안드로이드폰 SSID 변조를 통한 새로운 과금 유발 취약점에 관한 연구

허건일* · 유홍렬* · 박찬욱* · 박원형*

요 약

2010년 가장 중요한 보안 이슈 중 하나는 무선 네트워크이었다. 스마트폰의 보급이 본격화되면서 무선 인터넷 사용자가 급증하였고 무선 AP가 전국에 우후죽순으로 설치되었다. 그러나 대부분의 무선 AP가 보안적인 관점에서 제대로 관리되지 않고 있고 무선랜 이용자 또한 보안의 중요성을 인식하지 못하고 있다. 이러한 상황은 심각한 보안위협을 초래할 수 있다. 본 논문에서는 QR 코드를 통해 악성코드를 유포, 모바일 AP 기능 활성화를 통해 대량 과금을 유발하는 새로운 방식의 사이버 공격 기법을 설계하고 분석하였다. 제안한 새로운 취약점은 안드로이드폰의 모바일 AP 기능을 강제로 활성화시킨 후 주변에서 발생하는 모든 Probe Request에 대해서 응답하게 하여 과금 유발 및 통신 장애를 유발한다

A Study on the New Vulnerability of Inducing Service Charge Doctoring SSID of Smartphone Based on Android

Geon Il Heo* · Hong Ryul Yoo* · Chan Uk Park* · Won Hyung Park*

ABSTRACT

Wireless network is one of the 2010's most important security issues. As smartphone is popularize, the number of Wireless Internet users is really growing and wireless AP spring up everywhere. But most wireless AP haven't being managed properly in terms of security, Wireless Internet users also don't recognize important of security. This situation causes grave security threats. This paper design and analyze a new cyber attack whose it circulates malware via QR code and activates Mobile AP to induce service charge. The new vulnerability we suggest forces to activate Mobile AP of smartphone based on Android and responds to all Probe Request are generated around, and brings induction of service charge and communication problems in its train.

Key words : Wi-Fi, QR Code, Mobile AP, Malware

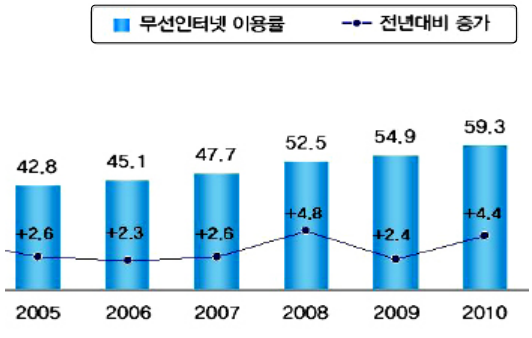
접수일 : 2010년 9월 28일; 채택일 : 2010년 12월 4일

* 서울과학기술대학교 산업정보시스템공학과

1. 서 론

최근 아이폰(iPhone) 도입 이후 일어난 스마트폰의 확산은 우리나라의 경제·사회 전반에 걸쳐 '스마트 혁명'을 촉발하였고 국내 모바일 시장에 새로운 패러다임을 가져다주었다. WCDMA, Wi-Fi (Wireless Fidelity), Wibro와 같은 무선인터넷의 인프라 확산 및 관련된 투자의 증가는 사람들이 시간과 장소에 구애받지 않고 인터넷에 접속하여 정보를 이용하는 것을 가능하게 해 주었다. 이러한 현상은 사업자들에게는 새로운 기회를, 일반 사용자들에게는 새로운 경험과 편의성을 주었다[1].

아래의 (그림 1)은 최근 6년 간 무선인터넷 이용률 변화 추이를 나타낸다.



(그림 1) 무선인터넷 이용률 변화 추이(%, %p)[2]

국내 스마트폰 보급이 확대되면서 스마트폰을 이용한 고객 서비스가 새롭게 증가하고 있다. 유통업체를 비롯한 사회 전반적인 부문에서 QR 코드를 활용한 서비스가 새로운 고객 마케팅 도구로 주목받고 있다. 광고나 전단지 혹은 웹 사이트에 모두 담아내지 못했던 상품 소개나 서비스의 연결고리 역할을 수행할 수 있기 때문이다. QR 코드는 기업 마케팅 외에도 개인 명함, 전시된 작품, 주소 표지판 등 다양한 곳에 삽입되고 있어 그 활용도가 점점 높아지고 있다[3].

