무선랜 환경에서 효과적인 Rogue AP 탐지 기법

강대현, 김강석, 최옥경, 김기형
아주대학교 대학원 지식정보보안학과
e-mail:nymew@ajou.ac.kr, kangskim@ajou.ac.kr,
okchoi@ajou.ac.kr, kkim86@ajou.ac.kr

Effective Rogue Access Point Detection Method in Wireless LAN

Daehyun Kang, Kangseok Kim, Okkyung Choi, Kihyung Kim
Dept. of Knowledge Information Security, Graduate School of Ajou University

요 약

지난 몇 년 동안 무선랜(Wireless LAN)은 다양한 영역에서 가장 널리 사용 되었으며, 가장 크게 발전을 하였다. 그러나 무선랜의 특성상 해킹과 침투에 취약한 약점을 안고 있다. 아직도 많은 보안적 취약점을 가지고 있으며, 특히 그 중에서도 Rogue AP(Access Point)는 가장 심각한 보안 취약점으로 대두되고 있다. 현재 Rogue AP 탐지를 위하여 넷스텀블러와 같은 스니핑 소프트웨어를 설치하여 주변 지역을 돌아다니는 워드라이빙 형태의 탐지방법은 아직도 사용되고 있다. 그러나, 이러한 방법은 대규모로 확장되어 가는 무선랜 환경에 적합하지 않다. 본 논문은 무선랜 환경에서 Rogue AP 탐지 문제의 해결책을 제시한다. AP의 전파 영역을 이용하는 방식으로, AP가 신호를 받을 수 있도록 수정하여, 주변에 새로운 AP가 탐지될 경우, AP가 서버와 새롭게 발견된 AP에 신호를 보내고, 이를 바탕으로 서버는 WhiteList를 통해서 Rogue AP 여부를 결정한다. 따라서 본 논문의 제안 방식은 기존의 탐지 방식에 비해 Rogue AP의 효과적 탐지가 가능하다.

1. 서론

무선 네트워크(Wireless Network) 장비의 가격 하락과, 손쉬운 네트워크 망 구성 및 분리, 통합의 유연성과 확장성을 제공해주기에, 무선랜 시스템의 수요는 해가 갈수록 급격하게 증가하고 있다. 또한 스마트폰의 도입 역시 무선랜 시스템의 증가에 큰 영향을 주고 있는 실정이다.[1]

그러나 무선랜 특성상 전파가 도달하는 거리내 어디든지에서 해킹과 침투가 가능하다는 커다란 취약점을 가지고 있다. 그러한 무선 네트워크에서의 보안 취약성 중 대표적인 것으로 Rogue AP를 통한 불법 접근 및 외부로의 중요 데이터 유출 문제가 있다.[2][3][4]

Rogue AP는 다음과 같은 네가지 형태의 분류가 가능하다. 공격자가 강제로 신호를 높여서 접속을 유도하는 AP, 구성원이 네트워크 내에서 관리자에게 등록없이 사용하는 AP, 타 회사 및 건물의 AP, 테더링이나 핫스팟, egg 등의 스마트폰을 이용하는 AP로 얘기할 수 있다. 이러한 모든 경우, 내부 네트워크의 모든 자원을 내부 사용자와 같은 자격으로 공격자 혹은 잠재적 해커에게 개방이 된다.[5]

공격자가 유도하는 Rogue AP에 접속을 한다면, 공격자는 IP, MAC 주소를 얻을 수 있으며, 위장 게이트웨이 주소, DNS 주소 등을 보낼 수 있으며, 이를 이용한 피싱(Phishing)이나 파밍(Pharming) 공격이 가능하다.[6][7]

