네트워크 취약점을 통한 공유기 공격동향 및 예방방법

이영현* · 김기환** · 이훈재**

*동서대학교

Trends and methods of preventing router attacks using network vulnerability

Young-Hyeon Lee* · Ki-Hwan Kim** · Hoon-Jae Lee**

*Dept. of Information and Communication Engineering, Dongseo University

**Dept. of Ubiquitous IT Graduate School of Dongseo University

**Dept. of Computer Engineering, Dongseo University

E-mail : cmc0835@naver.com, ghksdl90@naver.com, hjlee@dongseo.ac.kr

요 약

현대사회에서 컴퓨터와 스마트폰의 보급으로 인터넷은 생활의 일부가 되었으며, 이를 위해 대부분의 장소에는 유/무선 공유기가 설치되어 있다. 크래커는 네트워크의 취약점을 악용하여 공유기를 사용하는 사용자를 다양한 방법으로 공격할 수 있다. 공격기법 가운데 정상적인 인터넷 주소를 요청했지만 공유기의 DNS 변조를 통해 크래커가 만든 서버로 유도하는 공격기법을 통해 많은 사람들이 피해를 입고 있다. 이에 본 논문에서는 대표적인 네트워크 공격에 대하여 살펴보고 각 공격에 예방하는 방법을 살펴본다.

ABSTRACT

In modern society, the spread of computers and smart phones, the Internet has become part of life. Therefore, the most places, wired/wireless router is installed. Crackers can attack the user to use the router by exploiting network vulnerabilities. therefore, the administrator is able to try cracker variety of attacks sloppy router, vaccine is installed also computer and smartphone users , appearance and address of the usual Internet is not deer medium and similar. In this paper, we look at a method for preventing in each attack seen for typical network attacks.

키워드

공유기, 인터넷, DNS spoofing, Man In The Middle Attack, Evil Twin Attack

Ⅰ. 서 론

현대인에게 인터넷은 필수적인 요소로 자리잡고 있다. 대부분의 업무나 취미생활이 인터넷을 통해 처리되고 온라인상으로 물건을 주문하거나 금융업무도 수행되고 있다. 또한 스마트폰의 보급화를 통해 무선 통신 장비가 비약적으로 증가하였다. 따라서 우리가 생활하는 대부분의 장소에는 유/무선 공유기가 설치되어 사용되고 있다.

공유기를 사용하는 사용자들은 보안적인 측면보다는 별도의 이용료 없이 인터넷 서비스를 이용할 수 있는 경제적인 측면을 주로 생각한다. 최근 사례에 따르면 네트워크 취약점을 이용하여 우리나라에 설치된 유/무선 공유기를 공격하여 사용자의 개인 정보가 유출되는 피해사례가 나타나고 있다.

크래커들은 이러한 공유기의 취약점을 악용해 공유기의 DNS 정보를 변경하는 공격방법을 사용하여 크래커가 만들어 놓은 모방된 사이트로 유도할 수 있다. 또는 공유기를 통해 통신하는 사용자의 패킷 정보를 조작하는 중간자 공격 등을 통하여 가전제품까지도 크래커들이 공격할 수 있다. 따라서 공유기를 사용하는 사용자들의 공유기 보안에 대한 관심이 요구된다.

그림 1.은 우리나라에 설치된 유/무선 공유기의 보안실태에 대해서 설명한다.

