무선랜보안(Wireless LAN Security)

한국정보보호진흥원/기반보호사업단
해킹바이러스상담지원센터 김상철 선임연구원
kims@kisa.or.kr, kims@certcc.or.kr

1. 개요

IEEE는 IEEE 802.11b라 불리우는 무선랜에 대한 추가 확장된 표준을 제정하였으며 이 표준안에는 Ethernet에서 처리되는 속도처럼 11Mbps의 무선랜 제품에 대한 표준을 포함하고 있다. 이러한 무선랜 장비의 네트워크 처리속도는 기업이나 조직이 무선랜 장비를 도입하기 위한 무선랜장비의 요구사항 이기도 하다.

많은 무선랜 장비들의 호환성 때문에 WECA(Wireless Ethernet Compatibility Alliance)라 불리우는 공동체를 형성하였으며, 이러한 WECA에 대한 지원을 제품에 표현하기 위해 "Wi-Fi"라고 언급 규격문구를 사용하기도 한다. 수십 개의 벤더들이 Wi-Fi제품들에 대한 시장을 형성해 왔으며, 많은 업체 및 조직들이 무선랜의 도입을 고려하고 있다. LAN으로의 무선 접근에 대한 요구는 Mobile장비, Labtop, PDA, 네트워크에 "plug-in" 없이 연결을 하려하는 사용자들의 계속적인 성장에 의하여 가속화 되었으며, 2003년에는 10억개 이상의 Mobile장비들이 사용될 것이며, 무선랜 시장도 2002년에는 20억불이상으로 성장할 것으로 전문가들은 예상하고 있으며 무선랜 장비의 보안시장도 상당히 성장할 것으로 예상된다.

2002년에는 무선랜 장비의 시장이 주류를 형성할 것이며, 조직들은 유선랜(Wired Lan)과 연동되는 무선랜 장비를 도입하여 통합 운영하고자 할 것이다. 네트워크 관리자들은 무선랜 장비와 유선랜 장비에 의해 제공되는 확장성, 관리의 효율성 및 여러 가지 보안성이 제공되지 않는 다면 이러한 무선랜 장비의 도입에 반대를 하거나 주저할 것이다.

주요한 관심은 보안이며 이러한 보안 사항은 접근제어(Access Control)와 프라이버시(Privacy) 등일 것이다. 접근제어는 민감한 자료들이 허가된 사용자들에 의해서만 접근되어질 수 있도록 하는 것이며, 프라이버시는 송수신되는 자료들이 의도된 대상들에 의해서만 처리되어 지도록 되는 것이다.

무선랜에서 송수신되는 자료는 전파(Radio Wave)를 사용하여 공중으로 브로드캐스트(Broadcast)되기 때문에 자료의 송수신 기기에 의해 제공되는 공간에 있는 모든 무선랜 사용자들에게 자료가 전송된다. 전파는 천장, 바닥, 벽, 공중으로 송신되기 때문에, 전송된 자료는 의도되지 않은 대상들(다른층, 건물밖 등)에게 도달 할 수 있다. 비슷하게 무선랜의 송신을 하나의 대상으로만 지시할 수 없기 때문에 자료의 프라이버시는 매우 중요한 고려대상이다.

IEEE 802.11b 표준은 접근제어, 프라이버시를 보장하는 요소들에 대한 내용을 포함하고 있다. 이러한 무선랜 장비의 보안요소들은 무선랜 장비의 규격에 반드시 포함되어져야 한다. 수백, 수천의 무선랜 사용자들을 고용하고 있는 조직들은 중앙집중 및 효율적인 방법으로 관리되어질 수 있는 구체적인 보안 솔루션을 필요로 한다. 어떤 조직의 관리자는 무선랜 솔루션의 도입의 장애요소는 중앙집중화된 보안솔루션의 부족 때문이라고 한다.

