2020 한국정보보호학회 호남지부 추계학술대회

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)

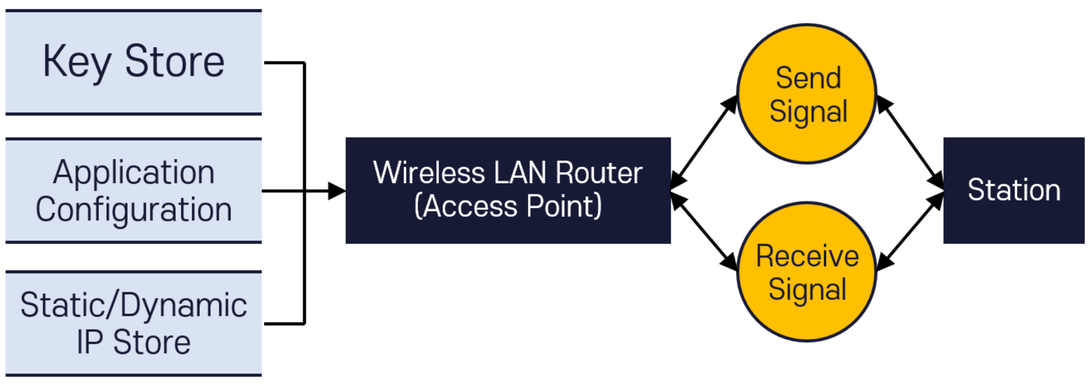
서론

국내 무선랜 시장은 크게 발달하였고, 현재 IEEE 802.11 표준들은 보편화 되어 무선랜은 어디를 가더라도 존재하는 중요 통신 기술이 되었다. 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. 본 논문에서는 WPA3와 같은 신규동향을 반영하여 기술적 위협모델을 구성한다. 그리고 위협 위험도를 측정하고 영향평가를 수행하여 침해지표를 제시한다.

DFD

전반적인 위협모델 도출을 위해, 신호 송수신을 중심으로 무선랜 환경을 구조화한 데이터 흐름 다이어그램(Data Flow Diagram, 이하 DFD)을 도출하였다.

1. 무선랜 위협 대상에 대한 요소 및 범위를 파악
2. 보안 위협모델링에 요구되는 모든 요소의 관계 및 흐름을 파악



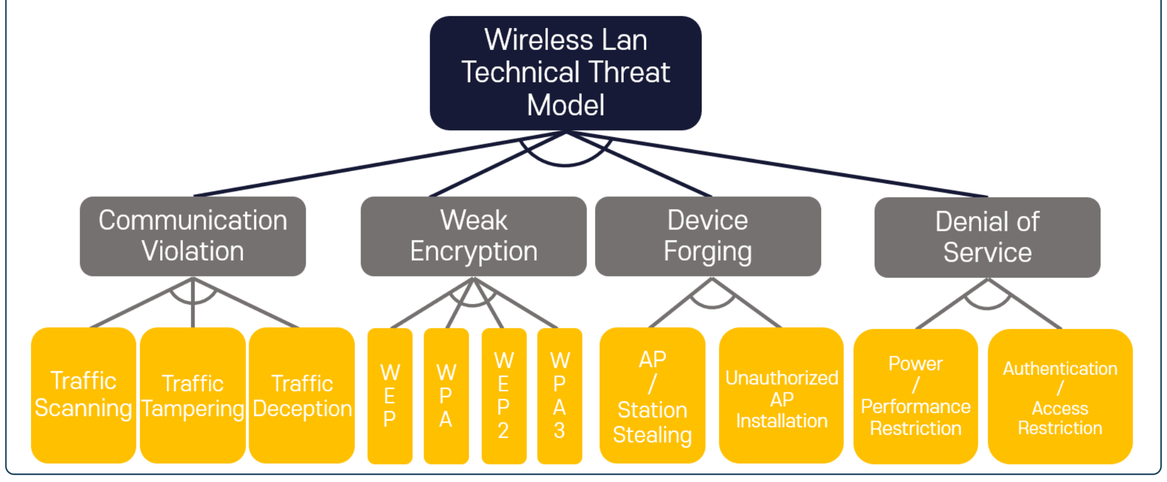
STRIDE

DFD로 도출된 무선랜 환경에서 STRIDE를 통해서 발생할 수 있는 위협들을 식별하였다. STRIDE는 사이버 보안 위협 식별을 위해 Microsoft에서 고안한 기법으로 모든 위협을 6가지 영역으로 분류하였으며 DFD 요소별로 STRIDE 기법을 활용해 위협을 식별한다.

DFD Element		Threat list						Contents
		S	T	R	I	D	E	
Entity	AP	◎	○	○				AP Device Forging, Unauthorized AP Installation
	Station	◎	○	○				Station Device Forging
Data Flow		○		○		◎		Performance · Access Restriction
Data Store	Key Store			○	○		◎	Weak Encryption (Key Crack)
	Application configuration	○		◎			○	Unauthorized Access
	Static/Dynamic IP Store		○		◎	○		Traffic Scanning
Process		○	◎	○	○	○	○	Traffic Deception · Tampering

Attack Tree

STRIDE를 통해 공격 유형을 분류하여 무선랜 기술적 위협모델 특성에 해당하는 34개의 위협에 대해 Attack Tree를 구성하였으며, 이를 통해 무선랜 환경에서 발생할 수 있는 위협 유형을 구조적으로 파악할 수 있다.



DREAD

도출된 위협에 대하여 아래와 같은 DREAD 기준으로 평가하였다.

D (Damage)

No Damage(0) ~ Total Damage(10)

R (Reproducibility)

Attack Impossible(0) ~ Attack Possible(10)

E (Exploitability)

Hard Skills(0) ~ Easy Skills(10)

A (Affected Users)

Effected No One(0) ~ Effected Most People(10)

D (Discoverability)

Effected No One(0) ~ Effected Most People(10)

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/Walking/...)	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

결론

본 논문에서는 신규동향을 반영하여 새로운 무선랜 기술적 위협 참조 모델을 도출하였다. 최종적으로 계층적으로 정리된 유형별 위협을 위한 위험지표를 도출하여 무선랜 기술 현황을 고려 및 반영한 체계적인 공격 참조 모델도출에 의의를 둔다. 이는 향후 진행될 무선랜 보안 대책 연구에 중요 지표로 작용할 것으로 기대한다.