특집 13

국방분야 무선Network 도입을 위한 보안기술 측면의 고려사항

목 차

안정철 · 권혁진
(한국국방연구원)

1. 서 론

오늘날 컴퓨터와 통신기술 인프라의 급속한 발전이 고도화된 정보 Network 구축을 가능하게 하였다. 그리고 정보 Network는 정보사용자의 폭발적인 확대로 인하여 사회 기반인프라로 인식되어져 가고 있다. 이러한 인프라는 사용의 편의성과 유비쿼터스라는 시대적 흐름으로 인하여 유선기반에서 무선으로 구축 중심이 변화되어 가고 있다. 이에 따른, 무선기술 및 휴대 기기의 상용화 및 발달은 언제 어디서나 네트워크에 쉽게 접속하고 서비스를 받을 수 있게 발전되었으며, 이러한 서비스를 기반으로 매년 무선 Network 사용에 대한 소요가 증가하고 있다. 군 또한 작전의 효율성, 생존성 및 업무의 편의성을 고려하여 무선Network 도입을 검토하고 있으며, 일부에서는 무선Network를 시범적으로 운영 중인 곳도 있다.

그러나 군에 무선Network 도입을 위해서는 군 특수성을 고려한 보안기술 측면에서 고려 요소들이 존재한다. 따라서 본고에서는 현재 사회 널리 인프라로 구축 및 보급되고 있는 IEEE802.11b/g 기술을 중심으로 무선보안기술을 분석하고 이를 기반으로 군에서 무선 Network를 도입 시 검토되어야 하는 보안기술 고려사항을 제안하고자 한다.

2. 무선Network 보안기술

현재 사회 널리 인프라 구축 및 보급되어 있는 IEEE802.11b/g Network의 보안 메커니즘은 기본적으로 WEP(Wired Equivalency Privacy)을 이용한 사용자 인증, 기밀성, 메시지 무결성 등의 보안 서비스를 제공하고 있다.

IEEE802.11b/g에서 네트워크에 접속하려는 무선 사용자를 인증할 수 있는 방법은 주로 SSID[1]를 이용한 방법과 암호화 기술 기반의 인증방식을 많이 사용하고 있다. 현재 많이 사용되어 지고 있거나 상용화 되어 있는 대표적인 보안기술은 〈표 1〉과 같다.

1) SSID : Service Set IDentifier(무선랜을 통해 전송되는 패킷들의 각 헤더에 덧붙여지는 32bit 길이의 고유 식별자로, 무선어뎁터들이 BSS(Basic Service Set)에 접속할 때 암호처럼 사용된다).

〈표 1〉 무선Network 보안기술

	설 명
WEP[2]	RC4 암호화 알고리즘을 이용하여 무선 AP와 Client 사이의 암호화[3]
SSID	AP장비에서 설정된 SSID 정보를 이용하여 사용자의 접속을 통제/관리하는 방법
MAC[4] ADDRESS 필터링	AP장비에 통신기기의 고유 MAC 주소를 등록하여 MAC주소 등록사용자와 미등록사용자의 접속을 통제/관리하는 방법
IEEE 802.1x	인증과 보안을 같이 사용하는 방법으로 LAN에서의 인증과 암호키 관리를 위한 IEEE 표준
동적WEP	IEEE 802.1x 보안을 보완한 방법으로 인증 방법을 EAP[5]-MD5[6]가 아닌 EAP-TLS[7] or TTLS[8]를 사용하는 방법
WPA[9]	동적WEP이 아닌 WPA를 사용하기 때문에 기존의 WEP의 보안취약점을 전반적으로 개선한 보안방법으로, 확장된 48-bit IV(initialization vector)를 사용 (기존의 WEP은 24-bit사용)
RSN[10]	RSN은 CCMP[11] 알고리즘을 기본 알고리즘으로 정의하고, 지속적인 패킷번호(PN, Packet Number) 변조를 통한 재시도 공격(Replay Attack)을 방지하며, MAC 헤더 정보의 일부인 추가 인증 데이터(AAD, Additional Authentication Data)를 CCM 암호화 과정에 포함시켜 보안기능을 강화

3. 무선Network 보안 취약성

무선Network는 다음 〈표 2〉와 같은 기술적인 측면과 관리적인 측에서 보안취약성을 보이고 있다.

