차세대 무선랜 보안 기술

Cyber Security Research Department
사이버보안연구단

디바이스 보안 분석 연구실

김신효

ETRI 한국전자통신연구원 www.etri.re.kr

2013. 12. 4.

차 례

I 기술 개요

II 시장 및 기술 동향

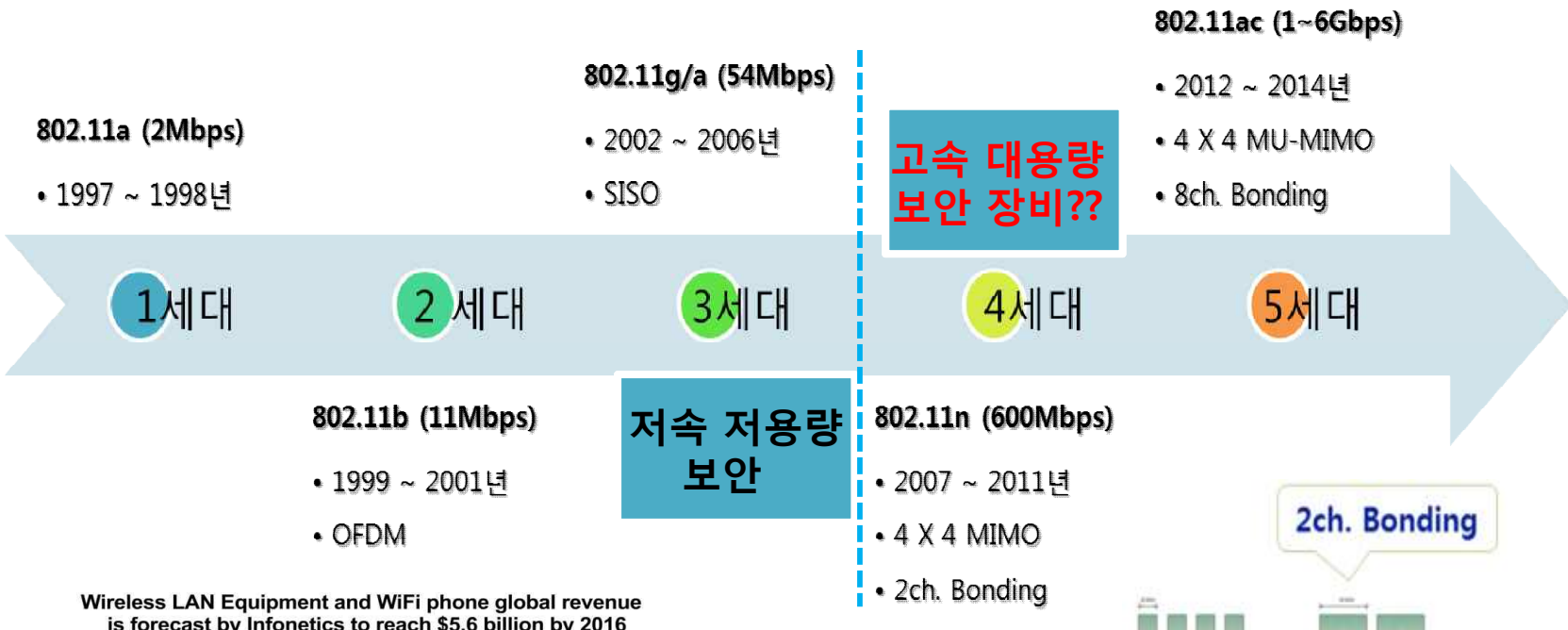
III 휴대형 무선랜 취약성 분석 도구 기술

IV MAC 위장 디바이스 탐지 기술

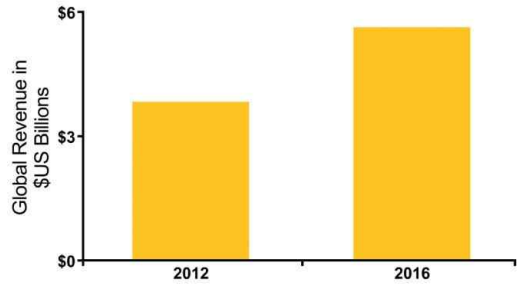
V 활용 분야

기술 개요 – 무선랜

- 스마트폰의 폭발적 증가 & **기가급 5세대(차세대)무선랜**
  ➔ 무선랜 사용 확산 가속화



Wireless LAN Equipment and WiFi phone global revenue is forecast by Infonetics to reach $5.6 billion by 2016