QR 코드의 가장 큰 장점은 누구나 쉽게 만들고 배포할 수 있다는 점이다. 하지만 이러한 장점은 제작자의 의도에 따라 보안 위협으로 작용할 수 있다. QR 코드에 유해한 정보를 담을 수 있기 때문이다. 아울러 안정적인 무선 인터넷 환경을 지속적으로 유지함에 있어서 필수적이라 할 수 있는 보안대책은 여전히 많은 개선이 필요하다. 손안의 PC라 불리는 스마트폰은 연락처, 통화내역, 문자 전송 내역은 물론 위치정보, 이메일 정보, 인터넷 접속내역, 검색어 정보, 개인사진, 전자결재, 기밀정보 등 개인 및 업무관련 중요 정보들을 가지고 있어 스마트폰 내 정보가 유출될 경우 큰 피해를 볼 수 있다. 스마트폰 악성코드는 방금 언급한 정보유출형 외에도 과금 유발형, 단말 장애 유발형, 배터리 소모형, 크로스 플랫폼형 등 다양한 형태로 존재한다[4].

최근 PMP, PSP, 닌텐도, 아이팟, 노트북 등 Wi-Fi 접속을 지원하는 수많은 모바일 기기들이 출시되고 있으나, 이동성이 없는 Wi-Fi의 한계로 인해 사용자들은 이동시 Wi-Fi를 사용할 수 없는 제한적인 불편을 감수해야만 했다. 이러한 약점을 보완하고자 최근 출시되는 안드로이드 스마트폰은 스마트폰 자체가 무선공유기(Access Point) 역할을 하고 있다.

사용자의 편리성과 무선랜 인프라 확충이라는 긍정적인 사실이 있으나 그 이면에는 심각한 보안 문제가 잠재하고 있었다. QR 코드를 통해 악성 코드의 실행을 유도할 수 있다는 측면과, 스마트폰의 무선 AP 기능이 자신의 의도와 관계없이 활성화될 수 있다는 점이다. 이때 무선 AP 기능을 하는 스마트폰이 주변에서 요청되는 모든 Wi-Fi 신호를 감지해 자신의 스마트폰으로 접속하도록 유도한다면, 스마트폰 사용자는 과도한 무선데이터(WCDMA) 이용료가 과금될 수 있기 때문이다.

본 논문에서는 근래 각광받고 있는 QR 코드와 안드로이드폰의 AP 기능을 이용한 새로운 취약점에 대해 알아보고 그 대응방안을 모색하였다.

2. 관련 연구

본 장에서는 제 3장에서 소개할 새로운 과금 유발 취약점의 이해를 돕기 위하여 QR 코드와 무선랜의 통신 방식에 대해서 알아본다.

2.1 QR 코드

QR 코드는 Quick Response 코드의 약자로서 1994년 일본 도요타의 자회사 '덴소 웨이브'가 물류관리를 위해 개발한 격자무늬 2차원 바코드이다. QR 코드는 '덴소 웨이브'가 지난 2000년 6월, ISO/IEC 18004 표준이 된 QR 코드에 대한 특허권을 행사하지 않을 것이라고 선언함에 따라 널리 도입될 수 있는 발판을 마련하였다[5, 6].

이를 바탕으로 1990년대 중반 일본에서는 QR 코드를 적극적으로 활용한 마케팅 사례가 붐을 이루었고, 이것이 성공적인 결과를 얻어냄으로써 QR 코드는 정보제공 수단의 새로운 축으로 단단히 자리 잡게 되었다. 이에 따라 국내 SK(네이트 코드), KT(핫 코드), LG U+(이지 코드) 등 주요 이동통신사들도 서둘러 서비스에 나섰지만 무선 인터넷 환경이 뒷받침되지 못한 국내에서는 곧 유명무실화 되었다.

