情報保護學會論文誌
第 22 卷 第 6 號, 2012. 12

무선 랜 환경 인증 메커니즘의 취약성 분석 및 대응방안 연구

최 진 호,[1†] 오 수 현[2‡]
[1](주)한국아이티평가원, [2]호서대학교

Study on Vulnerability and Countermeasures of Authentication Mechanism in Wireless LAN

Jin-Ho Choi,[1†] Soohyun Oh[2‡]
[1]Korea Security Evaluation Laboratory Co., Ltd, [2]Hoseo University

요 약

최근 들어 많은 사용자들은 WEP, WPA와 같은 보호 메커니즘을 이용하여 인증 및 기밀성이 제공되는 무선 랜을 이용하고 있다. 하지만 각 보호 메커니즘의 취약성이 발견되고 이를 이용하여 사용자의 정보가 제 3자에게 노출되거나 변조되어 악용하는 공격 기법들이 제안되었다. 본 논문에서는 무선 랜 보안 메커니즘을 분석하고 알려진 취약성을 이용하여 PSK(Pre-Shared Key) 크래킹 및 쿠키 세션 하이재킹 공격을 수행하고, PSK 크래킹 공격에 대응할 수 있는 개선된 4-way handshake 메커니즘과 쿠키 세션 하이재킹 공격을 방어할 수 있는 쿠키 재전송 탐지 메커니즘을 제안한다. 제안하는 메커니즘은 기존 방식의 취약성에 대응하여 보다 안전한 무선 랜 환경을 구축하는데 활용할 수 있을 것으로 기대한다.

ABSTRACT

Recently, lots of users are using wireless LAN providing authentication and confidentiality with security mechanism such as WEP, WPA. But, weakness of each security mechanism was discovered and attack methods that user's information was exposed or modified to the third parties with it and abused by them were suggested. In this paper, we analyzed architecture of security mechanisms in wireless LAN and performed PSK cracking attack and cookie session hijacking attack with the known vulnerability. And, an improved 4-way handshake mechanism which can counter PSK cracking attack and a cookie replay detection mechanism which can prevent cookie session hijacking attack were proposed. Proposed mechanisms are expected to apply to establish more secure wireless LAN environment by countering existing vulnerability.

Keywords: WEP, WPA, PSK Cracking, Session Hijacking

I. 서 론

IEEE 802.11 무선랜은 가격 및 속도 측면에서 효율적이지만, 무선 네트워크를 통해 전송되는 패킷들은 쉽게 스니핑할 수 있다는 취약성이 존재하기 때문에 통신 과정에서 사용자의 데이터가 노출될 수 있다. 따라서 이러한 취약성으로부터 안전한 네트워크 환경을 제공하기 위해서는 기밀성, 무결성 서비스가 반드시 제공되어야 하며, 이에 앞서 통신에 참여하는 개체의 신뢰성을 확인하기 위한 인증 과정이 필요하다. 그러므로 안전한 무선 네트워크 환경을 구축하기 위해서는 인증 메커니즘에 대한 연구·개발이 필수적으로 요구된다.

접수일(2012년 3월 6일), 수정일(2012년 10월 22일), 게재확정일(2012년 11월 26일)
† 주저자, ilovecch@nate.com
‡ 교신저자, shoh@hoseo.edu

IEEE(Institute of Electrical and Electronics Engineers)에서는 이러한 문제점들을 해결하기 위해서 암호화 통신 및 인증을 제공하는 WEP(Wired Equivalency Protocol) 및 WPA(WiFi Protected Access)와 같은 보안 메커니즘을 발표하였지만, 각 메커니즘에 대한 취약성이 발견됨에 따라 이를 보완할 수 있는 대응방안이 필요하게 되었다. 또한, 최근에 많은 사용자가 사용하고 있는 안드로이드 스마트폰 환경에서 세션 하이재킹 공격을 수행하는 droidsheep 애플리케이션이 공개되었다[3]. droidsheep은 동일한 WiFi에서 인터넷을 이용하는 사용자의 웹 뷰를 도청하여 사용자의 개인정보를 노출시킬 수 있는 위험성이 있음을 보여준다.

본 논문에서는 WEP와 WPA의 암호화 및 인증에 사용되는 공유 비밀정보인 PSK(Pre-Shared Key) 크래킹과 droidsheep을 이용하여 사용자의 웹 뷰를 도청하는 세션 하이재킹 공격을 수행한다. 그리고 PSK 크래킹 공격에 대응할 수 있는 개선된 4-way handshake 메커니즘과 쿠키 세션 하이재킹 공격을 방어할 수 있는 쿠키 재전송 탐지 메커니즘을 제안한다. 개선된 4-way handshake 메커니즘은 Diffie-Hellman 키 분배 방식을 이용하여 공격자가 PSK를 획득하더라도 매개변수 암호화에 사용한 암호화 키를 계산하는 것이 불가능하여, 취약한 패스워드를 사용하더라도 실제로 메시지 암호화에 사용된 키를 알아낼 수 없다는 장점이 있다. 또한 쿠키 재전송 탐지 메커니즘은 공격자가 알 수 없는 패스워드와 카운터 값을 이용하여 쿠키에 새로운 정보를 추가함으로써, 서버는 새로운 정보를 기반으로 쿠키 검증을 수행하여 재전송 여부를 확인할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구로 무선 랜과 무선 랜에서 사용하는 보안 메커니즘에 대해 기술하며, 3장에서는 사용하고 있는 보안 메커니즘의 취약성을 분석하고 이에 대한 공격을 수행한다. 4장에서는 PSK 크래킹 공격에 대해 안전한 4-way handshake 메커니즘과 세션 하이재킹 공격을 방어할 수 있는 대응방안을 제안하고, 마지막으로 5장에서 결론을 맺는다.

II. 관련 연구

2.1 무선 랜

오늘날 무선 네트워크의 발달로 인해 사용자들은 인터넷, E-mail 등과 같은 서비스를 공간의 제약없이 편리하게 사용할 수 있게 되었다. 특히 최근에는 스마트폰, 태블릿 PC 및 노트북 등과 같은 모바일 단말을 이용하여 언제 어디서나 무선 서비스를 제공받을 수 있다. [표 1]은 대표적인 무선 네트워크의 특징을 나타낸다.

[표 1] 무선 네트워크의 종류 및 특징

구분	3G	WiBro	무선랜
커버리지	전국	수도권 및 일부지역	Hot-spot
이동성	이동형	이동형	고정형
설치 및 유지비용	높음	보통	낮음
보안성	높음	높음	낮음
전송 속도	중・저속	고속	초고속

특히 무선 랜은 높은 데이터 전송율과 저렴한 설치 및 유지비용으로 다양한 환경에서 무선 서비스를 제공하고 있다. 현재 제공되고 있는 무선 랜은 구축 주체, 이용 주체 등과 같은 요소에 따라 사용 무선 랜 환경, 공중 무선랜 환경, 사설 무선 랜 환경, 기업 무선 랜 환경으로 구분하여 사용자에게 무선 서비스를 제공하고 있으며, 각 무선 랜 환경의 특징은 [표 2]와 같다.

