논문 19-44-10-14 The Journal of Korean Institute of Communications and Information Sciences '19-10 Vol.44 No.10
https://doi.org/10.7840/kics.2019.44.10.1878

안전한 무선랜 환경을 위한 WPA3 표준의 보안 프로토콜 비교 및 분석

남 지 현◆, 이 주 엽*, 권 송 희**, 최 형 기°

Comparative Analysis on Security Protocols of WPA3 Standard for Secure Wireless LAN Environments

Ji-Hyun Nam◆, Ju-yeop Lee*, Song-hui Kwon**, Hyoung-Kee Choi°

요 약

WPA2가 표준으로 채택된 이후 약 14년 만에 Wi-Fi Alliance는 WPA3 표준을 공개했다. WPA3는 WPA2의 한계점을 보완하여 더욱 안전한 무선 Wi-Fi 네트워크 환경을 제공한다. 본 논문에서는 WPA3에서 개선된 주요 특징을 1) 비밀번호 기반 보안 모드, 2) 개방형 네트워크 암호화, 3) 간편한 연결 프로토콜, 4) 관리 프레임 보호로 분류하였다. 각 특징별 WPA2의 한계점을 파악하고 이를 개선하기 위해 제공한 WPA3의 기능을 분석한다. 또한 최신 표준인 WPA3에 새롭게 적용된 보안 기능을 검토하여 보완점을 탐색하였으며, WPA3의 개선점에 대한 고찰을 통해 향후 무선 Wi-Fi 네트워크 보안에서 고려해야 할 요소를 제시한다.

Key Words : WPA3 Standard, Wi-Fi Network Security, Dragonfly Protocol, Opportunistic Wireless Encryption, Device Provisioning Protocol, Protected Management Frame

ABSTRACT

About fourteen years after the adoption of WPA2, the Wi-Fi Alliance has officially released WPA3 standard. WPA3 complements the limitations of WPA2 to provide a safer wireless Wi-Fi network environment. In this paper, we classify the main improved features in WPA3 as 1) Password-based security mode, 2) Open network encryption, 3) Easy connect protocol and 4) Management frame protection. We identify the limitations of WPA2 for each feature and analyze the functions of WPA3 to improve them. In addition, we explore the complementary points by reviewing the new security features in the latest standard, WPA3. Through our consideration of the improvements to WPA3, we present factors to consider in future wireless Wi-Fi network security.

Ⅰ. 서 론

WPA(Wi-Fi Protected Access)는 Wi-Fi Alliance에서 개발하고 있는 무선 Wi-Fi 네트워크 보안 프로토콜로 IEEE(Institute of Electrical and Electronics Engineers) 802.11i 표준으로 정의되어 있다[1]. Wi-Fi

※ 본 연구는 2016년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구 사업임(No.2016RID1A1B03936211).
◆ First Author : Sungkyunkwan University Department of Electrical and Computer Engineering, jhnam19@o365.skku.edu, 학생회원
° Corresponding Author : Sungkyunkwan University Department of Software, meosery@skku.edu, 정회원
* Sungkyunkwan University Department of Platform Software, daf198@o365.skku.edu
** Sungkyunkwan University Department of Electrical and Computer Engineering, songhee@o365.skku.edu
논문번호 : 201906-098-B-RN, Received June 3, 2019; Revised July 31, 2019; Accepted August 8, 2019

Alliance는 802.11i 표준이 완성되기 전에 무선 Wi-Fi 통신을 보호하기 위해 802.11i 표준을 일부 구현한 WPA를 임시로 도입하였다. 2004년 802.11i 표준이 최종적으로 발표되자 Wi-Fi Alliance는 WPA2를 채택하여 보안 네트워크를 제공하는 기준으로 사용하였다.

M. Vanhoef와 F. Piessens가 2017년에 발표한 키 재설치 공격(Key Reinstallation Attack, KRACK) 논문[2]과 2018년에 발표한 Kraken 논문[3]으로 WPA2의 주요한 취약점이 알려지게 되었다. KRACK과 Kraken 취약점들은 WPA2에서 이미 개선방안이 제시되어 더 이상 위협으로 남아 있지 않으나[4,5] WPA2에 잔존하는 한계로 새로운 표준의 필요성이 대두되었다.

Wi-Fi Alliance는 2018년 6월 WPA2를 보완한 새로운 보안 규격인 WPA3(Wi-Fi Protected Access 3)[6-7]를 공식 발표하였다. Wi-Fi Alliance에서 Wi-Fi 6로 명명한 차세대 Wi-Fi 표준인 IEEE 802.11ax에서 WPA3를 포함[8]하였으며 2020년 6월 표준으로 승인될 예정이다[9]. 퀄컴, 시스코 등의 다양한 기업에서도 WPA3를 지원하고 있어 앞으로 Wi-Fi 네트워크 시장에서 WPA3가 광범위하게 사용될 것으로 예측된다[10].