〈점검항목 및 실태점검 결과〉

구 분	점검 항목	취약한 공유기 수	취약 사례
무선 접속	1. 패스워드 설정 여부 확인	58개	패스워드 없이 SSID로만으로도 무선 접속 가능
	2. 기본 및 취약 패스워드 사용 여부 확인	148개	'1234' 등 쉬운 패스워드 사용 8자리 보다 짧은 패스워드 사용
	3. 무선 암호화 수준 확인(WPA2)	93개	무선 암호화를 적용하지 않음 WPA 혹은 WEP 등 취약한 암호화 사용
공유기 관리자 페이지	4. 패스워드 설정 여부 확인	141개	관리자 계정을 설정하지 않아 인증절차 없이 관리자 페이지 접근 가능
	5. 패스워드 보안성 평가	182개	기본 패스워드 사용(ex. admin/admin) 8자리 보다 짧은 패스워드 사용
	6. 원격 접속 기능 활성화 여부 확인	16개	원격 접속 기능 활성화 상태
서비스 보안	7. 공유기 설정 내 DNS 변조 여부 확인	5개	DNS IP가 해외 IP로 설정됨
	8. 불필요 서비스 실행 여부 확인	59개	uPnP, FTP 등 사용하지 않는 서비스가 실행 중
펌웨어 업데이트	9. 최신 펌웨어 업데이트 설치 여부 확인	166개	최신 펌웨어가 아닌 경우

그림 1. 유/무선 공유기 보안실태 점검결과[1]

II. 네트워크 공격 유형 및 사례

2.1 DNS spoofing

사용자는 특정 웹페이지에 접속하기 위해 DNS Query 패킷을 UDP 형식으로 DNS Server에 요청하게 된다. UDP 방식은 별도의 인증 없이 사용자의 컴퓨터에 먼저 도착한 DNS Query 패킷을 우선적으로 신뢰한다. 따라서 크래커가 정상적인 DNS Server보다 먼저 사용자에게 응답을 하게 된다. 당연히 사용자는 정상적인 응답이 아닌 크래커가 조작한 응답을 받게 된다. 결국 사용자는 응답받은 IP주소로 접속하게 되면 크래커가 모방한 웹페이지로 이동하게 된다. [2]

즉 DNS Spoofing은 그림 2와 같이 사용자가 원하는 웹페이지에 대한 IP요청을 크래서가 모방한 주소IP를 사용자에게 보냄으로써 조작된 웹페이지로 유도하는 공격이다.

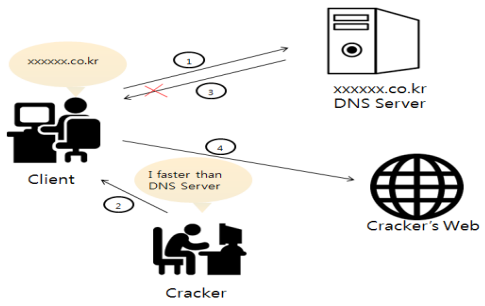

그림 2. DNS Spoofing 공격 절차

그림 3은 네이버에 접속을 시도할 때, 크래커가 DNS spoofing 공격을 이용한 사례이다.

사용자가 공격당한 공유기로 네이버 메일 페이지 접속 시 앞서 언급한 원리와 동일하게 크래커가 조작한 네이버 웹페이지로 접속된다. 모방된 웹페이지에 접속하면 조작된 어도비 플래시 플레이어(Adobe Flash Player)를 다운받게 하는 액티브X(Active X) 설치창이 생성된다. 조작된 어도비 플래시 플레이어를 설치 할 경우 악성코드에 감염되며, 사용자의 네이버 로그인 정보를 통해 피해를 입히는 공격이다.

이 공격은 Internet Explorer 뿐만 아니라 Chrome 에서도 동일하게 동작하기 때문에 사용자가 공격당하기 매우 쉽다.

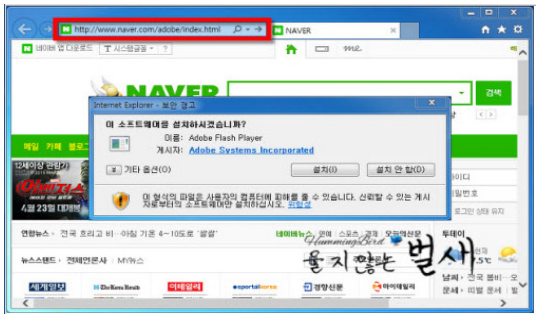

그림 3. DNS spoofing실행 후 네이버 포털사이트 접속 시[3]

2.2 Man in the Middle Attack

중간자 공격(Man In The Middle Attack, MITM)은 그림 4와 같이 네트워크 통신을 조작하여 통신 내용을 도청하거나 조작하는 공격 기법이다. 중간자 공격은 통신을 연결하는 두 노드 사이에 크래커가 침입하는 방법이다. 두 노드 사이에 크래커가 침입된 상태라면, 송신 측에서 패킷을 발신하면 크래커에게 수신된 후, 다시 크래커는 수신 측으로 발신한다.

