중소기업융합학회 논문지 제4권 제3호 pp. 15-20, 2014 ISSN 2234-4438

중소기업형 무선 네트워크의 해킹과 보안

신판섭[1], 김정민[1*]
[1]대진대학교 컴퓨터공학과

Security and Hacking on Wireless Networking for Small and Medium Business: Survey

Pan-Seop Shin[1*], Jeong-Min Kim[1*]
[1]Computer Science, Daejin University

요 약 무선 네크워크는 유선과 비교해서 편리하고, 또한 용이하다. 따라서 전국에 있는 중소기업에서는 무선을 더 선호하고 있어 많은 중소기업들이 유선 설치에 대한 부담을 느껴 유선네트워크의 확장개변으로 무선을 많이 사용하고 있는 추세이다. 무선네트워크는 유선 네트워크보다 보안에 취약한데, 그 이유는 브로드캐스팅을 통해 패킷을 전달하기 때문이다. 따라서 무선 네트워크의 취약점들을 분석하고, 중소기업에서 무선네트워크 보안에 관한 대응책을 제시하고자 한다.

키워드 : 무선 네트워크, Rogue AP, DoS 공격, Man-in-the-Middle, 암호화, 인증

Abstract Wireless network is convenient as compared to the wire, and it is also easy. Therefore, SMEs in the country is the trend that many SMEs prefer the radio using a lot of radio as an extension of the wired network modification felt the burden of fixed installations. Wireless networks are vulnerable to security together than a wired network, since it passes the packet through the broadcasting. Therefore, analyzing the vulnerability of wireless networks, and proposes countermeasures about wireless network security in small and medium-sized businesses.

Key Words : Wireless networks, Rogue AP, DoS attacks, Man-in-the-Middle, encryption, authentication

1. 서론

수 세기동안, 사람들은 회사, 대학, 그리고 도시에서 개인 컴퓨터와 서버를 연결하기 위하여 컴퓨터 네트워크를 사용해왔다. 그러나 네트워크를 무선으로 사용하려고 하는 변화가 생기고 있다. 현재의 무선 인터페이스는 어느 곳에서든지 e-mail을 사용하고 응용 장치를 접근하고 인터넷을 검색하기 위해 네트워크 서비스를 이용할 수 있게 해주었다.

이러한 무선 응용들은 사람들의 작업 공간을 확장시켜 주어서 상당한 이득을 있게 해준다. 예를 들어, 비즈니스 여행자는 공항에서 비행기 출발 시간을 기다리는 동안에 e-mail에 대한 답장을 할 수 있다. 집에서는 추가적인 케이블 없이 여러 대의 PC나 랩톱들을 인터넷에 접속할 수 있게 해준다.

그러나 무선 네트워크의 이용자가 많아짐에 따라 같은 네트워크에 접속되어있으면 스마트폰 같은 경우는 해킹에 잘 노출되어 있어서 최근에 많은 문제가 야기되고

Received 2014-08-05 Revised 2014-08-12 Accepted 2014-08-25
*교신저자 : Jeong-Min Kim (jmkim@daejin.ac.kr)

있다. 이번 보고서를 통해 무선 네트워크를 통한 해킹 종류들과 그에 대한 방안들이 어떻게 되어있는지 알아보고 새로운 대안 등을 모색해 나갈 것이다[1].

2. 무선 네트워크

2.1 무선 네트워크

무선 네트워크는 신호를 전달하는 연결선 대신 선이 없는 선을 사용하는 통신의 네트워크를 이르는 말이다. 무선 인터넷 규약에서 사용하는 넷스팟과 WAP등의 무선랜을 사용하는 방법이 대표적이다. 스마트폰이나 태블릿 PC의 사용자가 많이 증가하면서 무선 인터넷 사용을 위해 무선 인터넷 공유기를 찾는 경우를 볼 수 있다. 하지만 거리에서 사용 가능한 AP는 나쁜 목적의 해커가 사용자의 정보를 수집하기 위한 목적이 될 수 있다. 정보를 얻은 사람은 AP 이용자가 사용했던 정보를 통해서 기존의 사용자와 동일한 권한을 얻을 수 있다.

