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)

Study on Revision of Domestic Wireless LAN Security Guidelines: Identification of Improvements By Analyzing the Status of Wireless LAN Integration

Ji-Woong Ko, Jae-Ho Kong, Young-Woo Kwon, Nam-Seok Kim, Yu-Hyun Kim, Hyo-Jong Chung, Hong-Jin Kim

KITRI 차세대 보안리더 양성 프로그램(Best Of the Best)

요 약

모바일 장치, 사물인터넷 등의 시장이 확대됨에 따라 무선랜에 관한 관심은 증대되었다. 그러나 무선랜 기술에 대한 보안은 2011년 국내 무선랜 보안 지침이 발간된 이래로 추가적인 제·개정이 이루어지지 않았기에, 이후에 발표된 WPA3, IEEE 802.11ac 등과 같은 내용은 확인할 수 없었다.

이에 무선랜 보안 표준 개정의 필요성을 파악하여 개선 방향성을 제시하고자 한다. 따라서 본 논문은 무선랜 통합 실태를 분석하여 이를 바탕으로 신규 기술 및 동향을 적용한 물리·관리·기술 기준의 개선 방안을 연구한다. 결과적으로 기존 보안 지침을 개선하도록 제시하였으며 이를 통해 개정된 지침은 교육, 진단 등의 부문에 활용할 수 있을 것이다. 이는 더 나아가 무선랜 보안기술 활성화에 기여할 것이라 기대된다.

I. 서론

최근 모바일 장치, 사물인터넷 등 각종 무선랜 관련 기기들의 시장이 확대되고 있다. 이러한 스마트 기기들의 폭발적인 증가로 어디서나 인터넷에 접속하기 위해 'WiFi'에 대한 요구 역시 기하급수적으로 늘어나고 있다. 이에 따라 고객을 유치 및 유지를 위하여 통신망 회사와 각종 점포 운영자들은 무선랜 보급에 힘쓰고 있다. 또한, 국가적으로도 공공와이파이 확대 사업을 진행할 정도로 무선랜에 관한 관심은 늘고 있다.

그러나, 무선랜의 보급이 늘어난 만큼 무선랜 해킹 위협 역시 늘고 있다. 이에 따라 무선랜 관리를 위한 최신 보안 안내서가 필요하지만, 2011년에 개정된 한국인터넷진흥원 (이하 KISA) '무선랜 보안 안내서'와 2011년에 개정된 한국정보통신기술협회 (이하 TTA) '안전한 무선랜 사용 지침' 등은 오랜 시간 개정되지 않았다. 따라서 이후 발표된 IEEE 802.11ac, IEEE 802.11ax, WPA3와 같은 중요 이슈들이 반영된 무선랜 보안 지침을 확인할 수 없는 실정이다.

따라서 본 논문은 2020년을 기준으로 무선랜 환경의 실태를 통합적으로 분석하였으며 이를 바탕으로 하여 새로운 이슈를 적용한 무선랜 보안 표준의 개선 방안을 연구한다. 이를 통해 무선랜 보안 지침의 개정의 필요성을 알리고 본 논문이 무선랜 보안 연구를 위한 자료로 활용될 수 있을 것이라 예상된다.

II. 본론

1. 개정범위

본 논문에서는 TTA에서 발간한 '안전한 무선랜 사용 지침'을 기준으로 보안 표준의 제· 개정이 필요성을 확인했다. 기존 TTA의 지침이 발간된 이래로 오랫동안 제· 개정이 이루어지지 않았기에 신기술 등의 내용을 적용한 제· 개정 방향성을 제시한다.

1.1 IEEE 무선랜 표준

무선랜(IEEE 802.11) 기술은 지속해서 발전되어 왔으며 기존 TTA의 지침은 2011년에 선정되었기에 2009년 무선랜 표준으로 정해진 802.11n 표준에 관한 내용까지 설명하고 있다. 따라서 이후 발표된 표준의 내용도 추가가 요구된다.

1.2 용어 설명

기존 TTA 지침의 목차는 무선랜 일반 용어, 무선랜 장비 용어, 무선랜 보안 용어 등으로 용어에 대한 설명을 제시하고 있다. 본 논문에서는 기술이 발전하며 새롭게 추가되어야 하는 지침에서 누락 된 용어에 대해 제·개정 하였다.

1.3 위협모델

기존 TTA에 채택된 '안전한 무선랜 사용을 위한 지침'에서 정한 무선랜 보안 위협모델은 2011년 기술을 기반으로 수립된 이래로 최신화가 이루어지지 않았다.

무선랜 기술이 발전함에 따라 보안 위협 역시 발전하였으며, 2011년 대비 공격 영역(Attack Surface)은 더욱 확장되었다.