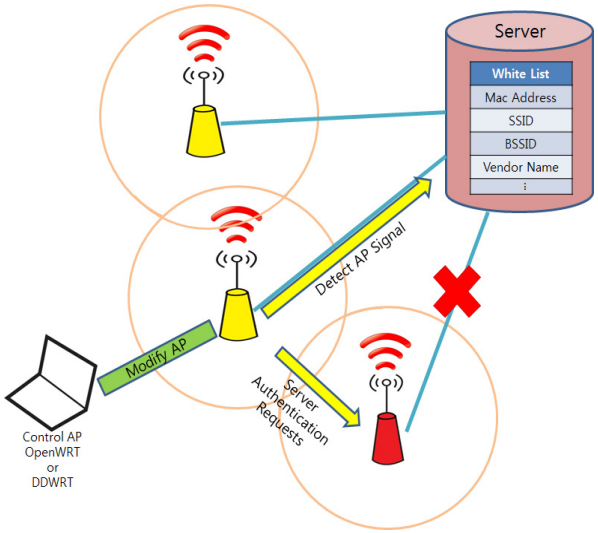
본 논문의 구성은 다음과 같다. 먼저 2장 관련연구에서 현재 Rogue AP 탐지 및 보안 방법과 그 취약점을 기술하고, 3장 제안기법에서 무선랜 환경에서 효과적인 Rogue AP 탐지 기법에 대해 고찰하고, 이를 바탕으로 기존 Rogue AP 탐지 기법을 보완한 효과적인 Rogue AP 탐지 기법에 대해 제안한다. 마지막으로 결론과 향후 연구 방향을 제시한다.

2. 관련연구

현재 시장에 나와 있는 무선 공유기 제품을 보면 기본적으로 Rogue AP의 탐지를 제공해주며, RADIUS (Remote Authentication Dial-In User Services)를 암호화 설정 시에 지원해주고 있다. 그러나 이러한 제품의 출시에도 불구하고, 무선랜 보안은 너무나 취약한 상황이다. 공격자가 AP에 불법 침입하게 되면, 인트라넷 환경하의 로컬 시스템의 접속이 자유자재로 가능하게 된다. 이로써 내부 보안망이 유출되게 되는 문제점이 발생하게 된다. 또한 WEP(Wired Equivalent Privacy), WPA(Wi-Fi Protected Access), WPA2(Wi-Fi Protected Access2) 등 암호화를 해도, WEP의 암호화의 경우 5분이면 해킹이 가능하고, WPA와 WPA2 역시 쉽게 보안이 유출되는 현상이 발생한다. 그렇다고 정확한 Rogue AP 방지를 위해서 수시로 관리자가 분석기를 들고 워드라이빙 (War Driving)을 할 수도 있으나,[8] 이 경우 간헐적으로 운용되는 Rogue AP의 경우 탐지가 불가능 하며, 물리적으로 접근이 불가능한 지역이 있을 수 있다.[9]

3. 효과적인 Rogue AP 탐지 기법

서버에는 WhiteList라는 인가된 AP List를 가지고, 새롭게 검색된 AP가 List가 없다면 AP의 MAC Address, SSID(Service Set Identifier), BSSID(Basic Service Set Identifier), Vendor Name 등의 정보를 바탕으로, 이상 여부를 판단하고, 이상이 있는, 즉, White List에 찾을 수 없는 MAC 주소의 AP는 불법적 AP, 즉 Rogue AP로 판단을 한다.[10]



(그림 1) Rogue AP 탐지 시스템

[그림1]과 같이, AP가 전파를 수신할 수 있도록 수정하여, 수정된 AP에서 새로운 AP(사용자가 사용하려고 설치한 AP이든, Rogue AP이든)가 발견될 경우, 서버에는 새로운 AP가 발견되었다는 신호를, 새롭게 발견된 AP에는 서버에 인증을 시도하라는 신호를 보낸다. 인가된 사용자가 사용하려고 설치한 AP라면 서버에 등록이 되어 있고, 신호를 받은 AP는 서버에 요청을 할 수 있으며, 그렇지 않은 Rogue AP라면 서버에 요청을 할 수 없다. 이러한 방식으로 Rogue AP를 탐지한다.

