주 제

무선 네트워크 침입탐지/차단 시스템 (Wireless IPS) 기술

한신대학교 소프트웨어학과 **이형우**

차 례

요 약

본 연구에서는 최근 무선 네트워크 환경이 급속도로 확산되면서 발생하는 무선 네트워크 현황 및 보안 취약점을 분석하고, 센서 AP(Access Point) 기반의 무선 트래픽 필터링 및 침입탐지/차단 기술 동향을 분석하였다.

유선 네트워크를 대상으로 한 IDS/IPS 시스템에 추가적으로 무선 트래픽에 대한 모니터링 체계를 제공하기 위하여 최근에는 통합형 유무선 네트워크 침입탐지/차단 시스템을 구성하고 있으며, 이를 위해서 필수적인 센서 AP 구성 방안 및 시스템 설계 방안 등에 대한 고찰을 통해 무선 네트워크 환경에서의 침해대응 기술을 고찰해 보고자 한다.

I. 서 론

네트워크에서 침입이란 컴퓨터 자원의 무결성, 비밀성, 가용성을 방해하는 모든 행위들의 집합을 의미한다. 또 다른 의미로는 컴퓨터의 보안 정책을 파괴하는 행위를 말하기도 한다. 이러한 침입의 형태와 기술은 시간과 비례하여 그 다양성이 나날이 증가되고 있으며 공격 시도 및 침입에 성공하는 공격의 횟수도 증가하고 있다. 네트워크 보안의 1세대 솔루션인 방어정책을 설정하여 침입을 차단하는 방화벽(Firewall)과 방화벽을 우회한 공격에 대해 분석하고 탐지하는 2세대 솔루션인 침입탐지시스템(Intrusion Detection System : IDS)이 등장하였다.

이들은 네트워크 위협을 최소화하고 공격을 완화

본 연구는 한신대학교 교내 연구비지원에 의해 수행되었습니다.

하는데 중요한 역할을 하지만 각각의 취약성으로 인해 또 다른 위협을 야기하기 때문에 이들의 취약성을 해결하고 공격에 보다 능동적인 대응이 가능한 침입차단시스템(Intrusion Prevention System : IPS)이 나오게 되었다[1,2,3].

IPS는 IDS와 마찬가지로 데이터 소스에 따라 호스트 기반 IPS와 네트워크 기반의 IPS으로 나눠진다. 네트워크 기반의 IPS는 기술적으로 실시간 패킷 처리와 오탐지를 최소화, 변형 공격과 오용공격의 탐지기술, 그리고 각 상황에 맞는 실시간 반응 기술이 요구된다[2]. 또한 IPS는 탐지 모델에 따라 시그너처(Signature) 기반 IPS와 비정상행위(Anomaly behavior) 기반 IPS로 구분되며, 시그너처 방법은 공격자와 피해자 중에서 공격자에 초점을 맞춘 것으로 해당 공격의 규칙을 바탕으로 네트워크 트래픽에서 해당 규칙을 찾아내어 이를 차단하는 방식이다. 비정상행위 방법은 기존 및 신종 공격에 대한 사전 대응을 위하여 피해자에 초점을 맞춘 것으로 피해자의 취약점을 악용할 수 있는 행위를 사전에 차단하는 방식이다[1,2,3].

일반적으로 비정상행위 IPS인 경우 과거의 경험적인 자료로부터 침입을 탐지하기 때문에 자료의 양과 질에 의존적이다. 또한 탐지 할 수 있는 가능성을 증명하는 것에 의의가 있을 뿐 탐지율이 낮다는 단점을 갖기 때문에 상대적으로 탐지율이 높은 시그너처 기반의 IPS가 널리 사용되고 있다. 하지만 시그너처 기반의 IPS는 공격 탐지 비율은 높지만 탐지 규칙의 증가에 비례하여 오탐율(false positive) 비율이 기하급수적으로 증가하여 네트워크 전반에 걸친 보안 서비스의 질을 하락시키는 원인이 된다[3,4].

유선망(wired network)에서의 네트워크 침해대응(network intrusion response) 기술은 점차 능동적이면서 지능적인 형태로 발전하고 있다. 이상탐지 기능을 지원하여 오탐율을 줄이기 위해 새로운 기술 개발이 진행되고 있으며, 인공지능 등 관련 기술을 접목하여 네트워크에 대한 공격 피해를 사전에 방지하기 위해 노력하고 있다.

본 연구에서는 최근 이슈가 되고 있는 무선 네트워크에 대한 침입탐지/차단 시스템에 관한 고찰을 통해 유무선 통합 형태의 IPS 시스템 구축의 타당성을 발견할 수 있는 근간이 되면서 Wireless IPS 구축에 핵심적인 요소인 센서(sensor) AP에 대해 살펴보고자 한다. 무선 네트워크 환경에서는 유선 네트워크 환경에서보다 더욱 다양한 방법들(예를 들어, Monkey Jack, KISMET, Wellenreiter, AirJack, Associate Flood, Auth Flood, De-auth Flood, Fake AP Flood 등)을 통한 공격이 가능하므로 본 연구를 통해 기존의 유선망 기반 IPS 시스템과의 연관성에 대한 비교 분석도 가능하다.

II. 무선 네트워크 보안 구조

1. 무선 네트워크 현황

최근 노트북 수요의 증가와 PDA 등 휴대폰 환경에서의 인터넷 서비스 증가로 일반 가정, 소규모 단독 사무실, 대학 등 일반 PC 네트워크 환경에서의 무선 LAN(Wireless LAN : WLAN) 사용이 급증하고 있다. WLAN 및 무선 인터넷 사용자는 매년 50% 정도로 급성장하고 있으며 가입자도 급증하여 2007년에는 93%의 사용자가 WLAN을 사용할 것으로 예측되고 있다.

WLAN에서 송수신되는 자료는 전파(Radio Wave)를 사용하여 공중으로 브로드캐스트(Broadcast)되기 때문에 자료의 송수신 기기에 의해 제공되는 공간에 있는 모든 WLAN 사용자들에게 자료가 전송된다. 전파는 천장, 바닥, 벽, 공중으로 송

신되며 전송된 자료는 의도되지 않은 대상들(다른층, 건물밖 등)에게도 도달 할 수 있다. 따라서 WLAN 환경에서는 유선망 환경과 달리 자료 전송 과정에서의 프라이버시 문제가 매우 중요한 고려사항이다[11].