WPA3는 WPA2에 비해 보안성과 편의성이 강조되었다. 특히 WPA3는 완전 순방향 비밀성(PFS, Perfect Forward Secrecy)[11]을 제공하여서 장기적으로 사용하는 키가 탈취 및 노출되더라도 이전 또는 이후에 사용한 일시적인 키를 추측할 수 없어 보안이 강화된다.

본 논문에서는 기존에 사용하고 있는 WPA2의 한계점을 특징별로 분류하여 파악하고 Wi-Fi Alliance에서 최근 새롭게 발표한 WPA3에서 제시한 개선책과 WPA3의 추후 발전 방향에 대해 분석한다.

Ⅱ. WPA2 한계점

WPA2는 2004년부터 표준으로 사용되며 많은 취약점이 보고되었다[12-14]. 특히 WPA2는 인증과 키 관리 측면에서 한계점이 존재한다. 본 장에서는 WPA2의 한계점들을 특징에 따라 분류하여 서술한다.

2.1 PMK(Pairwise Master Key) 생성 과정 취약

WPA2는 비밀번호로 도출한 PSK(Pre-Shared Key)를 PMK로 사용하는 WPA2-PSK 모드를 제공한다[15]. WPA2-PSK 모드는 비밀번호를 탈취하는 오프라인 사전공격(offline dictionary attack)에 취약하다[13]. PMK는 비밀번호만을 이용하여 도출되므로 STA(station)와 AP(Access Point) 간 모든 연결에서 동일한 PMK를 사용한다. 공격자가 PMK를 탈취할 경우 스니핑(sniffing)을 통해 암호화키를 획득할 수 있으므로 모든 연결의 메시지는 복호화된다.

2.2 개방형 네트워크 암호화 미지원

WPA2에서는 현실적으로 비밀번호를 배포하기 어렵거나 사용자 인증이 필요하지 않은 경우, 비밀번호 입력 없이 인터넷 연결을 지원하기 위해 개방형 네트워크 방식을 제공한다. 개방형 네트워크는 연결의 편의성을 제공하는 반면 STA와 AP 간 통신의 암호화가 이루어지지 않는다는 보안 문제점이 있다. STA와 AP 연결 절차에서 키를 생성하는 과정이 생략되기 때문에 STA와 AP 간 메시지는 평문으로 전송되며, 공격자가 개방형 네트워크의 통신을 스니핑할 경우 사용자 정보가 탈취된다.

2.3 PIN 취약점 및 사용자 인터페이스가 제한된 기기에서 WPS 지원 불가

WPA2는 사용자가 편리하게 AP에 사용자의 기기를 연결하도록 WPS(Wi-Fi Protected Setup)을 지원한다[16]. WPS는 숫자만으로 사용자를 인증하는 PIN(Personal Identification Number)이나 버튼을 누르는 방식인 PBC (Push-Button Configuration)를 제공한다. WPS 방식의 한계점은 첫째, WPS가 제공하는 PIN 방식의 검증과정은 무작위 대입 공격(brute force attack)에 취약하고[14], 둘째, WPS를 사용하기 위해서는 기기에 PIN을 입력하거나 PBC 버튼을 누르기 위한 사용자 인터페이스(UI, User Interface)가 구현되어 있어야 한다. 사용자 인터페이스가 제한적이거나 전혀 없는 Wi-Fi 기기들은 WPS를 사용할 수 없는데 최근 지속적으로 수량이 증가하고 있는 IoT(Internet of Things) 기기[17]는 사용자 인터페이스가 존재하지 않아 무선 Wi-Fi 네트워크 연결이 제한된다.

2.4 관리 프레임 보호 취약

STA와 AP 간 통신에 사용되는 프레임은 데이터 프레임, 제어 프레임, 관리 프레임으로 나누어진다. 특히 관리 프레임의 경우 STA와 AP 사이의 초기 통신을 확립하기 위한 관리용 정보를 포함해 보안에 유의해야 한다.

