한국산학기술학회논문지
Vol. 8, No. 5, pp. 1146-1151, 2007

무선 LAN 환경에서 AP운용의 보안 취약성 조사
(천안시 산업단지 지역을 중심으로)

홍진근[1*]

The Investigation of Security Vulnerability of AP operation in the WLAN
(in center around industrial area in Cheonan city)

Jin-Keun Hong[1*]

요 약 본 논문에서는 IEEE 802.11 무선 랜 보안 서비스의 특성과 취약성 도구를 살펴보았으며, 천안 공업단지를 중심으로 사용되고 있는 무선 랜 AP 운용현황을 조사하고 보안 취약성 상태를 분석하였다. 본 연구에 따르면 천안 산업단지에서 회사나 공장별로 사용되고 있는 무선 랜 AP 가운데 50%는 WEP 보안설정이 이루어지지 않은 취약한 상태에서 운용되고 있는 실정으로 보안상 취약하다. 따라서 연구 결과로부터 중소기업의 경우 정보시스템 관리자에 대한 보안교육이 필요함을 알 수 있다.

Abstract- In this paper, it is investigated to the security services and vulnerability tools of IEEE802.11 wireless LAN, and it is considered the employment state of wireless LAN AP (access point) and analyzed the state of security vulnerability. In according to this study, among wireless LAN APs, which are operated in each company or each factory, in center around industrial of Cheonan city, 50% of AP, which is used, is not operated on WEP, and therefore, it is stated the weakness of security so far. From the result of this study, in case of mid and small compay, it can be distingushed the necessity of the security training for the informaton system manager.

Key Words : War driving, Ssecurity, WLAN, Security manager

1. 서론

IEEE802.11 무선 랜 서비스는 인증, 접근통제, 권한부여, 기밀성, 무결성, 부인방지 등의 보안 기능을 제공한다. 무선랜 서비스는 IEEE 802.11규격에서 2.4GHz RF를 시작으로 802.11a가 54Mbps 전송속도에 OFDM 모드에 5GHz대역을 제공한다면, 802.11b는 11Mbps 전송속도에 CCK (complementary code keying) 모드에 2.4GHz 대역을 가진다. 802.11g는 802.11b와 유사하나 OFDM 모드에 20Mbps 속도가 향상되었다. IEEE 802.11i에서는 보안기능을 대폭 향상시켰다. 워 드라이빙은 2001년 피터에 의해 고안되었으며 실리콘 밸리를 드라이빙하며 수백 개의 액세스 포인트를 탐지한 바 있다. 801.11 규격의 무선 신호는 단 거리에 유효하며 워 드라이버로부터 안전하지 않는가 하는 물음이 제시되고 있다. 그러나 내부 감사를 수행할 경우 노트북을 가지고 여러 곳을 돌아다닐 수 있으며, 무선 장비, 특정 액세스 포인트를 풋 프린팅하는 것은 액세스 포인트 브로드캐스트 비콘에 대한 청취를 통한 수동적인 방법으로 가능하다.

전송 클라이언트 표지인 비콘신호를 AP에서 검색하는 공격적인 방법을 수행할 수 있으며, 무선 랜의 풋프린팅은 AP의 비콘신호나 패킷이 수신되는 범위에서 원격으로 수행될 수 있다. 무선 랜의 실제 8대 이슈는 거짓 AP 발견, 공격마다 받은 평균 금전적인 손실, AP의 현재 성장률, 보안을 적용하지 않은 디바이스 발견, 회사에서 보안이 되지 않는 무선 랜 적용, 단말의 현재 성장률, 월간

[1]백석대학교 정보통신학부
*교신저자: 홍진근(jkhong@bu.ac.kr)

발생하는 심각한 평균 공격 수와 관련이 있다. 이 가운데 중요한 이슈 가운데 하나인 회사에서 보안이 되지 않은 무선 랜을 적용하는 문제는 회사에 치명적인 손실을 초래할 수 있다. 본 논문에서는 천안 인근 공단지역의 무선 랜 AP 운용 실태를 분석함으로써 보안 관리자 측면에서 보안인식 교육 및 보안 훈련의 필요성이 얼마나 필요한지 점검하고자한다.