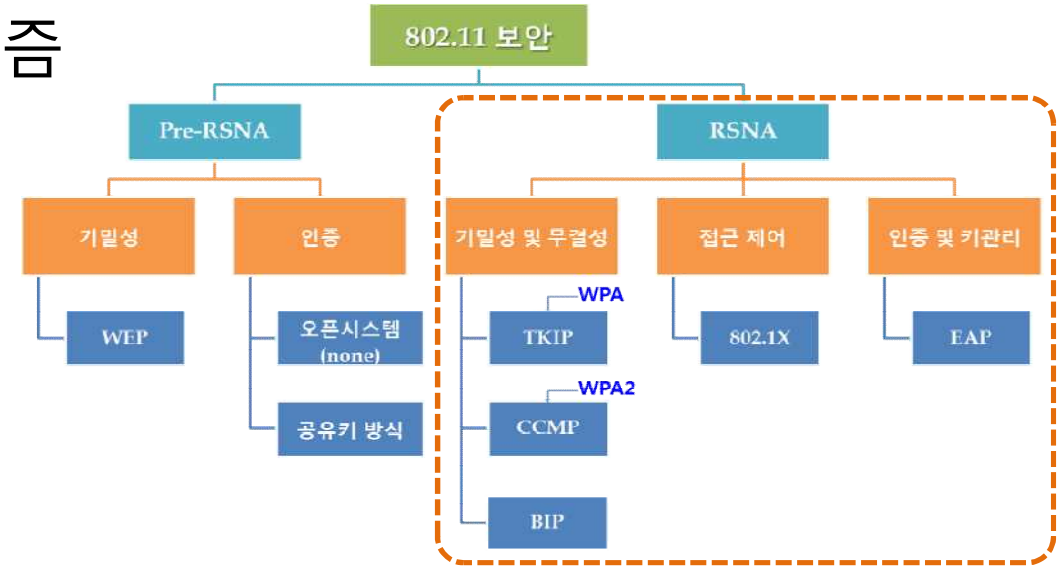
© Infonetics Research, *Wireless LAN Equipment and WiFi Phones Market Share, Size, and Forecasts*, Aug. 2012