IEEE 802.11w 표준으로 정의된 PMF(Protected Management Frame)[18]는 관리 프레임의 인증 및 암호화를 적용하여 보안을 강화한다. WPA2까지 PMF 적용이 선택 사항이었기 때문에 WPA2 기반의 통신

표 1. WPA2와 WPA3의 주요 특징 비교
Table 1. Comparison of features between WPA2 and WPA3

Features		WPA2	WPA3	Key Reference
Release		2004	2018	[15, 20]
Data confidentiality protocol	Personal	AES-CCMP		
	Enterprise	AES*-CCMP†	AES-GCMP‡	
Key length	Personal	128 bit		
	Enterprise	128 bit	192 bit	
Password-based security mode		WPA2-PSK	WPA3-SAE**	[7, 20-22]
Open network encryption		Not supported	OWE††	[23-24]
Easy connect protocol		WPS	DPP‡‡	[16, 25]
Management frame protection		Optional	Mandatory	[20]

* AES(Advanced Encryption Standard)
† CCMP(Counter Mode Cipher Block Chaining Message Authentication Code Protocol)
‡ GCMP(Galois/Counter Mode Protocol)
** SAE(Simultaneous Authentication of Equals)
†† OWE(Opportunistic Wireless Encryption)
‡‡ DPP(Device Provisioning Protocol)

에서 관리 프레임이 보호받지 못하는 경우가 발생한다. PMF가 적용되지 않은 경우 STA와 AP 간 통신에 공격자가 개입하여 관리 프레임을 도청할 수 있을 뿐만 아니라 획득한 정보를 이용하여 프레임을 변조, 전송해 임의 기능을 수행하도록 할 수 있다. 특히 STA와 AP 간 연결을 종료하는 기능을 가진 인증 해제(deauthentication) 프레임은 이블 트윈(evil twin)[19], 비밀번호 크래킹 등의 공격에 악용될 수 있다.

Ⅲ. WPA3 주요 특징

WPA3는 WPA2의 한계점을 개선하여 향상된 기능을 제공한다. WPA3와 WPA2의 특징별 차이점은 표 1에서 비교 및 정리한다. WPA3-개인용(Personal) 모드는 WPA2-개인용 모드와 동일한 암호화 알고리즘과 키 길이를 지원한다. WPA3-기업용(Enterprise) 모드는 암호화 무결성 알고리즘으로 GCMP(Galois/Counter Mode Protocol)를 도입하고 최소 192bit의 키를 사용하여 강화된 암호화를 제공한다[20]. WPA3에서 개선된 주요 특징은 1) 비밀번호 기반 보안 모드, 2) 개방형 네트워크 암호화, 3) 간편한 연결 프로토콜, 그리고 4) 관리 프레임 보호이다. 본 장에서는 WPA3의 네 가지 주요 특징을 중심으로 서술한다.

3.1 PMK 생성 과정 보안성 강화

WPA3에서는 비밀번호를 기반으로 PMK를 생성하기 위하여 WPA3-SAE(Simultaneous Authentication of Equals) 모드[7,21,22,26]를 사용한다. WPA3-SAE 모드는 WPA2 연결 과정 중 식별자만 교환하던 인증 단계에서 Dragonfly 프로토콜을 적용하였다. Dragonfly[20]는 RFC 7664에 정의되어 있으며 Diffie-Hellman 키 교환 방식을 통해 두 랜덤값과 비밀번호를 사용하여 매 연결마다 서로 다른 PMK를 유도한다. Dragonfly는 비밀번호의 변환을 통해 생성자로 사용하며 기존 Diffie-Hellman과 다르게 공개되지 않은 생성자를 통해 사용자 인증을 수행하여 중간자 공격을 방어한다.

Dragonfly는 그림 1과 같이 SAE 커밋(commit)과 SAE 확인(confirm)의 두 단계로 이루어져 있다. Dragonfly에서는 STA와 AP 모두 생성자를 공유하고 있어 연결 초기에 생성자를 협의하는 과정이 필요하지 않다. 각 단계에서 STA와 AP는 상대방의 메시지를 기다리지 않고 동시에 메시지를 전송할 수 있어 연결속도가 향상된다.

SAE 커밋은 STA와 AP 간 공통의 비밀값을 생성하는 단계이다. STA와 AP는 각각 2개의 랜덤값을 선택 후 랜덤값으로부터 공개키를 생성하여 서로에게 전송한다(그림 1의 ①,②). 각자 수신한 공개키와 자신

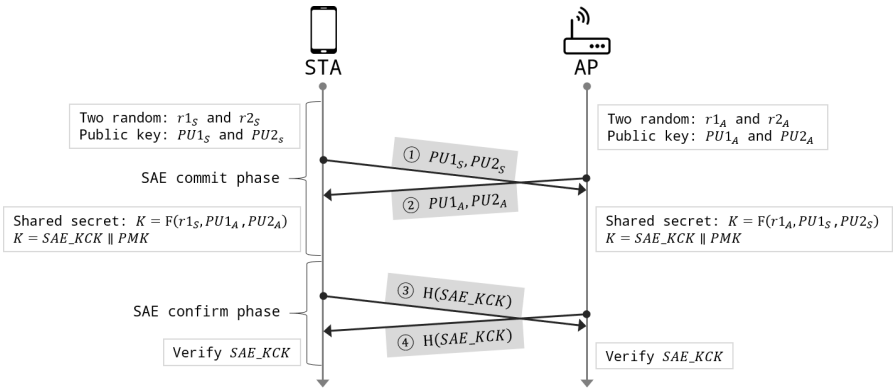

그림 1. PMK 생성을 위한 Dragonfly 프로토콜의 메시지
Fig. 1. Messages in Dragonfly protocol to generate PMK

의 랜덤값으로 공통의 비밀값을 유도하여 SAE_KCK(Key Confirmation Key)와 PMK를 생성한다.