2. 무선랜 보안의 1세대

IEEE 802.11b표준은 무선랜의 접근제어 및 프라이버시에 2가지 방식의 보안 메커니즘을

정의하고 있으며, 하나는 서비스 집합의 SSID(Service Set Identifier)이며, 유선랜과 동등한 형태의 보안 메커니즘인 WEP(Wired Equivalent Privacy)이다. 물론 프라이버시에 대한 보안은 암호화 방법을 이용하는 VPN(Virtual Private Network)을 사용하는 것이며, VPN에 대한 상세한 내용은 다른 참고문헌을 참조하기 바란다.

2.1 SSID

일반적으로 무선랜 주요 특징중의 하나는 SSID라 불리우는 도메인이름(Naming Handle, Domain Handle)을 처리하는 기능이다. 이것은 접근제어의 기본 수준을 제공한다. SSID는 보통 유선랜 장치들에 대한 네트워크이름이며, 네트워크를 세그먼트로 분리하여 사용할때 활용된다. 접근제어를 위해 SSID의 사용은 전형적으로 보안성이 약하기 때문에 위험하다. 유선랜에 무선 클라이언트를 연결해주는 장비인 엑세스포인트(Access Point)는 네트워크 이름으로 SSID를 브로드캐스트 하도록 설정되어 있기 때문에 외부의 무선랜장비에 SSID의 이름만 일치시키면 해당사이트로부터 전동되는 전파를 캡쳐(Capture)하여 도청이 가능한 취약점이 있다.

2.2 WEP (Wired Equivalent Privacy)

IEEE 802.11b 표준은 WEP라 불리우는 부가적인 암호화 기능을 규정하고 있다. WEP는 무선랜의 데이터 스트림을 보호하는 메커니즘을 제공한다. 그리고 대칭 암호화 알고리즘을 사용하기 때문에 자료의 암호화와 복호화를 처리할 때 동일한 키(Key)와 알고리즘을 사용한다. WEP의 주요 목적은 접근제어(Access Control)와 프라이버시(Privacy)기능을 제공하는 것이다. WEP에서의 접근제어는 올바른 WEP 키를 보유하고 있지 않는 사용자들이 네트워크에 대한 접근을 보호할 때 사용되며, 프라이버시는 올바른 WEP 키를 가지고 있는 사용자들에 의해서만 무선랜 구간에서 사용하는 자료들을 암호화하거나 복호화시킬 수 있도록 하는 것이다.

비록 WEP이 선택적인 부가기능이지만, WECA에 의해 Wi-Fi인증된 제품들은 40-bit의 암호화 키를 지원한다. 그래서 WECA 회원사들은 다양하게 WEP를 지원하고 있다. 일부 벤더들은 자료의 암호 및 복호처리 시 수반되는 시스템의 부하(Load)를 줄이기 위해 하드웨어 가속기를 장착된 제품들을 판매하고 있다.

IEEE 802.11 표준은 무선랜에 사용되는 WEP 키를 정의함에 있어서 두가지 방식을 사용한다. 첫번째는 4개의 디폴트 키를 정의하여 모든 장비들(Access Point, Clients)과 공유하는 체계이다. 즉 클라이언트가 디폴트 키를 획득하였을 때는 서브시스템에 있는 모든 다른 시스템들과 안전하게 자료들을 통신할 수 있다. 이러한 디폴트 키의 사용에 대한 문제점은 많은 시스템들이 넓게 분포되어 있을 때 디폴트 키들을 악의적으로 사용하고자 하는 시스템과 타협(Compromise)될 수 있다는 것이다. 두번째 방식은 각각의 클라이언트들이 다른 시스템들과 상호관계의 키 맵핑(Key Mapping)체계를 갖는 것이다. 이러한 방식은 일부 시스템들이 키들을 가지기 때문에 더 안전하게 운영될 수 있다. 그러나 이러한 단방향 키들의 분배는 시스템들의 수가 증가할수록 관리 및 운영이 어려워진다는 단점이 있다.

