The Journal of the Convergence on Culture Technology (JCCT)
Vol. 2, No. 4, pp.65-70, November 30, 2016. pISSN 2384-0358, eISSN 2384-0366

http://dx.doi.org/10.17703/JCCT.2016.2.4.65
JCCT 2016-11-9

무선공유기 보안공격 분석 및 무료와이파이 해킹 해결방안

Security Attack Analysis for Wireless Router and Free Wi-Fi Hacking Solutions

배희라*, 김민영*, 송수경*, 이슬기*, 장영현**

Hee-Ra Bae*, Min-Young Kim*, Su-Kyung Song*, Seul-Gi Lee*, Young-Hyun Chang**

요 약 공공와이파이를 이용한 메일확인과 인터넷뱅킹 등의 네트워크 통신량이 증가함에 따라 공공공유기 해킹의 위험성이 지속적으로 높아지고 있다. 국가적으로 공공공유기를 확대하는데 비해 사용자의 보안인식은 부족하여 개인정보 노출 위험성이 커지고 있다. 무선공유기는 접근성이 뛰어나지만 상대적으로 해킹이 용이하므로 대응차원의 해킹에 대한 분석이 중요하다. 본 논문에서는 와이파이에 사용되는 암호화 방식 및 무선공유기의 보안 공격에 대한 무료와이파이 해킹 사례분석 및 해결방안을 제안한다.

주요어 : 와이파이, 무선 공유기, 암호화, 해킹, 보안성 강화

Abstract As network communication increases by using public WiFi to check e-mail and handling Internet banking, the danger of hacking public routers continues to rise. While the national policy is to further propagate public routers, users are not eager to keep their information secure and there is a growing risk of personal information leakage. Because wireless routers implement high accessibility but are vulnerable to hacking, it is thus important to analyze hacking to tackle the attacks. In this study, an analysis is made of the encryption method used in WiFi and cases of hacking WiFi by security attacks on wireless routers, and a method for tackling the attacks is suggested.

Key Words : WiFi, Wireless Router, Encryption, Hacking, Security Enhancement

I. 서 론

애플 아이폰 3GS의 국내 출시를 스마트폰 확산 시점으로 정할 때 성인 다섯 명 중 네 명이 스마트폰을 사용하고 있으며, 한국 스마트폰 사용률은 2015년 8월 기준 85%이다. 60세 이상 49%가 스마트폰을 사용하여 스마트폰 사용자의 연령대가 점차 증가하고 있다는 것을 보여준다.[1] 스마트폰 보급률이 남녀노소 상관없이 지속적으로 증가하고 있는 추세다.

스마트폰 요금제는 제한된 데이터를 사용하는 것부터 무제한 데이터를 사용하는 것까지 다양하다. 무제한 데이터를 사용하게 되면 비용을 과다하게 지불해야 하므

*준회원, 배화여자대학교 스마트IT학과
**정회원, 배화여자대학교 스마트IT학과
접수일자: 2016년 9월 30일, 수정완료일자: 2016년 10월 15일
게재확정일자: 2016년 10월 26일

Received: 30 September, 2016 / Revised: 15 October, 2016
Accepted: 26 October 2016
**Corresponding Author: cyh@baewha.ac.kr
Dept. of Smart IT, Baewha Women's University, Korea

로 무제한 데이터 요금제보다 저렴한 제한된 데이터 요금제를 선택한 후 와이파이를 필수적으로 사용해야만 한다.

와이파이란, Wireless Fidelity의 약자로 무선 접속 장치(AP: Access Point)가 설치된 곳에서 전파나 적외선 전송 방식을 이용하여 일정 거리 안에서 무선 인터넷을 할 수 있는 근거리 통신망을 칭하는 기술이다. 최근에는 기술 향상으로 접속 지점 기준 50m에서 100m까지 거리에서도 통신할 수 있다. 이 기술이 상용화되면서 100m 이내에 있는 휴대폰, 카메라, 프린터, 컴퓨터, 헤드폰 등이 각각 또는 동시에 여러 대에 연결될 수 있으며, 통신 규격 완성 후 와이파이 다이렉트 인증을 받지 않은 기존 와이파이 기기도 서로 접속할 수 있다.[2]

무료 와이파이 서비스는 무한대로 확장되고 있으나 공공장소에서 무료로 제공하는 와이파이는 같은 AP를 사용하기 때문에 다른 사람이 스마트폰에 쉽게 접근할 수 있고 해커들에 의해 악성프로그램이 설치되어 개인정보유출 등 각종 사이버 범죄에 노출될 위험이 크다. 따라서 본 논문에서는 와이파이에 사용되는 암호화 방식 및 암호화 기술 공격에 대해 알아보고, 무료 와이파이 해킹 사례를 분석한 뒤 해결방안에 관하여 연구한다.

