국내 무선랜 기술적 위협 참조 모델 도출 및 위험 평가 분석

고지웅, 공재호, 권영우, 김남석, 김유현, 정효종, 김홍진

한국정보기술연구원 차세대 보안리더 양성 프로그램(Best Of the Best)

Deriving a Domestic Technical Threat Reference Model and Analyzing Risk Assessment for Wireless LANs

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. 현재 사물인터넷 활성화 및 5G 상용화와 더불어 국정 100대 과제로 '공공 와이파이 확대'가 선정되며 국내 무선랜 시장은 성장하고 있다. 그러나 무선랜 환경에 대한 위험성 역시 꾸준히 증가하고 있으며 이에 대한 보안성 향상 또한 요구되고 있다. 이에 본 논문은 무선랜 기술 활성화에 따라 WPA3 등과 같은 신규동향을 반영하여 기술적 위협모델을 구성하고 AP/Station을 기준으로 다양한 위협의 원리 및 구조를 분석하며 기존의 구형(2011년) 무선랜 위협 모델을 최신화하였다. 이는 결과적으로 무선랜 요소별 구조에 기반을 둔 기술적 위협을 도출하고, 각 위협별 위험도 측정 및 영향평가를 수행하여 침해지표를 제시한다. 이를 통해 무선랜 환경에 대한 보안 대책 수립 기준을 제시하며 향후의 무선랜 부문의 공격 및 보안 연구의 토대가 될 것을 기대한다.

I. 서론

스마트폰이 도입된 이후로 국내 무선랜 시장은 크게 발달하였고, 현재 IEEE 802.11 표준들은 보편화되어 무선랜은 어디를 가더라도 존재하는 중요 통신 기술이 되었다. 더불어 사물인터넷이 발달하고, 5G가 도입되어 상용화되는 단계인 상태에서, 국정 100대 과제로 '공공 와이파이 확대'가 선정될 정도로 국내 무선랜 시장은 지속해서 성장하고 있다.

그러나 무선랜 환경에 대한 위험성 역시 시장의 성장만큼 비례하여 증가하고 있기에, 이에 대한 보안성 향상 또한 요구되고 있다. 하지만 무선랜 보안에 관한 관심은 시장만큼 커지지 않았고, 무선랜에 대한 국내 자료들도 최신화가 제대로 이루어지지 않고 있다.

특히 기술적 무선랜 위협모델에 관한 표준화는 2011년 이후 개정이 되지 않았고, 다소 노후화된 상태로 유지되고 있다. 기존에는 위협모델에 대한 문서가 개별적으로 존재하지 않아서, 무선랜 환경에 따른 위협 요소 및 보안 대책을 식별하기 어려운 한계점을 내포하고 있다. 이에 무선랜 위협모델 도출의 필요성을 확인하였고 도출된 위협들의 위험 정도를 제시하고자 한다.

따라서 본 논문에서는 WPA3와 같은 신규동향을 반영하여 기술적 위협모델을 구성한다. 이후 각 위협 위험도를 측정하고 영향평가를 수행하여 침해지표를 제시한다. 이를 통해 최신화된 무선랜 위협모델을 제시하여 무선랜 환경에 대한 보안 대책 수립 기준으로 사용되고, 향후 무선랜 부문의 공격 및 보안 연구의 토대로 활용될 것을 기대한다.

II. 본론

1. 연구 범위

본 논문에서는 AP와 Station을 기반으로 발생할 수 있는 다양한 기술적 위협들을 모두 통합하여 새로운 기술적 위협 참조 모델 및 위험지표를 도출한다.

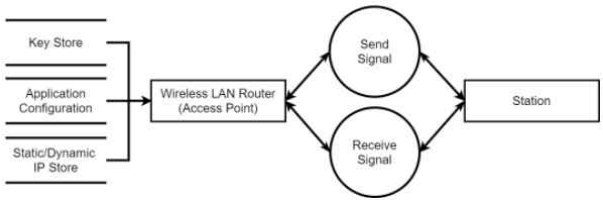
2. 무선랜 위협모델링

무선랜 환경에서 다양한 위협들을 단계별로 도출하여 모델링 하였고, 결과적으로 이를 통해 각 공격에 대한 위험도를 산출하였다.