하지만 최근 국내 스마트폰 이용자가 500만 명을 넘어서고 언제 어디서나 무선 인터넷을 사용할 수 있는 환경이 구축되면서 국내에서도 QR 코드

좌-드라마 '성균관 스캔들', 우-삼성물산 '빈폴'

(그림 2) QR 코드 활용 사례

를 활용한 마케팅이 매우 활성화되고 있다[7]. 다음의 (그림 2)와 같이 드라마 홍보, 제품 광고, 신선식품의 생산/유통이력 제공 등 다양한 분야에서 도입되어 사용되고 있고 일반 개인 사용자들도 자신의 명함 속에 블로그, 트위터 주소, 이미지, 동영상이 담긴 QR 코드를 삽입하는 등 생활전반에서 널리 사용되고 있다.

QR 코드는 아래의 (그림 3)과 같이 다양한 컨텐츠를 제공하며, 이 중 문자와 이미지는 QR 코드로 직접 인코딩되고, 동영상과 웹페이지는 해당 URL 주소가 QR 코드로 인코딩된다.

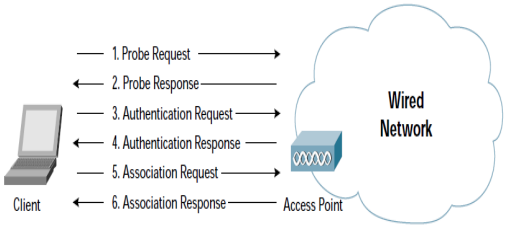
(그림 3) QR 코드가 제공할 수 있는 컨텐츠

대용량, 고밀도, 오류정정 기능 등 QR 코드는 기존 1차원 바코드보다 많은 장점을 가지고 있지만 누구나 쉽게 생성하고 배포할 수 있다는 점이 가장 매력적인 요소로 여겨지고 있다. 하지만 이러한 점은 유해한 정보를 담은 QR 코드 역시 어떠한 제재 없이 생성, 배포하는 것을 가능하게 한다는 문제점을 지니고 있다.

2.2 무선랜의 통신 방식

클라이언트가 무선 AP를 탐지하고 연결되는 절차는 아래의 (그림 4)와 같이 크게 6가지의 과정으로 이루어진다.

아래의 <표 1>은 (그림 4)에서 발생하는 사건에 대해 순차적으로 설명한다.

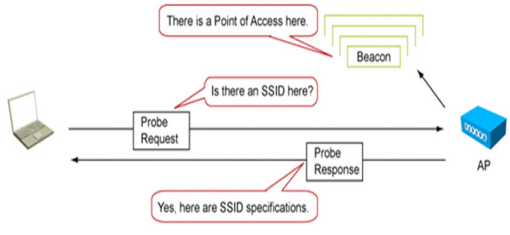


(그림 4) 802.11 클라이언트 인증 프로세스[8]

〈표 1〉 802.11 클라이언트 인증 프로세스

① 클라이언트가 모든 채널에서 Probe Request Frame을 송출한다.
② 범위 내에 있는 무선 AP가 Probe Response Frame을 통해 응답한다.
③ 클라이언트가 액세스에 가장 적합한 무선 AP를 결정한 후 Authentication Request Frame을 전송한다.
④ 무선 AP가 Authentication Response Frame을 전송한다.
⑤ 인증이 성공하면 클라이언트가 무선 AP에 Association Request Frame을 전송한다.
⑥ 무선 AP가 Association Response Frame을 통해 응답한다.

클라이언트가 무선 AP를 찾는 과정인 첫 번째, 두 번째 과정에 대해서 좀 더 자세히 살펴보면 다음의 (그림 5)와 같다.



(그림 5) Active Scanning을 통해 클라이언트가 무선 AP를 찾는 과정[9]

위의 (그림 5)와 같이 Active Scanning은 클라이언트가 먼저 Probe Request Frame을 브로드캐스트하기 때문에, 이웃한 무선 AP에서 Beacon Frame을 수신하여 무선 AP들을 감지하는 Passive Scanning과정보다 수행 속도가 더 빠르다. 하지만 일부 주파수 대역에서는 Active Scanning 기법을 사용하지 못하기 때문에 이러한 경우 Passive Scanning 방식을 사용하며 일반적으로 핸드오버 지연시간을 줄이기 위해 Active Scanning 기법을 사용한다.