워 드라이빙과 관련된 연구에서, Biju Issac 등은 말레이시아 사례 연구를 바탕으로 워 드라이빙 기술 및 보안 위협에 대한 연구를 발표한 바 있다[1]. 이 논문에서는 워 드라이빙 구성, 패킷 캡쳐, 통계적인 분석, WEP 크랙 검증, 넷 트래픽 필터링과 공격 등을 기술하고 있다. Kim Minkyong 등은 워 드라이빙을 통해 발견되는 AP위치의 위험과 관련하여 연구한 바 있다[2]. 이 논문에서는 실제적인 AP 위치, 워 드라이빙의 효과, 내부 및 외부에서의 AP 위치 추정을 위한 알고리즘, AP 간섭 문제를 다루고 있다. 또한 S. Fluhrer 등은 RC4의 키 스케쥴링 알고리즘의 취약성에 관한 연구[3] 한 바 있으며, A. T. Rager는 802.11 키 브레이커에관한 WEPCrack 주제로 연구[4]한 바 있다. 현재 사용되고 있는 IEEE802.11b의 무선 랜 보안 방식은 취약성을 안고 있으며 이를 해결하기 위해 IEEE 802.11i에서는 보안 강도를 강화시켰다[5-6]. 즉 EAP 확장 프로토콜을 사용하며 포트 기반의 802.1x 사용자 인증과 함께 상호인증기능을 도입 하였다. MIC 메시지 인증 코드를 적용하여 전송 중인 정보의 데이터 변조 기능을 갖도록 하였으며 TKIP를 동적인 키를 갖도록 하였다. 또한 암호화를 위해 AES를 적용하였다. 최근 무선 랜 서비스 기술은 이동의 편리성, 네트워크 배선 설치의 자유로움 등을 이유로 인해 가정 뿐만아니라 기업의 자산 관리에 긍정적으로 검토되어 도입되고 있는 실정이다. 그러나 이러한 기업의 편리성 측면에서 요구에도 불구하고 보안성 측면에서 한편 우려를 낳고 있는 것도 사실이다. 본 논문에서는 천안시 산업단지를 중심으로 무선 랜 AP의 운용실태를 살펴 보았으며, 연구결과를 통해 보안상 취약성이 존재함을 실험적으로 실증하였다. 연구를 통해 대부분의 산업단지내 기업들이 정보화시스템을 구축하는 과정에서 생산성 측면의 편리성을 너무 강조한 나머지 보안성 측면을 쉽게 간과하고 있음을 알 수 있었다.

본 논문에서는 2장에서 무선 랜 환경에서 보안 적용방식을 살펴본다. 3장에서는 무선 랜의 운용환경을 살펴보며 4장에서 공단지역을 중심으로 무선 AP 운용 사례를 조사한다. 5장에서 결론을 맺었다.

