무선랜 AP를 이용한 무선랜 침입자 탐지 방법 연구

신동훈° 김동현
한국정보보호진흥원
{dhshin°, dhkim}@kisa.or.kr

Study on intruder detection method using a wireless Lan AP

DongHoon Shin° DongHun Kim
Korea Infomation Security Agency

요 약

현대 사회는 무선통신 기술의 급속한 발달로 인해 사용자가 자신의 위치에 상관없이 어디서든지 네트워크에 접속하여 서비스를 제공받을 수 있게 되었다. 하지만, 무선은 유선에 비해 상대적으로 보안에 취약하여 정보보호에 특별한 주의가 필요하다. 유선 네트워크는 침투를 위해서 물리적으로 침투위치를 확보해야만 공격을 수행할 수 있었으나, 무선의 경우에는 전파도달 거리내의 아무 곳에서나 공격을 시도할 수 있어 무선랜을 통한 많은 공격시도가 현실화되고 있다. 또한, 공격자가 공공장소, 대학교, 카페 등의 개방된 곳에서 자신이 습득한 다른 사용자의 ID를 사용하여 공중 무선랜 서비스에 접속하여 어느 특정 기관을 공격, 해킹할 경우에 공격 근원지와 공격자에 대한 추적이 사실상 불가능하다. 이러한 무선랜이 갖는 취약성을 보완하고 안전한 무선랜 환경을 구축하기 위해서, 본 논문에서는 무선랜 장비인 AP를 이용하여 침입자를 탐지하는 방법을 제시하고 있다. 제시된 방법은 현재 사용되어지고 있는 무선랜 환경에 추가적인 장비의 도입을 하지 않고, AP의 기능을 이용하는 방법을 제시하고 있다. 향후 AP와 무선 센서를 기반으로 하여 좀 더 정밀하고, 정확하게 침입자를 탐지하는 기술을 보강할 예정이다.

1. 서 론

현대 사회는 무선통신 기술의 급속한 발달로 인해 사용자가 자신의 위치에 상관없이 어디서든지 네트워크에 접속하여 인터넷 서비스를 제공받을 수 있게 되었다. 기존 네트워크는 통신 케이블이나 전화선 등의 유선으로 연결되어 있었다. 이에 반해, 무선랜은 유선 케이블 대신 무선 전파를 이용하여, 무선 네트워크 환경을 구축한다. 무선 전파를 이용함으로 구축시간, 운영 경비 등의 절감을 가져올 수 있다. 무선을 이용하면 전파 도달 범위 안에서 이동하면서 네트워크 접속이 가능하게 된다. 즉, AP가 설치된 곳에서 전파도달 범위 내에서 무선랜 단말기인 노트북, PDA 등을 통해 초고속 인터넷을 사용할 수 있게 된다. 데이터 전송을 유선 케이블 대신 무선 전파를 이용하므로 통신 케이블이나 전화선 등은 필요 없으나, 노트북, PDA 등 무선랜 단말기에는 전파 송수신이 가능한 무선랜 카드가 장착되어 있어야 한다.

다른 무선기술과 비교하여 차별화되는 무선랜의 특성은 일반 이동전화가 사용하는 전력보다 낮은 저전력 사용한다는 것이고, 전 세계적으로 허가 없이 사용해도 되는 비허가 주파수 대역인 ISM(Industrial, Scientific, Medical) 대역을 사용하고 있다는 것이다. 또한, 신호간섭이 존재하는 곳에서도 수신 감도가 강한 대역확산기술(Spread Spectrum Techniques)을 이용하여 전송하고 있다는 것이다. 무선랜은 기존 유선랜을 대체, 확장하여 유연한 데이터 통신을 할 수 있는 환경을 제공하고 있고, 유선망 없이도 데이터를 주고 받을 수 있는 기능을 제공한다. 즉, 유선 케이블이 없이도 이더넷이나 토큰링과 같은 전통적인 LAN 기술의 장점과 기능을 모두 제공할 수 있다. 무선랜은 데이터전송을 위해 무선 전파를 이용함으로 단말기가 빈번히 이동하는 경우, 배선이 어렵거나 단기간 사용하는 경우에 유용하게 사용될 수 있다. 무선랜이 이렇게 많은 장점을 갖고 있기는 하지만, 무선은 유선에 비해 상대적으로 보안에 취약하여 정보보호에 특별한 주의가 필요하다. 유선 네트워크는 침투를 위해서 물리적으로 침투위치를 확보해야만 공격을 수행할 수 있었으나, 무선의 경우에는 전파도달 거리내의 아무 곳에서나 공격을 시도할 수 있어 무선랜을 통한 많은 공격시도가 현실화되고 있다. 무선랜 데이터가 기본적으로 브로드케스팅 방식을 채택하고 있어, 무선으로 송수신되는 사용자 데이터에 관한 도청·감청의 위험이 항상 도사리고 있다. 사용자 인증 및 데이터 암호화 등의 보안 솔루션을 적용하여 사용하여 보안성을 증대 시킬 수 있으나, 사용자 인증을 위한 데이터 전송으로 관리 패킷의 전송률이 높아져 실제 사용자 데이터 전송률 감소되는 현상이 생길 수 있다. 무선랜은 데이터 전송을 위하