2.1 DFD (Data Flow Diagram)

전반적인 위협모델 도출을 위해, 신호 송수신을 중심으로 무선랜 환경을 구조화한 데이터 흐름 다이어그램(Data Flow Diagram, 이하 DFD)을 Fig 1과 같이 도출하였다. 이를 통해 무선랜 위협 대상에 대한 요소 및 범위를 파악하였으며, 동시에 보안 위협모델링에 요구되는 모든 요소의 관계 및 흐름을 파악하여 위협 유입 가능성을 보다 효과적으로 식별하였다.

Fig 1. DFD based on Wireless LAN environment



2.2 STRIDE

DFD로 도출된 무선랜 환경에서 STRIDE를 통해서 발생할 수 있는 위협들을 식별하였다.

STRIDE는 사이버 보안 위협 식별을 위해 Microsoft에서 고안한 기법으로 Table 1과 같이 모든 위협을 6가지 영역으로 분류한다. STRIDE로 하여금 모든 위협을 6가지 영역 중 하나로 분류할 수 있게 했다.

각 DFD 요소별로 STRIDE 기법을 활용해서 위협을 식별한 결과는 Table 2와 같다.

Table 1. STRIDE Item

Spoofing identity	기기 도용
Tampering with data	데이터 변조
Repudiation	행동 부인
Information disclosure	정보 유출
Denial of service	서비스 거부
Elevation of privilege	권한 상승

2.3 Attack Tree

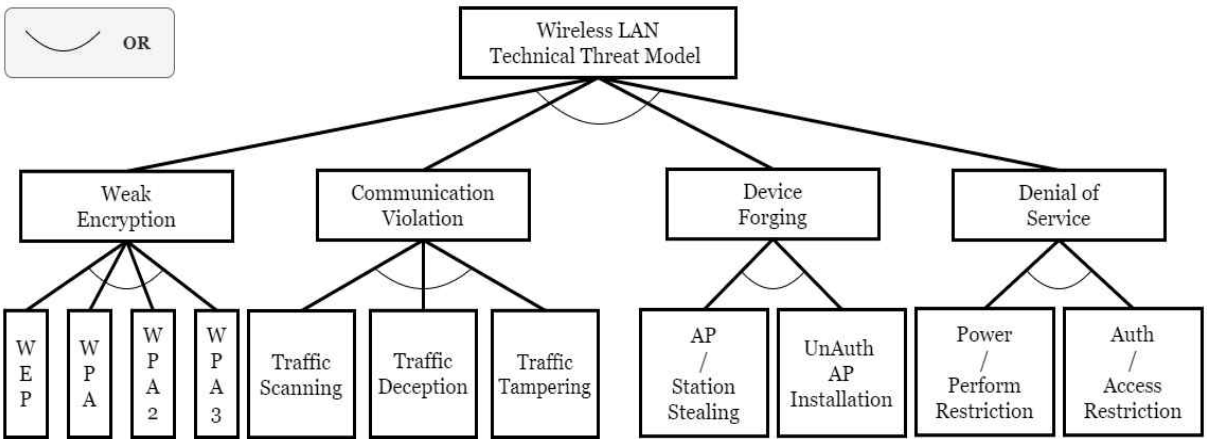
Attack Tree는 무선랜 환경에서의 공격을 계층적으로 정리하였으며, 이를 통해 무선랜 환경에서의 AP 및 Station에 대한 공격을 체계적으로 정립하였다.

본 논문에서는 STRIDE를 통해 공격 유형을 분류하여 무선랜 기술적 위협모델 특성에 해당하는 35개의 위협에 대해 Attack Tree를 Fig 2와 같이 만들었으며, 이를 통해 무선랜 환경에서 발생할 수 있는 위협 유형을 구조적으로 파악할 수 있다.