2. 무선 랜의 보안 적용 방식

2.1 무선 랜 보안 특징

무선 랜에서 1세대의 보안은 SSDI (service set identifier)를 사용하고, MAC (media access control)을 등록하여 접근을 제어하고 있다. 각 AP가 가지는 식별용 SSID는 관리자에 의해 설정되는 비밀 키 값이다. 따라서 클라이언트는 AP의 SSID를 알고 있을 경우 해당 AP로 접속이 가능하다. 넷 스니핑을 통해 이 SSID를 알 수 있다. 대부분의 AP는 SSID 브로드캐스트나 any SSID 를 허용한다. 이와 같은 옵션은 대부분 디폴트로 설정하여 사용하거나 이렇게 함으로써 무선 넷을 설정하기가 보다 쉽다. any SSID를 허용하는 것은 빈 SSID를 가진 클라이언트로 하여금 AP에 접속할 수 있도록 허용하는 것이며, SSID 브로드캐스트는 SSID를 광고하는 비콘 패킷을 전송한다. 위의 옵션을 무효화하는 것은 무선 스니퍼가 쉽게 정상적인 무선 트래픽으로부터 유효 SSID를 캡쳐할 수 있으므로 넷이 보호되지 않는다. SSID는 보안 특성으로 고려되어서는 안된다. IEEE802.11 표준은 도청으로부터 허가된 사용자를 보호하기 위해 WEP를 포함하고 있다. WEP표준은 40비트 키를 명시하고 있으며 대부분의 공급업자들은 128비트로 확장된 WEP를 제공한다. WEP을 사용할 때 클라이언트와 AP의 WEP 키가 일치되어야 하며 RC (Rivest Cipher) 4를 기반으로 하고 있다. 무선 랜 인증방식은 802.11 단말이 무선 AP와 통신하기 전에 무선 단말이 법위 내의 AP로부터 메시지를 청취한다. 단말이 SSID가 매칭되는 AP로부터 메시지를 발견하고 AP로부터 인증 요구를 한다. AP는 단말을 인증하며 단말이 AP에 연결 요구를 보내게 된다. 이어 AP가 단말과 연결되고 단말이 AP를 통해 무선 통신을 개시한다.

2.2 보안 취약성을 검증하기 위한 도구

무선 넷 보안 관련 도구에는 스캐너, 스니퍼, Multi use, WEP 도구, 부트 가능한 CD Rom 등이 있다. 이 가운데 무선 넷 스캐너에는 Netstumbler, Kismet, THC-WarDrive, Prism Stumber, MacStumbler, Wellenreiter, Stumbverter, AP Scanner, SSID Sniff 등이 있다. 스니퍼 도구에는 AiroPeek, NAI Wireless Sniffer, Ethereal, VPN monitor 등이 있으며, WEP 도구에는 WEPCrack, AirSnort, Wepwegie 등이 있다.

Kismet은 802.11 패킷 탐색을 위한 무선 채널 전환 기능, 리눅스 및 BSD 기반의 AP, GPS 위치 추적 기능, IP 주소및 CDP 등 넷 관련 정보 수집기능, SSID 넷 이름, 유형, WEP 설정 여부,채널 번호, 탐지된 IP 주소 ARP 요청 및 트래픽 정보 등을 제공한다. JiGLE 는 무선 넷 WiGLE DB 로부터 데이터를 볼 수 있도록 하는 자바 클라이언트이다. 침투 테스터 툴인 Wellenreiter 도구는 무선 디바이스 MAC 주소와 IP 주소를 결정하기 위해 사용되는 ARP, DHCP 트래픽을 청취할 수 있다. 넷 스텀블러는 무선 네트워크를 탐지하고 GPS로 적절한 위치를 표시하는 윈도우 기반 워드라이빙 도구로 알려져 있다. 즉 802.11 탐색 요청을 브로드캐스팅하여 목적지 주소에 보내는데 사용하며 이 영역 내의 모든 액세스 포인트에서 SSID와 WEP 상태 같은 네트워크 구성정보를 포함한 802.11 탐색 요청에 응답한다. Net stumbler에서 GPS 설치는 각 액세스 포인트에 최상위 신호 강도에 대한 GPS 좌표를 기록하며 네트워크와 GPS 데이터를 StumbVerter 나 MS 맵 포인트 같은 도구를 사용하여 지도를 작성한다. 넷 스텀블러는 MAC 주소, ESSID, 무선 채널 및 각 액세스 포인트의 상대적인 신호 세기를 수집할 수 있으며, AP의 보안 설정 상태 즉 WEP 설정 상태를 확인할 수 있고, GPS 시스템과 연동할 수 있다. Airsnort 의 경우 WLAN 도구로서 802.11b WEP 네트워크에서 암호 키를 크랙할 수 있다. 수동으로 전송된 패킷을 모니터링하여, 네트워크에서 수집된 패킷이 충분히 모여지면 암호 키를 계산함으로써 키 크랙이 가능하다. AP를 탐색하고 나면 이 데이터를 네트워크와 GPS 데이터 결과를 기반으로 지도를 작성할 수 있으며 워 드라이빙 도구는 현재 GPS 위치, 신호 강도, 각 AP 의 특성을 기록한다. 이 데이터를 기반으로 신호 강도가 높은 위치를 추측할 수 있으며, 추출 결과를 근거하여 GPS 좌표를 해석할 수 있다. 이때 사용되는 것이 MapPoint 나 MapBlast와 같은 맵핑 시스템에서 필요한 결과를 확인할 수 있다. 소프트웨어는 이러한 과정을 자동화시키며 워 드라이빙 도구로 직접 데이터를 읽을 수 있으며 자신의 데이터를 사용하거나 일부 그룹은 대규모 DB에서 정보를 수집하기 위해 www.wifimaps.com, www.gigle. net 사이트를 만들기도 한다. Stumverter 는 넷 스텀블러 형식 파일로부터 평면 데이터를 구성하기 위해 맵 포인트2002 를 사용한다. 각 액세스 포인트에 대한 맵 상에서 넷 스텀블러 스타일 아이콘을 생성하는데, 녹색 아이콘은 암호화되지 않은 아이콘이며 빨간색 아이콘은 WEP를 사용하는 네트워크를 나타낸다. 스텀버터를 사용하기 위해 import 를 클릭하고 스캔 결과를 선택한다. 맵은 SSID와 MAC 를 포함하여 모든 액세스 포인트 이름을 view/show 기능을 가진다. GPSMap 은 Kismet 무선 모니터링 패키지를 가지며 kismet GPS 와 네트워크 파일을 가져와 소스의 변수로부터 지도 상의 위치를 구성한다. 다기능의 워 드라이빙 맵 생성기로 각 액세스 포인트에 대해 많은 그리기 옵션을 제공한다