II. 무선 암호화 방식

무선 암호화 방식에는 WEP, WPA, WPA2가 있으며, 가장 널리 알려져진 프로토콜들이다.

데이터 암호화는 클라이언트와 AP 사이의 취약한 무선 링크를 보호하며, 이 방법이 취해지면 기밀 보호를 확실히 하기 위해 암호 보호, 전구간 암호화, VPN 그리고 인증 등과 같은 다른 일반적인 랜 보안 절차들이 시행된다. 무선 랜을 통해 전송되는 데이터를 암호화함으로써 유선 네트워크와 물리적 보안 대책에서 제공되는 것과 비슷한 방호를 제정하는 것을 추구한다.

2.1 WEP(Wired Equivalent Privacy)

WEP는 유선 랜에서 제공하는 것과 유사한 수준의 보안 및 기밀 보호를 무선 랜에서 제공하기 위하여 와이파이 표준에 정의되어 있는 보안 프로토콜이다. 초기 버전 암호화 수준 상한은 64비트였으나 지금 256비트까지 늘어났다. 주로 가정과 소규모 기업에서 설치가 편리한 WEP를 사용하였다.

WEP는 데이터 암호화를 위해 RC4 암호를 사용하고, 메시지 인코딩과 디코딩을 위해 40비트 키를 사용하기 때문에 적절히 사용하지 않으면 위험에 쉽게 노출된다. WEP에 사용되는 암호키의 값이 노출되는 경우에 누구나 통신의 내용을 해독해서 볼 수 있으며, 암호키의 값을 모르는 경우에도 널리 알려진 방법을 통해 누구나 데이터의 내용을 해독할 수 있다.

2.2 WPA(Wi-Fi Protected Access)

WPA는 Wi-Fi Alliance 및 IEEE(Institute of Electrical and Electronics Engineers)에 의해 제정된 보안 표준으로, 2002년 WEP 방식의 취약점을 보완하기 위해 개발되었다. 암호와 방식으로 TKIP(Temporal Key Integrity Protocol) 및 MIC(Message Integrity Check)를 사용한다. TKIP는 WEP에서 사용했던 RC4 알고리즘을 동일하게 채택하고 향상된 키 관리 방식과 공격자가 접속지점과 클라이언트 사이에 오고간 패킷(Packet)을 수집했거나 변경했는지 판단하기 위한 메시지 무결성 체크 방식이 추가되었다.

핵심 구성요소인 TKIP가 WEP 방식에서 사용된 몇 개의 요소들을 재활용함으로써 펌웨어 업그레이드를 통해 기존 WEP 기기에 설치될 수 있도록 설계되어 있으며 이는 결국 취약점 악용으로 이어졌다. WPA는 WEP와 마찬가지로 침투에 취약하며, 침탈되는 과정은 WPA 알고리즘 자체에 대한 공격과 기기와 접속지점의 연결을 용이하게 해주는 보조시스템인 WPS(Wi-Fi Protected Setup)에 대한 공격을 통해 이루어진다.

2.3 WPA2(Wi-Fi Protected Access 2)

WPA2는 미 정부 보안 요건인 FIPS140-2을 충족하기 위해 128비트의 AES(Advanced Encryption Standard) 알고리즘이 적용되며, CCMP(Computer Cipher Mode with Block Chaining Message Authentication Code Protocol)방식이 기존의 TKIP을 대체한다.

AES 암호화 방식을 채택해 보안 기능이 더욱 강화됐지만, WPA2를 사용하기 위해서는 데이터 암호화 및 복호화 처리를 위한 전용 칩이 필요하다. WPA2가 제공하는 강력한 보안 기능을 무선 네트워크에 적용하기 위해서는 기존의 무선 장비를 새로운 하드웨어로 업그레이드해야 한다. 또한, WPA 최대 취약점인 WPS 피

격위험은 WPA 지원 접속지점에도 그대로 남아있는데, 이를 방지하기 위해서는 WPS 기능이 차단되거나 접속지점 펌웨어를 WPS 지원이 불가능한 기종으로 바꿔서 공격 가능성을 아예 차단해야 한다.[3][4] 표 1.은 3가지 암호화방식에 대한 비교를 3가지 차원에서 보여준다.