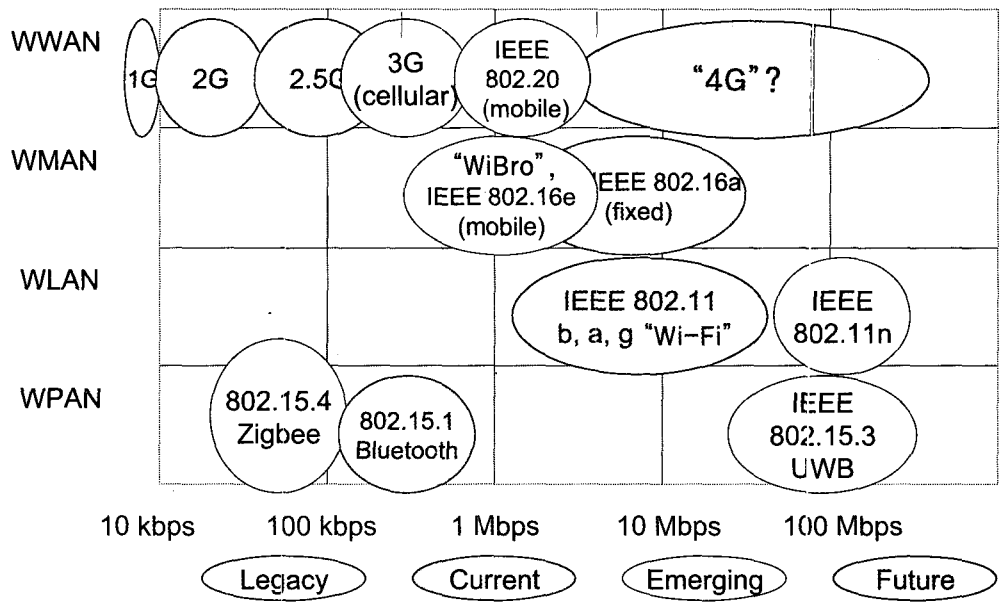
WLAN 프로토콜로 제시된 IEEE 802.11 표준은 접근제어, 프라이버시를 보장하는 요소들에 대한 내용을 포함하고 있으며 WLAN 장비의 보안 요소 역시 WLAN 장비의 표준 규격에 포함되어 있다[12]. AP에서는 IEEE 802.11 a,b,g 기반의 Wi-Fi 프로토콜을 적용하여 무선 단말에 대한 MAC 값을 검사하여 IEEE 802.11 기반 무선 주파수로 데이터를 전송하게 된다.

WEP(Wired Equivalent Privacy) 프로토콜 및 EAP(Extensible Authentication Protocol) 프로토콜을 이용하여 무선 트래픽에 대한 인증 과정을 수행하고 있다[13].

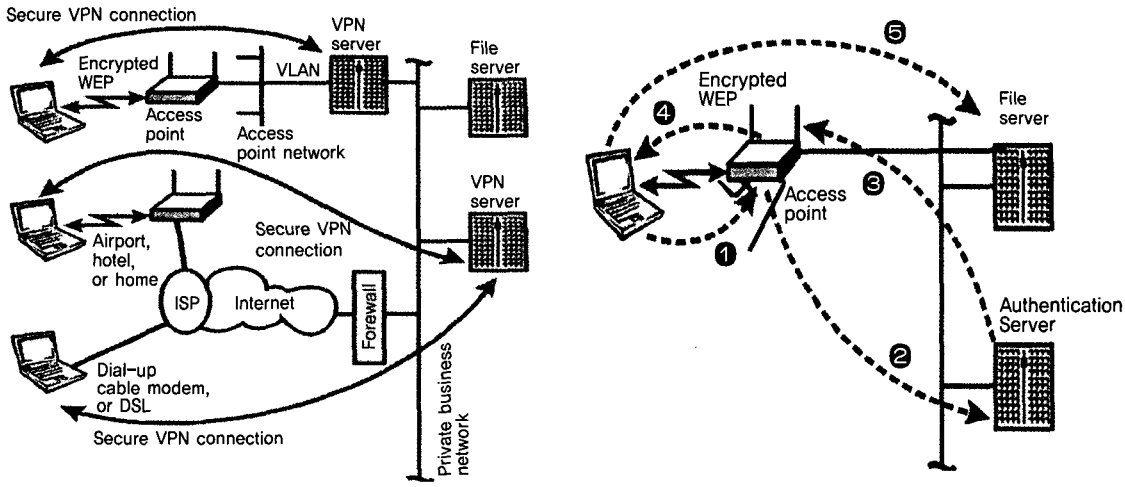
2. 무선 LAN 인증 기반 보안 구조

현재의 무선 네트워크 환경에서 보안 기능을 제공하기 위해서는 별도의 인증 서버에 기반하여 AP와의 VPN 터널링을 제공하는 것이다. SSL-VPN 기반의 터널링을 통해 인가된 시스템만을 대상으로 무선 데이터를 전송하는 구조이다. 하지만 VPN을 이용할 경우 WLAN 보안 기능을 제공할 수 있으나 별도의 인증 서버가 필요하다는 단점이 있다.

무선 도메인에서의 패킷에 대한 접근제어(access control) 서버를 이용하여 외부로부터의 불법적인 도청/감청 및 패킷 스니핑을 방지하는 기법이 제시되었다. WLAN에서는 접근제어 및 프라이버시 제공을 위해 여러 가지 형태의 보안 메커니즘을 정의하고 있다. SSID(Service Set Identifier), WEP 등을 제공하여 WLAN 구간에서의 전송되는 정보에 대한 암복호



(그림 1) 무선 네트워크 프로토콜 구조도



(그림 2) VPN 및 인증 기반 WLAN 보안 구조

화에 사용된다. WEP 프로토콜은 WPA(Wi-Fi Protected Access) 방식을 통해 접근제어 기능을 제공하고, TKIP(Temporal Key Integrity Protocol) 방식을 통해 안전성을 높이고자 하였다[10,14,15].

CISCO 시스템에서는 LEAP(Lightweight Extensible Authentication Protocol)을 제시하여 AP와 RADIUS 서버 간의 보안 및 인증 과정을 제시하였으며 상호 인증을 통해 공격 취약점을 해소하고자 하였다[14].

현재의 WLAN 시스템에서는 RADIUS 기반의 인증 서버를 두고 무선 서비스를 제공하고 있다. RADIUS 서버에 기반한 인증 과정을 수행하며, 구체적으로는 Kerberos 기법 등을 적용하여 무선 디바이스에 대한 보안 구조를 제공하게 된다. EAP을 통해 WLAN 클라이언트 아답터와 RADIUS 서버간의 통제된 포트 접근 제어 및 인증 기능을 제공한다. 근래에는 DIAMETER 기술을 이용한 무선 인증 방식으로도 발전하고 있으며, AAA 기술에 근간하여 무선 네트워크에서의 인증 및 과금 체계를 적용할 수 있다.