3. 무선 AP 운용 환경

먼저 워드라이빙을 실시하기 위해 적합한 구성품을 준비한다. 워드라이빙을 위해서는 윈도우 기반의 netstumbler, 애플 기반의 Kismet, 리눅스 기반의 Kismet이 있다. GPS를 사용할 경우 Wigle (*Wireless Geographic Logging Engine*) 소프트웨어를 사용할 수 있다. 안테나가 연결된 외장형 무선 랜 카드를 장착한다. GPS 디바이스는 USB 시리얼 어댑터를 통해 연결시킨다. 다양한 무선 AP가 있는 영역을 통해 드라이빙을 실시한다. 이때 Netstumbler, Kismac 또는 Kismet 프로그램을 구동한다. GPS는 자동적으로 AP 위치와 GPS 축을 맵상에서 표시하는데 사용하며 좌표들은 맵 프로그램을 통해 도식화된다. Netstumbler를 이용하여 일정 주기 동안 워드라이빙을 실시하고 결과를 로그로 남긴다. 로그로 남겨진 결과 파일을 맵상에서 도식이 되도록 한다. 그림1에서는 워드라이빙을 AP 탐색 구성도를 나타낸 것이다.

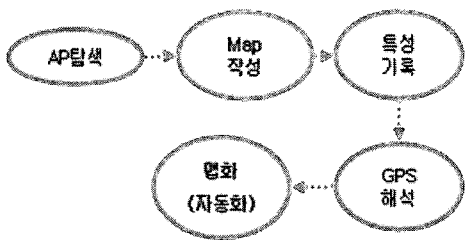


그림 1. AP 탐색을 위한 처리 과정

무선 환경에서 탐지된 AP가 위치좌표를 맵상으로 표시하는 맵 처리 도구와 관련된 수신전력, 신호 특성을 나타내고 있는 도구를 그림2에서 제시하였다.