[표 2] 무선 랜 환경의 종류 및 특징

종류	특 징
상용 무선 랜	이동통신사가 자사 고객 서비스용으로 구축한 무선랜 환경
공중 무선 랜	공공기관, 호텔, 카페 등의 서비스 업종에서 고객에게 편의성을 제공하기 위해 구성한 무선랜 환경
사설 무선 랜	일반 사용자가 무선 공유기를 통해 구축한 무선랜 환경
기업 무선 랜	기업이 내부 업무용으로 구축한 무선랜 환경

국내에서 제공되고 있는 상용 무선 랜은 2010년 4월 기준으로 한국인터넷진흥원에서 발표한 자료에 따르면 12,817개이다[13]. 뿐만 아니라 사설 무선 랜 환경 및 공중 무선 랜 환경 등과 같은 무선 랜 환경을 포함한다면, 많은 사용자들이 일상생활에서 더 많은 무선 랜 서비스를 이용하고 있을 것으로 추측된다.

2.2 무선 랜 보안 메커니즘

사용자에게 무선 네트워크 서비스를 제공하는 무선 랜의 통신 과정은 브로드캐스팅에 기반하므로 AP

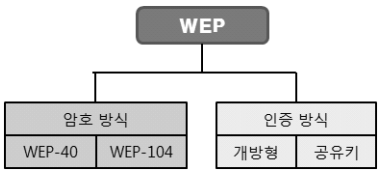
〔표 3〕 무선 랜 보안 기술

보안 기술	세부 기술
무선 랜 접속 인증기술	SSID 설정을 통한 접속제한
	MAC 주소 인증
	공유키 인증
	IEEE 802.1x
무선전송 데이터 암호화 기술	WEP(Wired Equivalency Protocol)
	WPA1/WPA2(WiFi Protected Access)

(Access Point)의 비콘(beacon) 수신 영역 내에 있는 모든 단말들은 다른 사람의 송·수신 데이터 내용을 도청할 수 있다. 따라서 무선 랜 환경에서 의도한 수신자 이외에 다른 사람이 메시지 내용을 알 수 없도록 데이터 암호화 기술과 인증 기술이 요구된다〔14〕〔15〕. IEEE에서는 안전한 무선 랜 환경을 구축하기 위해 무선 랜 접속 인증기술과 무선전송 데이터 암호화 기술을 제공하고 있으며, 제공하는 인증 및 데이터 암호화 기술은 〔표 3〕과 같다〔6〕〔7〕〔8〕〔9〕.

(1) WEP(Wired Equivalency Protocol) 보안 메커니즘

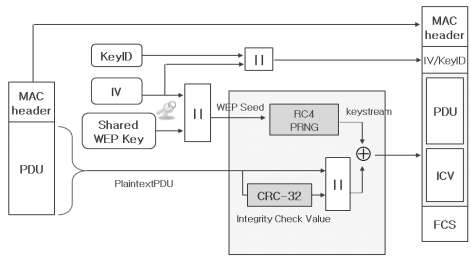
IEEE 802.1b 표준에서부터 무선 전송 데이터 암호화와 인증을 제공하기 위해 WEP를 규정하였으며, WEP에서 사용하는 암호방식 및 인증방식은 〔그림 1〕과 같다. WEP는 RC4 알고리즘을 사용하여 데이터 암호화를 제공하며, 암호화에 사용되는 키에 따라 WEP-40, WEP-104로 구분한다. 또한 개방형 인증 및 공유키 인증을 제공하여 정당한 사용자만이 무선 랜 서비스를 이용할 수 있도록 한다.



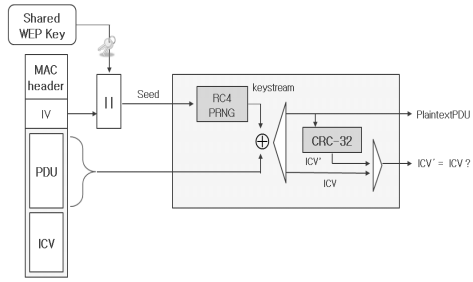
〔그림 1〕 WEP의 암호방식 및 인증방식

(가) WEP 데이터 암호화

WEP는 무선 통신 과정에서 전송되는 데이터에 대한 암호화를 통해 데이터가 노출되어도 암호화에 사용된 키 값을 알고 있는 사용자 외에는 데이터의 내용에 접근하는 것을 방지하여 기밀성을 제공하고 있다. WEP 암호 방식은 무선 구간에서 전송되는 MAC 프레임들을 40비트 또는 104비트의 사전 공유키와 임의로 선택한 24비트의 초기벡터(IV: Initialization Vector)로 조합된 64비트 및 128비트의 키를 사용하여 RC4 스트림 암호화 방식을 제공하고 있다. RC4의 암·복호화는 IV, 사전 공유키를 이용하여 키 스트림을 생성하고, ICV(Integrity Check Value)를 포함하는 데이터와 RC4 연산을 수행하여 암호문을 생성한다. RC4의 구체적인 암·복호화 과정은 〔그림 2〕, 〔그림 3〕과 같다.



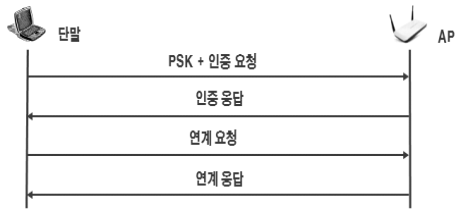
〔그림 2〕 RC4 암호화 과정



〔그림 3〕 RC4 복호화 과정

(나) 공유키 인증

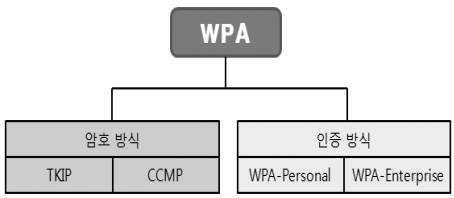
공유키 인증방식은 무선 AP 관리자가 사전에 설정한 사전 공유키를 알고 있는 사용자만이 무선 서비스를 이용할 수 있도록 하는 인증 기법으로, 단말은 AP에게 공유키와 함께 인증요청 메시지를 전송함으로써 단말과 AP가 동일한 공유키를 보유하였음을 확인한다. 사전에 공유한 키(PSK)를 기반으로 단말과 AP는 〔그림 4〕와 같이 인증요청 및 응답메시지를 교환하고, 이 과정을 통해 AP는 단말이 정당한 사용자임을 인증한다. 정당한 사용자임을 인증받은 단말은 서비스 연계를 위한 연계 요청 메시지를 AP에게 전송하고, AP는 응답 메시지를 단말에게 전송하여 무선 서비스를 제공한다.