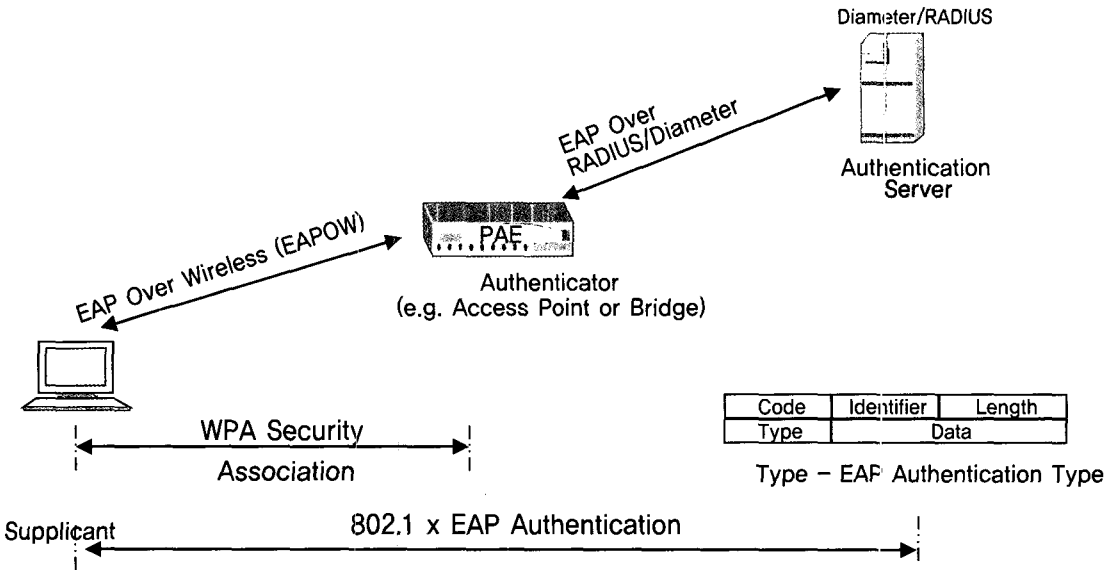
하지만 802.1x 프로토콜에 대한 보안 취약성 공격을 통해 무선 네트워크 공격이 가능하기 때문에 AP 기반 WLAN 환경에서의 무선 보안 취약성을 해소할 수 있는 방안에 대한 연구가 진행되고 있다.

III. 무선 네트워크 보안 취약점

1. 무선 네트워크 공격

악의적인 사용자들에 의해서 사이버 공격 기법은 날로 다양해고 있으며, 해킹 기법의 발달로 자동화, 지능화 된 해킹 툴이 공개적으로 유포되어 국내외 해킹 발생빈도는 급격히 증가하고 있는 추세이다. 특히 네트워크의 취약점이 지속적으로 증가하고 있으며 웜바이러스와 같은 치명적인 공격에 의해 네트워크 서비스를 마비시킬 수 있는 DDoS 공격이 급증하고 있다.

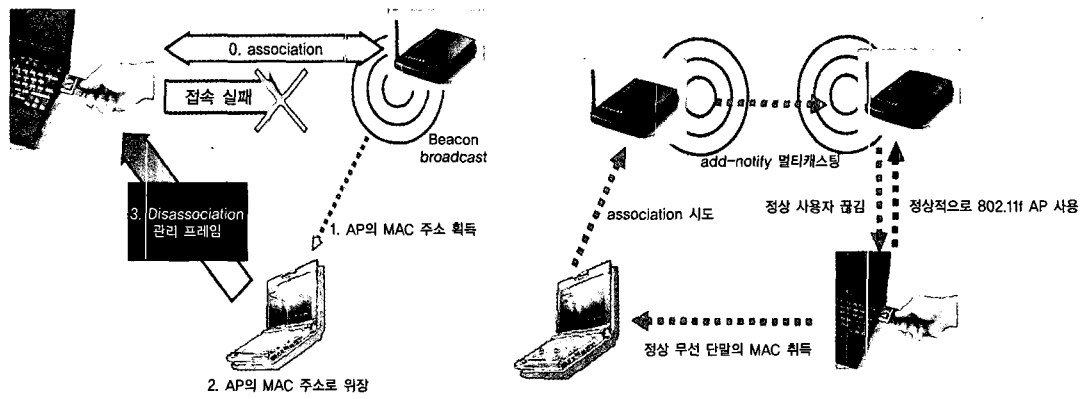
현재의 Wi-Fi 기반 AP는 보안 취약성에 노출되어



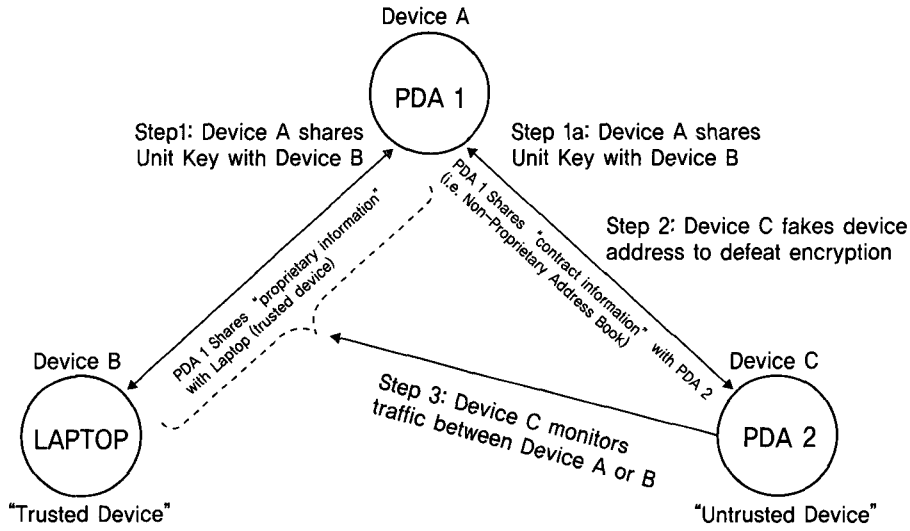
(그림 3) Diameter/RADIUS 기반 무선 인증 구조

있어 손쉽게 무선망을 침입할 수 있으며, 손쉽게 Rogue AP 등을 설치하여 802.11 프로콜에 대한 DoS 공격 등을 통해 내부 무선망을 무력화 시킬 수 있다. AP 기반 WLAN에서는 Man-In-The-Middle-Attack, 인가되지 않은 접근에 의한 트래픽 모니터링 및 Jamming 공격, Brute Force 공격에 의한 AP 패스워드 취득 및 변경이 가능하다.

