기에 제약이 있다. 향후 연구로는 API 버전에 제한받지 않는 방법에 대해 연구할 계획이다.

ACKNOWLEDGMENT

본 논문은 2020년도 국토교통부/국토교통과학기술진흥원의 지원(과제번호 20TLRP-B152768-02) 및 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원(No.NRF-2017M3C4A708367823, 더 나은 Web 경험을 위한 자율제어 네트워킹 애널리틱스 기술)으로 수행되었음

참 고 문 헌

〔1〕 유재욱, 한미정, 김규헌, 장준영, 진호용, 지한별, 신정훈, 김경곤. (2018). 안드로이드 간편결제 애플리케이션 보안 솔루션 결과값 변조를 통한 검증기능 우회 방법에 대한 연구. 정보보호학회논문지, 28(4), 827-838.

〔2〕 최학규, 김황래. (2019). 스미싱 예방을 위한 악성문자훈련시스템 설계 및 구현. 한국정보기술학회논문지, 17(10), 93-99.

〔3〕 오은, 김태성, 오하경. (2018). 간편결제 방식의 보안 및 간편성 사이의 상충관계. 한국통신학회논문지, 43(2), 452-460.

[4] 최관, 김민지. (2017). 스미싱 범죄의 범행 진행과정에 대한 연구. 한국행정학회 학술발표논문집, (), 543-553.