이러한 무선Network의 기술적, 관리적 측면의 취약성은 트래픽 정보의 누출, 네트워크 사용자 식별의 어려움 등을 야기 시키고 상시 비인가자에 대한 정보노출의 위험을 가지고 있다. 이러한 취약점으로 인한 두 가지 대표적인 위험요인은 다음과 같다.

첫 번째, 무선Network 대역폭으로 인하여 특정영역 안에서는 상시 외부 공격, 트래픽노출 및 접근에 노출되어 있다는 것이다. (그림 1)은 무선Network의 AP장비가 커버하는 무선범위를 나타낸 그림이다.

(그림 1)에서 짙게 색이 칠해진 범위는 한 개의 AP장비가 커버하는 무선영역을 나타낸 것이다. 표현된 범위에서 볼 수 있듯이 AP장비의 무선영역은 지형/건축물 등의 영향으로 불규칙적

〈표 2〉 무선Network 보안취약성

구 분	취약성		특 징
물리적 취약성	장비설치 및 운영		AP 불법접근 AP 도난/파손
	단말기 관리미흡		단말기 도난/파손/분실
기술적 취약성	구성 정보	SSID	SSID 노출정보를 이용한 접속시도
		MAC 주소	노출된 패킷정보를 기반 MAC 주소변조/도용
	프로토콜	WEP	WEP 설정 미흡, WEP 키노출
		TKIP[12]	WEP 취약성 내제 불안전한 RC4 알고리즘사용
	유선 연동시		무선 링크를 이용한 유선 트래픽정보 누출
관리적 취약성	장비관리		운용장비 현황파악 미흡 장비 기본설정 미 변경 사용
	사용자관리		사용자 보안의식 부족, Client 보안설정 미흡
	AP 전파관리		채널간섭 및 서비스거부 발생

2) WEP : Wired Equivalent Privacy(무선랜 데이터 스트림의 보안성을 제공하기 위해 1997년 IEEE802.11 표준에 정의된 암호화시킴으로 데이터의 암복호화에 동일키와 알고리즘을 사용하는 대칭형 구조다. WEP 키는 단말을 인증하고 데이터 프라이버시를 제공하는데 사용된다).

3) RC4 : 바이트 연산을 통해 키의 길이를 가변적으로 만드는 방법으로 무작위 치환에 기반을 둔 알고리즘에 기반을 두고 있다.

4) MAC : Media Access Control(네트워크 카드 제조사에 의해 부여된 48bit의 하드웨어 주소로)

5) EAP : Extensible Authentication Protocol(RFC 2284에 정의된 PPP 프로토콜의 확장판. EAP는 전통적 패스워드, 토큰카드, 커버로스,전자 증명 및 공중키 인증 등 여러 인증방식을 지원하는 전반적 인증 프로토콜)

6) MD5 : message digest 5(ID/PW, 단방향 인증 방식)

7) TLS : transport layer security(사용자와 인증 서버가 인증서를 이용해 상호인증하고 세션 기반의 동적 웹키를 생성 분배하는 인증방식)

8) TTLS : tunneled TLS(구현의 편의를 위해 유연한 단말인증 방법을 채택한 것으로 단말인증은 ID/PW로, 서버인증은 인증서를 이용해 인증하는 방식)

9) WPA : WiFi Protected Access(EAP와 TKIP,802.1X의 세가지 기술을 조합해 만든 무선통신데이터를 암호화하는 기술로 마스터 키 값을 이용해 사용자 인증 및 전송 데이터를 암호화하는 방식)

10) RSN : Robust Security Network(802.1X를 이용한 가입자 인증 및 키 관리 메커니즘 등의 보안프레임워크를 소프트웨어 패치로 강화시킬 수 있게 지원)

11) CCMP : Counter mode with CBC-MAC Protocol (CCM 모드를 사용하는 AES〈Advanced Encryption Standard〉 암호 알고리즘을 사용)

12) TKIP : Temporal Key Integrity Protocol(WPA의 기수중 하나로, WEP 암호 키를 빠르게 갱신해 향상된 데이터 암호를 지원함)

(그림 1) 무선AP의 전파노출 범위

인 무선영역을 가지게 된다. 이러한 불규칙적인 AP의 무선영역은 기존 사용자 접근이 제한된 유선Network에 비하여 더 많은 접근영역 및 편의성을 제공함으로써 기존 유선Network보다 더 많은 취약성을 보여준다.