표 1. 암호화 방식 비교

Table1. Comparing Encryption Methods

	WEP (Wired Equivalent Privacy)	WPA (WiFi Protected Access)	WPA2 (WiFi Protected Access 2)
인증	사전 공유된 비밀키 사용 (64bit, 128bit)	사전에 공유된 비밀키를 사용하거나 별도의 인증서버를 이용	사전에 공유된 비밀키를 사용하거나 별도의 인증서버를 이용
암호화	고정 암호키 사용 (인증키와 동일) RC4 알고리즘 사용	암호키 동적 변경(TKIP) RC4 알고리즘 사용	암호키 동적 변경 AES 등 강력한 블록 암호
보완성	64bit WEP 키는 수분 내 노출이 가능하여 사용이 줄음	WEP 방식보다 안전하나 불완전한 RC4 알고리즘 사용	가장 강력한 보안기능 제공

III. 무선 공유기 보안 공격

3.1 WEP Cracking

WEP는 Key값과 IV(Initial Vector)를 이용하며, 스트림 암호화 기법인 RC4를 통해 평문을 암호화한다. 그러나 2001년 초 암호학자들이 몇 가지 치명적인 취약점을 발견했으며, 공개 소프트웨어에 의해 쉽게 공격할 수 있음이 드러났다.

WEP Cracking은 여섯 단계로 구성된다.

첫 번째로 인터페이스를 설정한다. 사용할 인터페이스를 활성화 시키고, 무선 랜카드를 모니터모드로 바꾼다. 목적지가 자신이 아닌 패킷을 포함하여 감지할 수 있는 주변의 무선 패킷들을 모니터한다.

두 번째로 WLAN을 찾는다. 무선 랜카드가 주변에 있는 도달 가능한 AP를 탐색하여 BSSID(Basic Service Set ID), SSID(Service Set Identifier), 암호화 방식 등과 같은 중요한 정보를 얻는다.

세 번째로 가짜인증(Fake Authentifcation)을 시도한다. 공격자가 AP에 패킷 주입공격(Packet Injection)을 하기 위해서는 양측 간에 세션이 성립되어 있어야 한다.

네 번째로 무선 패킷을 캡쳐한다. WEP 방식의 취약점인 동일한 IV를 사용한다는 점을 이용해 WEP 크랙에 쓸 무선 패킷을 수집한다.

다섯 번째로 주입공격을 수행한다. 공격하려는 무선 네트워크 상에 트래픽이 없다면 패킷 캡쳐가 불가능하다.

여섯 번째로 WEP Crack을 수행한다. 충분히 많은 무선 패킷데이터를 수집하여 FMS 공격, Chopping 공격 등을 수행한다.

3.2 WPA/WPA2 Cracking

WPA는 TKIP을 기반으로 하고 WPA2는 AES-CCMP을 기반으로 한다. 이 방식들은 인증 시 PSK(Preshared Key)로 인증하면 크래킹이 가능하나, 무차별 사전 대입공격을 하기 때문에 공격대상의 패스워드가 사전파일에 존재하지 않으면 크래킹이 불가능하다.

WPA는 4way-handshaking을 하는 인증 과정 중에 WPA-KEY가 들어있음을 이용하여 크래킹한다. 먼저 공격자는 AP와 기존에 연결되어 있는 Station(AP와 연결되어 있는 기기)중 아무에게나 DoS공격(Denial of Service Attack)을 시도한다. 연결이 끊긴 Station은 재인증을 시도하게 되는데, 이때 공격자는 재인증 과정을 캡쳐한다. 캡쳐한 인증요청 리퀘스트 패킷에 사전공격을 시도하여 크래킹한다.[5]

WPA/WPA2 Cracking은 WEP Cracking에 비하여 사전공격이 통하지 않으면 크래킹하기 쉽지 않다는 점이 있으나, 두 기술 모두 인터넷 검색과 공개 소프트웨어를 통하여 비전문가도 어렵지 않게 시도할 수 있다.