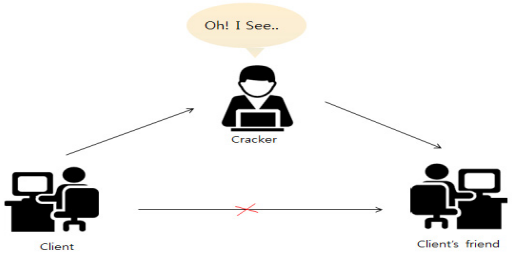

그림 4. MITM을 간략하게 표현

크래커는 MITM을 위해 대표적으로 사용하는 방법으로 ARP Soofing 공격방법을 사용한다.

ARP spoofing 공격원리는 ARP 패킷에 사용자의 IP주소와 MAC주소 대신, 사용자의 IP주소와 크래커의 MAC주소를 삽입하고 브로드캐스트 한

다. 그렇게 되면 네트워크 노드들이 사용자의 MAC주소대신 크래커의 MAC주소로 ARP Cache를 업데이트 하도록 한다. 공격이 성공하면 네트워크의 각 노드들은 사용자에게 가야할 패킷이 크래커에게 보내지게 된다. 특히 이러한 공격은 보안이 취약한 공유기를 사용할 때에 더욱더 쉽게 공격이 이루어 질 수 있다.[4]

특히 최근 주목받고 있는 IoT(Internet of Things)가 중간자 공격에 취약하다는 부분이 언급되고 있다.

스마트 냉장고에 SSL(보안 소켓 계층)을 설치하는 과정에서 취약점이 발견되었다. 스마트 냉장고를 통해 구글의 이메일 서비스를 이용할 수 있는데 G-mail 달력에 중간자 공격을 실행해 개인정보를 탈취 할 수 있다는 것이다.[5]

또한 스마트 자동차 내부에 탑재된 정보엔터테인먼트 시스템의 취약점을 공격하여 자동차의 핸들, 속도계 등을 조작할 수 있다는 것을 확인되었다. [6] 따라서 적극적인 공격을 통해 사용자에게 물리적인 피해도 입힐 수 있다.

2.3 Evil Twin Attack

Evil Twin Attack은 공공장소에서 흔히 볼 수 있는 실제 공개된 공유기의 이름과 무선랜 SSID가 동일한 가짜 공유기를 생성해 공격하는 방법이다. 그림 5와 같이 Evil Twin Attack으로 생성해낸 가짜 공유기는 정상적인 공유기보다 강한 신호를 발생시키기 때문에, 실제공유기보다 우선적으로 가짜 공유기에 연결하게 된다.

때문에 주의를 기울이지 않으면 언제든지 크래커의 공격대상이 될 수 있다. 대부분의 커피전문점에서는 암호가 걸린 공유기의 비밀번호를 영수증을 통해 제공한다. 크래커가 신뢰된 SSID와 동일한 암호를 가진 공유기를 이용하여 Evil Twin Attack 사용한다면 사용자들은 쉽게 크래커에게 공격당하게 된다. [7]

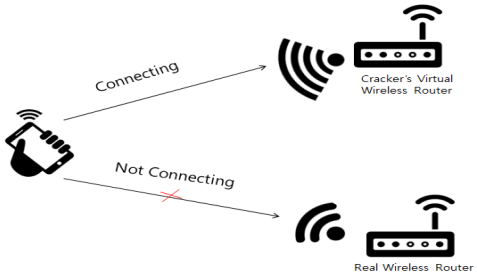

그림 5. Evil Twin Attack 방식

III. 유형에 따른 네트워크 공격의 예방방법

3.1 DNS Spoofing 예방방법

DNS Spoofing 공격을 통해 사용자의 개인정보유출이 쉽게 일어날 수 있기 때문에, DNS spoofing 공격에 대한 예방이 필요하다.

