2020 한국정보보호학회 호남지부 추계학술대회

국내 무선랜 보안 지침 개정 연구 : 무선랜 통합 실태 분석을 통한 개선 사항 식별

고지웅, 공재호, 권영우, 김남석, 김유현, 정효종, 김홍진

한국정보기술연구원 차세대 보안리더 양성 프로그램(Best Of the Best)

배경

- 국정 100대 과제 '공공 와이파이 확대'
- 5G 도입 및 상용화
- Mobile Device, IoT 등 각종 무선랜 관련 시장 확대
- WiFi에 대한 요구가 기하급수적으로 증가

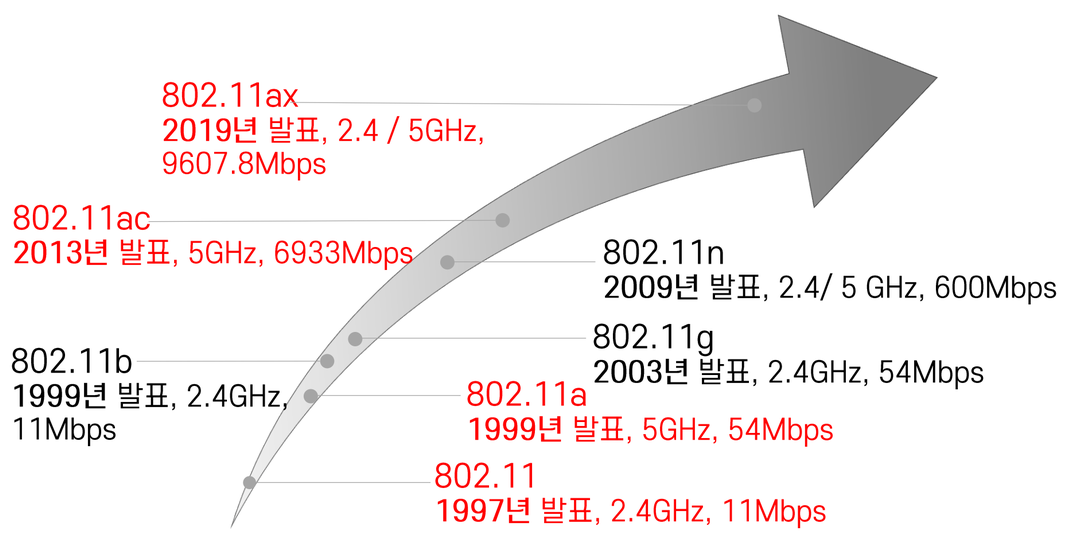
연구의 필요성

- 무선랜 보급의 증가로 무선랜 해킹 위협 증가
- 최신 무선랜 보안 안내서가 필요한 실정
- IEEE 802.11ac, IEEE 802.ax,WPA3와 같은 중요 이슈들 발생
- 중요 최신 이슈가 반영된 최신 보안 지침의 부재
- 따라서, 무선랜 보안 지침 개정 필요

기존에 진행된 내용

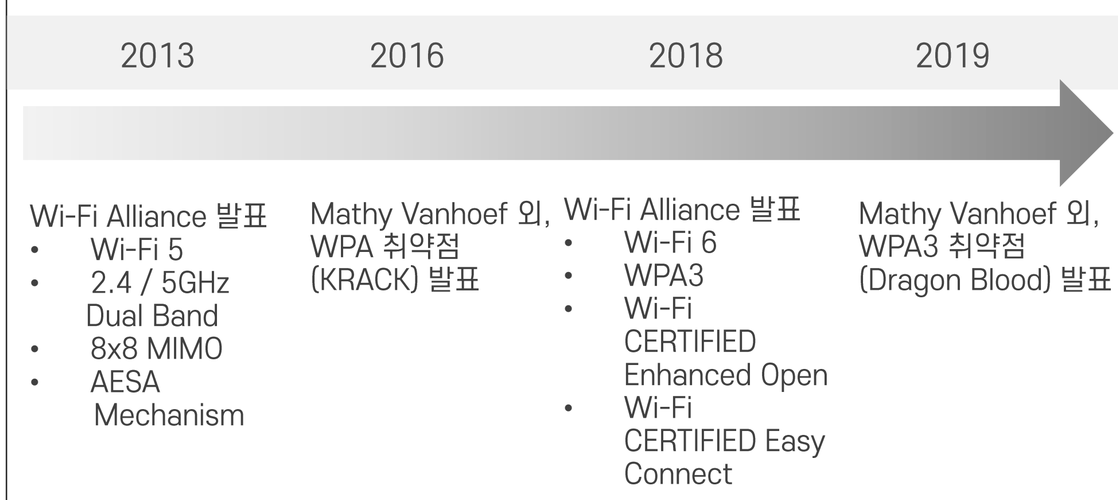
- 한국인터넷진흥원(KISA) '무선랜 보안 안내서' (2011년 개정)
- 한국정보통신기술협회(TTA) '안전한 무선랜 사용 지침' (2011년 개정)
- 2011년 이후 보안 지침이 개정되지 않음
- 그 외 국내 최신 무선랜 보안 자료는 찾을 수 없음