또한 보안 설정이 안 되어 있는 AP는 공격적인 해킹자가 접선하여 내부시스템으로 들어와 자신이 주인인 마냥 사용할 수 있다. 권한을 획득하게 될 경우, 공격은 악성코드, 악성 스크립트 등 내부시스템에 설치하여 정보를 얻을 수 있다 [2].

2.2 무선 네트워크의 장점과 단점

장점은 주로 편의성, 비용 절감, 다른 네트워크와 호환성이 보장되면서 일상에서 필수적이 되어가고 있다 [3].

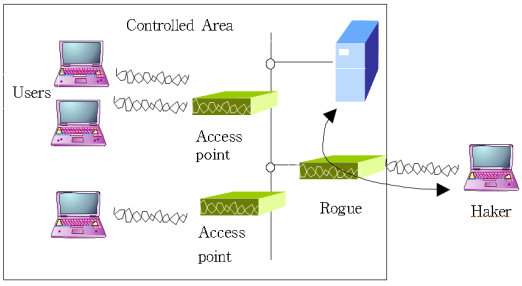

Fig. 1. 해커가 들어올 수 있도록 로그 AP가 문을 개방

Table 1. 무선 네트워크의 장점

편의성	집이나 회사에서 쉽게 이용할 수 있다.
휴대성	언제 어디서나 인터넷에 접속할 수 있다.
생산성	장소에 제약을 받지 않고, 자신이 원하면 접속할 수 있다.
배치	하나의 공유기만을 설치하여 다수의 장비에 연결할 수 있다.
확장성	기존의 장비를 사용하여 많은 고객들을 수용할 수 있다.

Table 2. 무선 네트워크의 단점

보안	무선 네트워크는 전파를 이용하므로, 누구나 패킷을 받아 볼 수 있다.
지원 범위의 한정	통상적으로 이용되는 802.11g 네트워크의 경우 수백 미터의 거리도 가능하다.
신뢰성	전파의 쇠퇴, 전파사이의 간섭 등의 이유로 패킷의 손상이 발생한다.
속도	대개의 무선 네트워크는 평균적으로 유선 네트워크에 비해서는 속도가 느리다.

2.3 무선 네트워크의 취약점

첫 번째로 Rogue AP는 무허가/불법 AP로 내부 관계자들이 편의를 위해 사용한다. 카페나 직장에서 Wi-Fi를 사용하기 위해 이용하는, 부정확한 경로의 공유기가 예이다.

따라서, Rouge AP는 보안설정이 안되어 있거나 취약한 경우가 대부분으로, 침입이 잦다. 실제로 일반 도시의 무선 LAN AP의 30%는 보안기능을 사용하지 않고 있다. 이것은 누구나 하드 드라이브를 접근하고 인터넷에 접속할 수 있다는 것을 뜻한다. 윈도우XP 운영 체제는 특히 공중 무선 LAN에서 무선 네트워크를 쉽게 접속할 수 있게 해준다. 무선 LAN에 결합된 랩톱의 사용자는 그 무선 LAN에 결합된 다른 랩톱들에 쉽게 접근할 수 있다. 개인 방화벽으로 랩톱을 보호하지 않으면, 누군가가 랩토의 하드 드라이브를 검색할 수도 있다. 이것은 상당한 수준의 보안 위협이다.

두 번째로 Air Signal Sniffing는 무선 서비스가 암호화를 사용안할 때 무선 랜 신호를 잡아내 주요정보를 Sniffing한다.

세 번째로 WEP Crack은 WEP 알고리즘의 취약으로 인해 Crack이 가능하고 Crack된 경우 패킷의 내용이 해커에게 노출되고, 또한 해커가 사용기능 키를 생성하며 이를 인증된 클라이언트로 사용한다.

네 번째로 Wireless Hijacking은 Hacker가 자신의 station을 gatway의 MAC으로 변조, 모든 traffic을 자신에게로 돌려 데이터 캡쳐 및 분석이 가능하다.