두 번째, 사용자 식별 및 통제가 어렵다는 점이다. 즉, 인가되지 않은 사용자가 AP장비를 무단으로 네트워크에 설치 후, 위조된 MAC 주소 정보 등을 이용하여 네트워크 접근할 때 사용자 식별이 쉽지 않다. 또한 내부에 들어온 외부사용자 혹은 내부사용자가 외부 AP(국방시설 이외의 무선Network)로의 연결을 시도할 때 통제가 제한되는 문제점을 가지고 있다.

국방분야는 (그림 2)과 같은 다양한 무선 어뎁터들로 인하여 폐쇄망인 국방망도 보안상 어려움이 예상된다.

(그림 2) 무선 어뎁터 종류

이러한 어뎁터들로 인하여 국방망 내부의 정보가 유출될 수 있는 경로는 다음과 같다.

첫 번째, 업체 및 내부 사용자자 비인가 무선 AP장비를 국방망에 연결할 때, 비인가 장비를 통하여 국방망 내부 트래픽정보 및 개인정보가 외부에 누출 될 수 있다.

두 번째, AP 장비의 중계 없이 Peer to Peer[13]로 통신하는 Wi-Fi Network기술을 이용하여 정보가 누출될 수 있다. 현재 상용화된 대부분의 노트북 또는 휴대폰은 블루투스, 적외선 통신 등의 기능들이 기본적으로 탑재되어 있다.

세 번째, 핸드폰 망(3G, HSDPA), 와이브로 등을 이용하여 외부 네트워크에 접속 후 내부 자료를 외부로 유출 할 수 있다.

앞의 3가지 취약점은 폐쇄적으로 운영 중인 국방망의 보안상 취약점을 유발시킬 수 있으므로 유의하여야 한다.

4. 무선Network 국방도입을 위한 기술적 고려사항

앞에서 고찰한 바와 같이 무선 어뎁터들의 발전으로 인하여 발생하는 취약성을 대처하기 위해서는 국방 분야에 무선Network에 대한 보안을 지속적으로 검토하여야 한다. 본 절에서는 미 NIST(National Institute of Standards and Technology)의 무선Network 보안지침 중 기술적 분야의 운영가이드를 기반으로 국방에 무선 Network 도입을 위한 기술적 고려사항을 제안한다. 미 NIST는 기술적 측면의 운영가이드로 크게 S/W 측면의 고려사항과 H/W 측면의 고려사항을 제시하고 있다. 그중 주요내용을 간략하게 정리해 보면

첫 번째, S/W 측면의 주요 고려사항으로 표 3과 같이 제시하고 있다.

13) Peer To Peer : 서버를 거치지 않고 PC와 PC간에 직접적으로 연결하는 방법

〈표 3〉 NIST SW 측면 주요가이드

고려사항	내 용
AP설정	AP관리패스워드설정 WEP 암호설정 MAC접근제어목록관리 SNMP관리 등
소프트웨어 패치 및 업그레이드	주기적으로 보고된 보안문제 및 이에 대한 패치수행
사용자 인증	ID/PASS,스마트카드,PKI등을 이용한 사용자 인증
개인용 침입차단 시스템사용	중앙관리자가 제어할 수 있는 개인침입차단시스템 설치
WEP 암호설정	WEP암호의 설정과 주기적인 변경
보안평가 및 보안감사	정기적 감사 및 평가를 통한 불필요한 AP식별 및 안전성이 떨어지는 보안설정 검토

〈표 4〉 NIST HW 측면 주요가이드

고려사항	내 용
스마트카드	사용자 인증의 방법 중 한가지로 이동성이 뛰어남
VPN	VPN을 이용한 기밀성, 무결성, 트래픽방지 등의 기능을 향상
PKI	IEEE 802.1X에서 사용가능함, 스마트카드와 병행 사용
생체인식	보안성이 요구될시 스마트카드,PKI와 더불어 사용

두 번째, H/W 측면으로 주요고려사항은 〈표 4〉와 같다.

NIST에서 제시하는 가이드의 내용을 살펴보면, 특정 기술에 종속된 기술보다는 기존체계와의 융합과 체계적인 관리에 중점을 두고 있다. NIST 무선Network 운영가이드에서 살펴보았듯이, 무선Network의 기술적인 고려사항은 새로운 기술을 요구하는 것이 아니다. 기존에 도입되어 있거나 상용화 되어 있는 기술들을 활용하는 방법이 무선Network 도입 시 발생되는 비용을 줄일 수 있는 방법이 된다. 따라서 국방 분야에 무선Network를 도입하려면 보안정책/운영/기술검토/감사정책 등의 지침이 먼저 수립되어야 한다. 본고에서는 무선Network에 대하여 보안기술 중심으로 정책적 고려사항과 기술적 검토사항을 다음과 같이 제안하고자 한다. 기술 중심으로 제안하고 하는 내용은 첫 번째, 무선Network 보안정책수립이다. 다음 〈표 5〉와 같이 필요성검토, 장비소요로부터 보안감사/평가에 이르는 전반적인 정책 수립지침이 필요하다.