* MIMO :Multi-Input Multi-Output

기술 개요 – 무선랜 보안

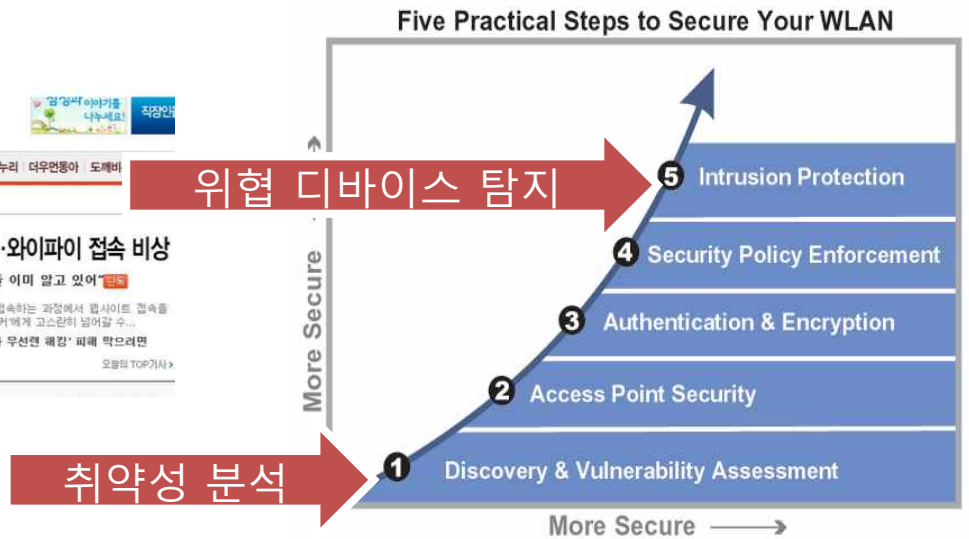
802.11 보안 메커니즘

- RSNA :
  Robust Security
  Network Association



- 제도/관리적인 수준의 "안전한 무선랜 이용 수칙 발표

➲ 현실



http://www.airdefense.net/eNewsletters/5stepsfeature.shtm

시장 및 기술 동향

무선랜 보안 관련 제품/서비스 시장 규모

- 무선랜 장비 시장 규모는 2016년 56억달러

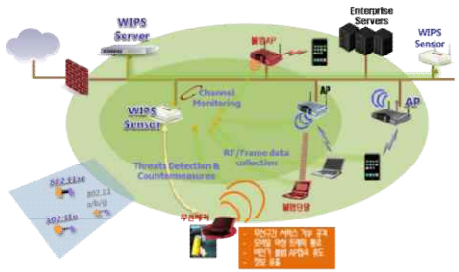
	2012년	2013년	2014년	2015년	연평균성장율
무선네트워크 보안 제품	213	375	660	1,161	76.0%
모바일 보안 제품	264	367	509	707	38.9%
합계	477	742	1,169	1,869	

* 무선/모바일 보안 제품 시장('국내 정보보안산업 실태조사' KISA, 2012년)

관련 기술 동향

- IEEE 802.11그룹과 Wi-Fi Alliance는 무선랜 PHY/MAC 전송 규격, 매쉬네트워크, 타네트워크연동, 상호 운용성 등 무선랜 표준화 진행
  - Gbps급 초고속 무선랜 표준화 완료 단계
  - 무선랜 보안 표준(WPA/WPA2, 802.11w 등)에 대한 장비인증
- 무선네트워크의 잘못된 설계/운용/설정으로, 표준을 준수 여부와 무관하게 운용상 보안 취약점은 존재

국내외 제품/서비스 동향

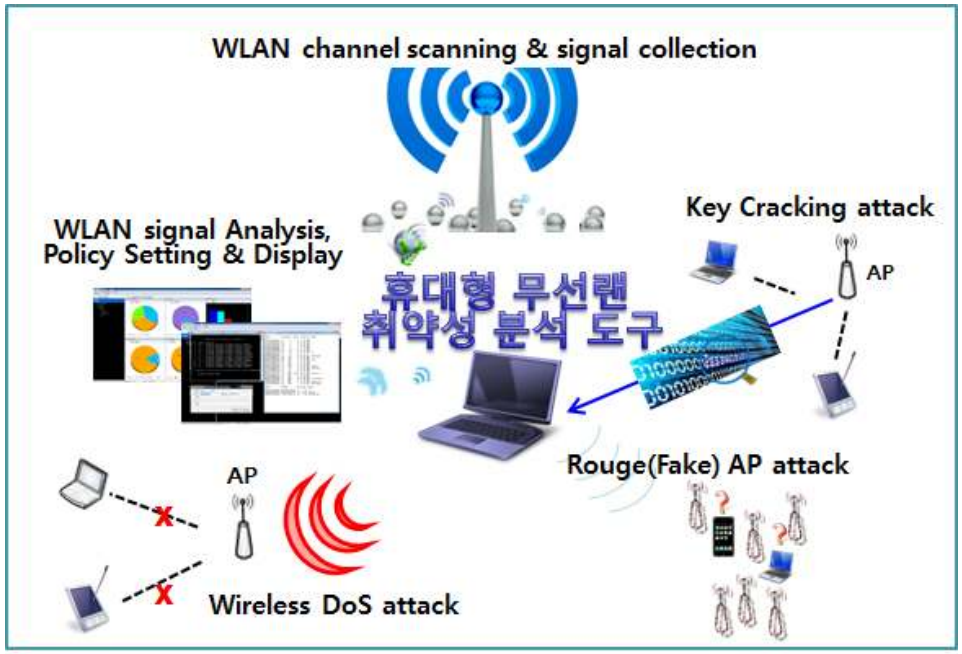


- 무선랜 침입 탐지 및 방지(WIDS/WIPS) 제품은 대부분 외산 솔루션 도입, 일부 국내 제품 출시
- 유무선 통합 보안관제 서비스
- 휴대형으로 무선랜 분석과 모의 공격을 연동하여 무선랜 취약성 분석에 특화된 제품은 국내외적으로 전무