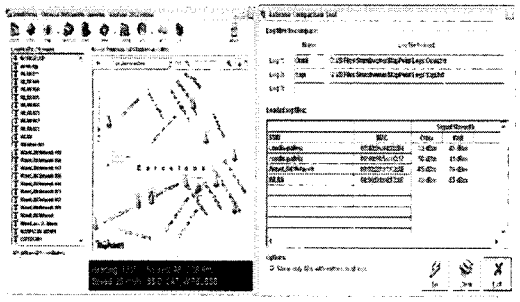


그림 2. AP탐색 결과에 대한 맵 처리 도식 (stumveter, 수신전력, 신호 특성 비교)

그림3에서는 무선 AP 탐색을 위한 시험 환경 구성품을 제시하고 있다. 구성품에는 방향성 안테나, 무선 랜 카드, GPS 수신기, 넷 스텀블러, 트래픽 수집의 확인 용도를 위한 Link sys AP로 구성된다.

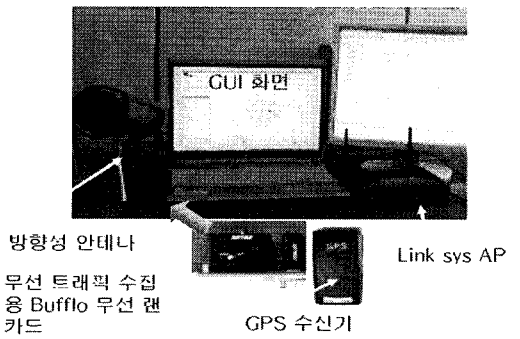


그림 3. 시험 환경 구성도
(안테나, 무선 랜 카드, GPS 수신기, Netstumbler)

천안 인근 공단지역을 넷 스텀블러를 통해 수집되는 결과에서 Fake AP를 탐지한 결과를 그림4에서 나타내었다. 결과에서 운용중인 AP 대부분이 WEP 설정이 되지 않은 상태로 운용되고 있는 실정이다.

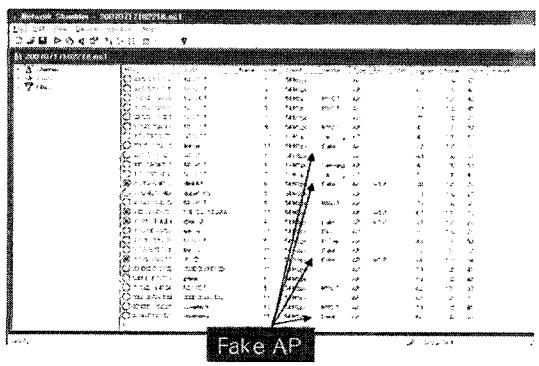


그림 4. Netstumbler 구동을 통한 Fake AP 탐지 화면

4. 공단지역을 중심으로 AP 운용 사례 분석

실제 기업들의 무선 랜 AP 운용 사례를 분석하기 위해 인근 천안 산업단지를 중심으로 AP 운용실태를 살펴보았다. 산업단지에서 설치된 대부분의 무선 랜 AP 장비들은 사무실 및 공장 생산라인에서 운용되고 있으며, 생산정보를 수집하는 용도로 주로 활용되고 있다.

그림5에서는 시간대별로 수집되는 무선 트래픽을 신호대 잡음비로 나타낸 화면이다. 현재 알려져 있는 대부분의 무선 공격 도구를 활용할 경우, 무선 트래픽에 대한 캡쳐 및 분석이 가능하다는 결과가 제시되고 있다. 따라서 제시된 결과를 통해 알 수 있는 것은 전송되는 대부분 정보가 기업의 주요 자산에 관련된 정보이거나, 생산량 수집 정보들로써 실시간으로 서버에 전송되고 기업의 자산관리 및 평가에 주요하게 사용되고 있다. 만일 전송되는 정보가 공격자에 의해 변조되거나 방해될 경우 정확한 생산 정보를 수집하기 어려워지고 이로 인해 기업의 BOM 관리, 기타 품질관리, 재고관리, 발주관리 등에 심각한 손해를 끼칠 수 있다.