〔그림 4〕 공유키 인증과정

(2) WPA(WiFi Protected Access) 보안 메커니즘

다양한 공격 기법에 의해 WEP의 취약성이 발견됨에 따라 IEEE는 이를 보완하기 위해 WPA를 발표하였으며, WPA는 인증절차에서 생성된 키로부터 매 패킷마다 상이한 암호 키와 메시지 무결성 키를 사용하여 보다 안전한 네트워크 환경인 RSN(Robust Secure Network)을 제공한다. RSN에서 제공하는 데이터 암호방식과 인증방식은 〔그림 5〕와 같다.



〔그림 5〕 WPA의 암호방식 및 인증방식

WPA의 데이터 암호 방식은 WPA1 버전과 WPA2 버전으로 구분하고, 각 버전의 암호 알고리즘은 TKIP(Temporal Key Integrity Protocol)와 AES-CCMP(Counter mode with Cipher-block chaining with Message authentication code Protocol)를 사용하여 데이터에 대한 암호화를 제공한다〔10〕. 또한 WPA의 인증방식은 인증서버의 유무에 따라 WPA-PSK 방식과 WPA-Enterprise 방식으로 구분할 수 있다. PSK 방식은 AP와 단말이 사전에 공유한 비밀키를 가지고 있다는 것을 4-way handshake 절차에 의해 확인하는 방식이고, Enterprise 방식은 인증서버를 이용한 인증방식으로 802.1x/EAP 인증 방식을 사용한다.

(가) WPA1 / WPA2 데이터 암호화

WPA는 WEP에서 사용되는 고정된 사전 공유키를 동적으로 변경하여 사용하는 TKIP 알고리즘을 사용하고 있으며, WPA2는 블록 암호인 AES를 CCMP모드로 사용한다. 최근에는 WPA1과 WPA2 모두 사용자가 암호화에 사용하는 알고리즘을 TKIP와 CCMP 모드 중에서 선택할 수 있으며, WPA1과 WPA2는 선인증 및 마스터 키 관련 정보의 캐시 기능이 존재하는지에 따라 구분된다.

(나) TKIP

TKIP는 EAP(Extensible Authentication Protocol)에 의한 사용자 인증결과로부터 단말과 AP간에 무선 보안 채널을 형성하기 위해 단말은 임시 공유 비밀키인 TK(Temporal Key)를 동적으로 생성한다. 이 방식에서는 각 프레임마다 다른 키를 적용하여 무선 구간에서 전송되는 패킷들에 대한 암호화를 제공한다.

(다) AES-CCMP

WPA2는 TKIP 알고리즘을 대체하여 CCMP (Counter mode with Cipher-block chaining with Message authentication code) 모드를 사용하는 AES 암호 알고리즘을 이용하여 데이터 암호화 및 무결성을 제공한다. 안전성이 검증된 블록 암호 알고리즘인 AES를 사용하여 충분한 안전성을 제공할 수 있으며, CCMP 모드를 통해 패킷에 대한 기밀성뿐만 아니라 패킷의 헤더 및 데이터에 대한 무결성을 제공할 수 있다. 또한 암호화에 필요한 파라미터들은 패킷이 수신되기 전에 계산할 수 있어, 패킷이 도착했을 때의 부하를 최소화하여 지연시간을 단축시킬 수 있다.

(라) WPA-PSK 인증

WPA-PSK 인증은 인증서버를 설치하지 않는 소규모 망에서 주로 사용되며, AP와 단말이 동일한 PSK(Pre-Shared Key)를 가지고 있음을 4-way handshake 과정을 통해 확인함으로써 인증을 수행한다. 즉, AP와 단말간에 설정된 PSK로부터 생성되는 PMK(Pairwise Master Key)의 확보여부를 4-way handshake 절차를 통해 상호 확인함으로써 인증서버의 역할을 대체할 수 있다. 사용자는 4-way handshake 과정을 수행하기 위해 단말과 AP간의 공유 비밀키로 사용되는 PMK를 구성하여야 한다. 단말과 AP는 WPA-PSK, SSID, SSID 길이 등의 정보를 이용하여 PMK를 생성하여 공유키로 사용하며, 자세한 PMK 생성과정은 다음과 같다.

PMK = $SHA1^{4096}$(WPA-PSK, SSID, SSID 길이)
※ $SHA1^{4096}$() : 4096번의 SHA1 반복 연산

〔그림 6〕은 단말과 AP간에 동일한 PMK를 가지고 있는지를 확인하는 4-way handshake 절차를 나타내며, AP의 MAC 주소, 단말의 MAC 주소, AP의 Nonce 값, 단말의 Nonce 값을 교환하여 단말과 AP간에 상호인증을 수행한다. 사전에 공유한 PMK와 4-way handshake 과정을 통해 획득한 파라미터들인 ANonce, SNonce를 이용하여 단말과 AP는 다음과 같이 PTK를 생성한다.

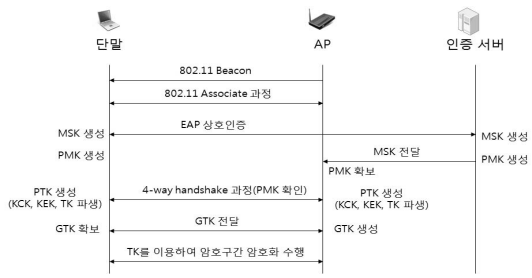
PTK = PRF-512(PMK, AP의 Mac 주소 || 단말의 Mac 주소 || ANonce || SNonce)

의사 난수 함수인 PRF-512를 이용하여 마스터 키 PMK로부터 PTK(Pairwise Temporal Key)를 생성할 수 있으며, PTK는 KCK(EAPol-Key Confirmation Key, 128bit), KEK(EAPol-Key Encryption Key, 128bit) 및 TK(Temporal Key, 128bit)로 파생되어 무결성 검증, 그룹키 전송 및 데이터 암호화에 사용된다. 이 중 KCK는 단말과 AP간에 송수신하는 메시지의 무결성을 확인하는 데 사용된다.

〔그림 6〕 4-way handshake 절차

(마) WPA-Enterprise 인증

WPA-Enterprise는 기관과 기업에서 주로 사용하는 인증 방식으로 RADIUS와 같은 인증서버를 이용하여 상호인증을 제공한다. 인증서버는 단말과 EAP-TLS, EAP_AKA 및 EAP-TTLS 등과 같은 인증 프로토콜을 수행하고, 그 결과를 기반으로 AP는 해당 단말의 접근 허용여부를 결정한다. 성공적인 인증 시 인증서버는 AP가 사용할 임시 암호키를 전달하며, 인증이 실패할 경우에는 단말은 AP에 접근할 수 없다. 〔그림 7〕은 WPA-Enterprise의 인증 절차를 나타낸다.