그림 6과 같이 hosts 파일에 도메인과 IP주소를 정적으로 고정시켜주면 그에 해당하는 사이트 DNS Spoofing 공격이 통하지가 않는다. 외부에 있는 DNS Server에 패킷을 보낼 필요가 없이 Local에서 DNS를 참조하기 때문이다. hosts 파일은C:\Windows\System32\Drivers\etc 에 위치해 있고 있다. 이를 그림 7과 같이 커맨드창에서 ping 명령어를 이용하여 도메인을 입력하여 IP주소를 알아낸 후 파일을 열고 IP 와 도메인을 입력하여 저장하면 된다.

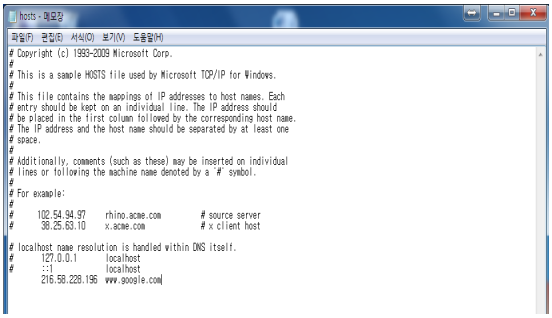

그림 6. 도메인과 IP를 고정시키는 방법

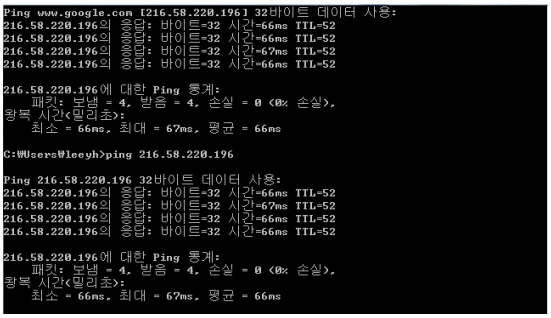

그림 7. 커맨드창을 이용하여 자주 가는 사이트 IP주소를 알아내는 방법[8]

3.2 Man In The Middle Attack 예방방법

중간자 공격을 예방하는 방법은 HTTPS 또는 VPN(가상 사설망) 기술에서 제공하는 보안이 강화된 네트워크 연결을 사용하는 것이다. HTTPS를 통해 네트워크 통신을 할 경우, 신원 또는 출처를 확인하기 위해 인증서를 확인하게 된다. 통신하는 과정에서 특정 서버에서 전송 된 인증기관을 인식하지 않는 경우 나 신뢰할 수 없는 페이지라고 나타날 경우 중간자 공격을 의심해야한다. 또는 이메일이나 문자 메시지의 링크를 클릭하거나 첨부파일을 함부로 열지 않는 곳이 좋다. 굳이 사이트에 들어가야 할 경우 브라우저 아래쪽의 자물쇠 모양 아이콘이나 열쇠 아이콘이 있는지 확인하는 것이 중간자 공격을 예방하는 방법이다.[9]

3.3 Evil Twin Attack 예방방법

Evil Twin Attack 공격의 예방방법은 사용자가 조작된 공유기와 정상적인 공유기를 구별하는 것이다.

사용자의 컴퓨터가 공유기에 연결되어 있다고 가정한다. 사용자가 조작된 공유기로 웹페이지에 접속한다면 정상적인 공유기보다 소모되는 시간이 더 길며 커맨드 창에서 traceroute 명령어를 통해 알 수 있다. 스마트폰을 자주 사용하는 사용자는 신호강도가 비정상 적으로 강한 공유기를 이용하는 것을 피해야 하며, 공개적인 공유기 사용 또한 피해야 한다.