기존 공격 영역 및 신규 무선랜 기술 요소를 대상으로 새로운 공격 기술이 개발/도입되었고 이는 결과적으로 위협 인지 필요성의 증대를 요구한다. 따라서 본 논문은 무선랜 신규 기술 개발 및 현황을 기반을 둔 개선된 위협모델을 제안하고자 한다.

Table 1. 기존 TTA 무선랜 보안 위협모델

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

추가로, 기존의 위협모델은 물리적, 기술적, 관리적 보안뿐 아니라 환경적 위협으로도 분류한다. 그러나 보안 프레임워크에서 각 위협을 물리적·관리적·기술적으로 분류하는 것이 일반적이며, 환경적 위협에 기재된 내용이 나머지 위협에 분류될 수 있음을 파악하여 이를 개편하였다.

1.4 정보 보호 가이드

기존 TTA 지침의 정보 보호 가이드는 정책 및 관리, 보안기술 도입 그리고 정보 보호 인식 제고 3가지로 분류되어 제시된다. 이후 제시된 각 가이드 항목들과 관련된 위협들을 분류한다. 이에 따라 개편된 위협모델을 토대로 분류의 재구성이 요구된다.

.

2. 개정 내용

앞서 제시한 개정범위를 토대로 제· 개정에 필요한 내용을 상술한다.

2.1 개정된 IEEE 무선랜 표준 및 특징

기존 TTA에 채택된 안전한 무선랜 사용을 위한 지침이 2011년에 마지막으로 개정됨에 따라 표준으로 정해진 2013년의 802.11ac, 2019년의 802.11ax에 관한 내용이 포함되어있지 않았다. 새로운 무선랜 표준을 포함한 내용 추가의 필요성을 확인했다.

Table 2. 새로운 표준이 추가된 무선랜 표준 리스트

무선랜 표준	제정 시기	주파수 대역	데이터 속도(최대)
802.11	1997	2.4GHz	2Mbps
802.11a	1999	5GHz	54Mbps
802.11b	1999	2.4GHz	11Mbps
802.11g	2003	2.4GHz	54Mbps
802.11n	2009	2.4 / 5GHz	600Mbps
802.11ac	2013	5GHz	6933Mbps
802.11ax	2019	2.4 / 5GHz	9607.8Mbps

2.2 추가 용어

기존 지침이 개정된 이래로 기술이 발전하여 무선랜 주요 기술에 대한 현황을 분석한 결과 아래와 같은 변화들을 파악했다.

- 2016년, Mathy Vanhoef 외, WPA2 취약점 (KRACK) 발표
- 2018년, Wi-Fi Alliance, Wi-Fi CERTIFIED Enhanced Open 발표
- 2018년, Wi-Fi Alliance, Wi-Fi CERTIFIED Easy Connect 발표
- 2018년, Wi-Fi Alliance, WPA3 발표
- 2019년, Mathy Vanhoef 외, WPA3 취약점 (Dragon Blood) 발표

따라서 현재 현황을 반영하여 WPA3, SAE 등과 같은 용어 추가가 필요함을 확인했다.

2.3 위협모델

앞서 서술하였듯이 본 논문에서는 기존의 무선랜 사용 지침을 개선하기 위해 환경적 보안 위협 항목을 제외하였다. 기존의 환경적 위협에 있던 TE03은 관리적 위협으로 분류함에 따라 관리적 위협의 TM04로 추가하였다. 기존의 TE01과 TE02는 무선랜을 활용한 연계 공격이므로 무선랜 위협모델에 들어가기에 적합하지 않아 제외하였다.

기술적 보안 위협 항목의 세부 위협 내용을 상세하게 분류하여 신규 기술 및 동향을 적용했다. Table 3과 같이 개선된 무선랜 보안 위협 모델을 제안한다.

Table 3. 개편된 무선랜 보안 위협모델

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	

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

위 모델링을 토대로, 지침이 개정된 이후 화제가 된 KRACK, Dragon Blood, Captive Portal을 활용한 FakeAP 공격 등 신규 취약점을 포

함하기 위해 각 항목을 더 상세하게 분류하였다.

STRIDE 위협모델의 각 항목은 다음과 같다.

Table 4. STRIDE 위협 모델(Microsoft)

Spoofing identity
Tampering with data
Repudiation
Information disclosure
Denial of service
Elevation of privilege

이를 적용하여 기존 기술적 보안 위협의 세부 위협 내용을 구분하였으며 이에 대한 상세 내용은 다음과 같다. 각 구분에 STRIDE 각 항목이 중복 없이 포함될 수 있는 것을 볼 수 있다.