개정 내용 ① : IEEE802.11 무선랜 표준



개정 내용 ② : 용어 및 신규 이슈

2011년과 2020년 사이에 발표된 무선랜 용어 및 이슈 반영 추가 필요
(아래 사진은 일부 예시)



개정 내용 ③ : 위협 모델

Microsoft에서 고안한 STRIDE 위협모델이 사이버 보안의 취약성을 효과적으로 파악할 수 있다는 점에 주목하여 채택하였다. 이를 활용하여 기존 기술적 보안 위협을 식별하고 관련 항목을 개정하였다.

< 개정 전 > → < 개정 후 >

구분		세부 위협 내용
물리적 보안 위협	TP01	무선 장치에 대한 물리적 보안 위협
	TP02	무선 단말기에 대한 물리적 보안 위협
기술적 보안 위협	TT01	무선랜 이용자에 대한 도청
	TT02	무선 AP에 대한 서비스 거부
	TT03	가짜 AP (불법, Rogue/Fake AP) 설치
	TT04	무선 AP에 설정된 암호 크랙
	TT05	무선랜에 대한 비인가 접근
관리적 보안 위협	TM01	무선랜 장비 관리 미흡
	TM02	무선랜 사용자의 보안의식 결여
	TM03	전파관리 미흡
환경적 보안 위협	TE01	공중 무선랜을 이용한 악성코드/스팸 유포
	TE02	기업용 무선랜을 이용한 기업 내부 네트워크 침투
	TE03	초기 보안 설정 유지에 따른 무단접속 허용

구분		세부 위협 내용	
물리적 보안 위협	TP01	무선 장치에 대한 물리적 보안 위협	
	TP02	무선 단말기에 대한 물리적 보안 위협	
기술적 보안 위협	TT01	무선랜 이용 시 취약한 암호 설정	WEP
			WPA
			WPA2
			WPA3
	TT02	무선랜 이용 시 통신 침해	트래픽 수집
			트래픽 변조
			트래픽 탈취
	TT03	공격자의 무선 기기 위장	AP/Station 도용
			비인가 AP 설치
	TT04	서비스 거부	전원/성능 제한
			인증/접속 제한
관리적 보안 위협	TM01	무선랜 장비 관리 미흡	
	TM02	무선랜 사용자의 보안의식 결여	
	TM03	전파관리 미흡	
	TM04	초기 보안 설정 유지에 따른 무단접속 허용	

개정 내용 ④ : 대응 가이드와의 맵핑

위의 STRID 모델을 통해 개편된 위협모델을 반영하여 재구성 된 "무선랜 보안 위협과 대응 가이드 분류"는 다음과 같다.

대응가이드 \ 보안위협			물리적 위협		기술적 위협				관리적 위협			
			TP 01	TP 02	TT 01	TT 02	TT 03	TT 04	TM 01	TM 02	TM 03	TM 04
정책 및 관리	운용현황 및 장비관리	DME 01				√						
		DME 02					√					
		DME 03	√	√					√			
		DME 04							√			√
		DME 05	√	√	√	√	√	√	√	√	√	√
	네트워크	DMN 01										√
		DMN 02									√	
		DMN 03									√	
보안기술 (솔루션) 도입		DTS 01				√						
		DTS 02				√	√					
		DTS 03			√				√			√
		DTS 04					√	√			√	
정보보호 인식제고		DSA 01	√	√	√	√	√	√	√	√	√	√
		DSA 02	√	√	√	√	√	√	√	√	√	√
		DSA 03							√			

추후 기대 방향

- 국내 신규 무선랜 위협 모델 제작
- 무선랜 보안 연구에 최신 참고자료가 될 것
- 무선랜 보안 교육, 컨설팅 다양한 분야에 활용가능

향후 연구 예정 사항

- 개편된 무선랜 위협모델을 바탕으로 취약점 진단 연구
- 무선랜 진단 툴 제작 및 연구
- 무선랜 위협 대응가이드 연구