Probing과정에서 사용되는 SSID는 보안 메커니즘으로 고안되지 않았고 그러한 목적으로 사용되는 것도 아니기 때문이다.

3. 새로운 과금 유발 취약점 분석

3.1 취약점 흐름도

새로운 과금 유발 취약점이 어떻게 이루어지는 살펴보면 다음의 (그림 6)과 같다.

3.2 단계별 분석

본 절에서는 다음 (그림 6)의 취약점 흐름도를 감염 및 전파 단계, 피해 단계, 피해인지 및 대응 단계로 구분한 뒤 순차적으로 분석한다.

3.2.1 감염 및 전파 단계

① 음란물, 경품 제공 이벤트, 티저 광고, 연예인 사생활 등 사람들의 호기심을 자극할 수 있는 단순 게시물 또는 파워블로거의 이벤트를 활용하여 QR 코드를 찍도록 유도한다.

② QR 코드를 찍은 피해자의 스마트폰은 URL 확인절차 없이, 공격자가 만들어 놓은 특정 웹페이지로 이동한다.

③ 악성 스크립트가 삽입된 웹페이지는 사용자의 동의 없이 임의의 웹서버에서 Dropper를 다운받는다. 또는 “이 영상(음란물)을 재생

(그림 6) 새로운 과금 유발 취약점 흐름도

하기 위해서는 해당 파일을 다운받아야 합니다." 등의 메시지를 띄어 사용자가 Dropper를 다운받도록 유도한다.

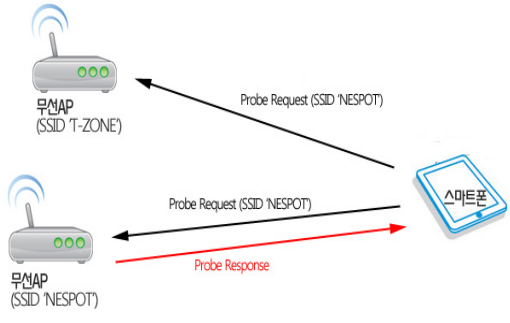
④ 스마트폰에 다운된 Dropper는 악성코드가 담긴 파일을 특정 장소에 설치하고 Dropper 자신은 삭제한다. 설치된 악성코드의 생성 날짜는 실제 날짜에서 의심하지 않을 만한 다른 날짜로 변경된다(향후 악성코드가 분석될 경우, 감염경로가 QR 코드라는 사실과 Dropper의 존재를 최대한 은닉하기 위해서이다).

⑤ 악성코드가 작동하면 스마트폰의 모바일AP 기능을 활성화한다. 모바일AP 기능은 겉으로 보기에 비활성화 되어 있기 때문에 사용자는 눈치 채지 못한다.

3.2.2 피해 단계

⑥ 감염된 스마트폰 주변에서 제 3자가 스마트폰 또는 노트북으로 무선랜(Wi-Fi)을 이용하려고 시도하면, 단말기가 요청한 SSID와 상관없이, 무조건 감염된 스마트폰으로 연결된다. 제 3자의 단말기에서는 원래 연결하고자 했던 AP에 접속된 것처럼 표시되므로 감염된 스마트폰을 통해 인터넷을 이용하고 있다는 사실을 알지 못한다. 단, 이것은 원래 연결하고자 했던 무선 AP보다 감염된 스마트폰이 근거리에 위치하고 신호상태가 양호할 때만 가능하다. 이는 다음과 같은 방식으로 가능하다.

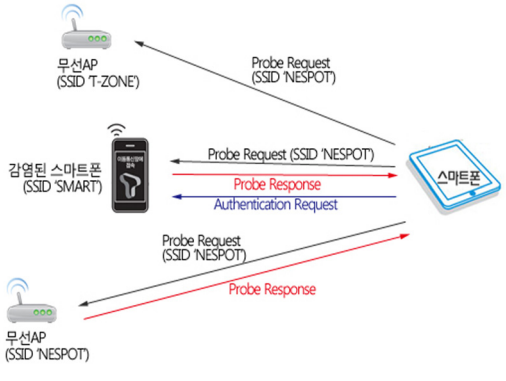
기본적으로 무선랜의 클라이언트는 Passive Scanning을 통해 주변의 모든 무선 AP를 검색한다. 이후 검색된 무선 AP 중 사용자가 원하는 특정 무선 AP를 선택하면 해당 무선 AP로 Active Scanning을 한다. Active Scanning은 주파수가 다른 모든 물리 채널로 Probe Request Frame을 브로드캐스트하고, 무선 AP로부터 Probe Response Frame을 받는 과정을 통해 최적의 조건을 갖춘 무선 AP를 찾는다. 가령 다음 (그림 7)과 같이