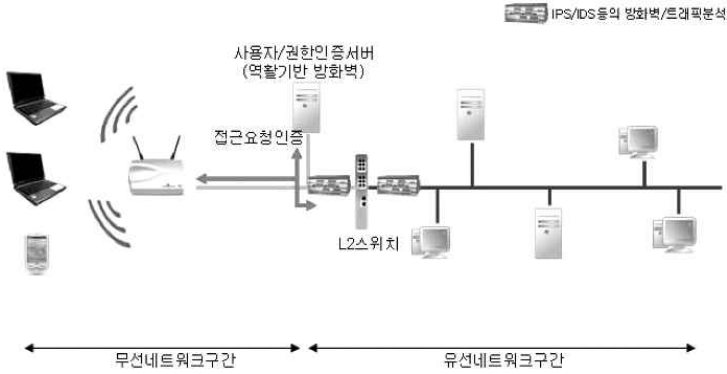
두 번째, 기술측면의 지침수립을 위하여 〈표 6〉과 같이 무선Network 특유의 보안기술 및 타 보안장치에 대한 지침을 수립한다.

〈표 5〉 국방분야 정책적 지침분야

고려사항	내 용
필요성검토	·무선장비의 사용 적정성에 대한 사전검증 및 승인체계유지
장비소요	·설치 AP,어뎁터 목록작성 및 책임자 선정 ·미승인하 추가 설치 및 장소 이관제한
AP설치위치에 대한 물리적 보안대책	·AP장비의 전파수신거리 측정 및 위험요인 식별 의무화 ·설치된 AP장비에 대한 시건
사용 프로토콜 통제	·무선Network에서 사용할 수 있는 프로토콜을 명시
위험평가계획	·자산목록과 위협식별을 분석 후 평가계획 수립
보안감사/평가	·보안평가의 주기, 범위 및 보안교육 등을 정의

〈표 6〉 국방분야 기술적 검토분야

고려사항	내 용
VPN, 스마트 카드, PKI, 생체인식 등을 이용한 접근통제	·자료의 중요성에 따른 사용자 접근 통제방안구축
채널관리	·무선랜 통신의 원활함을 지원하기 위하여 인접 AP간 다른 채널을 설정
환경관리	·기본적으로 설정 관리해야 하는 시스템이름 및 프로토콜, IP주소,SSID 등의 환경을 주기적으로 관리/변경 참고적으로, WEP의 경우 내부결함이 존재하지만 IEEE802.11a/g의 경우 152bit/128bit의 암호화를 지원한다. 따라서 보안의 강도를 최고로 하면 보안성이 증가될 수 있다.
DHCP 사용금지	·자동 IP를 제공하는 DHCP 기능 차단
트래픽관리	·이상 징후 발생 시 트래픽 차단을 위한 주기적 트래픽 모니터링
IDS/IPS/ 방화벽 사용	·AP와 유선망 또는 AP와 허브/L2 스위치 사이에 설치/관리
개인방화벽 사용	·백신프로그램, 악성코드검색등과 같은 중앙 사용자가 통제가능한 개인방화벽 설치/운영
파일공유금지	·보안업무 시행규칙 파일공유지침에 의거 관리
무선Network에 대한 감사로그 관리	·정기적인 감사와 비정기적인 감사에 대한 로그확인
주기적 SSID 변경/설정관리	·보안업무 시행규칙의 비밀번호 변경지침에 의거 월 1회 이상 변경 및 브로드캐스트 차단
S/W업그레이드	·취약점에 대한 모니터링 및 패치 프로그램 UPDATE/반영
MAC주소관리	·ACL(Access Control List)을 이용한 MAC 주소 관리를 통한 기본적인 Client 접근통제
프로토콜관리	·불필요하거나 보안상 취약한 프로토콜은 식별하여 사용제한
L2스위치사용	·AP와 유선연결지점에 보안성을 위하여 HUB 보다 L2스위치 사용



(그림 3) 역할기반의 네트워크 구성도(예시)

〈표 5, 6〉과 같은 관리적, 기술적 지침 등을 고려하여 네트워크 구축 시는 사용자 인식의 어려움 해결 및 감사기능 지원을 위하여 (그림 3)과 같은 감사시스템을 확대/구축 후 운영되어야 한다. (그림 3)은 역할기반을 고려한 네트워크 구성도의 예를 든 것이다.