Table 2. Wireless LAN STRIDE Threat List by DFD Element
(◎ : Main Threat / O : Sub Threat)

DFD Element		Threat list						Contents
		S	T	R	I	D	E	
Entity	AP	◎	O	O				AP Device Forging, Unauthorized AP Installation
	Station	◎	O	O				Station Device Forging
Data Flow		O		O		◎		Performance · Access Restriction
Data store	key store			O	O		◎	Weak Encryption (Key Crack)
	application configuration	O		◎			O	Unauthorized access
	static/dynamic IP store		O		◎	O		Traffic Scanning
Process		O	◎	O	O	O	O	Traffic Deception · Tampering

Fig 2. Attack Tree



2.4 DREAD

DFD와 STRIDE를 통해서 무선랜 환경에서 발생할 수 있는 34개의 취약점을 식별하였고, Attack Tree를 통해 각 취약점을 계층적으로 정리하였다. 이에 대하여 유형별 위험지표를 도출하기 위해 DREAD 기법을 도입하였다. 객관적인 위험도 측정을 위한 DREAD 기준은 다음의 Table 3과 같다.

Table 3. DREAD Item

Damage potential	예상 피해 규모
Reproducibility	공격 성공 확률
Exploitability	공격을 위한 노력 정도
Affected users	영향받는 사람 규모
Discoverability	취약점 발견 난이도

항목별로 점수를 0/5/10점 중 하나를 부여하였으며 각 점수의 기준은 Table 4와 같다. 본 논문은 DREAD의 항목들을 측정하기 위해 Wi-Fi5/6 기반 AP 환경 아래의 일반적 환경을 가정 및 구성하고 Station으론 WPA2/3가 지원되는 기기를 사용하여 측정하였다.

각 공격 유형별 환경으로 진행되었으며. 이에 대한 위험도를 측정한 결과는 Table 5와 같다.

Table 4. DREAD Classification Criteria

D	0	피해가 거의 없다.
	5	일부 데이터에서만 피해가 발생한다.
	10	대부분 데이터에서 피해가 발생한다.
R	0	성공 확률이 매우 희박하다.
	5	공격까지 일련의 단계를 요구한다.
	10	한두 단계만으로 쉽게 공격할 수 있다.
E	0	많은 기술력을 요구하는 공격으로 많은 시간과 노력이 필요하다.
	5	도구와 약간의 숙련도를 통해 공격할 수 있다.
	10	도구 없이 누구나 쉽게 성공할 수 있다.
A	0	영향을 받는 사람이 없다.
	5	관련된 일부 인원만 영향을 받는다.
	10	대부분 사람이 영향을 받는다.
D	0	해당 취약점을 발견하기 매우 어렵다.
	5	일련의 시간과 시도를 통해 발견할 수 있다.
	10	누구나 볼 수 있게 노출되어 있다.

각 항목을 합산한 점수가 높을수록 더 위험한 공격임을 의미한다. 이를 통해 무선랜 환경에서 발생할 수 있는 대부분의 취약점에 대한 위험 정도를 효과적으로 분류했다. 결과적으로 무선랜 환경의 취약성 및 위험 정도를 도출하여 보안 대책 고안에 대한 중요 지표를 마련하였으며, 이로 하여금 대응 우선순위를 제시한다.