휴대형 무선랜 취약성 분석 도구 기술 (1/4)

기술 정의

- 사용자 친화적인 실시간 무선랜 취약성 분석 도구
- 휴대형 장치에 장착하여 무선네트워크의 채널 감시, 신호 분석, 무선랜 단말 연결 상태 및 패킷 분류로 보안 현황을 다양한 그래픽으로 분석하고,
- 분석 결과를 이용하여 무선랜 모의 공격을 수행해 봄으로써 분석 대상 네트워크의 보안 취약점을 간편하게 진단하는 SW 도구



휴대형 무선랜 취약성 분석 도구 기술 (2/4)

주요 내용

- 무선랜 네트워크 분석 기술
  - 무선랜 카드/채널 설정 및 스케줄링 모듈
  - 무선랜 채널 분석 및 L2 프레임 수집/분류 모듈
    - ✓ L2 패킷 수집, 분류, 분석, 필터링, 저장/불러오기
  - 무선랜 패킷 분석/공격 결과 확인 모듈
    - ✓ 무선랜 신호 분석 결과에 대한 대시보드
    - ✓ AP-단말 정보, 연결상태 확인, 관심 AP/단말 등록

- 취약점 분석 및 모의 공격 에뮬레이션 연동
  - Fake AP 공격
  - WEP/WPA 키 크래킹 공격
  - DoS 공격 등 연동

휴대형 무선랜 취약성 분석 도구 기술 (3/4)

기술의 우수성 (경쟁기술과 비교)

- 백트랙(BackTrack)
  - 모의침투 (Penetration) 테스트를 위한 리눅스 오픈 소스
  - 무선랜 모의공격을 포함하나, 무선랜 신호 분석은 별도의 툴 필요
- 무선랜 신호 분석 SW
  - 무선랜 모니터링, 분석 결과에 대한 디스플레이 제공, 무선랜 모의 공격 기능 미포함
  - 유무선 패킷 분석 등 다양한 기능이 내장된 반면 고비용 도구임

➔기존 기술은 무선랜 분석과 모의공격을 별도의 도구로 수행하여, 고비용이고 사용이 불편함

경쟁/대체 기술	본 기술의 우수성
백트랙 (모의 해킹)	❖ End-user에 의한 사용편의성을 위해 윈도즈 상에서 운용 ❖ 무선랜에 특화하여 무선랜 분석 정보와 바로 연동하는 모의 공격 및 공격 확인이 가능함
무선랜신호분석 SW (에어마그넷/에어로피크)	❖ 무선랜 모니터링, 분석 결과에 대한 디스플레이와 모의공격을 연동 수행함 ❖ 외산 솔루션에 비해 저비용

휴대형 무선랜 취약성 분석 도구 기술 (4/4)

기술의 사업성

▪ 시장 환경

- 무선랜 보안 관련 시장이 연평균 56% 수준으로 급성장
- 무선랜에 대한 보안 취약점에 대한 인식이 커지고 있어, 취약성 분석 서비스 필요성 증대

▪ 예상 응용 제품 및 서비스

예상 제품/서비스	예상 수요자(층)
휴대형 무선랜 취약성 분석 도구	❖ 무선랜을 사용하는 중소 규모 업체 및 공공기관/학교, 보안 컨설팅 업체 등

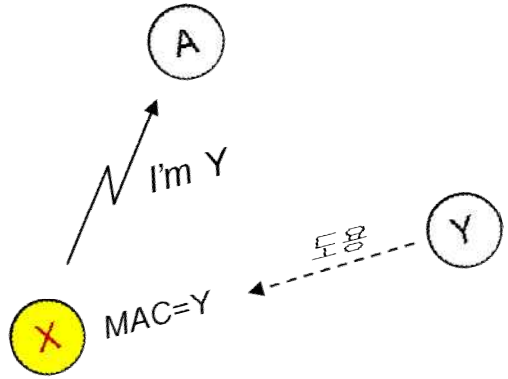
▪ 경쟁력

- WIPS에 취약성 분석 기능 내장 : WIPS 제품에 고부가 가치 부여
- 무선랜 보안 분석 제품화 : 가격경쟁력 우수 (기존 무선랜 분석 단독 제품 5,000천원~30,000천원 수준)
- 현재, 윈도 플랫폼에서 GUI 기반으로 무선랜 분석과 모의 공격이 가능한 제품은 없음