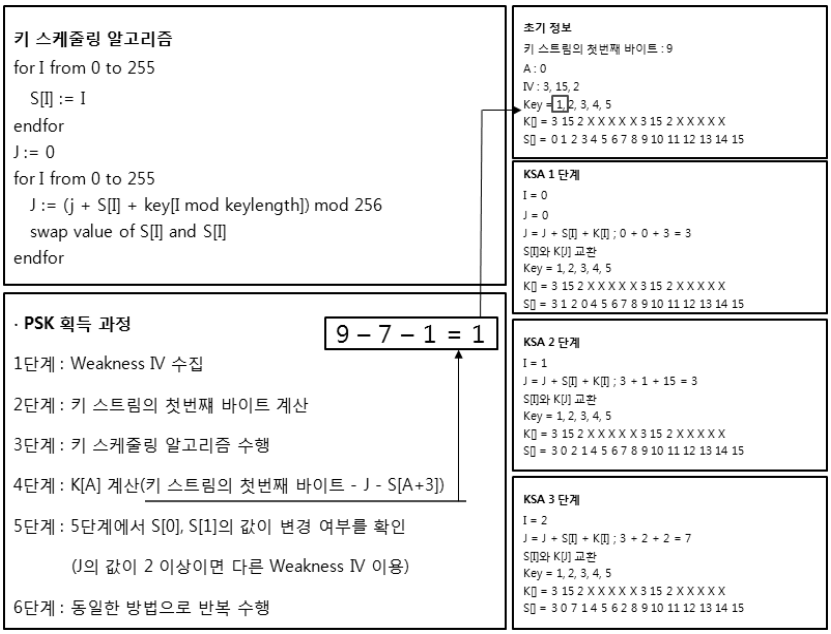
〔그림 7〕 WPA-Enterprise 인증 절차

III. 무선 랜 보안 메커니즘의 취약성 분석

3.1 WEP 취약성 분석

사용자 인증 및 데이터 암호화를 제공하는 WEP에는 여러 취약성이 존재하며, 공격자는 이러한 취약성을 통해 AP와 단말간에 패스워드로 사용되는 사전 공유키를 획득할 수 있다. 대표적인 공격 기법으로 전수공격, 키 스트림 재사용, IV(Initial Vector) 충돌, FMS(Fluhrer, Mantin, Shamir) 공격 등이 존재한다[5]. WEP 암호화에 사용되는 RC4 알고리즘의 중요 요소인 키 스트림은 IV와 KeyID로 구성되지만, 세션이 연결 후에는 KeyID는 변경되지 않으며, 24비트의 IV는 짧은 길이로 구성되어 있다. 따라서 생일 공격(birthday paradox)에 의해서 약 5000개의 IV를 수집으로 50% 확률로 동일한 IV를 획득할 수 있으므로 키 스트림이 재사용되거나 충돌이 발생하는 잠재적인 취약점이 존재한다.

또한 FMS 기법은 RC4 암호화의 키 스케줄링 알고리즘(KSA: Key Scheduling Algorithm)과 Weakness IV를 이용한 공격 기법으로 Weakness IV는 IV 값 중에서 사전 공유키의 정보를 노출시키는 IV를 의미한다. 공격자는 암호화된 패킷의 첫 바이트와 SNAP(Subnetwork Access Protocol) 헤더의 첫 바이트에 고정적으로 사용되는 0xAA를 XOR 연산하여 키 스트림의 첫 바이트를 획득한다. 그리고 키 스케줄링 알고리즘 연산 과정에서 Weakness IV 여



〔그림 8〕 FMS 공격 순서 및 공격 예

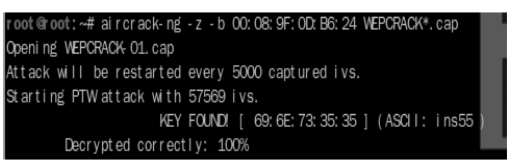
부를 확인하고, 도출되는 인덱스 정보를 이용하여 K[A]를 계산할 수 있다. K[A]를 획득한 공격자는 반복적으로 수행하여 K[]을 완성하여 PSK를 획득할 수 있다. 〔그림 8〕은 키 스케줄링 알고리즘과 K[]를 획득하기 위한 공격 순서 및 공격 예이다〔11〕.

K[]를 획득하기 위한 공격 예는 간단한 계산과정을 위해 mod 256 대신에 mod 16을 사용하였으며, K[]를 알지 못하는 공격자가 Weakness IV를 이용하여 PSK를 도출하는 과정의 일부분을 나타낸다. 본 논문에서는 backtrack 환경에서 FMS 공격을 제공하는 Aircrack-ng을 이용하여 WEP의 사전 공유키를 획득하는 공격을 수행한다〔1〕〔2〕. Aircrack-ng는 윈도우 버전, 리눅스 버전 및 Mac OS 버전에서 사용할 수 있다. 이러한 Aircrack-ng는 컴퓨터에 장착되어 있는 무선 랜카드 칩셋에 기반하며, "http://www.aircrack-ng.org/doku.php?id=compatibility_drivers"에서 명시한 칩셋만이 WEP 공격을 수행할 수 있다. WEP 크래킹 공격은 무선 랜카드 모드 변경, 패킷 수집, PSK 추출 등과 같은 공격으로 수행되며, 공격에 사용되는 대표적인 명령어는 〔표 4〕와 같다〔4〕.