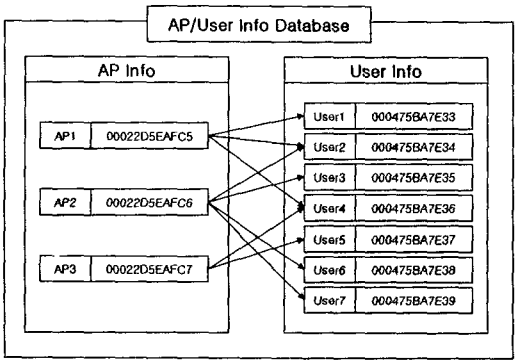
여 전파를 사용하고 있어, 전파 특성으로 인한 발생하는 서비스 거부가 있을 수 있다. 특히 무선랜이 ISM 대역을 사용하여 ISM 전파를 발생하는 다른 무선 기기인 전자레인지, 엘리베이터 모터, 플라즈마 전구 무선 리모콘(TV, 오디오) 등에서 나오는 전파로 인해 연결이 끊기는 현상이 생길 수 있다. 또한, 무선랜을 통한 공공장소, 대학교, 카페 등의 개방된 곳에서 해커가 무선 데이터를 분석하여 습득한 다른 사용자의 ID를 도용하여 해킹을 시도할 경우에 공격 근원지와 공격자에 대한 추적이 사실상 불가능하다.

이러한 무선랜이 갖는 취약성을 보완하고 안전한 무선랜 환경을 구축하기 위해서, 본 논문에서는 무선랜 장비인 AP를 이용하여 침입자를 탐지하는 방법을 제시하고 있다. 제시된 방법은 현재 사용되어지고 있는 무선랜 환경에 추가적인 장비의 도입을 하지 않고, AP의 기능을 이용하는 방법을 제시하고 있다. 향후 AP와 무선 센서를 기반으로 하여 좀 더 정밀하고, 정확하게 침입자를 탐지하는 기술을 보강할 예정이다.

2. 무선랜 침입자 탐지를 위한 시스템

2.1 무선랜 침입자 탐지를 위한 시스템 구조

AP를 이용하여 무선랜 침입자 탐지를 위한 시스템을 구현하기 위해 사용하는 기본적인 자료구조는 (그림 1)과 같다.



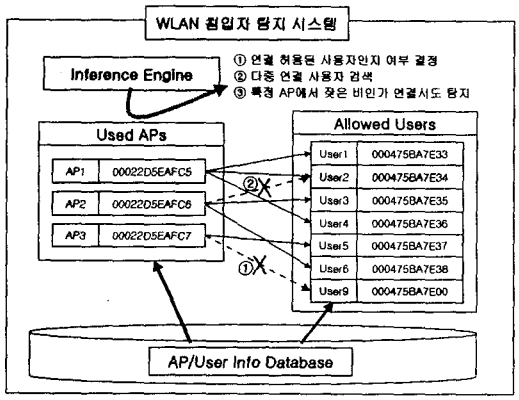
(그림 1) AP와 사용자 정보 데이터베이스

무선랜에 사용되는 AP 정보인 AP id와 AP의 MAC 주소로 이루어진 AP Info 자료구조와 무선랜 접속이 허용되는 사용자 정보를 관리하기 위하여 사용자 id와 사용자 단말기 MAC 주소로 이루어진 User Info 데이터 베이스로 구성되어진다. 또한, 각 AP에서 연결 접속이 허용되는 사용자 MAC 주소 정보를 링크시켜 놓았다. 이 정보를 이용하여 사용자가 인가되지 않은 지역에서 무선랜 AP를 이용하여 접속하려는 시도하려는 것을 탐지해 낼 수 있다.