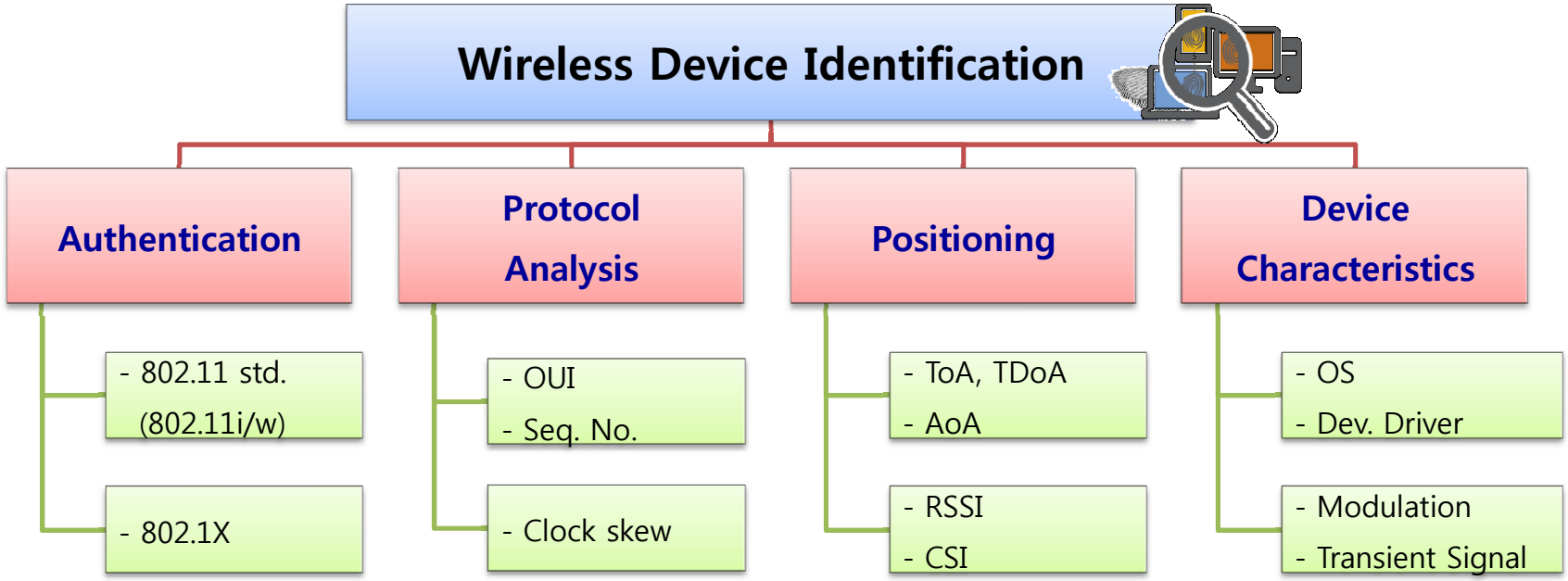
MAC 위장 디바이스 탐지 기술 (1/4)

기술 개요

- MAC 주소 위조에 의한 무선랜 보안 취약성
  - Deauthentication 공격
  - Disassociation 공격
  - Power-saving 공격
  - **AP/단말 위장 공격**



➔ MAC 위조를 판단하는 무선 디바이스 식별 기술 필요

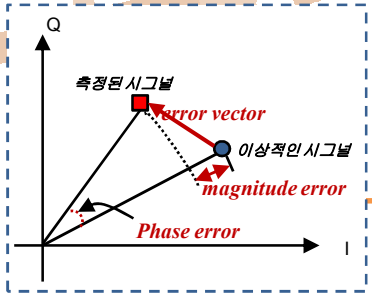


ToA : Time of Arrival
TDoA : Time Difference of Arrival
AoA : Angle of Arrival
RSS : Received Signal Strength Indicator
CSI : Channel State Information

MAC 위장 디바이스 탐지 기술 (2/4)