SAE 확인은 SAE 커밋 단계에서 생성한 키를 검증하는 단계이다. STA와 AP는 SAE_KCK의 해시값을 전송하고 수신한 해시값을 통해 올바른 PMK를 생성하였는지 검증한다(그림 1의 ③,④). 검증이 완료되면 PMK를 4-회 핸드셰이크에서 암호화키를 생성하기 위해 사용한다.

Dragonfly는 STA와 AP간 모든 연결에서 서로 다른 키를 가져 PFS를 만족하였다. 하나의 연결에서 PMK를 탈취당하더라도 다른 연결의 보안성은 유지된다. 공격자가 오프라인 사전공격 시 가능한 비밀번호와 랜덤값을 모두 추측해야 하므로 공격 비용이 증가하여 PMK가 보호된다.

3.2 개방형 네트워크 메시지 암호화

Wi-Fi Alliance에서는 개방형 네트워크 방식에 보안을 강화한 Wi-Fi certified enhanced open 방식을 제공한다[23]. Wi-Fi enhanced open은 OWE (Opportunistic Wireless Encryption) 프로토콜을 기반으로 STA와 AP 간 통신을 보호한다. OWE를 지원하기 위한 필요조건인 PMF는 WPA3에 필수로 적용되어 추가적인 구현 없이 OWE를 사용할 수 있다.

RFC 8110에 정의된 OWE[24]는 그림 2와 같은 절차로 진행된다. Diffie-Hellman 키 교환 관련 정보를 전달하기 위해 연결(association) 요청, 연결 응답 프레임에 매개변수를 추가한다. 연결 요청 메시지를 이용해 STA는 AP에게 키 교환 관련 정보와 자신의 공개키를 전달하고 연결 응답 메시지로 AP의 공개키를 전달받는다(그림 2의 ①,②). 이 두 메시지 교환이 완료되면 STA와 AP는 자신의 개인키와 상대방의 공개키로 공통의 비밀값을 유도한다. HKDF(Hashed Message Authentication Code-based Key Derivation Function)[27]를 사용하여 공통의 비밀값으로부터 PMK를 생성하고 4-회 핸드셰이크를 통해 STA와 AP 간 암호화 통신을 진행한다.

OWE는 WPA2의 개방형 네트워크 방식과 동일하게 비밀번호를 입력받지 않아 사용자의 편의성을 보장한다. 뿐만 아니라 STA와 AP 간 통신의 암호화를 제공하여 개방형 네트워크에서 사용자의 정보가 노출되는 문제를 해결한다. OWE 적용 시 공격자가 STA와 AP 간 메시지를 획득하더라도 키를 계산할 수 없으므로 메시지를 복호화하지 못한다. STA와 AP 간 연결에서 서로 다른 각각의 비밀키가 생성되므로 공격자가 한 연결의 키를 탈취하더라도 다른 STA의 메시지를 복호화할 수 없다.

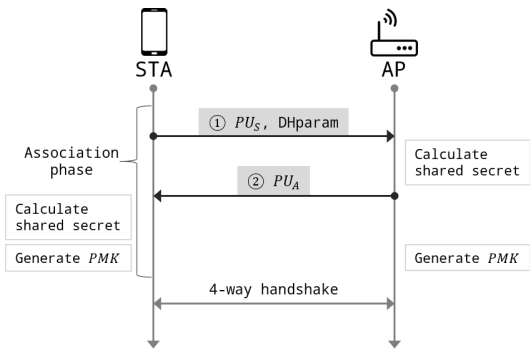

그림 2. PMK 생성을 위한 OWE 프로토콜의 메시지
Fig. 2. Messages in OWE protocol to generate PMK

3.3 UI가 제한된 기기와 AP 간 연결

Wi-Fi Alliance는 Wi-Fi easy connect로 중계 단말을 이용하여 STA와 AP 간 인증을 수행하는 프로토콜로 DPP(Device Provisioning Protocol)을 제공한다[25]. DPP는 사용자 인터페이스가 존재하지 않는 STA에서도 사용자 입력 없이 간편하게 인증을 수행하기 위해 QR코드, 블루투스, 근거리 무선 통신(NFC, Near Field Communication)을 활용하여 Wi-Fi와 연결되지 않은 환경에서 STA의 공개키를 획득하는 OOB(Out-Of-Band) 인증 기능을 제공한다. STA는 AP에 연결되고자 하는 기기로 IoT 기기가 이에 포함된다. 중계 단말은 STA와 AP의 중간자 역할을 수행하는 기기로 스마트폰이 이에 포함된다. AP는 DPP 시작 전에 중계 단말과 Wi-Fi로 연결되어 있어야 하며 Wi-Fi를 통해 인증 정보를 교환한 상태여야 한다.