위의 (그림1)에서 AP1은 User1, User2, User4와 연결을 허용하고 있고, AP2는 User2, User3, User6, User7과 연결을 허용하고 있는 모습을 표현하고 있다.

2.2 무선랜 침입자 탐지 시스템의 기능 및 동작

무선랜 침입자 탐지 시스템의 아래 (그림 2)와 같다. 무선랜 침입자 탐지 시스템은 앞에서 설명한 AP/User Info 데이터베이스, 현재 Power가 On 되어, 서비스가 제공되어지고 있는 AP의 정보를 표현하는 부분, 각 AP와 연결이 허용되어 현재 무선랜으로 네트워크 서비스를 제공받고 있는 사용자에 관한 정보를 표현하는 부분과 이런 정보를 기반으로 비인가 사용자를 탐지해내는 추론엔진으로 구성된다.



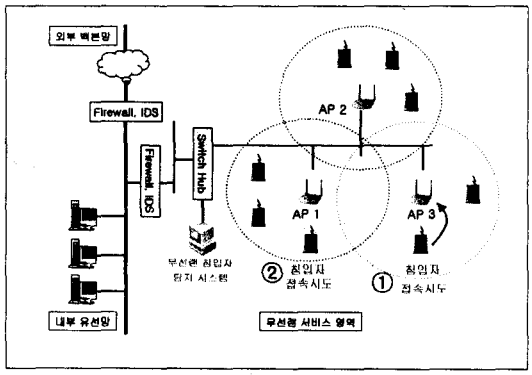
(그림 2) 무선랜 침입자 탐지 시스템

추론 엔진의 기능은 다음과 같다. 우선 (그림 2)의 ①과 같이 사용자의 연결 요청이 있는 경우에, 연결을 요청한 사용자 정보와 AP/User Info 데이터베이스의 사용자 정보를 비교 분석하여 연결이 허용된 사용자인지의 여부를 결정하는 기능을 수행한다. 연결을 허용하는 경우에는 Used APs와 Allowed Users에 새로 추가된 연결에 관한 정보를 추가한다. 즉, 어느 AP에 사용자 누가 연결하여 무선랜 서비스를 사용하고 있는지의 여부를 기록하는 것이다. 추론엔진의 두 번째 기능은 (그림 2)의 ②에서 표현하고 있는 것처럼, 비인가 사용자가 현재 무선랜 서비스를 제공받고 있는 사용자의 데이터를 분석하여, 연결이 허용된 사용자의 MAC 주소를 도용하여 연결을 요청하는 경우이다. 이러한 경우에 서로 다른 AP에 하나의 사용자 MAC주소로 연결이 허용되는 결과가 초래된다.

추론엔진에서는 이러한 하나의 MAC 주소로 다중 접속을 설정하려는 연결을 탐지하여 연결을 모두 보류시키고, 인가된 사용자에게 통보하여 보안 기능을 업그레이드 하도록 유도한다. 추론엔진의 세 번째 기능은 (그림 2)의 ③과 같이 하나의 AP에 잦은 비인가 접속을 시도하는 경우로, 이런 접속 시도가 계속해서 발생하는 경우에는 특정 AP의 보안 기능을 강화하거나, 특정 AP의 서비스 영역에 대한 무선 패킷 분석 도구를 이용한 침입자를 찾는 작업을 실시하여, 해커의 활동을 근절시킬 수 있다.

3. 무선랜 침입자 탐지 시스템 테스트

무선랜 AP의 기능을 이용한 침입 탐지 시스템의 기능을 테스트하기 위한 환경은 아래 (그림 3)과 같다.