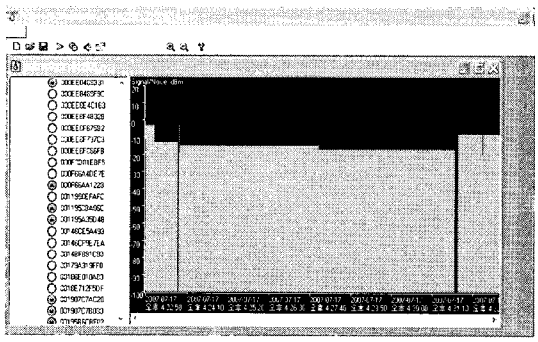


그림 5. 시간대별 수집되는 무선트래픽의 S/N분포

제시된 그림6과 표1에서는 공단지역에서 조사된 바에 따르면 대부분 WEP 설정이 이루어지지 않고 있으며, 일부분만 WEP 설정하고 있는 실정이다. WEP 설정과 관련하여 공단지역에 존재하는 대부분의 중소기업 전산관리자들이 아직까지 무선 랜 환경에서 보안 의식이 떨어져 있는 것을 확인할 수 있는 화면이다.

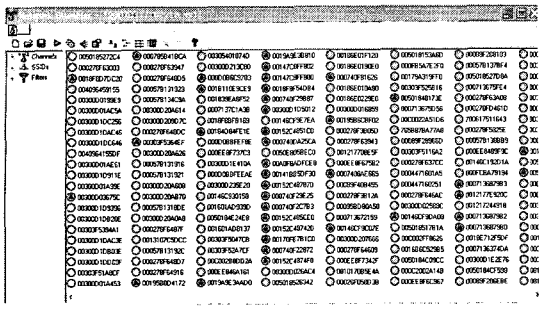


그림 6. AP별 WEP 설정 유무를 제시한 화면

대부분 운용되고 있는 무선 AP는 회사 내의 보안관리자나 정보시스템 관리자, 또는 정보화 사업을 통해 구축되었다. 구축된 AP 가운데 약 50% 수준이 WEP 보안설정이 이루어져 운용되고 있는 실정이다.

표 1. 무선AP 운용시 WEP 설정 분포

	WEP 미설정	WEP 설정
전체 AP 개수	140	69
SSID 제공	11	1
회사용	51	68
Netspot ISP	78	0

표2에서 D사의 경우 운용하고 있는 AP에 대해 WEP 보안이 모든 AP에서 설정되어 있는 것을 볼 수 있는 것과 상반되게 제시한 대부분의 회사 AP 들은 WEP 보안설정이 미흡한 실정이다.

표 2. 무선AP 운용시 특정기업의 WEP 설정 상태

	전체 AP	WEP 설정
A사	13	1
B사	11	1
C사	12	0
D사	9	9
E사	8	1
F사	8	1
G사	9	0
default AP	12	0

인근 중소기업이 운용하고 있는 무선 주파수 채널은 대부분의 주파수 채널이 "11", "1", "6", "5", "9" 채널 순서로 운용되고 있다.