(그림 7) 정상적인 무선랜 연결 요청 과정

임의의 단말기가 SSID가 'NESPOT'인 무선 AP에 접속하려고 하면, SSID가 포함된 Probe Request Frame을 모든 채널로 전송한다. 그리고 SSID가 일치하는 무선 AP만 응답(Probe Response)한다.

그러나 악성코드에 감염된 스마트폰은 주변에서 발생하는 모든 Probe Request에 대해서 응답한다. 이것은 감염된 스마트폰이 모든 Probe Request를 받아들여 Frame에 들어 있는 SSID를 알아낸 후, 알아낸 SSID를 Probe Response Frame에 포함시켜 단말기에게 응답함으로써 이루어진다. 가령 아래의 (그림 8)과 같이 제 3자가 'NESPOT'이라는 무선 AP에 접속을 시도(Request)하면, 감염된 스마트폰(모바일 AP 기능 작동)은 자신의 SSID가 'SMART'임에도 불구하고 마치 자신이 'NESPOT'인 것처럼 자신의 SSID를 'NESPOT'으로 변조 한 Frame을 응답(Response)하여, 감염된 스마트폰(모바일AP 기능 작동)에 접속하도록 한다. 이 때 감염된 스마트폰은 SSID가 'NESOPT'인 실제 무선 AP보다 클라이언트에 가까운 거리에 위치해 있어야 한다.



(그림 8) 감염된 스마트폰(무선AP)으로 연결되는 과정

⑦ 감염된 스마트폰을 통하여 다른 단말기들이 인터넷 서비스를 이용하게 됨으로써 피해자는 과도한 데이터 통신요금을 지불하게 된다. 그리고 감염된 스마트폰들이 증가하고 서로간의 거리가 가까워질 경우 주파수 간섭 및 이로 인한 Wi-Fi 품질 저하 현상이 발생한다.

3.2.3 피해 인지 및 대응 단계

⑧ 피해자는 과금 지불 후, 스마트폰에 뭔가 문제가 있다는 것을 인식하게 된다. 그래서 피해자가 스마트폰을 안철수연구소와 같은 백신업체에 맡길 경우, 악성코드를 탐지하고 삭제하는 것은 어렵지 않지만 생성날짜를 변경했기 때문에 Dropper의 존재를 파악하는 것은 쉽지 않다.

⑨ 악성코드의 시그니처가 백신 엔진에 등록되었기 때문에 공격자는 추후 공격코드를 변형(난독화 또는 암호화, 메소드 이름 변경)하여 유포한다. 이에 따라 QR 코드를 통한 악성코드의 지속적인 유포가 가능해진다.

3.3 취약점 분석

기존의 과금 유발형 악성코드는 스팸, MMS, 애플리케이션 등을 통해 단순 유포되었기 때문에 백신업체에 의해 악성코드가 탐지되고 분석되어 엔진에 시그니처가 적용되면 재감염이 어려웠다. 하지만 본 논문에서 제시한 새로운 취약점은 기존의 악성코드와 마찬가지로 Life Cycle은 짧지만 Dropper에 탑재하여 유포하기 때문에 Dropper가 탐지되어 분석되지 않는 한 이미 감염경력이 있는 스마트폰이라 할지라도 재감염시키는 데 큰 문제가 없다.