Table 5. DREAD Modeling

유형	분류	위협	DREAD					Rating
			D	R	E	A	D	
Weak Encryption	WEP	Keystream reuse attack	10	10	5	10	10	high
		ICV(Integrity Check Value) Tampering	10	10	5	10	10	high
		FMS(Fluhrer, Mantin, Shamir)	10	10	5	10	10	high
	WPA	Key Re-Installation	10	10	5	10	10	high
		TKIP(Temporal Key Integrity Protocol) ChopChop Attack	10	5	5	10	10	medium
		Bruteforce WPS(Wi-Fi protected Setup) PIN	10	5	5	10	10	medium
	WPA2	Bruteforce PSK(Pre-Shared-Key)	10	5	5	10	10	medium
	WPA3	Downgrade	10	10	5	10	10	high
		Side-Channel	10	10	5	10	10	high
Communication Violation	Traffic Scanning	Sniffing	10	10	5	10	10	high
		Scanning	5	10	5	10	10	medium
		War-attack(War-Drivig/Cycling/Biking/training/Walking/Jogging/Droning/Flying)	5	10	5	10	10	medium
	Traffic Tampering	Packet Tampering	10	5	5	5	10	medium
	Traffic Deception	Packet Replay	10	5	5	5	10	medium
		Wi-Fi Hi-Jacking	10	5	5	5	10	medium
Device forging	AP/Station Stealing	Construction Stealing	5	10	5	5	10	medium
		Service Stealing	5	10	5	5	10	medium
	Unauthorized AP Installation	Rougue AP(Access Point)	10	10	5	10	10	high
Denial of Service	Power / Performance Restriction	Authentication Flood	10	10	5	10	10	high
		Sleep Interference	10	5	0	10	10	medium
		Battery Exhaustion	10	0	10	10	0	low
		Clean Sleep Buffer	10	5	5	10	10	medium
		Channel/Signal jamming	10	5	0	10	5	low
		Fake POLL Frame/TIM(Traffic Indication Map) Field	10	5	5	5	10	medium
		Fake Sleep Signal	10	5	5	10	10	medium
		Beacon Flood	10	10	5	10	10	high
	Authentication / Access Restriction	Send Deauthentication Signal	10	10	5	10	10	high
		Send Disassociation Signal	10	10	5	5	10	medium
		Send Rreassociation Signal	10	5	5	5	10	medium
		RTS(Request To Send) Request Flood	10	5	5	10	10	medium
		WPA3-SAE Connection Deprivation Flaw	10	5	5	10	10	medium
		Cutting CW(Contention Window) Expiration	10	0	0	5	10	low
		FCS (Frame Check Sequence) Collision	10	0	0	5	10	low

III. 결론

본 논문에서는 신규동향을 반영하여 새로운 무선랜 기술적 위협 참조 모델을 도출하였다. 무선랜 환경을 구조화한 DFD를 구성하고 구성된 요소를 기반으로 STRIDE를 통해 위협을 식별하였다. 이후 Attack Tree를 통해 무선랜 공격들을 계층적으로 분류하였으며, 유형별 위협에 대해 구조화하였다. 최종적으로 DREAD 기법을 활용하여 계층적으로 정리된 유형별 위협을 위한 위험지표를 도출하여 무선랜 기술 현황을 고려 및 반영한 체계적인 공격 참조 모델 도출에 의의를 둔다. 이는 향후 진행될 무선랜 보안 대책 연구에 중요 지표로 작용할 것으로 기대한다.

[참고문헌]

[1]. 한국인터넷진흥원 해킹대응팀, “무선랜 보안 안내서”, 한국인터넷진흥원(KISA), 2010.1.

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

[3]. 최영남, 조성목, “무선랜 워드라이빙 공격의 위험성과 대응방안” 2009

[4]. 최석환, 신진명, 최윤호, “Received Signal Strength의 상관관계를 이용한 Rogue AP 탐지 기법“ 2017.01

[5]. 박은주, 김승주, “STRIDE 위협모델링에 기반한 스마트팩토리 보안 요구사항 도출“, 2017.12.

[6]. 박근덕, 박정수, 하재철, “Wi-Fi를 이용한 스마트폰에서 사전 공격에 안전한 WPA-PSK 프로토콜”, 2012.04.

[7]. 김신효, 이석준, 권혁찬, 안개일, 조현숙, “차세대 무선랜 보안 기술 동향“, 2013

[8]. 이윤환, 박상건, “스마트홈 서비스 환경에서의 보안 위험 분석을 위한 위협모델링 적용 방안”, 2017.06.

[9]. Karim, Hohammad, “Attacks and Defenses in Short-Range Wireless Technologies for IoT”, 2020.04.

[10]. Mathy, Eyal, “Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd”, 2019.07.