3. Authentication

하나의 클라이언트가 인증시스템에 의해 인증을 받지 못할 때는 무선랜의 서브시스템과 연결될 수 없다. IEEE 802.11b 표준은 두가지 방식의 인증 메커니즘을 제공한다. 하나는 공개(Open) 인증 방식이며, 다른 하나는 공유키(Shared Key) 인증 방식이다. 인증방법은 각각의 클라이언트에 키값이 설정되어 있어야만 하며, 설정된 값은 클라이언트가 접속하고자 하는 엑세스포인트(Access Point)의 키값과 일치하여야만 한다.

공개인증방식은 전체 인증 흐름이 평문(Clear-text)으로 이루어지며, 클라이언트는 올바른 WEP 키 없이도 엑세스포인트에 접속할 수 있다. 공유키 인증방식에서는 엑세스포인트는

클라이언트가 올바른 WEP 키를 가지고 암호화해서 엑세스포인트로 반환해야만 하는 첼린지(Challenge) 텍스트 패킷을 송신한다. 이때 클라이언트가 잘못된 키나 키를 갖고 있지 않으면 인증에 실패해서 엑세스포인트와 연결할 수 없을 것이다.

일부 무선랜 벤더들은 클라이언트의 MAC주소에 근간한 인증방법을 지원하기도 한다. 즉 엑세스포인트는 인증테이블에 존재하는 클라이언트의 MAC주소 테이블 정보를 유지하고 있으면서, 테이블에 존재하는 MAC주소만을 사용하는 시스템만 엑세스포인트에 접속하도록 하는 방법이다. 이러한 MAC의 인증방법은 카드나, 하드웨어 장비의 분실 및 악의적인 사용에 대응할 수 없다는 단점을 갖고 있다.

4. 무선랜의 보안위험들

4.1 하드웨어 장비의 분실

클라이언트에 WEP키를 할당하는 일반적인 방법은 클라이언트의 저장장치에 저장하거나, 클라이언트 무선랜 장비의 아답터에 기억시키는 방법을 사용한다. 클라이언트의 MAC주소나 WEP키를 사용하여 무선랜에 접근권한을 획득할 수 있다. 만약 다수의 사용자가 클라이언트를 공유한다는 것은 MAC주소나 WEP키를 공유하는 것과 동일한 것이다.

하나의 클라이언트를 분실하였을 때, 허가된 사용자들은 더 이상 MAC주소나 WEP키를 사용하여 접근 권한을 얻지 못할 것이며, 이러한 무선랜 사용을 알고있는 의도되지 않은 사용자들은 무선랜에 접근할 수 있을 것이다. 이러한 이유로 관리자들은 보안위험을 탐지하는 것이 불가능해질 것이다. 그렇기 때문에 클라이언트의 사용자들은 이러한 장비의 분실에 대한 내용을 반드시 관리자에게 알려주어야 하며 관리자는 무선랜 접근에 대한 WEP키와 MAC주소를 더 이상 사용하지 못하도록 하여야 하며, 보안정책을 수정해 주어야 한다. 클라이언트의 수가 많으면 많을 수록 WEP키나 MAC 주소의 관리업무는 많아 질 것이다.

이러한 문제점을 극복하는 방법은 무선랜에 대한 보안정책을 수립하는 것이며 다음 두가지 사항에 주안점을 두어야 할 것이다. 첫번째는 사용자들이 사용하거나 소유하고 있는 사용자명, 암호와 같은 장비 독립적인 무선랜 인증체계를 수립하여 운영하는 것이며, 다른 하나는 사용자 인증에 근거하여 동적으로 생성된 WEP키를 사용하는 것이다.