Table 5. STRIDE가 적용된 기술적 위협모델

TT01	무선랜 이용 시 취약한 암호 설정	WEP	I,E
		WPA	
		WPA2	
		WPA3	
TT02	무선랜 이용 시 통신 침해	트래픽 수집	T,R
		트래픽 변조	
		트래픽 탈취	
TT03	공격자의 무선 기기 위장	AP/Station 도용	S
		비인가 AP 설치	
TT04	서비스 거부	전원/성능 제한	D
		인증/접속 제한	

2.3.1 무선랜 이용 시 취약한 암호 설정

무선랜에 이용되는 Access Point의 보안 설정이 제대로 설정되어있지 않은 경우, 공격에 취약해진다. 따라서 안전한 암호화 방식을 선택·설정하여 데이터의 암호화가 필요하다.

2.3.2 무선랜 이용 시 통신 침해

무선 패킷에는 많은 정보가 담겨있다. 사용자가 송수신하는 패킷을 탈취하여 공격에 필요한 정보를 수집할 수 있다. 수집된 정보를 바탕으로 변조된 패킷을 보내어 공격에 사용할 수 있다.

2.3.3 공격자의 무선 기기 위장

AP나 Station의 MAC, SSID 등을 모방·도용하여 사용자에게 접속하도록 유인한 후 중요한 정보를 수집할 수 있다.

2.3.4 서비스 거부

서비스 거부(DoS)는 무선 AP 기기에 대량의 무선 패킷을 전송해 가용성에 문제를 일으키는 공격으로 이를 통해 무선랜을 무력화시킬 수 있다.

2.4 정보 보호 가이드

개편된 위협모델을 반영하여 재구성된 ‘‘무선랜 보안 위협과 대응 가이드 분류‘는 다음과 같다.

Table 6. 개편된 보안 위협과 대응 가이드 분류

보안위협 / 대응가이드			물리적 위협		기술적 위협				관리적 위협			
			TP 01	TP 01	TT 01	TT 02	TT 03	TT 04	TM 01	TM 02	TM 03	TM 04
정책 및 관리	운용 현황 및 장비 관리	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							√			

III. 결론

TTA '안전한 무선랜 사용 지침'을 기준으로 신규동향을 반영하여 제·개정 필요성을 확인했다. 최근 무선랜 환경의 실태를 분석하고 이를 보안 지침에 적용할 수 있도록 각 내용을 설명하였다. 또한, 기존의 위협모델을 STRIDE 모델링을 통해 개편하고 최신 이슈가 반영된 새로운 모델을 제시하여 개편된 모델을 바탕으로 대응 가이드에 대한 분류를 갱신하였다. 따라서 본 논문은 무선랜 연구에 최신 참고자료로 쓰여 최종적으로 노후화된 각종 보안 지침의 개편을 촉구하는 성과를 보일 것이라 기대한다.

[참고문헌]

[1]. 한국인터넷진흥원 해킹대응팀, "무선랜 보안 안내서", 한국인터넷진흥원(KISA), 2011.1.

[2]. 한국정보통신기술협회, "안전한 무선랜 사용 지침", 한국정보통신기술협회(TTA), 2011. 12.

[3]. 한국정보통신기술협회. "TTA 정보통신 용어사전"

[4]. 임권택, 정수환, "단말 기반 무선랜 Rogue AP 탐지 기법", 2012

[5]. 박은주, 김승주, "STRIDE 위협 모델링에 기반한 스마트팩토리 보안 요구사항 도출", 2017.12.

[6]. 남지현, 이주엽, 권송희, 최형기, "안전한 무선랜 환경을 위한 WPA3 표준의 보안 프로토콜 비교 및 분석", 2019.10.

[7]. 박근덕, 박정수, 하재철, "Wi-Fi를 이용한 스마트폰에서 사전 공격에 안전한 WPA-PSK 프로토콜", 2012.04.

[8]. 김신효, 이석준, 권혁찬, 안개일, 조현숙, "차세대 무선랜 보안 기술 동향", 2013

[9]. 황종규, 조현정, 백종현, 김백현, 정락교, "무선기반 열차제어 전송시스템을 위한 무선보안모듈과 WPA2 보안기술의 성능비교", 2013.06.

[10]. 이윤환, 박상건, "스마트홈 서비스 환경에서의 보안 위험 분석을 위한 위협 모델링 적용 방안", 2017.06.

[11]. 이윤환, 박상건, "스마트홈 서비스 환경에서의 보안 위험 분석을 위한 위협 모델링 적용 방안", 2017.06.

[12]. Wi-Fi Alliance, "discover-wi-fi"