3.3 보안설정 우회

ESSID 숨기기와 맥 필터링(MAC Filtering)은 인가된 사용자와 그렇지 않은 사용자를 구분하는데 유용하지만, 악의를 가진 공격자에게는 쉽게 우회할 수 있는 보안설정이다. 공격자는 다른 사용자가 송수신하는 패킷을 엿듣는 행위를 뜻하는 스니핑(Sniffing) 기법과 자신의 맥 주소 등을 속임으로써 다른 사용자인 것처럼 위장하는 행위를 뜻하는 스푸핑(Spoofing) 기법을 사용해 숨겨진 ESSID를 알아낼 수 있다.

숨겨진 ESSID를 알아내기 위해 공격자는 피해자 AP의 맥 주소로 스푸핑한 뒤 인증해제 패킷을 전송한

다. 인증해제 패킷을 받은 사용자는 AP로부터의 연결이 해제된다. 다시 AP로 접속하기 위해 프로브 요청(Probe Request) 패킷을 전송하는데, 이 패킷에는 ESSID가 숨겨지지 않은 채로 담겨있다. 이를 스니핑하여 숨겨진 ESSID를 알 수 있다.

맥 필터링은 AP가 인가된 맥 주소 목록을 작성한 후 해당 맥 주소를 가진 사용자만 접속할 수 있도록 하는 보안 설정이다. 공격자는 자신의 무선 인터페이스를 인가된 맥 주소로 스푸핑하여 기존의 사용자인 것처럼 위장하고 AP에 접속할 수 있다.

3.4 로그 AP(Rogue Access Point)

로그 AP는 내부 네트워크의 관리자를 허락을 받지 않고 사용자가 개인적으로 설치한 비인가 AP의 취약점을 이용하여 공격자가 불법으로 설치한 AP를 말한다. 공격자가 비인가 AP을 이용하여 불법으로 접근할 경우, 사용자와 같은 권한을 가질 수 있다. 공격자가 사용자와 같은 권한을 가지기 때문에 네트워크 전체를 감시하는 보안 시설이나 프로그램이 없다면 설치된 뒤에는 사용자가 알기 어렵다. 로그 AP을 이용한 공격에는 이블 트윈(Evil Twin), 중간자 공격(Man in the middle attack) 등이 있다.

이블 트윈은 대표적인 와이파이 피싱(Wi-Fi Phising)이다. 공격자가 진짜 AP 근처에서 SSID가 같은 가짜 AP를 설치하고 신호를 강하게 보내면, 사용자가 무선AP를 켰을 때 신호가 강한 쪽으로 자동으로 연결되므로 공격자는 가짜 AP에 접속한 사용자의 패스워드나 파일 등을 해킹할 수 있다.

중간자 공격이란 사용자와 서버 사이에 끼어들어 패킷을 도청 및 조작하는 것을 말하는데, 사용자는 서버에 정상적으로 연결된 것으로 보이기 때문에 알아채기 어렵다. 중간자 공격은 로그 AP를 이용하여 SSL을 이용한 인증서 웹 사이트에 주로 발생한다. 웹 사이트에 접속할 때 인증서에 문제가 있다고 뜨는데, 이 때 확인을 누르면 공격자가 만들어 놓은 인증서로 바뀌면서 접속하는 사이트에 입력하는 아이디나 패스워드 등 신상 정보가 공격자에게 넘어간다.

3.5 서비스 방해 공격(Denial of Service)

서비스 방해 공격은 해커들이 특정 컴퓨터에 대량 접속을 유발해 해당 공유기의 정상적인 동작을 방해하여 상대방 서버가 서비스를 하지 못하도록 하는 서비스 거부 공격이다. 공격대상이 수용할 수 있는 능력 이상의 정보나 사용자 또는 네트워크의 용량을 초과시켜 정상적으로 작동하지 못하게 된다. 공격대상 시스템의 서비스, 하드웨어, 소프트웨어 기능을 저하시키고 서비스를 원활하게 제공하지 못하게 된다. 공격자 입장에서는 아주 단순하지만 공격자의 추적이 어렵고 공격에 완벽히 대처할 수 있는 방법이 없으며 공격 즉시 효력을 발휘한다.