다섯 번째로 Dos 침입은 해킹자가 AP를 사용하는것처럼 위장하고, 접속을 허가하지 않는다는 내용의 패킷을 전송하면 정상적인 장소와 AP의 연결을 해제할 수 있다. 그러나 DOS 공격을 효과적으로 방어할 수 있는 방법은 없다.

여섯 번째로 Man-in-the-Middle 공격이다. 암호화와 인증 기술을 사용하면 무선 네트워크의 보안을 향상시킬 수 있는데, 해커들은 네트워킹 프로토콜의 동작 방식 때문에 여전히 취약성을 찾을 수 있다.

확실한 단점 중의 하나는 man-in-the-middle 공격이며, 이것은 해커가 사용자와 무선 네트워크 사이에 가짜 장치를 설치함으로써 된다. 예를 들어, 일반적인 man-in-the-middle 공격은 모든 TCP/IP 네트워크에서 사용되는 ARP를 사용한다. 제대로 된 도구를 갖고 있는 해커는 ARP를 이용해서 무선 네트워크를 제어할 수 있다.

마지막으로 Covering Tracks는 불량 접속점(허가를 받지 않고 무료의 무선 LAN을 서비스하는 장소, 혹은 간단한 인증을 이용하는 곳)으로부터의 해킹은 물리적 추적이 불가능하다.[4]

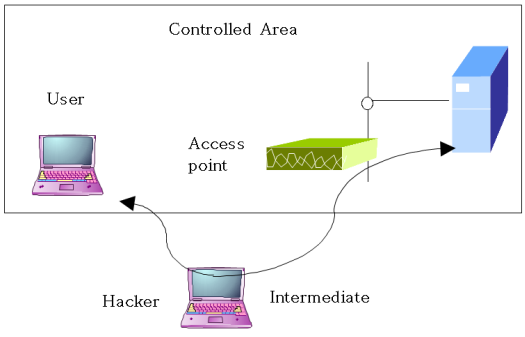

Fig. 2. man-tn-the-middle 공격

3. 무선 네트워크 해킹 대응방법

3.1 암호화

다양한 보안 위협으로부터 무선 LAN을 보호하기 위한 방법으로 암호 방식과 네트워크 접근인증 방식이 사용된다. 다양한 암호를 통해서 공격자의 침입을 막는 방법과 기존에 의한 보안 기법방법으로 IEEE 802.11 무선망으로, Pre-RSN이라고 부른다.[5]

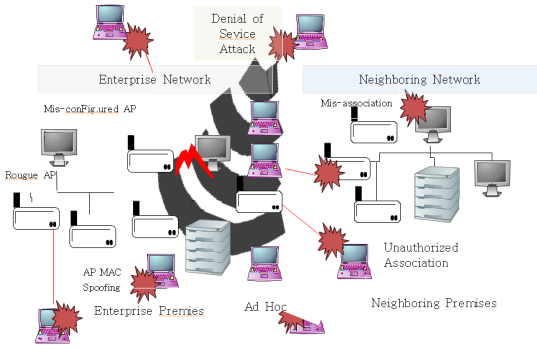

Fig. 3. 무선랜 보안 위험요소

암호화는 평문을 쌍방이 공유한 비밀 키를 사용하여 해커가 인지할 수 없는 문장으로 변경하는 작업으로서, 무선 LAN에서는 3가지가 사용된다.