먼저 무선 AP로 전달되는 패킷을 수집하기 위해 공격자는 airmon-ng 명령어를 이용하여 관리자 모드로 설정된 무선 랜카드를 모니터 모드로 변경하여야 한다. 모니터 모드로 변경된 무선 랜카드를 이용하여 공격자는 공격 대상 AP에 대한 정보를 수집하고, airodump-ng 명령어를 이용하여 AP와의 통신을 통해 IV 수집 및 저장한다. 해당 AP가 통신량이 많지 않은 네트워크일 경우에는 공격자가 IV를 수집하기 위해 많은 시간이 소요될 수 있으므로, 공격자는 aireplay-ng를 사용하여 거짓 인증을 통해 패킷을 수집할 수 있다. 성공적인 크래킹을 위해서는 WEP-64와 WEP-128에서 각각 50,000개와 200,000개 이상의 패킷이 요구된다. 이러한 공격 방법을 이용하여 충분한 양의 패킷을 수집하면, FMS 공격을 수행하는 aircrack-ng 명령어를 이용하여

〔표 4〕 대표적인 aircrack-ng 명령어

명령어	내용
airmon-ng	무선 랜카드 모드 변경 명령어
airodump-ng	패킷 수집을 위한 명령어
aireplay-ng	트래픽 발생 명령어
aircrack-ng	WPA-PSK 추출 명령어

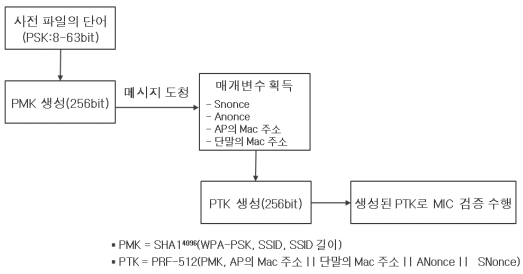


〔그림 9〕 WEP-PSK 추출

WEP-PSK를 추출할 수 있다. 〔그림 9〕는 수집된 패킷을 기반으로 해당 네트워크의 WEP-PSK를 추출한 결과이다.

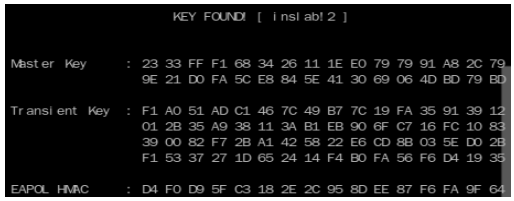
3.2 WPA 취약성 분석

WPA1와 WPA2의 사전 공유키 방식은 인증서버를 운영하지 않고 4-way handshake 절차를 통해 단말과 AP간에 상호인증을 제공하므로, 사전 공격 및 4-way handshake 절차에서 발생하는 취약성을 이용하여 공격자는 AP와 동일한 PTK를 생성할 수 있다. 따라서 사용자가 안전하지 않은 패스워드를 사용하는 경우, 악의적인 공격자는 스니핑을 통해 평문으로 전송되는 4-way handshake 절차에서 교환되는 4개의 파라미터 획득하고, 사전 공격으로 공격자가 알 수 없는 정보인 PSK를 추측하여 정상적인 PMK를 추측할 수 있다. 따라서 추측한 PMK와 이전에 획득한 4개의 파라미터를 사용하여 AP와 단말이 사용한 PTK를 계산할 수 있게 된다. 〔그림 10〕는 공격자가 사전 공격을 이용하여 PMK를 생성하고 메시지 도청으로 획득한 4개의 매개변수를 이용하여 WPA 크래킹을 수행하는 공격과정을 나타낸다.



〔그림 10〕 WPA 크래킹 과정

본 논문에서는 WPA 크래킹을 수행하기 위해 backtrack 환경에서 WPA-PSK를 추측한 사전 파일과 aircrack-ng를 이용한다. 먼저 WPA 크래킹은 WEP 크래킹과 동일한 방법으로 무선 랜카드 모드 변경, 패킷 수집을 수행한다. 공격자는 패킷 수집과정에서 재 인증을 유발하여 평문으로 전송되는 단말과 AP간의 4개의 매개변수를 WireShark와 같은 패킷 모니터링 툴을 통해 획득할 수 있다. 공격자는 획득한 매개변수와 사전 공격을 이용하여 PSK 추측하고, 이를 이용하여 PTK를 생성한 후, PTK로부터 파생된 KCK를 이용하여 MIC 검증을 수행한다. 공격자는



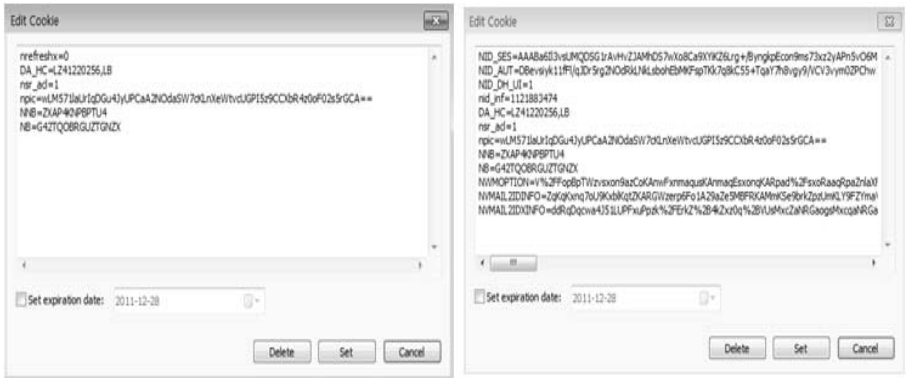
〔그림 11〕 WPA-PSK 크래킹 결과

MIC 검증을 수행하여 정당한 메시지를 획득할 수 있다면, AP와 단말이 사용된 정당한 PSK를 추측한 것이라 할 수 있다. 〔그림 11〕은 사전 공격과 도청된 4개의 매개변수를 이용하여 추출한 WPA-PSK를 나타낸다.

3.2 세션 하이재킹 취약성 분석

droidsheep 애플리케이션은 루팅 된 안드로이드 폰을 이용하여 정상 경로를 통해 무선 랜을 접속하여 무선 서비스를 제공받는 방법으로, WEP 및 WPA를 우회하여 동일한 네트워크에서 다른 사용자의 웹 브라우저를 도청하거나 권한을 획득할 수 있다. droidsheep은 ARP 스푸핑 및 세션 하이재킹을 통해 사용자의 mobile URL, URL 및 쿠키 등과 같은 정보를 획득하고, 웹 페이지에 대한 정보와 세션 유지를 위한 쿠키를 재전송하여 공격을 수행한다. 이러한 공격은 SSL과 같은 보안 채널을 통해서 방지할 수 있지만, 많은 서버들은 SSL을 제공하지 않거나 로그인 과정에서만 보안 채널을 형성하고 있다. 따라서 로그인 과정이 종료되어 평문으로 패킷이 전송되므로 사용자의 웹 페이지가 도청되어 개인정보가 노출될 수 있다.