무선 랜에서의 서비스 방해 공격은 프레임의 송수신시 암호화가 일어나지 않는 약점을 이용해 일어난다. 공격에는 가장(Masquerading) 공격, 자원고갈(Resource Depletion) 공격, 매체 접근 공격(Media Access Attack)이 있다.

가장 공격은 공격자 자신을 진짜 AP인 것처럼 속여 인증해체 패킷은 정송하여, 공격대상자와 AP 사이의 연결을 방해하는 공격이다. 연결이 해제된 공격대상자는 다시 AP를 연결하려 하므로 이 과정에서 이블 트윈과 암호 크랙 공격으로 이어질 수 있다.

자원고갈 공격은 공격 대상자 AP에 인증요청 패킷을 끊임없이 전송하여, AP의 메모리를 고갈시켜 더 이상 서비스하지 못하도록 하는 공격기법이다.

매체 접근 공격은 AP와 공격 대상자가 통신하는 동안 다른 사용자가 데이터 전송시도를 하지 못하도록 통신이 끝나는 시간을 알려주는 NAV(Network Allocation Vector)값을 크게 연장해 전송하여 다른 사용자들이 채널이 계속 사용중인 것으로 간주해 데이터를 전송하지 못하도록 한다. 연장한 NAV값을 전달하여도 외형적으로는 아무 문제가 없는 패킷이므로 주변 엔터페이스들은 이를 수신한다.[6]

Ⅳ. 무료 와이파이 해킹 사례

2015년 초 커피전문점 등에 설치된 와이파이에 접속했을 때 '한층 개선된 구글 크롬 최신버전이 출시됐습니다. 업데이트 후 이용해주십시오.' 란 창이 뜨며 업데이트를 유도하는 경우가 발생한 바 있다. 승인 버튼을 누르지 않으면 아예 무선 인터넷에 접속되지 않고, 버튼을 누르면 한 시간 가량 먹통이 된다. 유명 웹 브라우저인 크롬 등을 최신버전으로 업데이트하라

며 사용자 승인을 유도해 악의적인 프로그램을 노트북 PC나 스마트폰에 다운로드한다. 이 프로그램은 정상 금융 앱을 가짜 앱으로 대체하여 조회나 이체를 하면 전자금융사기에 노출된다.[7]

2016년 10월, 경찰청 사이버테러수사과는 2월부터 6월까지 불특정 다수의 공유기를 해킹하고 이를 이용하는 스마트폰을 허위의 포털사이트로 접속하도록 유도해 악성 앱을 유포한 후, 감염된 스마트폰 포털 사 가입에 필요한 인증번호를 수신 받아 총 1만 1,256개의 포털계정을 부정 생성한 사실을 확인했다고 밝혔다. 부정 생성된 계정은 개당 4,000원에 거래됐으며, 이 계정을 통해 제품홍보 글을 작성하거나 댓글 등록에 이용하는 등 마케팅 사업에 부정 사용하였다.[8]

한국인터넷진흥원이 전국 4개 권역 공공장소에서 실시한 공유기 보안 현장점검 실태조사 결과, 257개 장소 와이파이가 해킹 등 보안에 취약한 것으로 드러났다. 공공장소의 공유기 관리자들이 해킹이나 관리자 계정의 중요성을 알지 못하거나, 편의를 위해 패스워드를 공개하고, 번거롭다는 이유로 보안에 취약한 펌웨어 업데이트를 하지 않는 등 보안 불감증이 심각한 것으로 드러났다.[9]

보안이 허술한 개방형 와이파이는 해커들에게 무방비로 노출되어 있어 해당 와이파이를 사용하는 모든 사용자들의 개인정보가 유출 될 위험이 크다.

V. 무료 와이파이 해킹 해결방안

5.1 인증된 와이파이 사용 및 해킹에 대한 경각심 고취

사용자들은 공공 와이파이 중 인증되지 않은 와이파이는 해킹 가능성이 높기 때문에 사용을 금지하고 신뢰할 수 있는 와이파이만을 사용하며, 이미 사용하고 있는 와이파이라고 해도 해킹 가능성이 있으므로 안전한 와이파이인지 확인하는 습관을 길러야 한다. 온라인 뱅킹과 같은 민감한 업무를 하게 되면 아이디와 비밀번호, 결제정보 등 각종 개인정보가 노출될 수 있으므로 자제하고, 개인정보를 취급하는 앱들은 사용되기 전 '와이파이로 이용할 시 해킹될 위험이 있습니다.' 와 같은 알림창을 띄워 사용자들에게 경각심을 일깨워 주어야 한다.