DPP의 인증 과정은 DPP 인증(authentication), DPP 설정(configuration), 그리고 DPP 네트워크 개시(network introduction)의 세 단계로 나뉜다. 이해의 편의를 위해 DPP 인증 과정에서 중계 단말은 스마트폰으로, STA는 IoT 기기로 예시를 들어 설명한다. DPP의 인증 과정은 그림 3에 나타나 있으며 그림 3에서 사용한 용어와 수식은 표 2에 정의되어 있다.

DPP 인증은 스마트폰이 OOB 방식으로 IoT 기기의 정보를 획득하여 스마트폰과 IoT 기기 간 메시지 암호화키를 생성하는 단계이다. 스마트폰은 IoT 기기가 제공하는 OOB 인증 방식으로 IoT 기기의 영구 공개키를 수신하며 DPP를 시작한다(그림 3의 ①). IoT 기기는 스마트폰이 전송하는 자신의 영구 공개키 해시값을 통해 스마트폰이 근거리에 있음을 확인한다(그림 3의 ②). 스마트폰과 IoT 기기는 각각 통신을 위한 임시 공개키와 개인키 쌍을 생성한다. 생성한 임시 공개키 교환을 통해 스마트폰과 IoT 기기 간 암호화 통신을 위한 비밀키를 생성한다(그림 3의 ②,③). 이때 스마트폰과 IoT 기기는 메시지에 포함된 IoT 기기의 장기 공개키 해시값을 검증함으로써 상대가 정상적인 통신 상대임을 확인한다. 서로 올바른 비밀키를 생성하였음이 검증되면 다음 단계로 넘어간다(그림 3의 ③,④).

DPP 설정은 스마트폰이 IoT 기기가 스마트폰에게 인증되었음을 나타내는 인증값을 생성하여 IoT 기기에게 전달하는 단계이다. DPP 설정 단계의 모든 메시지는 DPP 인증 단계에서 생성한 비밀키로 암호화된다. IoT 기기는 스마트폰에게 네트워크 연결 정보를 전송하며 DPP 설정 단계를 시작한다(그림 3의 ⑤). 스마트폰은 IoT 기기의 임시 공개키를 자신의 서명키로 서명하여 IoT 기기에게 반환한다(그림 3의 ⑥). 서명된 IoT 기기의 임시 공개키가 변조 없이 전송되었음이 검증되면 다음 단계로 넘어간다.

DPP 네트워크 개시는 IoT 기기와 AP가 각각 스마트폰으로부터 서명받은 공개키를 교환하여 상호인증을 수행하는 단계이다. AP는 DPP 시작 전에 스마트폰과 Wi-Fi로 연결되어 있으며 스마트폰은 자신의 서명키로 AP의 공개키를 서명하여 반환한 상태이다. IoT 기기와 AP는 서로의 서명된 공개키를 교환하여 자신이 스마트폰에게 인증된 기기라는 것을 증명한다(그림 3의 ⑦,⑧). 두 기기의 공개키가 동일한 스마트폰에 의해 서명되었다면 이는 사용자가 연결하고자 하는 AP와 IoT 기기가 알맞게 매칭되었음을 의미한다. STA와 AP의 공개키 서명값이 검증되면 두 기기의 공개키로 PMK를 생성한 뒤 4-회 핸드셰이크를 통해 암호화 통신을 수행한다(그림 3의 ⑨).

DPP는 다음의 세 가지 장점을 지닌다. 첫째, 중계 단말의 사용으로 STA 또는 AP에 사용자의 입력이 필요하지 않아 사용자 인터페이스가 구현되지 않은 기기와 AP를 안전하게 연결한다. 둘째, 중계 단말로 스마트폰을 사용하는 경우 STA 인증을 위한 QR코드,