먼저 공격자는 ARP 스푸핑 공격을 수행하여 ARP 메시지를 해당 네트워크의 사용자에게 브로드캐스트함으로써 정당한 사용자들이 공격자를 게이트웨이로 인식하도록 한다. 게이트웨이로 인식된 공격자는 libcap 라이브러리를 통해 세션을 도청하여 세션 ID 및 쿠키를 획득하고, 획득한 사용자의 세션 ID와 쿠키값을 이용하여 사용자의 계정 및 웹 뷰를 획득할 수 있다. 공격에 이용되는 쿠키는 세션 쿠키와 로그인 쿠키로 구분할 수 있으며, 세션 쿠키는 웹 페이지에 연결되었을 때 생성되는 쿠키 값으로 웹 페이지에 대한 정보들이 포함되고, 로그인 쿠키는 로그인 과정을 통해서 사용자 인증을 수행한 후 생성된 쿠키 값으로, 인증과 관련된 정보가 포함되어 있다. 〔그림 12〕는 쿠



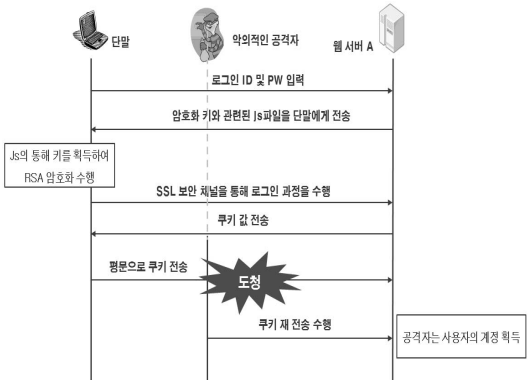
〔그림 12〕 세션 쿠키와 로그인 쿠키 값

키 값의 확인 및 수정이 가능한 Cooxie 프로그램을 이용하여 포털 사이트인 네이버에서 생성되는 세션 쿠키와 로그인 쿠키를 나타낸다.

로그인 쿠키에는 추가적으로 여러 정보들이 포함되었으며, 그중에서 인증과 관련된 NID_AUT 정보가 포함되어 있다. 본 논문에서는 웹 페이지에 대한 쿠키 확인 및 변조가 가능한 프로그램인 Cooxie를 이용한 세션 하이재킹 공격을 수행하였다. 먼저, 정상적인 사용자와 악의적인 공격자가 로그인 과정을 통해 로그인 쿠키를 생성하고, 악의적인 공격자가 평문으로 전송되는 정상적인 사용자의 쿠키를 도청하였다고 가정한다. 악의적인 공격자는 자신의 NID_AUT 값을 도청한 사용자의 NID_AUT 값으로 변조함으로써, 악의적인 사용자는 정상적인 사용자의 계정을 획득할 수 있고 정상적인 사용자의 메일 및 가입된 커뮤니티에 글을 쓰거나 읽을 수 있게 된다. 〔그림 12〕는 Cooxie를 이용하여 악의적인 공격자 "심심풀이"는 사용자 "커브"의 NID_AUT 값으로 변조함으로써 정상적인 사용자 "커브"의 계정을 획득한 결과를 나타낸다. 공격자는 인가된 사용자와 동일한 권한이 주어지며, 메일 송수신 및 개인 블로그 사용 등과 같은 행위를 하여 사용자의 개인정보를 침해할 수 있다. 하지만 사용자는 공격자가 자신의 계정 사용 여부를 사이트 접속 로그 확인과 같은 수동적인 검사를 통해서만 확인할 수 있으므로 즉각적으로 대응하기 어렵기 때문에 많은 문제점이 야기될 수 있다.

droidsheep은 Cooxie를 이용한 세션 하이재킹과 유사한 방식으로, http 통신 시 NULL로 생성된 자신의 쿠키 값을 사용자의 쿠키 값과 교환하여 사용자의 권한 및 웹 뷰를 획득할 수 있다. 〔그림 14〕는 공격자가 평문으로 전송되는 쿠키를 스니핑하여 쿠키 재전송 공격을 통해 사용자의 권한을 획득하는 공격을 나타내며, 구체적인 공격 과정은 다음과 같다.

〔그림 13〕 세션 하이재킹 공격 전후 비교



〔그림 14〕 공격자의 쿠키 재전송 공격

① 단말은 웹 서버에 자신의 ID 및 패스워드 전송
② 서버는 암호화와 관련된 키가 포함된 js파일을 단말에게 전송
③ 단말은 자바 스트립트로 구현된 RSA 코드를 C/C++로 마이그레이션하고 js로부터 키 획득
④ 단말과 서버간에 SSL 보안 채널이 형성되어 안전하게 ID 및 패스워드 전송
⑤ 로그인 과정이 종료되면, 사용자는 평문으로 서버에게 쿠키 값 전송
⑥ 공격자가 평문으로 전송되는 쿠키 값 도청
⑦ 공격자는 사용자의 쿠키 값을 웹 서버에게 재전송하여 다른 사용자의 계정 획득

IV. 무선 랜 환경의 취약성 대응 방안

4.1 WEP 취약성 대응 방안

공격자는 WEP 암호화에 이용되는 IV의 취약성을 이용하여 인증 및 암호화에 사용된 PSK를 획득하여 공격에 악용할 수 있다. IV는 매번 변경되는 임의의 수이지만, IV의 비트길이가 짧아서 IV의 충돌이 발생하거나 재사용될 수 있으므로 WEP에 사용되는 PSK를 추측할 수 있게 된다. 따라서 짧은 길이의 IV를 확장하고, 정적으로 사용되는 공유키를 동적으로 사용함으로써 보다 안전한 메커니즘을 제공할 수 있다. WPA는 WEP의 취약성을 보완한 메커니즘으로 확장된 IV 및 동적 공유 비밀키를 사용하여 IV 충돌 및 IV 재사용 공격을 방어할 수 있다.

4.2 WPA 취약성 대응 방안

본 절에서는 4-way handshake 절차를 통해 WPA-PSK에서 발생하는 파라미터를 악의적인 공격자에게 노출되지 않도록 기밀성을 제공하는 메커니즘을 제안한다. 제안하는 메커니즘에서 사용하는 기호 및 의미는 〔표 5〕와 같다.

〔표 5〕 기호

기 호	내 용
PSK	단말과 AP 사이에 사전에 공유한 비밀 키
PMK	PSK와 SSID 정보를 이용하여 생성한 마스터 키
PTK	KEK, KCK, TK를 생성하기 위해 PMK로부터 유도된 공유 비밀키
KCK	MIC를 계산하는데 사용하는 키
TK	데이터 암호화에 사용하는 키
SK	단말과 AP가 SNoce를 암·복호화하기 위해 사용하는 일회용 세션키
PRF	의사 난수 함수
ANonce	AP가 생성한 Nonce 값
SNonce	단말이 생성한 Nonce값
MIC	KEK로 암호화된 결과로 무결성 검증을 위한 파라미터
Sn	재전송 공격을 방어하기 위한 순서번호
SSID	AP 식별번호
p	1024비트 이상의 소수
g	Zp상의 원시원소
H()	일방향 해쉬 함수

제안하는 개선된 4-way handshake 절차에서는 Diffie-Hellman 문제의 안전성에 기반하여, 공격자가 PSK를 추측하더라도 전송되는 파라미터인 $X = H(PSK) \cdot g^{r_A} \bmod p (r_A \in_R Z_p^*)$, $Y = H(PSK) \cdot g^{r_B} \bmod p$ $(r_B \in_R Z_P^*)$로부터 세션키 생성에 사용되는 r_A, r_B를 획득할 수 없으므로 전송되는 메시지의 암호화에 사용한 세션키 $SK = g^{r_A r_B} \bmod p$를 계산할 수 없다[12]. 〔그림 15〕는 제안하는 개선된 4-way handshake 절차를 나타내며, 구체적인 동작과정은 다음과 같다.