4.2 Rogue Access Points

IEEE 802.11b의 공유키(Shared-key) 인증체계는 상호인증방식이 아닌 단방향의 인증방식을 사용한다. 즉 엑세스 포인트는 한 사용자를 인증하지만, 사용자는 엑세스포인트를 인증할 수 없다는 것이다. 올바르게 설정되어 운영되지 못하는 엑세스포인트가 무선랜 구간에 위치되어 질 경우에는 합법적인 사용자의 하이재킹(Hijacking)에 의하여 서비스 거부공격의 시발점이 될 수 있는 문제점이 있다. 이러한 문제점을 해결할 수 있는 방법은 클라이언트와 인증서버간의 상호인증방식을 사용하여 양측간의 적절한 시간을 두고 합법성을 증명하는 것이다. 클라이언트와 인증서버간의 통신은 엑세스포인트를 사용하기 때문에, 엑세스포인트는 상호인증 체계방식을 지원해야만 한다. 상호인증체계 방식은 부적절한 엑세스포인트를 고립시키거나 탐지를 가능하게 한다.

4.3 다른 위험들

표준적인 WEP 키는 패킷당 암호방식을 지원하지만 패킷당 인증을 지원하지는 않는다. 그렇기 때문에 해커는 응답과 알려진 데이터 패킷을 사용하여 데이터 스트림을 재구성할 수 있으며, 패킷들을 스푸핑(Spoofing)할 수 있다. 이러한 보안 문제점들을 완하시키는 방법은 WEP 키들을 주기적으로 변화시키는 것이다.

802.11 제어와 데이터 채널들을 모니터링함으로써 해커들은 다음과 같은 정보들을 수집할

수 있다.

- 클아이언트와 엑세스포인트의 MAC주소
- 내부 호스트들의 MAC주소
- 클라이언트와 엑세스포인트간의 연결(Associate) 및 단절(Disassociate) 시간

해커는 장시간의 트래픽 수집 및 분석을 수행하기 위하여 이와 같은 정보들을 사용할 수 있다. 이러한 해커들의 활동을 막기 위해서는 세션당(per-session) WEP 키를 별도로 사용하는 것이다.

5. 무선랜의 보안 위험들을 예방하기 위한 방법

동적인 WEP 키 전개방식을 사용함으로써 무선랜에 있어 취약한 여러 가지 보안 문제점을 해결할 수 있으며, 안전한 사용자 세션 및 네트워크 로그온을 수행할 수 있을 것이다. 앞에서 언급한 무선랜의 보안 체계를 수립하기 위한 방법으로는 다음과 같은 내용으로 요약 할 수 있다.

- 사용자들이 사용하거나 소유하고 있는 사용자명, 암호와 같은 장비 독립적인 무선랜 인증 체계를 수립하여 운영
- 클라이언트와 인증서버(Radius Server)간의 상호 인증체계방식 사용
- 사용자 인증에 근거하여 동적으로 생성된 WEP키를 사용
- WEP 키에 근거한 세션방식 사용
- 사용자에 대한 WEP 세션 키의 시간종료 값을 정의가능

5.1 무선랜의 보안 해결책 (Complete Security Solution)

무선랜의 안전한 보안체계를 구축하기 위해서는 802.11b의 보안 요소들을 이용한 표준체계 및 공개된 구조를 사용하여 강력한 수준의 이용 가능한 보안수준을 제공하는 것이며 중앙집중화된 효율적인 보안 관리체계를 보장하는 것이다. 이러한 보안 메커니즘의 핵심은 인증키에 대한 보안 솔루션을 제공하는 것이며 CISCO, Microsoft 및 다른 조직들이 참여하여 다음과 같은 요소들을 포함하고 있는 표준제안을 하였다.

- EAP(Extensible Authentication Protocol) : 무선랜 클라이언트 아답터와 RADIUS 서버간의 통신를 가능하게 하는 프로토콜
- 통제된 Port 접근에 대한 표준인 IEEE 802.1X

위의 기능을 지원하는 무선랜의 보안 솔루션들을 사용하면, 엑세스포인트에 접속하려하는 무선 클라이언트 사용자가 네트워크 로그인을 수행할 때까지 네트워크에 접근 권한을 얻지 못한다. 이때 사용자는 네트워크에 로그인하기 위해 사용자명과 암호를 입력하여야 하며, 입력된 사용자명과 암호를 사용하여 클라이언트와 RADIUS서버는 상호 인증을 수행한다. RADIUS서버와 클라이언트는 현재의 네트워크 로그인 세션에 대한 WEP 키를 유도하며, 사용자명과 암호와 같은 모든 민감한 정보들은 암호화 처리되는 방식 등으로 인하여 악의적인 네트워크 모니터링 및 다른 공격 등에 대하여 보호되어 질 것이다. 이러한 보안 메커니즘의 이벤트 절차(Event Sequence)는 다음과 같은 순서로 이루어진다.