그리고 모든 트래픽은 감염된 스마트폰을 경유하므로 MITM 공격에도 매우 용이하다. 이는 수동적인 형태의 스니핑이 아닌 네트워크 트래픽을 조작하고 주요 정보를 빼내는 것이 가능함을 의미

한다. 본 취약점은 스푸핑 등을 통한 강제적인 데이터 경유지 변경이 아닐 뿐더러 사용자 입장에서는 정상적인 네트워크 접속인 것처럼 보이기 때문에 MITM 공격이 시도될 경우 인지하는 것은 매우 어렵다.

4. 대응 방안

4.1 사용자 기반 대응 방안

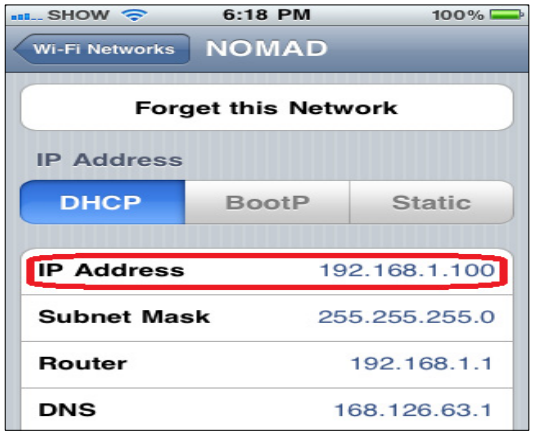
개별 사용자가 이러한 취약점에 취할 수 있는 대응방안은 주로 예방하는 것이다.

우선 QR 코드로 인한 피해를 막기 위해서 출처가 불분명한 QR 코드를 무턱대고 인식하는 행동을 피해야 한다. 특히, QR 코드를 자동으로 읽고 접속하는 리더 애플리케이션은(scanny등) 가급적 이용을 삼가고, 사용자에게 웹 사이트의 정보를 제공한 후 접속여부를 사용자가 직접 선택하도록 하는 방식의 리더 애플리케이션을 이용하는 것이 바람직하다[8].

그리고 현재 스마트폰에서는 단축 URL의 유해여부를 검증하는 시스템이 없기 때문에 단축 URL이 악성코드를 유포하는 수단으로 악용될 가능성이 매우 크다. 따라서 의심스러운 단축 URL은 접속을 자제하고 주의를 기울일 필요가 있다[9].

외부에서 Wi-Fi를 이용할 때도 여러 가지 주의사항이 있다. 대다수의 스마트폰 사용자들이 이전에 접속한 무선 AP에 자동으로 접속하는 설정을 이용하고 있는데, 이 기능은 SSID를 변조해서 기존 무선 AP로 가장하는 방식의 해킹 공격에 아주 취약하다. 따라서 무선 AP 자동접속 설정을 해제하고 접속한 무선 AP 리스트는 주기적으로 지워야 한다[10].

그리고 Wi-Fi에 접속시에는 항상 IP주소를 확인하여야 한다. 제시된 취약점에서는 SSID 값을 기존 AP와 똑같이 변조하여서 사용자의 접속을 유도하고 있다. 아래의 (그림 9)와 같이 테더링을 통해 만든 AP의 경우 사설 IP주소를 가지고 있기 때문에 IP주소만으로 쉽게 식별할 수 있다.



(그림 9) 접속한 무선 AP의 IP주소 확인

마지막으로 스마트폰 전용 백신을 이용한 사용자 차원의 주기적인 보안 점검이 필요하다. 이를 통해 악성코드를 사전에 예방할 수 있고, 악성코드에 감염 되었더라도 지속적인 보안 점검으로 피해를 최소화 할 수 있다.

4.2 기술적 대응 방안

기술적 대응 방안은 크게 네트워크 단과 시스템 단으로 구분할 수 있다.

4.2.1 네트워크 영역의 대응 방안

외부로부터 공격 대상이 되는 취약 포트에 대한 차단 정책을 수립하고, 모바일 인터넷 트래픽 분석으로 침입 패턴 개발과 적용을 통한 실시간 탐지/차단 체계를(WIDS/WIPS) 구현해야 한다.

또한 모바일 인터넷망 분석을 통해서 보안 취약구간을 파악하고, 적절한 보안 솔루션을 구성하여 외부로부터의 보안 위협에 대응해야 한다.