(그림 3) 무선랜 침입자 탐지 시스템 테스트 환경

무선랜 AP를 정보를 이용하여 무선랜을 통한 침입자 탐지를 위한 실험환경은 위 (그림3)과 같다. 무선랜 네트워크에서 사용하는 AP는 3개이고, 무선랜 네트워크를 구성하는 스위치/허브에 무선랜 침입자 탐지 시스템을 연결하여 구성하였다. 침입자가 연결을 시도하기 전, 시스템의 AP/User Info의 정보를 (그림 1)과 같고, 무선랜 침입자 탐지 시스템의 내부 구성은 앞의 (그림 2)와 같다. (그림 2)에서 표현하고 있듯이, 연결 설정되어 무선랜 서비스를 제공받는 사용자에 관한 정보는 다음과 같다. AP1에서는 User1, User2, User4가 연결되어 사용되어지고 있고, AP2에서는 User3과 User6이 연결되어 사용되어지고, AP3에는 User 5가 연결되어 무선랜 서비스를 사용하고 있다. 이러한 상황에서 침입자가 연결을 시도하는 경우를 생각해 본다.

우선, (그림3)의 ①과 같이 User 9가 자신의 MAC 주소의 변경 없이 AP3을 통하여 연결을 요청하였을 경우를 생각해 본다. 이 경우에는 무선랜 침입자 탐지 시스템의 추론엔진에서 User9의 연결이 AP3에게 허용되었는지 여부를 AP/User Info 데이터 베이스를 이용하여 추론을 한다. 현재 시스템의 AP/User Info의 정보를 (그림 1)과 같으므로, AP 3에 User9의 연결 허용에 관한 정보가 없다. 즉, User9는 침입자인 비정상 사용자로 여겨져 접속을 허용하지 않는다. 이제 침입자 User9는 다양한 방법으로 AP3을 통한 연결을 시도할 것이다. 즉, AP을 통한 비정상 연결 접속 요청이 급증할 것이다. 이러한 경우에, 추론엔진에서는 비정상 연결 요청이 증가하는 AP를 특별히 관찰하여, 비정상 연결요청이 많을 경우, 직접 AP 3의 영역을 순찰하는 등의 사후 조치를 취할 수 있다.

다음으로, (그림3)의 ②와 같이, User 9가 무선 데이터 분석도구를 이용하여 User 2의 MAC 주소를 알아내어 AP 3에게 접속을 요구하는 경우를 알아본다.

이 경우, 무선랜 침입자 탐지 시스템에서 AP1,2,3의 정보를 수집하여 추론엔진을 통해 분석해 본 결과 User2의 MAC 주소로 AP1과 AP2에서 동시에 접속을 시도하고 있으므로, User2의 접속을 막고, User2에게 연락하여 실제 위치 정보를 알아낸 후, 침입자를 식별하여 접속을 차단하는 등의 사후 조치를 취할 수 있다.

4. 결론 및 향후연구

이제까지, 무선랜 장비인 AP를 이용하여 침입자를 탐지하는 방법에 대해서 알아보았다. 현재 사용되어지고 있는 AP와 간단한 시스템을 이용하여 무선랜 침입자를 탐지하는 기술을 제시하였다. 또한, 추가적인 장비의 도입 없이 AP의 기능을 이용하여 무선랜 침입자를 탐지하는 시스템을 설계하고, 그 동작원리를 알아보았다. 논문에서 제시하는 방법은 무선랜 AP를 이용하여 침입자를 탐지하기 때문에 현재 AP에서 제공하는 기능을 이용하여 침입자를 탐지하고 있으나, 향후 추론엔진의 지능화와 무선랜 AP뿐만 아니라 무선 센서와의 연동을 통한 좀 더 정밀하고, 정확하게 침입자를 탐지하는 기술을 보강할 예정이다.

참고문헌

[1] 김기태, 무선랜 공격유형분석, 네트워크 타임즈, 2003.12
[2] 양대현, 무선 네트워크 보안의 허와실, WSF 2003
[3] J. Hightower, G. Borrillo, " Location systems for ubiquitous computing" IEEE Computer, vol 34, no.8, 2001, pp. 57-66.
[4] 정보통신부, 무선랜 보안운영 권고안, 2003.