Man-In-The-Middle-Attack인 경우 무선 디바이



(그림 4) 무선랜에서의 802.11 DOS 공격



(그림 5) AP 기반 WLAN에서의 Man-In-The-Middle Attack 취약점

스에 대한 인증 취약점을 공격할 수 있다. 따라서 무선 AP에 대한 침입탐지 모듈 및 패킷에 대한 필터링 기능을 제공할 필요가 있다. 특히 앞으로 WiBro 및 WiMAX 방식을 통한 무선 네트워크 환경이 확산된다면 현재의 AP와 유사한 인터페이스를 통해 무선 네트워크 서비스가 제공되기 때문에 AP 기반 무선 보안 구조에 대한 연구는 더욱더 필요할 것으로 예상된다.

2. 무선 네트워크 취약점 공격 기법 진화 단계

네트워크에 대한 공격 기술을 발전단계별로 살펴보면 다음과 같다. 패스워드 공격에 기반을 둔 1세대 공격에서 Sniffing, Spoofing 등으로 발전하는 3세대 공격, 버퍼 오버플로우 공격 등에 의한 4세대 공격으로 발전하였으며 현재는 웜, DDoS 공격 및 웹 공격을 통한 5세대 공격 형태를 보이고 있다. 앞으로의 공격은 P2P 기반 서비스 공격과 무선 공격, DB 공격 및 커널 공격 등으로 구분할 수 있으며 새로운 신규 공격 기법도 출현할 것으로 예상된다[2,3].

좀더 구체적으로 네트워크 공격 방식을 진화 단계별로 정리하면 아래 그림과 같다. 무선 네트워크 공격은 툴의 발전으로 인해 점차 고도화/지능화되는 형태로 발전하고 있다. 초기 단계에서는 무선 LAN 검색 등을 통해 무선 트래픽에 대한 캡춰, 변경 등의 기능을 수행하였으며, 점차 MAC spoofing 등의 기법을 이용해 위조/침입 방식으로 발전하였다. 최근에는 AirJack, Hunter-Killer 등을 통해 무선 네트워크에 대한 DoS 공격으로 발전하고 있다.

- 1단계 : WLAN AP 검색 기반 취약성 공격 (Detect WLAN)
  - Netstumbler, Kismet 등을 이용한 공격
- 2단계 : WLAN 패킷 캡춰 기반 공격(Capture Traffic)

- Protocol Analysis, data Credentials with Ethereal, Kane
- 3단계 : WLAN 위장 기반 공격(Masquerading)
  - Stealth Intrusion, MAC Spoofing, WEP Wedgie, MITM attack, AirSnarf
- 4단계 : WLAN 네트워크 변조 기반 공격(Insertion & Injection)
  - ARP win, ARPoisoning
- 5단계 : WLAN DDoS 공격(Disruption)
  - AirJack, Hunter-Killer

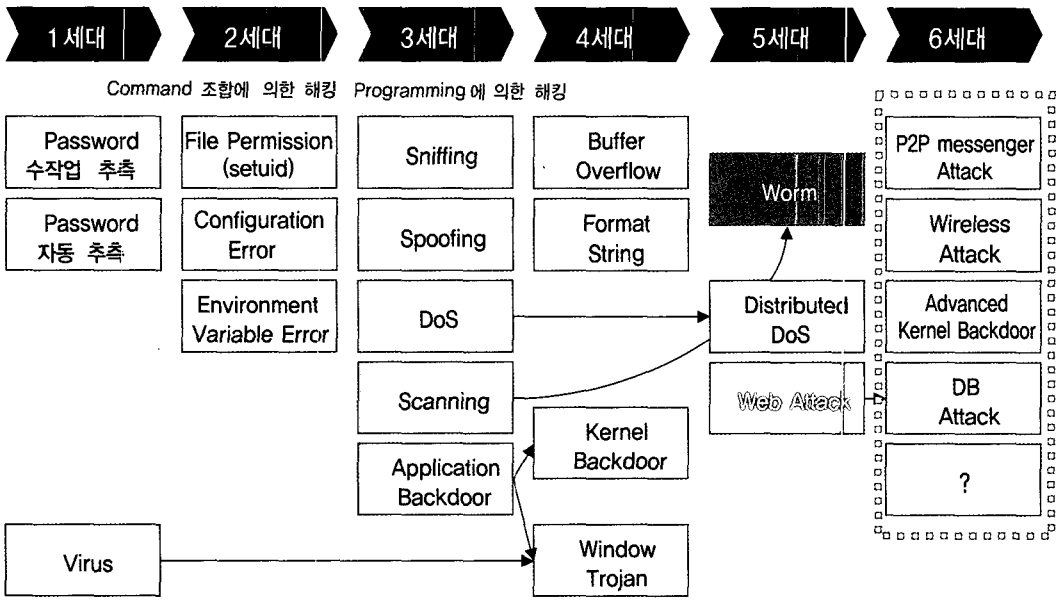
따라서 가장 위협적인 공격은 WLAN 디바이스에 대한 DDoS 공격에 해당하여 해결방안으로는 AP에서 DDoS 공격 등에 대한 필터링 및 침입탐지/차단 기능을 제공하는 모듈 개발이 필요하다.

IV. 무선 네트워크 침입탐지/차단 기술

1. 네트워크 침입탐지/차단 기술

유무선 네트워크에 대한 바이러스 및 웜 공격으로부터 피해를 최소화하기 위해 제시된 기술이 침입탐지/차단 기술이다. 악의적인 사용자들이 새로운 해킹 툴을 사용하여 고난도의 공격을 가하고 있으며 응용 프로그램의 수와 복잡성이 증가하여 취약점이 노출되고 있다. 또한 여러 가지 프로토콜들이 등장하면서 해당 프로토콜에 내재된 약점 등이 해커에 의해 악용되고 있다. 따라서 새로운 종류의 공격이 감지되면 효율적인 보안 시스템 구축을 위해 시그너처 개발이 시급하다.