사용자/권한인증서버는 무선구간의 사용자가 유선구간으로 접속을 시도 할 때 사용자의 접근권한을 검토/제공하는 역할과 유선/무선 구간의 사용자가 망을 사용하고자 할 때 사용자 인증을 하는 역할을 수행하게 된다.

본고에서 분석/제안한 국방의 당면 문제점 및 기술적 검토사항들을 기준으로 가장 기본적인 몇 가지의 점검리스트를 〈표 7〉과 제안한다.

5. 결 론

국방망은 폐쇄 망으로서 매우 높은 보안성을 가지고 있다. 그러나 무선 어뎁터 발전 및 국방내부 무선Network 시범적용/운영, 무선Network의 군전용 개량을 통한 작전망 전력화 추진 등을 고려한다면 이 시점에서 국방망의 보안에 대한 새로운 정책 및 기술검토가 요구된다.

본고에서는 이러한 국방의 당면한 몇 가지 주요 이슈를 분석하고 문제점 해결을 위한 주요 고려사항 및 점검리스트를 제안을 하였다. 하지만, 본고에서 제안한 기술관점의 고려사항은 국방 네트워크도입을 위한 전체적인 제안이 아니라 도입 및 운영간 기본적으로 검토되어야 할 분야에 국한되므로, 제안한 기술 이외에도 추가적인 검토사항이 존재한다. 따라서 국방 분야의 무선Network 도입을 위해서는 기술적인 분야 뿐 아니라 국방 무선Network 구축과 연계한 국방네트워크 전반에 걸친 보안 프레임워크와 관련한 연구 등의 폭 넓은 사전검토 및 연구가 필요하다.

〈표 7〉 무선Network 기술관점의 제안 점검리스트(예제)

보안조치		체크리스트		
		중요도	선택	확인란
관리적 조치				
필요성검토	·사용의 필요성은 얼마나 되는가	A		
	·지원되어야 하는 범위는 어떻게 되는가	A		
장비소요/사용자 관리	·AP/무선 장비에 대한 목록은 작성되었는가	A		
	·지원범위를 초과하는 장비는 없는가	A		
	·전출/퇴직한 사용자 정보는 갱신하였는가?	A		
	·리스만료 및 폐기된 장비목록은 갱신되었는가?	A		