① 단말은 AP에게 인증 메시지를 전송하여 인증을 요청한다.
② AP는 단말에게 다음과 같이 생성한 MSG1을 전송한다. 이때 X는 다음과 같이 생성한다.

MSG1 = (AP의 MAC 주소, ANonce, Sn, X)

$$X = H(PSK) \cdot g^{r_A} \bmod p (r_A \in_R Z_p^*) \quad (1)$$

③ 단말은 사전에 공유한 PMK와 MSG1으로부터 획득한 매개변수 및 랜덤하게 생성한 SNonce를 이용하여 PTK를 생성하고, SNonce 암호화에 사용할 세션키 SK를 다음과 같이 생성한다.

$$Y = H(PSK) \cdot g^{r_B} \bmod p \ (r_B \in_R Z_P^*) \quad (2)$$

$$SK = \left(\frac{X}{H(PSK)} \right)^{r_B} \bmod p \quad (3)$$

단말은 SK를 이용하여 SNonce를 암호화하고 PTK로부터 파생된 KCK를 이용하여 MIC를 생성하여 AP에게 전송한다.

MSG2 = (단말의 MAC 주소, E_{SK}(SNonce), Y, MIC)

④ AP는 MSG2로부터 획득한 Y와 사전에 공유한 PSK 그리고 자신이 선택한 랜덤수 r_A를 이용하여 다음과 같이 SK를 생성하고, 암호화된 SNonce를 복호한다.

$$SK = \left(\frac{Y}{H(PSK)} \right)^{r_A} \bmod p \quad (4)$$

AP는 PTK로부터 생성된 KCK로 메시지에 대한 메시지 검증을 수행하여 단말이 AP와 동일한 PMK를 소유하고 있는 확인한다.

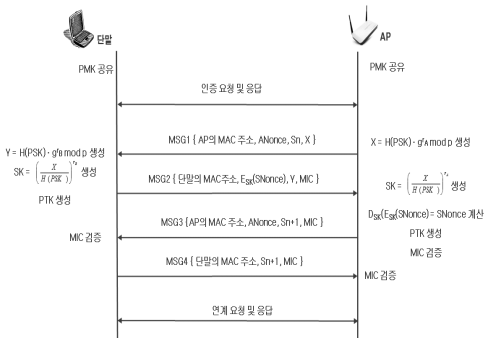
⑤ AP는 다음과 같은 값을 포함하는 MSG3을 단말에게 전송한다.

MSG3 = (AP의 MAC 주소, ANonce, Sn+1, MIC)

⑥ 단말은 MSG3의 MIC를 검증하여 AP가 단말과 동일한 PMK를 소유하고 있음을 확인한다.

⑦ 단말은 다음과 같은 확인 메시지 MSG4를 AP에게 전송한다.

MSG4 = (단말의 MAC 주소, Sn+1, MIC)

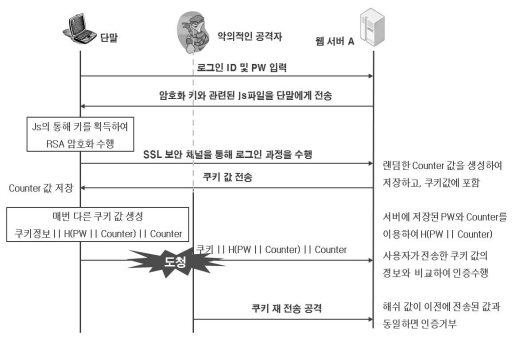


〔그림 15〕 제안하는 4-way handshake 동작 과정

제안하는 개선된 4-way handshake 절차에서는 공격자가 사전공격으로 PSK를 추측하더라도, SNonce를 암호화하는데 사용한 세션키 SK를 얻기 위해서는 전송되는 X, Y로부터 r_A, r_B를 획득해야 한다. 하지만 1024비트 이상의 큰 소수를 사용하는 경우 Diffie-Hellman 문제가 안전하므로, r_A나 r_B를 획득하는 것은 계산상 불가능하다. 따라서 공격자가 사전공격을 통해 PSK를 추측하는데 성공하더라도, SNonce를 복호할 수 없으므로 PTK 생성에 필요한 매개변수를 모두 획득할 수 없게 된다. 그러므로 제안하는 개선된 4-way handshake 방식에서는 취약한 패스워드를 사용하더라도, 공격자가 도청을 통해 실제 메시지 암호화에 사용된 키를 획득하는 것은 불가능하다.

4.3 세션 하이재킹 취약성 대응 방안

본 절에서는 SSL이 적용되지 않은 웹 서버와 로그인 부분에서만 제공되는 SSL에서 쿠키 재전송 공격에 대한 대응방안을 제안한다. 제안하는 대응방안에서



〔그림 16〕 제안하는 쿠키 재전송 보호 메커니즘

는 기존의 정보들과 함께 쿠키 값이 재전송 되는 것을 방지하기 위해 단말이 사용자의 패스워드와 Counter 값을 해쉬한 값을 쿠키에 포함시켜 서버에게 전송하고, 서버는 이러한 정보가 추가된 쿠키를 검증함으로써 쿠키의 재전송 여부를 검사한다. [그림 16]은 제안하는 쿠키 재전송 보호 메커니즘의 동작 과정을 나타내며, 자세한 동작 과정은 다음과 같다.