IPS는 고속 침입탐지 엔진에 능동적인 해킹차단 기능을 더한 차세대 보안 솔루션으로 IDS에서 진화된



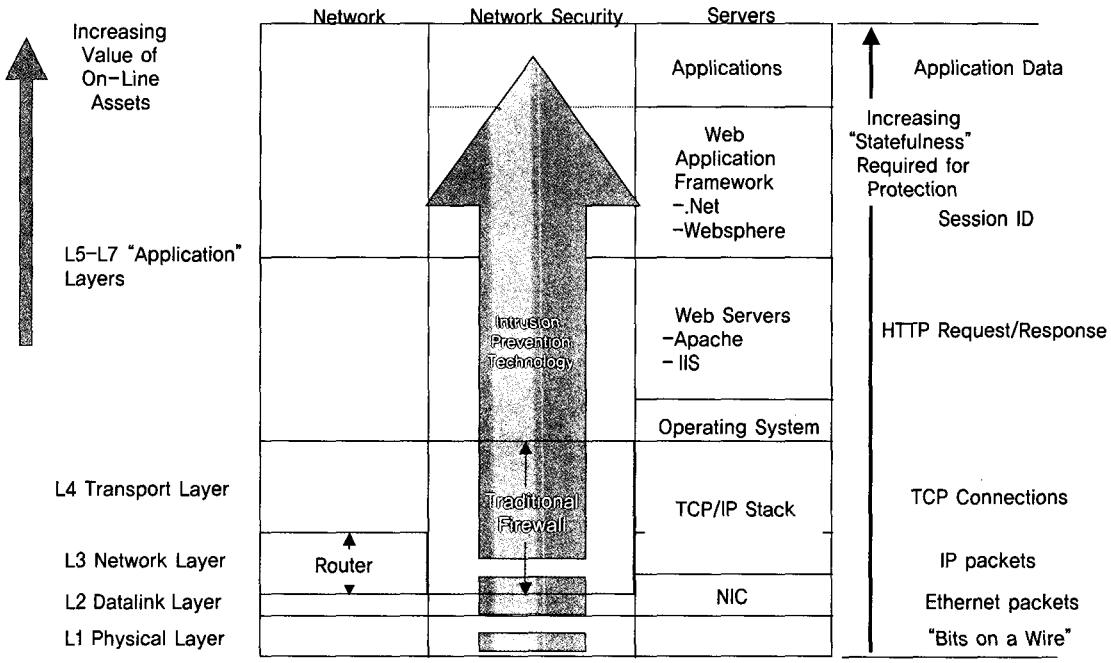
(그림 6) 네트워크 공격 진화 단계

시스템으로 정의할 수 있다. IPS는 패킷 해더와 패킷 내용에 대한 검사를 실시하고, 침입 혹은 유해 정보 여부를 자체적으로 판단하여 유해 패킷에 대해서는 즉시 차단(operating in in-line mode)하는 기능을 제공한다. IPS는 웜이나 DDoS와 같이 알려지지 않은 공격에 대비하기 위해서 비정상 트래픽의 흐름을 탐지하고 차단하는 기능(anomaly detection and prevention)을 제공하며, 대규모 트래픽에 견뎌내기 위해서 고속의 침입탐지/차단 기능을 제공하는 시스템이다.

현재까지 수행된 기존의 연구는 유선 네트워크 환경에서의 침임탐지 및 차단 기술에 대한 모듈 개발이었다. 기존 연구를 고찰하면 크게 호스트 기반 IDS/IPS와 네트워크기반 IDS/IPS로 나눌 수 있다. Host 기반 IPS인 경우 개별 호스트에 대한 보안 기능을 제공하고, 랩톱, 데스크톱 및 서버에 대한 침입탐지/차단 기능을 제공한다.

Network 기반 IPS인 경우 라우터 및 망을 관리하기 위해 네트워크 트래픽을 대상으로 한 침입탐지/차단 기능을 제공하며, 유선망에 대한 차단 기능을 제공하지만, WLAN과 같은 무선망에 대한 보안 기능을 제공하지는 못하고 있어서 이에 대한 연구 개발이 필요하다. 기존 IPS에서의 침입탐지/차단 방식에 대한 고찰해 보면 크게 아래와 같이 세 가지로 분류할 수 있다.

- Known Attacks에 대한 침입탐지/차단 기술



(그림 7) 계층 구조 관련 IPS 최신 기술 동향

: 수동적인 측면에서의 대응기술, 간단히 구현 가능한 기술

- Anomaly Detection 기술
  : 새로운 공격 및 신규 공격에 대한 지능형 탐지 기능을 제공, 오탐율이 문제
- Encrypted Attack에 대한 탐지/차단 기술
  : 악성코드 및 바이러스 공격 등 최신 공격에 대한 대응 기술

현재까지의 IDS/IPS 기술 발전 동향을 단계적으로 제시하면 다음과 같다. IPS 기술은 점차적으로 상위 계층으로 이동하면서 차단기능을 제공하는 추세이지만, 현재까지의 IPS는 유선망을 대상으로 한 연구에 중심을 두고 있어 무선망에 대한 연구도 필요한 실정이다.

- 1단계 : Detection without Prevention
  : 룰에 기반을 둔 침임탐지 기능만을 제공하는 IDS 시스템
- 2단계 : In-line Detection without Prevention
  : 인라인 방식으로 모든 패킷에 대한 검사, 오탐율을 최소화하는 방식
- 3단계 : Detection& Selective Prevention
  : 선택적 차단 기능을 제공하여 신뢰성과 성능을 향상시키는 방식
- 4단계 : Detection & Broad Prevention
  : 지능형 탐지 및 차단 모듈을 적용하여 모든 패킷에 대한 검사/차단 기능 제공

2. 침입탐지/차단 기술 시장 수요

아래 표에서 확인할 수 있는 바와 같이 IDS 시장 규모는 점차 감소하고 있으며, 네트워크 트래픽에 대한 필터링 기능과 차단 기능을 제공하는 IPS 장비는 대략 30% 정도의 성장률을 보이고 있다. 2005년도 현재 IPS 시장은 약 700 억원 이상을 형성하여 보안 시장을 주도할 것으로 예측된다.