표 2. 그림 3에 사용된 키워드와 수식
Table 2. Keywords and equations used in Fig. 3

Keywords	Information	Equations
ke	Encryption key	$ke = \mathrm{HKDF}(L\_PR_D \cdot E\_PU_S \parallel E\_PR_D \cdot E\_PU_S)$ $= \mathrm{HKDF}(E\_PR_S \cdot L\_PU_D \parallel E\_PR_S \cdot E\_PU_D)$
$auth_D$	Authentication value from IoT device	$auth_D = \mathrm{HKDF}(E\_PU_S \parallel E\_PU_D \parallel L\_PU_D \parallel 0)$
$auth_S$	Authentication value from smartphone	$auth_S = \mathrm{HKDF}(E\_PU_D \parallel E\_PU_S \parallel L\_PU_D \parallel 1)$
PMK	PMK for 4-way handshake	$PMK = \mathrm{HKDF}(E\_PU_D \cdot E\_PR_A)$ $= \mathrm{HKDF}(E\_PU_A \cdot E\_PR_D)$

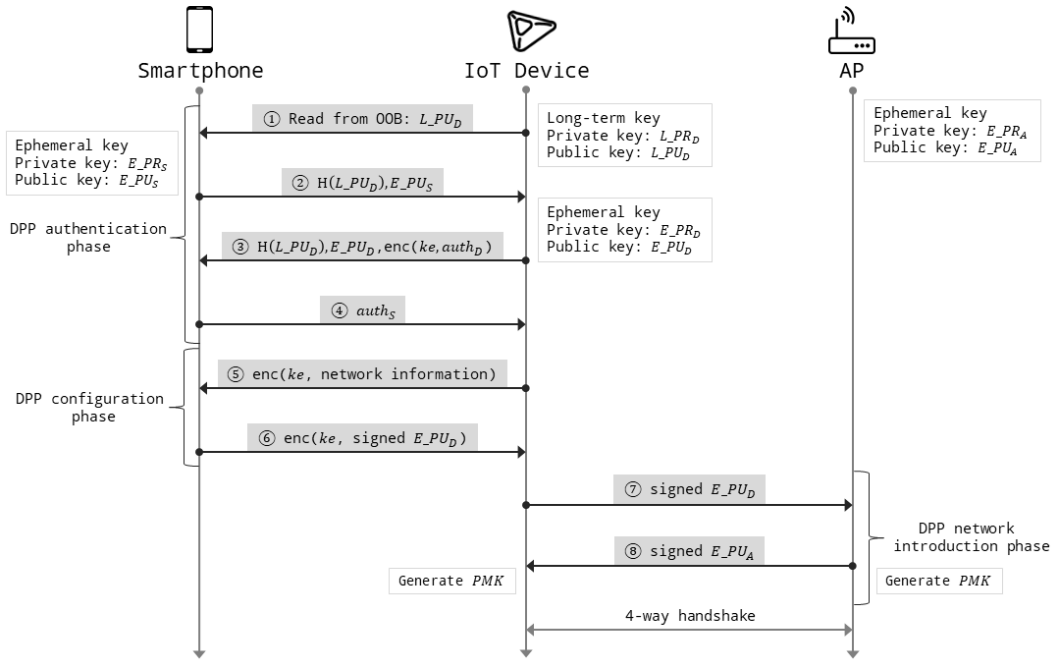

그림 3. DPP의 DPP 인증, DPP 설정, 그리고 DPP 네트워크 개시 단계
Fig. 3. DPP authentication, DPP configuration, and DPP network introduction phases in DPP

블루투스, 근거리 무선 통신이 모두 구현되어 있으므로 추가적인 인터페이스 구현이 불필요하다. 셋째, STA와 AP 연결 시 일시적인 키를 사용하여 WPS에 비해 높은 보안성을 지원한다. DPP는 STA와 AP 연결 시 각 연결마다 서로 다른 임시 공개키를 사용하여 각 연결마다 서로 다른 PMK를 생성함으로써 PFS를 만족한다.

3.4 관리 프레임 보호 기능 필수 적용

WPA2까지 PMF 적용이 선택 사항이었지만 WPA3에서 PMF가 필수로 적용되어 WPA3를 통해 연결하는 STA와 AP 모두 PMF를 지원해야 한다[20]. PMF 적용 시 4-회 핸드세이크를 통해 생성한 키를 이용하여 특정 관리 프레임[18]의 인증 및 암호화를 수행한다. PMF의 관리 프레임 보호 메커니즘은 유니캐스트(unicast) 통신과 브로드캐스트/멀티캐스트(multicast) 통신으로 분류된다.

유니캐스트 통신에서 PMF를 적용하지 않은 경우 관리 프레임은 보호되지 않는다. PMF를 적용하면 유니캐스트되는 관리 프레임은 AES-CCMP (Advanced Encryption Standard-Counter Mode Cipher Block Chainning Message Authentication Code Protocol)로 보호되어 기밀성과 무결성이 보장된다.