표 3. 무선AP 운용시 사용 주파수 채널

주파수채널	운용AP	주파수채널	운용AP
1	67	7	5
2	2	8	1
3	3	9	27
4	2	10	7
5	32	11	81
6	49	13	19

본 논문에서 얻은 결과를 통해 대부분의 산업단지내 기업들이 정보화 시스템을 구축하는 과정에 보안성을 고려하지 않고, 생산정보 수집 및 관리의 효율성과 편리성 측면에서만 접근하고 있다는 것을 알 수 있다. 즉 기업의 보안 인식이 낮은 전산관리자 또는 정보시스템 관리자가 자사의 보안체계를 고려하지 않고 IT지원기관 기술력에 의존하여 정보화 시스템을 구축하고 있는 실정임을 예측할 수 있다. 아직까지 대부분의 중소기업의 경우 자산을 보호하기 위한 보안정책이 수립되지 않았거나 미흡한 실정이며, 전산관리자나 정보시스템 관리자의 보안 교육 또한 미흡한 실정이다. 이와 같은 환경에서 지속적인 보안관리가 정상적으로 이루어지기는 매우 어렵다. 무선 랜의 보안 취약성을 해결하기 위해서는 지속적인 패치, 동적인 WEP 패스워드 설정, 주기적 및 비주기적으로 패스워드 변경 설정해야 한다. SSID 는 벤더가 설정해 놓은 공급자 ID 디폴트 값을 변경해야 하며 인증시스템을 두고 넷 자원에 접속하기 이전에 라디우스나 커버러스 인증을 거치도록 설계해야 한다. 건물 중심부에 AP를 설치함으로써 외부로 전파 노출을 최대한 차단시켜야 하며 40비트 WEP이 아닌 104비트 키를 사용하여야 한다. 알려진 MAC만을 허가하도록 AP와 방화벽 상에 ACL을 설정하는 것 또한 매우 중요하다. 동적인 호스트 제어 프로토콜인 DHCP를 차단해야 한다.

5. 결 론

본 연구에서는 보안 취약성 문제가 거론되고 있는 무선 랜 환경에서 먼저 워드라이빙 도구를 살펴 보았다. 무선 랜 환경에서 운용되는 AP 상태가 보안상 취약성이 존재함을 실험적으로 실증하였으며, 연구를 통해 여전히 대부분의 산업단지내 기업들이 정보화시스템을 구축하는

과정에서 생산성 측면의 편리성과 효율성을 너무 강조한 나머지 보안성 측면을 간과하고 있으며 뚜렷한 보안 대책을 수립하지 않고 정보시스템을 운용하고 있음을 알 수 있었다.

따라서 본 논문에서는 실증된 결과를 통해 기업들이 자산을 보호하고 기업 이윤을 효율적으로 관리하기 위해서는 반드시 정보시스템 관리자 및 전산관리자에 대한 보안 인식 및 훈련이 강화되어야 하며, 넷 구축에 선행하여 회사 정보시스템 관리자의 정보보호 교육에 대한 훈련이 선행되어야 함을 강조하고자 한다.

참고문헌

[1] Issac, B.; Jacob, S.M.; Mohammed, L.A, "The art of war driving and security threats - a Malaysian case study," Networks, 2005. Jointly held with the 2005 IEEE 7th Malaysia International Conference on Communication., 2005 13th IEEE International Conference on Volume 1, 16-18 Nov. 2005.

[2] Minkyong Kim, Jeffrey Fielding, and David Kotz, "Risks of using AP locations discovered through war driving," In Proceedings of the 4th International Conference on Pervasive Computing (Pervasive), Dublin, Ireland, May 2006.

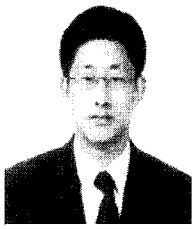
[3] S. Fluhrer, I. Mantin, and A. Shamir, "Weakness in the Key Scheduling Algorithm of RC4,"8th Annual Workshop on Selected Areas in Cryptography, Aug. 2001.

[4] A. T. Rager, "WEPCrack - An 802.11 key breaker," HTTP://wepcrack.sourceforge,net/]

[5] JYH-CHENG CHEN, MING-CHIA JIANG, and Yi-WEN LIU, "Wireless LAN security and IEEE802.11i," IEEE Wireless Communications, Feb. 2005.

[6] Daji Qi ao and Sunghyun choi, "New 802.11h mechanism can reduce power consumption," IEEE computer society: Wireless Networks, March 2006.

홍 진 근(Jin-Keun Hong) **[정회원]**



- 2000년 경북대학교 전자공학과 (공학박사)
- 국가보안기술연구소 선임연구원
- 현 백석대학교 정보통신학부 교수

<관심분야>
정보보호, 텔레매틱스 시스템, 헬쓰케어시스템, NCW/전술넷/센서넷