5.2 비밀번호 필수 설정 및 펌웨어 업데이트

공유기 관리자들은 보안에 대한 책임을 갖고 관리자 페이지에서 초기 설정된 비밀번호 대신 보안 수준이 높은 비밀번호로 재설정한다. 동일한 비밀번호를 일정 기간 사용하게 되면 보안성이 낮아지므로 주기적으로 변경한다. 보안 강도가 낮을수록 위협에 노출될 위험이 크기 때문에 암호화 방식을 WPA2로 선택한다. 오래된 펌웨어를 사용할 경우 이미 알려진 취약점을 이용해 해커가 침투할 확률이 높으므로 정기적으로 공유기 펌웨어 업데이트 여부를 확인하고 새로운 버전의 업데이트가 있으면 적용한다.

5.3 국가적 차원의 와이파이 해킹 탐지서비스 제공

국가에서 공공 와이파이를 확대하고 있다. 하지만 다른 공공 공유기 만큼 보안에 취약하여 이 와이파이를 사용하는 국민들의 개인정보 노출 위험이 크다. 이를 개선하기 위해 국가는 국내보안업체와 협력하여 지금까지 나타났던 무선 랜 해킹 패턴들을 분석한 후 국민들에게 알려야만 한다. 카카오톡 등 사용률이 높은 메신저를 이용하여 국민들에게 개인정보동의를 구한다. 이 서비스를 제공받고자 하는 국민들은 동의를 누르고 최소한의 정보만을 국가에게 내어준다. 국민들이 접속하고자 하는 와이파이가 해킹되었는지 즉각적으로 탐지하여 알림을 띄우고, 해킹 위험이 탐지되었을 경우에는 해당 와이파이에 접속할 수 없도록 차단하고 주변에 있는 다른 안전한 와이파이에 연결할 수 있도록 알려준다.

VI. 결 론

본 논문에서는 와이파이에 사용되는 암호화 방식 및 기술 공격을 서술하고 무료 와이파이 해킹 사례를 분석하여 해결방안을 제시하였다. 무선 공유기 환경이 범용화 됨에 비해 보안에 대한 인식이 부족하여 대다수의 사람들이 해킹에 노출되어 있다. 공공 와이파이를 이용하는 대상자 중 일반 사용자가 높은 비율을 차지하고 있기 때문에 금융이나 개인정보가 쉽게 유출되므로 공유기 보안이 중요하다. 공유기 사용자들은 인증된 와이파이만을 사용하고 안전한 와이파이인지 확인하는 습관을 길러야 하며, 개인정보가 필요한 업

무는 자제한다. 개인정보를 취급하는 앱들은 사용되기 전에 알림창을 띄워 사용자들에게 경각심을 일깨워준다. 공유기 관리자들은 보안 수준이 높은 비밀번호를 설정하고, 정기적으로 펌웨어를 업데이트한다. 국가는 와이파이 해킹 탐지 서비스를 제공하여 국민들의 개인정보가 해커들에 의해 노출되지 않도록 해야 한다. 향후 본 논문을 통해 국가와 국민들의 공공 와이파이 보안에 대한 인식을 높이고 본 논문에서 제안한 해결 방안을 기반으로 하는 기술개발과 효율성 증명에 대한 연구가 필요할 것으로 판단된다.

References

[1] Korea Gallop Research Institute, "Smartphone and Clock", 2015.
[2] http://terms.naver.com/entry.nhn?docId=300477&cid=43665&categoryId=43665
[3] Kwon Chae Hwan, “Wireless VoIP Hacking Attacks through the Analysis of Vulnerability against Wireless APs”, 2011.
[4] Korea Radio Promotion Agency, "Wi-Fi security infringement and security technology status “, 2010.
[5] Jung Wan-seo and 2 others, "Wireless Router Vulnerability and Cracking Cases Analysis", 2016.
[6] Jung Woo Hyuk and 1 other, “Detecting and responding to security attacks on wireless routers”, 2016.
[7] http://www.boannews.com/media/view.asp?idx=45112&kind=1
[8] http://www.boannews.com/media/view.asp?idx=52023&skind=O
[9] http://www.daejeontoday.com/news/articleView.html?idxno=382218