브로드캐스트/멀티캐스트 통신에서는 새로이 BIP (Broadcast/Multicast Integrity Protocol)를 도입하여 브로드캐스트/멀티캐스트로 전달되는 관리 프레임을 보호한다. BIP를 적용할 경우 AP가 생성한 IGTK(Integrity Group Temporal Key)로 프레임에 대한 MIC(Message Integrity Check)값을 생성 및 삽입하여 관리 프레임을 인증한다. IGTK는 4-회 핸드세이크를 통해 STA로 배포되며 AP에 연결된 STA는 모두 같은 키를 가진다.

WPA3는 WPA2에서 중요하게 고려되지 않았던 관리 프레임의 보호를 위해 PMF를 필수로 적용하였다. 브로드캐스트/멀티캐스트 통신의 경우 인증 기능을 통해 무결성을 제공하며 유니캐스트 통신의 경우 추가로 암호화를 적용하여 기밀성을 보장한다. 인증된 관리 프레임을 기반으로 안전한 STA와 AP 간 연결 절차를 제공[28]함으로써 관리 프레임의 취약점을 이용한 공격을 방어한다.

Ⅳ. WPA3 보완점 모색

WPA3는 WPA2에 지원하지 않았던 프로토콜을 도입하였기 때문에 새로이 발생할 수 있는 취약점에 대한 검토가 필요하다. Dragonfly[21]와 같이 기존에 발표된 프로토콜이 적용된 경우 프로토콜에 식별된 취

약점이 존재할 수 있으며 취약점이 존재하지 않더라도 WPA3에 프로토콜을 적용하며 문제가 발생할 우려가 있다. WPA3에서 새롭게 고안하여 도입한 프로토콜의 경우 신규 취약점이 탐색 될 수 있다. 본 장에서는 WPA3의 보안 기능을 위 세 가지 접근 방식으로 검토하여 각 기능별 보완점을 서술한다.

4.1 Dragonfly 중간자 공격 위협

M. Vanhoef와 E. Ronen는 WPA3에서 WPA2로의 다운그레이드(downgrade) 공격을 통한 사전공격을 제안하였다[29]. 다운그레이드 공격은 WPA2와의 하위 호환을 보장하기 위해 WPA2-PSK와 WPA3-SAE를 모두 지원하는 WPA3-SAE 변환(transition) 모드에서 실행된다. 공격자는 다운그레이드 공격을 통해 WPA2-PSK 모드로 연결을 수행한 뒤 4-회 핸드세이크의 메시지를 획득하고 사전공격을 실행하여 비밀번호를 탈취한다. Dragonfly에서 비밀번호가 노출되면 중간자 공격에 취약해져 STA와 AP 간 메시지가 복호화되는 위협이 존재한다.

4.2 OWE의 인증 기능 미비

OWE는 개방형 네트워크 환경에서 메시지의 암호화만 제공하고 인증 기능은 제공하지 않는다. 인증 기능이 없어 공격자는 중간자 공격을 통해 PMK를 생성하고 STA와 AP가 주고받는 메시지를 복호화한다. 인증을 위해 캡티브 포털(captive portal) 등의 부가적인 인증 기능을 제공하여 OWE를 안전하게 사용할 수 있다.

4.3 DPP의 중계 단말 추가에 따른 공격 벡터 확대

DPP가 인증 과정에서 중계 단말로 사용하는 모바일 기기에는 다양한 애플리케이션들이 동작하고 이러한 애플리케이션을 통해 악성코드에 감염될 위험이 존재한다. 감염된 모바일 기기를 사용할 경우 기기의 인증 정보가 공격자에게 노출된다. 중계 단말을 추가하며 확장된 공격 벡터는 WPA3에서 개선할 수는 없지만 DPP를 이용하고자 하는 사용자는 모바일 환경에서의 위험을 인지하고 대비해야 한다.

4.4 4-회 핸드세이크 절차 보호 취약

PMF는 4-회 핸드세이크를 정상적으로 마치고 비밀키를 이용하여 관리 프레임을 보호하기 때문에 비밀키를 공유하기 전에는 관리 프레임이 보호받지 못한다. 키 생성 이전에 인증 해제 프레임을 STA에게 전송하면 STA와 AP 간 연결이 종료되며 반복적으로 프레임을 전송하여 서비스 거부 공격(DoS, Denial of Service)이 가능하다[30]. 또한 키 생성을 유도하는 메시지를 반복적으로 전송함으로써 4-회 핸드세이크 과정의 STA를 대상으로 서비스 거부 공격이 가능하다[31]. 4-회 핸드세이크 절차를 보호하기 위해서는 키 교환 이전에 프레임을 인증 및 보호하는 기법을 제공해야 한다.