- 기술 정의
  - 무선랜 디바이스 고유의 **물리적 특징**을 인지하여 MAC 주소를 위장 또는 복제하는 디바이스를 식별하고 불법을 탐지하는 HW 센서 및 SW 기술

* RF Fingerprint : 디바이스의 물리계층에서 나타나는 독특한 RF 신호 특성 (예: QPSK에서 변조 에러)



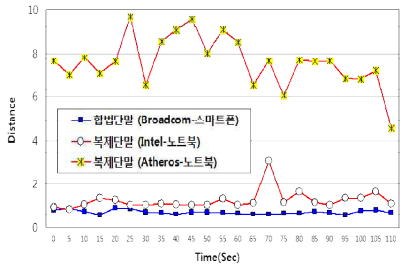
- 주요 내용
  - 탐지센서 SW 구성
    - 추출 : RF 특성 정보
    - 학습 : 합법 단말의 RF 지문 학습 및 등록
    - 탐지 : K-NN(또는 SVM) 등 학습 기반의 위장/복제 단말 탐지
  - 탐지센서 HW 제원
    - QCA(Athoros) 무선랜 칩, 저전력 인텔 CPU 등

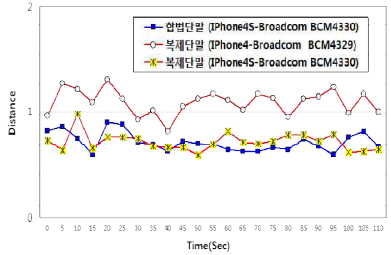
MAC 위장 디바이스 탐지 기술 (3/4)

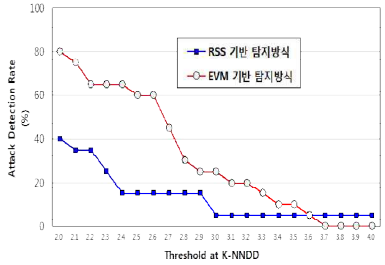
기술의 우수성

- 센서 레벨에서 RF 지문을 이용하여 MAC 위장/복제 디바이스를 식별하는 원천 기술 확보
  - RF 지문 기술 feasibility test 완료
    - ✓ 무선랜 센서 기반 실시간 RF 지문 추출/분석/탐지
    - ✓ HW로부터 RF 특성값(무선 지문) 정보를 직접 추출하는 기술
      * 기존방식은 무선 계측장비를 통한 RF 특성값 추출 수준

  - 고정형 무선 디바이스 식별 성능







- 다양한 무선 환경에서 디바이스 식별에 활용 가능

MAC 위장 디바이스 탐지 기술 (4/4)

기술의 사업성

시장 환경

- 2013년 국내 WIPS 시장 규모는 대략 200억원대, '12년 대비 20% 상승
  (출처 : ciociso 매거진 자료)
- 국내 WIPS는 에어타이트, 아루바, 시스코 등의 국외업체가 70% 이상 선점
- 하지만, MAC 주소 복제를 통한 불법 접속을 근본적으로 막을 수 없음

예상 응용 제품 및 서비스

예상 제품/서비스	예상 수요자(층)
무선 침입탐지/방지 시스템 (WIDS/WIPS)	❖ 무선 보안 업체 ❖ 기업, 공공기관 등 무선랜 보안 제품 수요자

- 외산에 비해 열세인 국산 WIPS 제품에 내장하여 기술적 차별화 가능

기타

- WIPS 센서에 내장한 RF지문 기반 MAC위장 디바이스 탐지 기술은 독창성을 지님
- 모바일 디바이스의 폭발적 증가로 RF 지문을 포함하는 **무선 지문 (Wireless Fingerprint) 기술의 높은 시장성** 기대

기술 활용 분야

기술이 적용될 수 있는 산업 분야의 범위

기술이 적용되는 제품/서비스

- 기업 및 공공 부문 무선랜 보안 서비스
- 무선랜 보안 컨설팅 도구
- WIPS 센서 또는 AP 제품의 보안 기능 모듈로 내장
- 가격 경쟁력 있는 무선랜 취약점 분석 도구 제품화
- 보안 제품군(WIPS, 유무선보안관제 등) 판매 촉진에 활용