오픈 소스 펌웨어(Open Source Firmware)인 DD-WRT를 이용해서 AP에 리눅스 기반의 오픈 소스 운영체제를 올려서 AP를 수정하여, Rogue AP를 탐지하는 방식을 사용한다.[11]

네트워크 관리자는 이 방식을 이용하면, 관리하는 무선 네트워크 망을 확실하게 관리할 수 있다. 인가된 사용자가 설치하는 AP나, 공격자가 의도적으로 설치하는 AP 모두 찾을 수 있다.

본 논문은 Rogue AP 탐지에 있어서, 어떤 특별한 하드웨어도 필요하지 않으며, 비용적으로나, 사내 네트워크 망을 구성함에 있어서나 효과적이다.

4. 결론

차세대 네트워크 발전 방향과 직접적으로 관계된 무선 네트워크 보안 문제는, 이러한 특정 주제에 대하여 심층적인 연구의 가치가 있다. 현재 시중에서 Rogue AP를 탐지, 제거하는 방법으로는, Wireless IDS(Intrusion Detection System)이나 Wireless IPS(Intrusion Prevention System) 등이 있다. 그러나 이러한 제품들은 하드웨어적으로 설정을 해야하며, 그 장비 역시 고가의 비용을 자랑한다. 본 논문은 이렇게 값비싼 WIDS / WIPS 제품 등을 이용하는 하드웨어 적인 Rogue AP 탐지가 아닌, 소프트웨어 적으로 Rogue AP를 탐지할 수 있는 방법을 기대하며, 또한, 기존에 제시되고 있는, 소프트웨어 적인 방식에 대한 취약점에 대한 보안점을 기술한다.

현재 D-Link 사의 DIR-300 공유기에 DD-WRT를 펌웨어 업데이트를 하였고, 수정된 AP 사이에서의 무선 메시지 통신에 대한 작업을 진행 중이다.

제안된 시스템을 활용하면, 네트워크 관리자는 서버에 저장된 White List를 이용하여, 해당된 AP가 인가된 AP인지 아닌지를 판단하고, 그 판단을 기준으로, Rogue AP 손쉽게 탐지를 할 수 있다.

향후 연구로, 수정된 AP가 서버에 인증시킨 AP에 계속적인, 인증 요청 메시지를 보내지 않는 방법 및 Server에서 가지고 있는 WhiteList 정보 외에 추가적으로 필요한 정보에 대한 부분은 향후 연구로 남겨 놓는다.

참고문헌

[1] Wikipedia, [online] http://en.wikipedia.org/

[2] AirDefence : a wireless intrusion prevention system, [online]. http://airdefense.net

[3] AirMagnet : Enterprise WLAN Management, [online], http://airmagnet.com

[4] Airwave : Wireless Network Management, [online], http://airwave.com

[5] Xiao qiang peng, Cheng Zhang, Dian gang Wang, “The Intrusion Detection System Design in WLAN Based on Rogue AP” Computing Engineering and Technology (ICCET) 2010 2nd International Conference on

[6] Hao Han, Bo Sheng, Chiu C. Tan, Qun Li, Sanglu Lu, “A Measurement Based Rogue AP Detection Scheme” InfoCom 2009, IEEE Journal

[7] Hao Han, Bo Sheng, Chiu C. Tan, Qun Li, Sanglu Lu, “A Timing-Based Scheme for Rogue AP Detection” InfoCom 2009, IEEE Journal

[8] NetStumbler, [online] http://www.netstumbler.com

[9] V. S. Shankar Sriram, G. Sahoo, Krishna Kant Agrawal, "Detecting and Eliminating Rogue Access Points in IEEE-802.11 WLAN - A Multi-Agent Sourcing Methodology”, Advance Computing Conference(IACC), 2010 IEEE 2nd International, pp. 256-260.

[10] Chia-Tai Tsai, Rong-Hong Jan “A Rogue AP Detection System for Wireless LANs” 2007

[11] DD-Wrt : What is DD-Wrt?, [online] http://www.dd-wrt.com