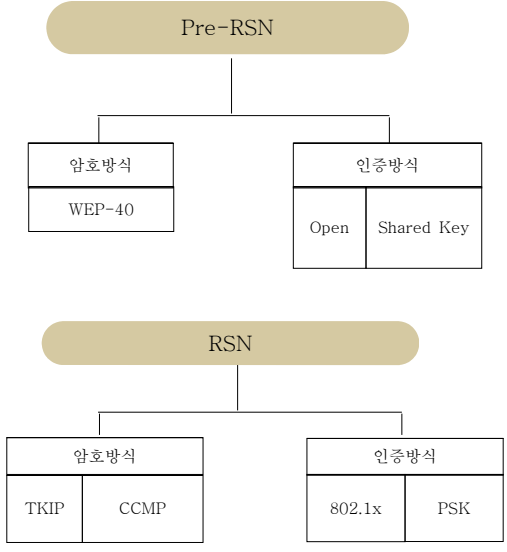

Fig. 4. 무선 LAN의 보안 기술

3.1.1 WEP(Wired Equivalency Privacy)

무선 LAN용 기본 암호 방식이다. 기본적으로 단말과 AP는 동일한 암호 문장으로부터 4개의 고정된 장기 공유 키를 생성한 후, 이들 중에서 하나를 선택하여 암호 및 인증을 활용한다. 그러나, 선택이 된 공유 키의 KeyID와 IV값을 평문으로 상대방에게 알려 주어야 하기 때문에 WEP 키가 추출 될 수 있는 약점이 있다.

3.1.2 TKIP(Temporal Key Integrity)

WEP과 동일한 RC4스트림 암호 방식을 사용하지만, 각 프레임별로 상이한 키를 적용하고, 필요한 경우 임시 비밀 키를 자동으로 갱신함으로써 보안성을 강화한 것이다. 또 다른 장점은 기존 WEP 암호 방식과 같이 소프트웨어로 동작하므로, 단순히 해당 장비의 펌웨어만 교체하면 된다는 점이다. WPA에서는 이것을 WPA-1 보안 방식이라고 한다.

3.1.3 CCMP(Counter with CBC-MAC Protocol)

블록 사이퍼를 사용한 가장 강력한 암호 방식이다. 최근에 출시되는 일부 무선 LAN 장비에 적용되고 있다. WPA에서는 이것을 WPA-2 보안방식이라고 한다.[6]

3.2 인증

무선 네트워크에서 상호 인증을 사용하는 것은 중요하다. 인증은 man-tn-the-middle 공격과 같은 여러 가지 보안 문제를 해결해준다. 상호 인증을 하는 경우 무선 클라이언트와 무선 네트워크는 서로의 신분을 입증해야만 한다. 인증과정에서는 RADIUS와 같은 인증 서버를 사용한다.

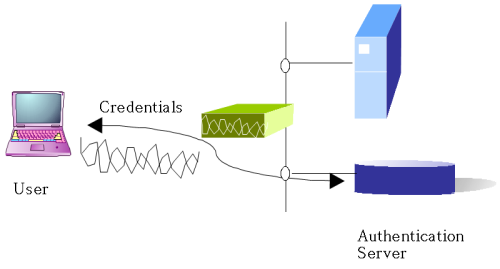

Fig. 5. RADIUS 서버 인증

Fig. 5에서 인증은 암호와 디지털 서명과 같은 자격 정보를 사용해서 사용자 및 클라이언트 장치의 신분을 검증.

3.2.1 802.11 인증

WEP는 무선 NIC를 AP에 인증하는 방법만 제공한다. 따라서 해커는 보안 기법을 우회하는 대체 비인증 경로를 통해서 데이터를 보낼 수도 있다. 이 문제를 해결하기 위해서 무선 네트워크에서는 단방향 인증 대신에 상호 인증을 구현해야만 한다.

802.11은 디폴트로 개방 시스템 인증이라고 하는 인증 방식을 제공한다. 이 방식에서 AP는 인증에 대한 임의의 요구에 대해서도 승인해 준다. 클라이언트는 단순히 인증 요청 프레임을 전송하고 AP는 인증 승인에 대한 응답을 하며, 따라서 정확한 SSID(Service Set Identifier)를 갖고 있는 사람은 누구나 AP와 결합할 수 있다. 또한, 802.11 표준은 선택 가능한 보다 향상된 형태의 인증 방식인 공유키 인증을 포함하고 있으며, 다음 네단계의 절차로 구성된다.