① 서버와 단말은 보안 채널 형성
② 단말은 보안채널을 이용하여 서버에게 ID와 PW 전송
③ 서버는 ID와 PW가 일치하는 경우 로그인 과정을 종료하고, 랜덤한 Counter 값을 생성하여 저장한 후 쿠키에 포함시켜 단말에게 전송
④ 단말은 수신한 Counter 값을 쿠키 값과 함께 저장
⑤ http 통신 시 단말은 H(PW||Counter)||Counter를 생성하여 쿠키 값에 추가하여 서버에게 전송하고, Counter 값 1 증가
⑥ 서버는 자신이 저장하고 있는 Counter 값과 쿠키에 포함된 Counter 값을 비교하여, 저장된 값보다 작은 값이 쿠키에 포함된 경우에 세션 종료
⑦ Counter 값이 일치하는 경우, 서버는 자신이 저장하고 있는 PW와 Counter 값을 이용하여 H(PW||Counter)를 계산하고, 쿠키에 포함된 값과 일치하는지 확인
⑧ 해쉬 값이 일치하는 경우 세션을 유지하고, Counter 값 1 증가

제안하는 메커니즘에서는 쿠키를 전송할 때 마다 Counter 값을 증가시켜 H(PW||Counter)값을 생성하므로, 이전에 전송된 쿠키 값을 재전송하는 경우에 서버는 공격을 탐지하고 세션을 종료시킬 수 있다. 그리고 만일 쿠키에 포함된 Counter 값이 서버가 저장한 Counter 값보다 큰 경우에는, 재전송 공격은 아니지만 동기화에 문제가 생긴 것으로 판단하여 서버는 쿠키에 포함된 값으로 Counter 값을 변경하여 해쉬 값을 인증하고 세션을 유지시킬 수 있게 된다. 공격자는 보안 채널을 통해 전송된 패스워드를 스니핑할 수 없으므로 Counter에 대응하는 정당한 해쉬 값을 생성할 수 없다. 그리고 Counter 값은 로그인할 때 마다 랜덤하게 생성되어 해당 세션에서는 계속 변경되는 값으로, 공격자가 이전에 전송된 쿠키를 획득하여 재전송하는 경우에 서버는 이를 탐지할 수 있게 된다.

V. 결론

최근 들어 네트워크 기술과 스마트폰, 태블릿 PC 등 무선 디바이스 기술의 발전으로 무선 네트워크의 사용자가 증가하고 있으며, 많은 사용자들이 저렴하고 빠른 속도를 제공하는 무선 랜을 이용하고 있다. IEEE에서는 무선 랜 환경에서 보안 서비스를 제공하기 위해 WEP, WPA와 같은 보안 메커니즘들을 제안하였지만, 보안 메커니즘의 취약성이 발견됨에 따라 이를 이용한 다양한 공격 기법들이 제안되었다. 또한 안드로이드 환경에서는 droidsheep 애플리케이션을 이용하여 다른 사용자의 계정권한 획득 및 사용자의 웹 뷰를 도청할 수 있는 공격 기법이 제안되었다. 본 논문에서는 WEP 및 WPA 메커니즘의 취약성을 이용하여 단말과 서버사이의 비밀 공유키 PSK를 획득하는 공격과 세션 하이재킹 공격을 통해 안드로이드 환경에서 타인의 계정을 획득하는 공격을 수행하였다. 그리고 이러한 취약성에 대한 대응방안으로 개선된 4-way handshake 메커니즘과 쿠키 재전송 탐지 메커니즘을 제안하였다.

개선된 4-way handshake 메커니즘은 사전공격에 대한 안전성을 제공하기 위해 Diffie-Hellman 키 분배를 이용하여 세션키를 생성하고, 생성된 세션키로 PTK 생성에 필요한 매개변수 중 SNonce를 암호화한다 따라서 Diffie-Hellman 키 분배 방식의 안전성에 의해, 공격자가 PSK를 획득하더라도 암호화에 사용된 세션키를 알아내는 것은 계산상 불가능하기 때문에, 사용자가 취약한 패스워드를 사용하더라도 메시지 암호화에 사용된 세션키를 알아낼 수 없다는 장점이 존재한다. 그리고 쿠키 재사용으로 인한 세션 하이재킹 공격에 대응하기 위해, 패스워드와 카운터 값을 사용하여 생성된 정보를 쿠키 값에 포함하여 매번 다른 쿠키 값을 전송함으로써 쿠키 재전송을 탐지하는 메커니즘을 제안하였다. 서버는 전송된 쿠키와 이전에 전송된 쿠키를 비교하여 인증 허용 및 거부를 수행하여 세션 하이재킹 공격을 예방할 수 있다. 제안한 메커니즘들은 기존 방식의 취약성에 대응하여 보다 안전한 무선 랜 환경을 구축하는데 활용할 수 있으며, 이를 통해 인증, 기밀성, 무결성 및 사용자의 프라이버시 보호가 강화된 무선 랜 서비스를 제공할 것으로 기대한다.

참고문헌

〔1〕 http://www.aircrack-ng.org/
〔2〕 http://www.backtrack-linux.org/
〔3〕 http://droidsheep.de/
〔4〕 Vivek Ramachandran, "BackTrack 5 Wireless Penetration Testing," Packt Publishing Ltd, Sep. 2011.
〔5〕 J. R. Walker. "Unsafe at any key size; an analysis of the WEP encapsulation", IEEE Document 802.11-00/362, Oct. 2000.
〔6〕 IEEE, "Standard for Local and metropolitan area networks- Port-Based Network Access Control," IEEE Std 802.1X, June 2001.
〔7〕 IEEE, "IEEE 802.11n: Wireless LAN medium access control(MAC) and physical layer (PHY) specification : enhancements for higher throughput," IEEE Std 802.11n, Sep. 2006.
〔8〕 LAN Medium Access Control(MAC) and Physical Layer(PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements, "IEEE Std 802.11i, July 2004.
〔9〕 IEEE, "IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 2007
〔10〕 Brad Heins, "해킹 초보를 위한 무선 네트워크 공격과 방어," 에이콘출판사, pp.21-52, 2011, 7월
〔11〕 Jon Erickson, "해킹: 공격의 예술," 에이콘출판사, pp.470-483 , 2004년 5월
〔12〕 국제전기통신연합, "Password-authenticated key exchange(PAK) protocol", ITU-T Recommendation X.1035, Feb. 2007.
〔13〕 한국인터넷진흥원, "2011년 무선인터넷이용실태조사," pp.4-28, 2011년 12월
〔14〕 윤종호, "무선 LAN 보안 프로토콜," 교학사, pp.-155-183, 2005년 8월
〔15〕 윤종호, "윈도우 서버와 프로토콜 분석기를 활용한 네트워크 보안 프로그램," 교학사, pp. 31-57, 2004년 10월

〈著者紹介〉

최 진 호 (Jin-Ho Choi) 정회원
2010년 2월: 호서대학교 정보보호학과 졸업
2012년 2월: 호서대학교 대학원 정보보호학과 석사(공학석사)
2012년 3월~현재: (주)한국아이티평가원 연구원
〈관심분야〉 네트워크 보안, 정보보호제품 평가 및 인증, 포렌식

오 수 현 (SooHyun Oh) 종신회원
1998년 2월: 성균관대학교 정보공학과 졸업
2000년 2월: 성균관대학교 전기전자 및 컴퓨터공학과 석사(공학석사)
2003년 8월: 성균관대학교 전기전자 및 컴퓨터공학과 박사(공학박사)
2004년 3월~현재: 호서대학교 정보보호학과 교수
〈관심분야〉 암호 프로토콜, 네트워크 보안, 정보보호제품 평가 및 인증 등