이동통신사 가입자의 무선 트래픽이 과도하게 급증하고 있거나 일정 용량 이상 발생한 경우, 경고 문구가 담긴 SMS를 발송하는 것도 하나의 방법이 될 수 있다.

4.2.2 시스템(단말) 영역의 대응 방안

PC환경에서 구현되고 있는 Endpoint 보안관점에서 스마트폰 단말 간의 Hardware와 Software보안으로 대응 방안을 모색해야 한다. 우선 스마트폰 단말기 제조사에서는 출고 단계부터 Hardware 보안에 주목해야 하고, Software 보안은 스마트폰 OS 개발사와 보안 Software(백신) 개발사가 주도하여 설치-유지-관리의 체계적인 과정을 수립할 필요가 있다[11].

4.3 정책적 대응 방안

국가기관(방송통신위원회 등)에서 어플리케이션 자체를 통제할 필요가 있다. 허가/불허가 애플리케이션을 리스트로 작성해서 스마트폰이 불허된 애플리케이션에 접속하는 것을 제한한다.

그리고 스마트폰 출고 시 내장된 백신프로그램 설치를 의무화해야 한다. 단말기 제조사와 보안 software 개발업체의 제휴를 통해 사용자는 특정 기간 동안 백신프로그램을 무료로 이용할 수 있게 하는 등의 방법이 있을 수 있다. 이런 방법 외에도 라이센스 갱신시 정부차원의 지원을 통하여 사용자의 부담을 최소화한다[12].

무분별한 QR 코드의 난립을 막기 위해 관련 정책 도입이 필요하다. 우선 모든 QR 코드에는 반드시 유효기간을 명시하도록 하고, 공공장소나 대형 포털 사이트에 QR 코드를 게시할 때는 방통위에 신고하도록 법규를 제정한다.

보안캠페인과 주기적인 의식교육을 통해 스마트폰 보안의 중요성을 강조하고 사용자의 보안의식을 증대시킨다. 스마트폰을 작동시키는 건 사용자이므로 스마트폰 보안의 성패는 결국 사용자에게 달려있다.

5. 결 론

우리나라는 초고속 인터넷 보급률 1위 국가로서 급속한 발전을 거듭, 현재는 유선을 넘어서서 무선영역(Wi-Fi)에서도 빠른 성장세를 보이고 있다. 하지만 너무나도 급속도로 앞만 바라본 나머지 필수적인 보안대책이 미비하여 세계 각국 블랙 해커들의 해킹 경유지가 되었다.

이러한 현상이 최근 스마트폰의 확산에서 또 다시 반복될 조짐이 보이고 있다. 스마트폰은 대한민국에 '스마트 혁명'을 촉발하여 국내 모바일 시장에 새로운 패러다임을 가져왔으나, 이런 환경의 안정적인 발전을 지속적으로 뒷받침할 수 있는 적절한 보안 대책이 뒤따라오지 못했다. 그리하여 우리는 스마트폰의 보안에 대한 중요성을 일깨우고자, 새로운 취약점 시나리오를 구성하였고 그에 대한 대응 방안을 제시하였다.

악성코드는 QR 코드를 통해 유포된다. 오픈소스인 QR 코드의 특성상 누구나 생성, 배포할 수 있고 현재 사회 전반에 걸쳐 다양한 분야에서 쓰이고 있는 만큼 악성코드 유포에 있어서 매우 적합하다. QR 코드로 인터넷에 접속하면 일단 Dropper의 다운로드를 유도하여 사용자의 스마트폰에 Dropper를 설치한다. Dropper는 실행압축이나 인스톨 형태로 존재하고 Dropper가 실행되면 애드웨어, 스파이웨어 형태의 악성코드를 설치하는 역할을 수행한다. Dropper는 악성코드 설치 후 스스로를 삭제한다. 설치된 악성코드는 모바일 AP 기능을 활성화시키고, 주위에서 감지할 수 있는 모든 Probe Requet Frame의 SSID를 탐지한다. 그리고 탐지한 SSID 값으로 다시 Probe Response를 하고 이를 통해 임의의 클라이언트가 어떤 SSID를 가지고 요청을 하더라도 항상 감염된 스마트폰이 응답하는 상황이 발생한다. 피해자는 요금이 과금되기

전까지 악성코드 감염여부를 발견하기가 어렵다. 악성코드의 생성날짜를 변경했기 때문에 Dropper의 존재를 파악하기 어렵고 이로 인해 악성코드의 시그니처가 백신 엔진에 등록되어도 약간만 변형하여 재유포하면 쉽게 재감염시킬 수 있다. 그리고 감염된 스마트폰을 통하여 인터넷을 사용하는 모든 단말기의 패킷은 스니핑되고 있기 때문에 MITM 공격에 의한 정보 유출 공격으로 발전할 수도 있다.