1) 클라이언트는 인증 요청 프레임을 전송한다.
2) AP는 챌린지 텍스트라고 하는 문자열을 포함하는 프레임으로 응답한다.
3) 클라이언트는 공통의 WEP 암호화 키를 사용해서 챌린지 텍스트를 암호화한다. 클라이언트는 암호화된 챌린지 텍스트를 AP에게 돌려보내며, 공용키를 사용해서 텍스트를 해독하고 그 결과를 원래 보내온 텍스트와 비교한다.
4) 독된 텍스트가 일치하면 AP는 클라이언트를 인증한다.

이 방법은 인증에는 적합해 보이지만, 문제는 공유키 인증 방법이 정확한 WEP 키를 클라이언트가 갖고 있다는 것만 입증한다는 것이다.

3.2.2 MAC 필터

일부 무선 기지국은 MAC(Medium Access Control) 필터링을 제공하는데, MAC 필터링을 구현할 때 AP는 도착 프레임마다 근원지 MAC 주소를 검사한다. AP는 관리자가 입력한 리스트에 존재하지 않는 MAC 주고를 갖고 있는 프레임을 거부한다. 따라서 MAC 필터링은 기본적인 형태의 인증을 제공해 준다.

하지만 해커가 쉽게 프레임 전송을 스니핑해서 유효한 MAC 주소를 발견할 수 있으며, 합법적인 사용자가 네트워크에 없을 때 자신이 실제 사용자인 것처럼 가장해서 AP를 속일 수 있다는 단점이 있다.

3.2.3 공개키 암호화를 사용하는 인증

스테이션은 해커들로부터 정보를 보호하기 위해서, 그리고 다른 스테이션이나 AP들에게 자신을 인증하기 위해서 공개키 암호화를 사용할 수 있다. 스테이션은 사설키를 사용해서 패킷의 텍스트 문자열을 암호화함으로써 자신을 인증시킨다. 수신 스테이션은 송신 스테이션의 공개키를 사용해서 텍스트를 해독한다. 만약에, 해독한

텍스트가 스테이션의 이름 등과 같이 미리 정해진 텍스트와 일치하다면, 수신 스테이션은 송신 스테이션이 유효하다는 것을 알게 된다. 이 경유, 특정 텍스트 스트링을 암호화 하는 것이 디지털 서명의 역할을 한다.

3.3 사용자의 해킹 대응 방법

첫 번째로 소비자들에게 널리 알려지고 신뢰할 수 있는 어플을 신중하게 다운로드 한다.

두 번째로 신뢰할 수 있는 사이트만 방문을 한다.

세 번째로 주소가 명확하지 않은 알림이나 메일들은 삭제를 한다.

네 번째로 비밀번호를 정기적으로 바꿔준다.

다섯 번째로 무선 활용은 자신이 사용할 때에만 켠다. 암호가 걸려져 있지 않거나 암호가 있다고 하더라고 해킹을 당할 수 있다.

여섯 번째로 특이사항 발견 시 악성코드 의심여부를 확인한다. 미리 백신 어플을 깔아놓는게 좋고 수시로 검사를 실시하는게 좋다.

일곱 번째로 스마트폰 플랫폼임을 변경하지 않는다.

마지막으로 운영체제나 백신 프로그램은 최신 버전으로 업데이트한다.

4. 결론

무선네트워크는 설치와 사용의 편리함 때문에 중소기업에서 많이 사용하고 있으나, 브로드캐스팅 기법을 사용하기 때문에 보안에 취약하여 대기업에서는 사용을 하지 않는 추세이나, 중소기업은 보안인력도 부족하고, 보안장비도 부족하지만 유선네트워크 추가 구축에 대한 비용 부담으로 여전히 무선네트워크를 유선의 확장 개념으로 사용하고 있기 때문에, 중소기업에서 무선네트워크를 사용하면서 보안도 충족시킬 수 있는 방법들을 제시하여 무선네트워크 사용시 해킹의 피해를 줄이기 위해 이 연구를 하였고, 앞으로 유무선 결합형 보안 솔루션을 통해 향후에 있을 새로운 형태의 공격을 막기 위한 연구를 진행할 예정이다.