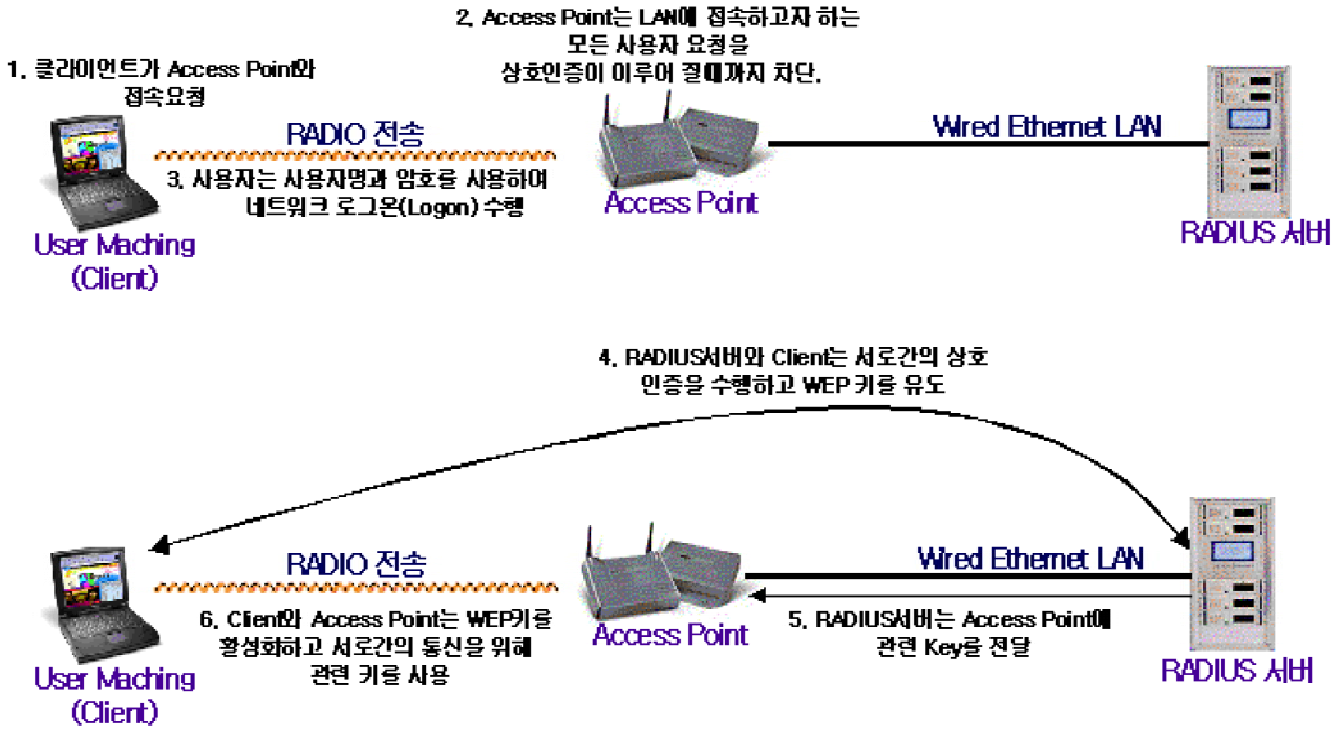
- 무선랜 클라이언트가 엑세스포인트와 네트워크 접속 시도
- 엑세스포인트는 네트워크에 클라이언트가 로그온할 때까지 클라이언트의 네트워크 접근시도를 차단.
- 클라이언트의 사용자는 네트워크에 로그온하기 위해 사용자명과 암호를 입력창을 통하여 입력
- 802.1X, EAP를 사용하여 무선랜 클라이언트와 유선랜에 연결되어 있는 RADIUS서버는 상호인증을 수행