대응책으로는 사용자, 기술적, 정책적 측면으로 나눠서 체계적으로 제안하였다. 사용자의 보안의식을 제고시키기 위한 노력이 꾸준히 행해지고 기술적인 보완과 정책적인 뒷받침이 되어준다면 보안사고로 인한 피해를 점점 줄여나갈 수 있을 것이라 판단된다.

스마트폰을 사용하는 주체는 사용자이다. 아무리 훌륭한 보안기술이 개발되어도 사용자의 보안의식이 낮다면 스마트폰은 보안에 취약할 수밖에 없다. 소 잃고 외양간 고치는 식의 허술한 보안의식은 지양하고 보다 스마트한 의식을 가지고 보안사고를 줄여나가야 하겠다.

참 고 문 헌

[1] 권지혜, “아이폰 1년 … ‘스마트 시대’ 열렸다”, 국민일보 쿠키뉴스, 2010.

[2] “2010년 무선인터넷 이용실태조사 요약보고서”, 한국인터넷진흥원(KISA), 2010.

[3] 이민형, “QR 코드 찍어봤니? … 급성장 중인 QR코드”, IT전문 미디어 블로그 딜라이달넷, 2010.

[4] 강동호, 한진희, 이윤경, 조영섭, 한승완, 김정녀, 조현숙, “스마트폰 보안 위협 및 대응 기술”, 전자통신동향분석 제25권, 제3호, 2010.

[5] “일본 QR 코드 시장 현황”, INFIDES Reseach and Consulting, 2006.

[6] “QR Code란”, SCANY, 2010.

[7] 김영대, “스마트폰 시대의 마케팅 첨병, QR 코드”, Midas, 2010.

[8] 장윤정, “QR 코드 막 찍다간 개인정보 유출 낭패”, 전자신문, 2010.

[9] 연합뉴스, “윈도-맥 OS 동시 감염 악성코드 출현”, 보안닷컴, 2010.

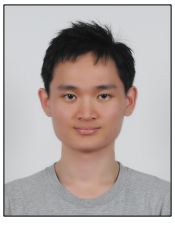
[10] 한국인터넷진흥원 무선인터넷팀, “알기 쉬운 무선랜 보안 안내서”, 방송통신위원회, 한국인터넷진흥원, 2010.

[11] 민준희, “모바일 인터넷 환경에서 보안 위협 대응방안 연구”, 건국대학교 정보통신대학원, 2010.

[12] 장윤정, “PC 백신 1위 이스트소프트, 스마트폰 백신 1위 안랩에 도전장”, 전자신문, 2010.

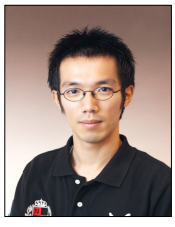
허 건 일

2004년 서울과학기술대학교
산업정보시스템공학과
입학
2010년 KISA 정보보호동아리
융합보안연구회 회장
현재 서울과학기술대학교
산업정보시스템공학과
네트워크보안 Lab 연구원



박 찬 욱

2004년 서울과학기술대학교
산업정보시스템공학과
입학
현재 KISA 정보보호동아리
융합보안연구회 회장
서울과학기술대학교
산업정보시스템공학과
네트워크보안 Lab 연구원



유 홍 렬

2007년 서울과학기술대학교
산업정보시스템공학과
입학
2010년 KISA 정보보호동아리
융합보안연구회
학술부장
현재 서울과학기술대학교
산업정보시스템공학과
네트워크보안 Lab 연구원

박 원 형

2010년 서울과학기술대학교
산업정보시스템공학과
겸임교수