기존 장비인 경우 아래 그림과 같이 크게 유선망 중심의 장비와 무선 트래픽을 대상으로 한 장비로 나눌 수 있다. 유선망에서의 트래픽 필터링 및 차단 장비는 이상탐지 기능 저하, 자체코드/검증문제, 성능 저하 및 트래픽 탐지 한계성 등의 문제점이 있다. 무선 LAN 기반 장비는 다양한 무선 트래픽 공격 유형에 적절히 대응하지 못하고 있어서 이에 대한 보완이 절실하다. 따라서 임베디드 기반 유무선 트래픽 필터링/차단 기술을 제공하는 장비 개발이 필요하다. 최근의 유무선 네트워크 공격에 대한 능동적인 대응 기

〈표 1〉 침임탐지/차단 시장규모 및 성장률

시장규모 및 성장률	2003	2004	2005	2006	2007	2008	성장률
IPS/IDS 총시장규모	337.5	481.9	594.5	703.1	787.3	888.0	18.7%
성장률	13.5%	27.6%	23.4%	18.3%	12.0%	12.8%	
IPS 시장규모	222.9	356.6	499.3	624.1	717.7	825.4	29.9%
성장률	45.9%	60.0%	40.0%	25.0%	15.0%	15.0%	
IDS 시장규모	154.6	125.3	95.2	79.0	69.5	62.6	-16.6%
성장률	-14.0%	-19.0%	-24.0%	-17.0%	-12.0%	-10.0%	

〈표 2〉 주요 IPS 제품 동향

분 류	제품명	회사명	기 능	비 고
IDS 기반의 IPS	드래곤 IPS	엔터라시스	이상탐지 기능 제공	유선망 기반
	스나이퍼 IPS	윈스테크넷	자체코드 /검증	-
	맥아피 인터루쉴드	NA	이상탐지 /차단 기능	-
	세이프존 IPS	LG엔시스	트래픽 탐지 성능	-
방화벽 기반의 IPS	인터셉트	체크포인트	침입탐지 기능	-
	NXG 시리즈	시큐아이닷컴	코드 /시스템보완	-
스위칭 기반의 IPS	디펜스프로	라드웨어	탐지/차단 성능	-
	AM IPS 5500	탑레이어	고속 탐지/차단	-
바이러스월기반 IPS	포티게이트	포티넷	바이러스 차단 기능	유선망 기반
무선랜 AP기반 IDS	AnyGate	AL Tech	무선트래픽 탐지한계	무선 LAN 기반

능을 제공하며, 무선 중심의 컴퓨팅 환경에 적용 가능한 필터링/차단 기능을 제공할 필요가 있다. 결국 임베디드 SW 기술을 이용하여 소형화된 통신기기에 탑재할 수 있는 침입탐지/차단 모듈에 대한 연구가 필요하다.

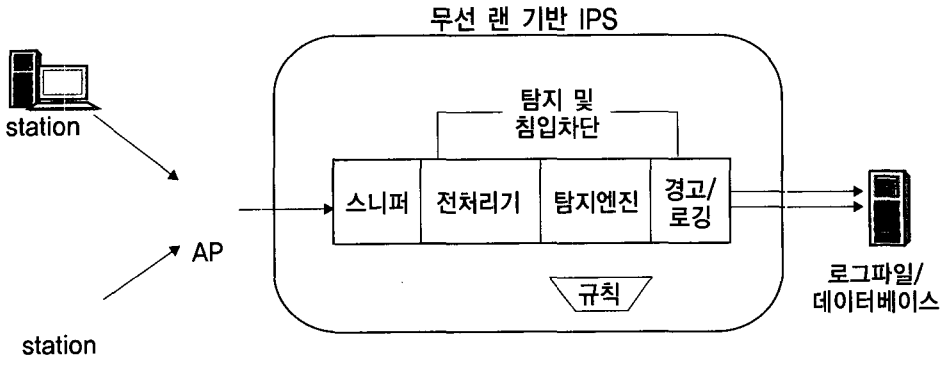
3. Wireless IPS 구조

Wireless IPS 시스템은 네트워크상에서 전송되는 트래픽에 대한 모니터링 기능을 수행하게 된다. 특히 AP를 통해 전송되는 트래픽에 대한 모니터링 기능을 통해 패킷 필터링 및 차단 기능을 제공하는 것을 목적으로 한다. 따라서 Wireless IPS 시스템 구성을 위해서는 IPS 센서(Sensor)를 유무선 네트워크 사이에 구축하여 무선 트래픽에 대한 모니터링 기능을 수행하게 된다.

일차적으로 Wireless IPS는 비인가 된 MAC 어드레스에 대한 검사 기능을 제공하고 공격 트래픽에 대한 차단 기능을 제공해야 한다. 무선 트래픽에 대한 차단을 위해서는 무선 트래픽에 대한 모니터링 기능을 제공하는 공개 소프트웨어를 사용하여 WLAN 트래픽에 대한 분석 및 추적이 가능하다.

802.1x 기반 WLAN은 손쉽게 공격 가능하다는 취약점을 보이고 있다. 무선 패킷에 대한 스니핑, 변조 및 조작 등을 탐지하고, AirJack 등의 DDoS 공격에 대해 AP 단에서 사전에 탐지/차단하는 기술을 제공한다. 구체적으로 패킷 스니핑, 룰 기반 침입탐지/차단 기능을 제공하는 임베디드 형태의 AP 통합형 고성능 IPS 모듈을 개발한다. 내부망 및 외부망에서의 패킷에 대한 실시간 검사 및 능동적 대응 방안을 제공하며, WLAN 환경에서 AP에 의해 전송되는 패킷에 대해 snort 기반 필터링 모듈을 적용하여 무선 LAN 환경에서의 공격에 대응한다. 무선 트래픽 역시 IDS와 같은 deep packet inspection 기능이 필요하고, in-line 모드로 구성하여 침입 방지/차단 기능을 제공한다.