AP설치위치에 대한 물리적 보안대책	·AP장비는 물리적 접근이 제한되어 있는가	A		
	·AP장비는 건물 안쪽으로 설치 되었는가	A		
사용 프로토콜 통제	·암호화된 프로토콜이외 다른 프로토콜은 통제되고 있는가	A		
위험평가계획	·보안성검토는 맡았는가	A		
	·추가된 장비에 대한 보안성검토는 계획되어 있는가	A		
보안감사/평가	·무선랜에 허가받지 않는 AP가 있는지 점검하였는가	A		
	·무선Network 사용자들에게 무선 기술 위험성에 대해 교육하였는가	A		
	·사용되지 않는 AP장비의 전원은 꺼져있는가	A		
	·보안업무시행규칙에 의거 보안감사 및 평가는 이루어지고 있는가	A		
기술적 조치				
VPN, 스마트카드, PKI, 생체인식 등을 이용한 접근통제	·IPSEC 기반의 VPN으로 구축되었는가	A	√	
	·스마트카드, 생체인식과 같은 접근제안 방법은 구축되었는가	A	√	
	·무선Network 접근자에 대한 PKI인증은 하였는가	A	√	
채널 및 무선영역	·무선Network의 외부 경계를 건물의 경계나 사용하는 건물들로 정확하게 한정하였는가	A		
	·전파충돌 및 전파방해를 방지/감시하기 위해 AP장비의 채널을 근처 무선 Network와는 다르게 설정하였는가	A		
	·AP장비의 영역 경계를 테스트 하였는가	A		
	·인가되지 않는 무선영역이 군지역에 걸쳐있지는 않는가	A		
환경관리	·최초 설정된 SSID값은 변경하였는가	A		
	·브로드캐스트 SSID 및 AP에서 지원하는 브로드캐스트는 정지시켰는가	A		
	·암호키는 최소 128비트 이상 설정 되었는가	A		
프로토콜 관리	·AP장비가 SNMP3이상의 암호화 프로토콜을 지원하는가	A		
	·SNMP3이상의 암호화 프로토콜은 사용 중인가	A		
트래픽관리	·트래픽분석은 모니터링 되고 있는가	A		
	·트래픽분석결과는 저장되고 있는가	A	√	
개인방화벽 사용	·개인 방화벽은 설치되었는가	A	√	
	·개인 백신은 설치되었는가	A	√	
	·설치된 개인방화벽은 중앙에서 관리가 가능한가	A		
파일공유금지	·무선Network 구간에서 공유되고 있는 파일 또는 폴더는 없는가	A		
무선Network에 대한 감사로그 관리	·무선 구간에 침입탐지 장치는 구축되었는가	A		
	·무선 구간에 대한 로그저장/관리체계는 정상적으로 운영되는가	A		
	·무선구간에 저장된 감사로그는 주기적으로 분석하는가	A		
주기적 SSID 변경/설정관리	·SSID값은 최소 1개월 단위로 바꾸고 있는가	A		
	·변경된 SSID정보는 접근 인가된 무선 사용자에게만 공개되어 있는가	A		
S/W업그레이드	·클라이언트의 NIC와 AP장비는 펌웨어 업그레이드는 가능한가	A		
	·클라이언트의 NIC와 AP장비는 최신 버전으로 업그레이드 되어있는가	A		
MAC주소관리	·접근 장비에 대한 MAC주소는 관리하는가	A		
	·MAC과 IP정보는 연계해서 관리하는가	A		
방화벽 설치	·유선Network와 무선Network 사이에 IDS/IPS등과 같은 방화벽은 설치되어 있는가	A		
	·유선Network와 무선Network 사이 연결점은 허브가 아닌 L2스위치로 구축되어 있는가	A	√	

참고문헌

[1] "IEEE802.11b Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification", IEEE Standard 802.11b, 1999

[2] IEEE, "Standards for Local and Metropolitan Area Networks Port-Based Network Access Control", IEEE Std 802.1x, 2001

[3] IEEE, "Local and metropolitan area networks - Specific requirements - Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security", IEEE Std 802.11i, 2004

[4] NIST Draft SP 800-48 : Wireless Network Security 802.11, Bluetooth and Handheld Devices, 2002

[5] 무선LAN의 안전한 사용을 위한 보안대책1, 국가사이버안전센터, 2004

[6] 안전한 무선랜 사용을 위한 가이드, 한국정보통신기술협회, 2005

[7] 무선랜 WPA 보안 핵심기술, [IT 리포트], 한국기술거래소, 2004.10

[8] 무선랜 보안 구조 , 정보과학회, 2002

[9] IEEE 802.11을 중심으로 한 무선 LAN 바이블, 세화, 2003.

[10] 무선 LAN 보안 체크리스트, on the net, 2005.3

[11] 무선랜 보안 실태 조사 및 분석을 통한 보안 강화 방안 연구, 한국정보처리학회,2006.5

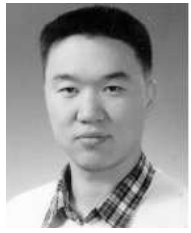
[12] 침입방지시스템과 역할기반 보안정책을 이용한 정부기관 네트워크 방화벽 시스템 설계, 정보보호학회, 2004

[13] http://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/wireless.html

[14] http://www.cisco.com/web/KR/networking/ensol/aironet/WLAN_Security.pdf

[15] http://www.hackerschool.org/HS_Boards/data/Lib_wireless/wireless.pdf

저자약력



안 정 철

1998년 밀양대학교 컴퓨터공학과(공학사)
2004년 세종대학교 정보통신대학원(공학석사)
1998년~2003년 해병대 전산실장/개발팀장
2003년~현재 한국국방연구원 IT컨설팅그룹 전문연구원
관심분야 : 정보보호정책, 유비쿼터스 구축전략
이 메 일 : kkillban@daum.net

권 혁 진

1982년 성균관대학교 산업공학과(공학사)
1989년 성균관대학교 산업공학과(공학석사)
2000년 성균관대학교 산업공학과(공학박사)
2008년~현재 한국국방연구원 정보화연구센터 연구위원
관심분야 : 정보화수준평가, IT전략컨설팅
이 메 일 : khjsjy@paran.com