참 고 문 헌

[1] Sunghyuck Hong, “Disconnection of Wireless LAN attack and countermeasure”, The Journal of Digital Policy & Management, Vol. 11, No. 12, pp. 453-458, Dec. 2013.

[2] Manley, M.E.; McEntee, C.A.; Molet, A.M.; Park, J. S.; "Wireless security policy development for sensitive organizations," IEEE June 2005 pp. 150 - 157.

[3] Garry, Barker. Technology Editor of The Age, " X marks the Spot for Hackers" July 8, 2002.

[4] Chan, F.K.L.; Ang Hee Hoon; Issac, B.; " Analysis of IEEE 802.11b wireless security for university wireless LAN design", Networks, 2005. Jointly held with the 2005 IEEE 7th Malaysia International Conference on Communication. 2005 13th IEEE International Conference on Volume 2, pp. 6 pp, 16-18 Nov. 2005.

[5] William, S. "Cryptography and Network Security": "Principles and Practice", Prentice Hall, July 1998.

[6] Chan, H.A.; "Requirements of interworking wirelessLAN and PLMN wireless data network systems", AFRICON, 2004. 7th AFRICON Conference in Africa, Volume 1, pp. 251 - 255 Vol.1, 2004.

[7] Lapiotis, G.; Byungsuk Kim; Das, S.; Anjum, F.; " A policy-based approach to wireless LAN security management", Security and Privacy for Emerging Areas in Communication Networks, 2005. Workshop of the 1st International Conference on 5-9 Sept. 2005 pp. 181 - 189, 2005.

[8] Branch, J.W.; Petroni, N.L., Jr.; Van Doom, L.; Safford, D.; "Autonomic 802.11 wireless LAN security auditing", Security & Privacy Magazine, IEEE Volume 02, Issue 3, pp. 56 - 65, May-June 2004.

[9] Imai, I.; SeongHan Shin; Kobara, K.; " Authenticated key exchange for wireless security", Wireless Communications and Networking Conference, 2005 IEEE, Volume 2, pp. 1180-1186,13-17 March 2005.

[10] S. McClure, J. Scambray and G. Kurtz, Hacking Exposed: Network Security Secrets &, Solutions, 4th ed., McGraw-Hill/Osborne, 2003.

[11] J. Edney and W.A. Arbaugh, Real 802.11 Security: Wi-Fi Protected Access and 802.11i, Addison-Wesley, 2004.

[12]L. Barken, How Secure Is Your Wireless Network? Safeguarding Your Wi-Fi LAN, Prentice Hall PTR, 2004.

[13] B. Schneier, Secrets &, Lies: Digital Security in a Networked World, John Wiley &, Sons, 2000.

[14] A. Engst and G. Fleishman, The Wireless Networking Starter Kit: The Practical Guide to Wi-Fi Networks for Windows and Macintosh, 2nd ed., Peach- pit Press, 2004.

[15] V. Moen, H. Raddum and K.J. Hole, "Weaknesses in the

Temporal Key Hash of WPA," ACM Sig-Mobile Mobile Computing and Comm. Rev., vol. 8, no. 2, 2004, pp. 76-83.

저 자 소 개

신 판 섭(Shin, Pan-Seop) [일반회원]

- 1994년 2월 : 홍익대학교 컴퓨터공학과(공학석사)
- 2000년 8월 : 홍익대학교 컴퓨터공학과(공학박사)
- 현재 : 대진대학교 컴퓨터공학과 부교수

<관심분야> : 데이터베이스, 시맨틱 웹, 멀티미디어 시스템

김 정 민(Kim, Jeong-Min) [일반회원]

- 1994년 2월 : 홍익대학교 컴퓨터공학과(공학석사)
- 2007년 2월 : 서울대학교 컴퓨터공학과(공학박사)
- 현재 : 대진대학교 컴퓨터공학과 조교수

<관심분야> : 온톨로지, 시맨틱웹, 지식표현, 인터넷미디어