무선 네트워크에 대한 IPS 기능을 제공하기 위해서는 AP를 통해 전송되는 무선 트래픽에 대해 아래

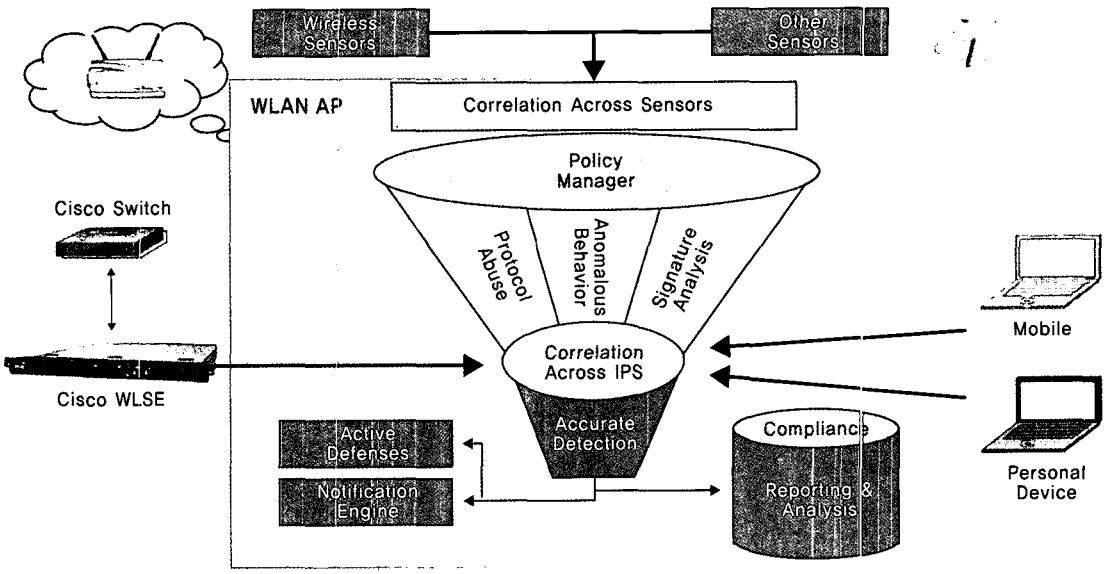


(그림 8) WLAN에서의 공격 대응을 위한 IPS 구조개요

그림과 같이 무선 센서(wireless sensor)를 통해 WLAN을 모니터링하게 된다. 무선 센서는 802.11 네트워크와 무선 트래픽에 대한 수집 기능을 제공한다.

4. Wireless IPS 시스템

현재 Wireless IDS/IPS 기능을 제공하기 위해 수행된 연구 결과는 AirMagnet[16,17], AirDe-



(그림 9) AirDefense Wireless IPS 시스템 구조도

fense[18] 등이 있다. Airmagnet 센서는 SQL DB를 기반으로 WLAN 관리 및 모니터링 기능을 수행한다. Rogue AP 탐지 및 추적 기능을 제공하며 DoS 공격에 대한 대응을 통해 무선 네트워크에 대한 안전성 확보를 목적으로 하고 있다.

AirDefense 시스템은 wireless AP 센서와 자바 기반 웹 콘솔 시스템으로 구성된 Red Hat 리눅스 서버로 구성되어 있다. AirDefense 웹 콘솔과 AP 센서는 서버와 안전한 무선 통신을 통해 트래픽에 대한 관리 및 차단 기능을 수행한다. AirDefense에서 제시하는 Wireless IPS는 정책 기반 IDS/IPS 시스템으로 네트워크에 대한 관리, 성능 및 안전성을 설정하며 WLAN 세션에 대한 보안 기능을 제공한다. 또한 일반적으로 리눅스 운영체제를 기반으로 공개 소프트웨어 형태로 개발되어 현재 활발한 연구가 진행되고 있으며 현재 Snort-Wireless[20] 및 WIDZ와 같은 코드가 제시되고 있다.

〈표 3〉 Wireless AP 탑재 보안 모듈 Spec

구 분	AP 보안 모듈	알고리즘
패킷 캡춰	Sniffer	-
전처리 모듈	MAC Spoof/Auth, De-Auth Detection	Using Hash Algorithm (SEED, HAS-160)
패킷 디코딩	TCP/UDP	Table/Pointer
패킷 스위칭	Packet Classification	Rule based Classification
프로토콜 파싱	TCP/UDP/IP	Snort based Parsing
인증 모듈	HMAC/Hashing	Hashed MAC
액션 핸들러	Action Engine	5 Action
키 관리	Kerberos	3-DES, IDEA

〈표 4〉 Wi-Fi Wireless AP 원격 모니터링 툴

구 분	AP 탑재 모듈	원격 관리 프로그램
적용 시스템	임베디드 A. P. 단말	윈도우 XP or 리눅스
CPU(clock)	Arm 계열(160M)	펜티엄 2G
OS	Embedded 리눅스	Windows XP or 리눅스
적용 프로토콜	WEP	-
개발언어	C/C++	C/C++/MFC
IPS Engine	Snort-inline	Monitoring
Script	Perl	Rule DB
Library	IPtable/Libpcap	-

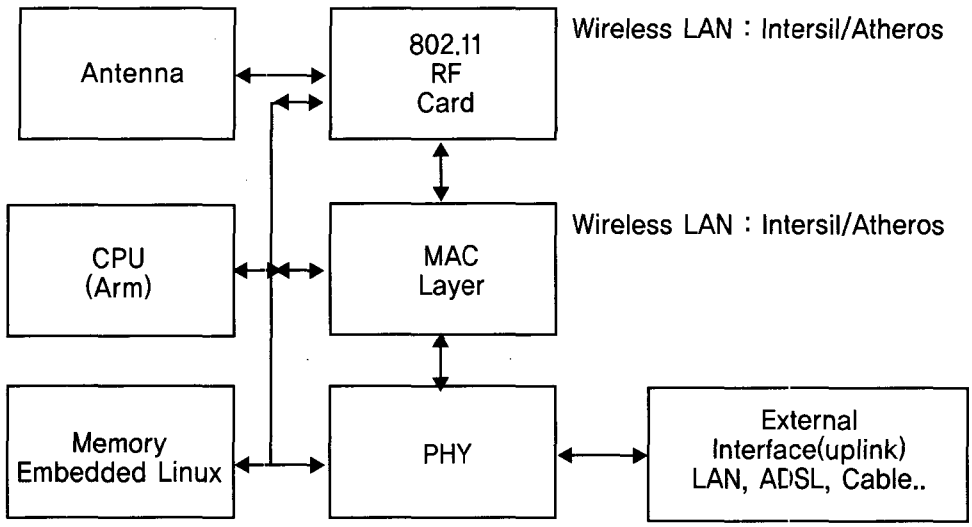
5. Wireless IPS 구성을 위한 무선 센서

Wireless IPS 시스템은 크게 중앙 집중 형태와 분산 형태의 두 가지 형태로 시스템을 구성할 수 있다. 중앙 집중형 IPS인 경우 중앙 관리 시스템을 통해 802.11 기반 무선 트래픽에 대한 처리 과정을 수행하는 경우이며, 분산형 IPS인 경우는 하나 이상의 장비를 통해 지역별로 무선 트래픽에 대한 필터링 및 공격 탐지/차단 기능을 수행하는 구조이다.