추가적으로 학교 또는 기업 등 보안성이 더욱 요구되는 환경이라면 WIPS(Wireless Information Protection System)를 통하여 사용자 자신을 제외한 타인이 공유기에 접근을 허용하지 않는 방법도 존재한다.[10]

Ⅳ. 결 론

본 논문에서는 네트워크 취약점을 통한 네트워크 공격유형 및 피해사례, 예방방법에 대해 살펴보았다. 현대사회의 비약적인 통신기술의 발전으로 인해 앞으로 유/무선 네트워크를 이용하는 사용자는 계속해서 증가 할 것이며, 이를 위하여 대부분의 장소에는 사용자의 편의를 위한 공유기가 지속적으로 설치 될 것으로 생각한다.

앞서 언급한 바와 같이 네트워크 취약점을 통한 세 가지 공격방법은 대부분 보안에 대한 관심이 부족하거나 컴퓨터나 스마트폰 조작이 미숙한 사용자들을 대상으로 개인정보를 탈취하는 것이다. 탈취된 개인정보를 악용한 피싱, 파밍 등 금전적인 피해를 입히고 있다는 것이다. 또한 위의 세 가지 공격방법은 시대에 유행타지 않고 지속적으로 나타나 사용자들에게 피해를 주는 사례가 나타나고 있다. 최근에 인터넷을 사용하는 IoT장비가 매 해마다 출시되고 있다. 하지만 IoT와 관련된 공격사례는 빈번하게 발견되고 있다. 따라서 기존의 보안방법 보다 효과적인 대응방법 연구가 필요하다고 생각한다. 또한 사용자들의 보안의식에 대한 중요성 및 보안과 관련된 홍보활동이 다양한 매체를 통하여 알려질 필요가 있다고 생각한다. 향후 효율적인 방어방법에 대한 연구를 진행할 계획이다.

감사의 글: 이 논문은 2015년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(과제번호: 2011-0023076). 또한 부산광역시에서 지원하는 BB21 과제에서 지원받았음

참고문헌

[1] 김국배, “카페·도서관 공유기, 해킹에 취약”,아이뉴스24, ttp://news.inews24.com/php/news_view.php?g_serial=920157&g_menu=020310, (2015.09.21.)

[2] 구글, DNS spoofing, http://www.securitysupervisor.com/security-q-a/network-security/195-what-is-dns-spoofing, (2015.09.23.)

[3] 민세아, “네이버에서 어도비 액티브X설치창이? 공유기 해킹의심”, 보안뉴스, http://www.boannews.com/media/view.asp?idx=45953, (2015.04.15)

[4] 구글, “how to man in the middle attack”, http://null-byte.wonderhowto.com/how-to/hack-like-pro-conduct-simple-man-middle-attack-0147291/ (2015.09.13)

[5] 한동희, “삼성전자 스마트 냉장고 해킹 취약점 발견...이메일 개인정보 탈취 가능“, 조선비즈,http://biz.chosun.com/site/data/html_dir/2015/09/02/2015090200734.html?right_ju, (2015.09.02)

[6] 김경애, “추석 전 다시 체크해보는 하반기 보안위협 4가지, http://www.boannews.com/media/view.asp?idx=47960, (2015.09.24)

[7] 김인순, “공짜 와이파이 해킹 공포가 밀려온다.”, 전자신문, http://www.etnews.com/20150115000079, (2015.01.15)

[8] 구글, “DNS 스푸핑 대응”, http://www.slideshare.net/the1900/ss-43403572, (2015.9.21)

[9] 구글, “Man-in-the-middle Attack defence", http://blog.trendmicro.com/what-are-man-in-the-middle-attacks-and-how-can-i-protect-myself-from-them/, (2015.9.30)

[10] 김기환, “이블트윈 공격에 따른 클라우드 취약성”, 정보통신학회, 18권 2호, p383~386, 2014.10.30.