ex)
1) RADIUS서버는 클라이언트에 인증 첼린지(Challenge)를 전송
2) 클라이언트는 첼린지에 대한 응답으로서 사용자명과 암호를 단방향(One-way)의 해쉬(HASH)를 사용
3) 사용자 관리 DB 정보를 사용하여 RADIUS서버는 첼린지의 응답에 대한 자신의 대응 메시지를 생성하여 클라이언트의 응답메시지와 비교
4) RADIUS서버가 클라이언트를 인증하면, 이러한 과정을 역으로 수행하여 클라이언트가 RADIUS서버를 인증하여 클라이언트와 엑세스서버와의 상호인증.

- 클라이언트와 RADIUS서버의 상호인증이 성공적으로 완료되면 네트워크 접근을 위한 적당한 클라이언트의 수준을 정의하고 클라이언트를 구별할 수 있는 WEP키를 결정
- RADIUS서버는 세션 키(Session-Key)라 불리우는 WEP키를 유선랜에 위지한 엑세스 포인트에 전송
- 엑세스포인트는 세션 키를 가지고 브로드캐스트 키를 암호화하여 클라이언트에 암호화된 키를 전송

- 엑세스포인트는 세션 키를 가지고 브로드캐스트 키를 암호화하여 클라이언트에 암호화된 키를 전송하며, 클라이언트는 브로드캐스트된 암호화 키를 복호화하기 위해 세션키를 사용

- 클라이언트와 엑세스포인트는 WEP를 활성화하여, 세션의 유지시간동안 모든 통신에 세션과 브로드캐스트 키를 사용



[그림] 세션에 근거한 사용자명과 암호를 사용한 무선랜의 상호인증과정

EAP와 802.1X의 지원은 중앙집중화된 관리기능, 표준, 개방된 접근방법에 대한 근간을 제공한다. 부가적으로 EAP의 프레임워크는 유선랜으로도 확장가능하며, 모든 접근 방법에 대하여 단일의 보안구조로도 활용 가능하다. 여러 벤더들이 그들의 무선랜 제품에 802.1X, EAP의 지원이 되도록 하고 있다. 일부 업체는 다가오는 표준을 위하여 802.1X에 대응하는 완전한 End-to-end의 보안 솔루션을 지원한다. 즉 클라이언트의 무선 아답터, 엑세스포인트, 접근제어 서버 솔루션을 지원하며, 필요한 802.1X, WEP의 보안 기능을 제공한다.

6. 결론

조직이나 업체가 무선랜을 도입하여, 강화된 보안정책을 수행하기 위해서는 다음과 같은 보안기능을 제공하는 지 점검하여야 한다. 첫번째는 하드웨어의 분실, 부적절한 엑세스포인트의 활용, 해커의 공격에 대한 보안위협을 최소화 할 수 있는 보안기능을 지원하는지 체크하여야 하며, 두번째는 상호인증을 위한 키가 클라이언트 및 엑세스포인트의 저장 메체에 정적으로 저장되는 방식이 아닌 사용자의 네트워크 로그온 시에 동적으로 WEP키가 생성되어 사용자 세션방식으로 관리되는 지 점검하여야 하며. 세번째는 중앙집중제어방식으로부터 무선랜의 사용자들에 대한 전반적인 보안을 관리할 수 있어야 한다. 이러한 보안기능 및 관리기능을 지원하는 무선랜의 솔루션을 도입함으로써 조직은 조직의 요구에 맞는 안전한 무선랜을 구성할 수 있을 것이다.

7. 참고문헌

[1]. CISCO Systems, http://www.cisco.com, 2002

[2]. CISCO Systems, Managing Cisco Network Security Version 2.0, 2001

[3]. Univ. of Maryland, http://www.cs.umd.edu/~waa/wireless.pdf