이와 같이 무선 네트워크에 대한 IPS 시스템을 구축하기 위해서는 공통적으로 Wireless AP에 대한 센서 구축 기술이 제시되어야 한다. Wireless IPS 시스템의 주요 역할은 침입탐지/차단 기능을 제공하기 위해 무선 트래픽 Signature 기반 탐지, 트래픽 감시, 폭주 방어 및 패턴 분석을 통한 DDoS 방어 기능을 제공한다. Wireless AP를 구축하기 위해 AP에 탑재하는 보안 모듈 spec과 AP 센서에 대한 원격 모니터링 툴 구성은 〈표 3〉과 같다.

유선망에서의 침입탐지/차단 기능과 유사하게 무선 트래픽에 대한 제어를 위해서는 snort-inline 방식의 필터링/차단 모듈을 적용하게 된다. 무선 트래픽 고유의 시그너처 정보를 추가로 검사할 수 있는 모듈을 설계/구현하여 WLAN 환경에서의 AP Traffic을 분석하며 각 서비스 별로 트래픽 감시 및 방지 기능을 제공한다. Wireless IPS 구성 요소 중에서 센서 AP에 대한 개발을 위해서는 임베디드 형태로 보안 모듈을 탑재하여 원격 관리 서버와의 네트워크 센서 기능을 제공한다.

센서 AP에 대한 설계 및 시험을 위해 임



(그림 10) WLAN AP 센서 내부 블럭도

베디드 리눅스 커널 포팅, 통신 프로토콜 설치 및 운용 프로그래밍 과정을 수행하고 WLAN 접속 및 데이터 송수신 운용 시험을 통해 센서 AP 시스템에 대한 성능을 검사한다. 센서 AP는 802.11 a/b/g 규격의 WLAN AP 단말기로 LinkSys와 같은 AP에 Firmware 형태로 탑재가 가능하다. Wireless IPS 센서 기능을 제공하는 WLAN AP 시스템 내부 블록도는 (그림 10)과 같다.

V. 결 론

Wireless IPS 시스템은 WLAN 네트워크의 안정적 운영을 위해 점차 필수적인 요소로 인식되고 있다. 물론 무선 네트워크에 대한 침입탐지/차단 기능을 제공하는 과정에서 전체적인 네트워크 성능 저하가 발생한다는 단점을 초래하기도 하지만, Wireless IPS 구축을 통해 무선 프로토콜 상에서의 보안 취약점을 해소하고 해킹 및 DoS 공격으로부터 안정성을 확보할 수 있다는 장점을 제공한다. 현재 기존의 유선망 기반 IPS 시스템에 무선 트래픽에 대한 차단 기능까지 제공하는 유무선 통합형 IPS 시스템으로 발전하고 있으며 이를 위해서는 센서 AP를 기반으로 무선 트래픽에 대한 침입탐지/차단 기능을 제공하는 방식으로 연구가 진행되고 있다. 802.11 기반 WLAN 뿐만 아니라 WiBro, WiMAX 등 무선 네트워크 환경은 더욱 확대될 것으로 예상되기 때문에 본 연구에서 고찰한 Wireless IPS 기술 역시 적용 범위가 넓어질 것으로 기대된다.

[참 고 문 헌]

[1] 전용희, "침입방지시스템(IPS)의 기술분석 및

성능평가 방안" 정보보호학회지, 제 15권, 제 2호, pp.63-73, 2005

[2] 조현정, "차세대 네트워크 보안기술 기반의 침입방지시스템" 정보과학회지, 제 23권, 제1호, pp.21-26, 2005

[3] 정보홍, 김정녀, 손승원. "침입방지시스템 기술 현황 및 전망" ETRI IT정보센터, 주간기술동향 1098호, 2003

[4] 전원용, 김은희, 신문선, 류근호, "점진적 연관규칙을 이용한 침입탐지 시스템의 오경보 패턴 분석 프레임워크 설계", 한국정보과학회, Vol,31, No2, 2004

[5] 이은영, 김병학, 박찬일, 정상갑, 임채호, 이광형 "NIDS에서 False Positives를 줄이기 위한 동적 중요도 계산 방법에 대한 연구", 정보보호학회지, 제 13권 제1호, pp.22-31, 2003

[6] 김길한, 이형우 "kNN학습을 이용한 시그너처 기반 IPS의 오탐지 최소화 기법", 2005

[7] R. Lippman et als., "Evaluation intrusion detection system : The 1998 DARPA Off-line intrusion detection evaluation." Proc. Of DARPA Information Survivability Conference and Exposition, pp.12-26, 2000

[8] Cuppens, F.. Miege, A. "Alert correlation in a cooperative intrusion detection framework", In Proceedings of the IEEE Symposium on Security and Privacy, 2002

[9] H. Debar, A.Wespi, "Aggregation and Correlation of intrusion-Detection Alert", In Recent Advances in intrusion Detection, number 2212 in Lecture Notes in Computer Science, pp.85-103, 2001

[10] 김경곤, "WLAN Security & Hacking and Next Generation Wireless", A3SC

[11] Matthew Gast, "802.11 Wireless Networks: The Definitive Guide", OReilly, Apr., 2002

[12] Bruce Potter, "802.11 Security", OReilly, Dec., 2002

[13] John Wiley & Sons, "Building Secure Wireless Networks with 802.11", Jan., 2003

[14] Ken Hutchison, "Wireless Intrusion Detection Systems" GIAC Security Essentials Certification (GSEC), 2004

[15] Barken, Lee, "WEP Vulnerabilities - Wired Equivalent Privacy? in: How Secure is Your Wireless Network? Safeguarding Your Wi-Fi LAN" http://www.phptr.com/articles, 2003

[16] Borque, Lyne, "Wi-Fi Security Review: AirMagnet", http://www.enterpriseitplanet.com/security, 2004

[17] http://www.airmagnet.com

[18] http://www.airdefense.com

[19] http://www.networkchemistry.com

[20] http://snort-wireless.org/

[21] http://www.snort.org/

이형우

1994년 고려대학교 컴퓨터학과 졸업(이학사)
1996년 고려대학교 컴퓨터학과 졸업(이학석사)
1999년 고려대학교 컴퓨터학과 졸업(이학박사)
1994년 ~ 1996년 (주)삼성전자 산학연구원
1996년 ~ 현 재 컴퓨터과학기술연구소 연구원
1999년 ~ 2003년 천안대학교 정보통신학부 조교수
2003년 ~ 현 재 한신대학교 소프트웨어학과 부교수
관심분야 : 정보보호, 네트워크 보안, 해킹 · 바이 러스, 침해대응/스팸대응 기술, 컴퓨터 포렌식스 기술 등