4.5 BIP 디자인 상 인증 절차 취약

BIP에서 사용하는 키는 IGTK로 AP에 연결된 모든 STA는 같은 키를 공유한다. 브로드캐스트/멀티캐스트 프레임은 일반적으로 AP가 생성하여 전송하지만 프레임이 AP에 의해 전송된 것인지 인증하는 별도의 메커니즘이 존재하지 않는다. 이 점을 이용해 공격자는 정당한 STA를 가장하여 보유한 IGTK로 인증된 브로드캐스트/멀티캐스트 프레임을 생성할 수 있다. 공격자는 인증 해제 프레임을 다른 STA에게 전송하여 네트워크 내부에서 서비스 거부 공격이 가능하다[28]. 악의적인 STA의 서비스 거부 공격을 방지하기 위해 브로드캐스트/멀티캐스트 프레임의 송신자를 인증할 수 있는 절차가 필요하다.

Ⅴ. WPA3 발전방향 논의

본 장에서는 WPA3가 지닌 두 가지 장점인 완전 순방향 비밀성 및 투명성(transparent) 제공과 프로토콜 적용에 있어 우려되는 성능 저하 문제를 논의한다.

보안 관점에서 완전 순방향 비밀성을 프로토콜에 제공하면 공격자가 임의의 연결에 비밀키를 획득하더라도 동일한 STA와 AP 간 이전 연결에서 전송되었던 메시지는 복호화 불가하다. 완전 순방향 비밀성은 보안 프로토콜이 반드시 만족해야 하는 요소이다. WPA3에서는 연결마다 서로 다른 PMK의 생성을 통해 완전 순방향 비밀성을 제공한다. WPA3의 방식 중 OWE와 Dragonfly 프로토콜에서 사용한 Diffie-Hellman 방식은 랜덤값을 사용하여 하나의 키가 단 하나의 연결에서만 유효하도록 하여 완전 순방향 비밀성을 제공한다[8].

WPA3의 프로토콜은 투명성을 제공하여 사용자가 STA와 AP 간의 복잡한 연결과정을 의식하지 않아도 연결이 이루어지도록 한다. 사용자는 프로토콜이 요구하는 연결을 위한 최소한의 행위만으로 프로토콜의 보안 기능을 제공받는다.

WPA3에서 보안성 강화를 위해 추가된 기능으로 성능 저하가 우려된다. WPA3의 프로토콜은 WPA2에 비해 STA와 AP 간 전송되는 메시지의 수와 양이

증가하였고 Diffie-Hellman 기반의 높은 연산량을 처리한다[32]. 프로토콜 설계 시 성능과 보안의 상충관계(trade-off)를 고려하여 최적의 성능 및 보안을 제공해야 한다.

Ⅵ. 결 론

WPA3는 WPA2에 비해 강화된 보안 기능을 가진다. 특히 PMK 생성과정의 보안이 강화되었고 개방형 네트워크의 메시지의 암호화를 지원한다. 또한 사용자 인터페이스가 제한된 기기와 AP 간 연결을 지원하며 관리 프레임 보호 기능이 필수로 적용되었다. 본 논문에서는 기존 WPA2가 가지고 있던 문제점들을 파악하고 WPA3에서 적용된 보안 기능이 문제점을 어떻게 개선하였는지 살펴보았다.

WPA3는 WPA2에서 발생한 문제점을 개선하여 기존 공격들을 효과적으로 방어할 수 있지만 여타 공격에 대해 보안 측면에서 안전하다고 단언할 수 없기 때문에 WPA3 발전 방향에 대한 논의가 필요하다. WPA3에 적용된 기존 프로토콜과 새롭게 도입된 보안 기능에서 취약점이 발생할 수 있으며 본 논문에서는 이 같은 관점에서 WPA3의 보완점을 탐색하여 제시하였다. 또한 WPA3가 개선된 방향을 분석하여 무선 Wi-Fi 네트워크 보안 프로토콜의 발전에서 고려해야 할 요소를 세 가지 측면에서 논의하였다. 첫째, 보안 프로토콜 설계 시 완전 순방향 비밀성을 필수로 만족해야 하며 둘째, 투명성을 제공함으로써 사용자의 편의를 보장해야 한다. 셋째, 보안 기능뿐 아니라 성능을 고려하여 프로토콜의 활용성을 높이는 방향으로의 발전이 필요하다. 본 논문의 WPA3에 대한 고찰이 더욱 안전한 무선 Wi-Fi 네트워크 환경을 구성하기 위한 연구의 기반이 되기를 희망한다.

References

[1] K. H. Baek, S. W. Smith, and D. Kotz, “A survey of WPA and 802.11i RSN authentication protocols,” *Dartmouth Comput. Sci. Tech. Report*, Nov. 2004.

[2] M. Vanhoef and F. Piessens, “Key reinstallation attacks: Forcing nonce reuse in WPA2,” in *Proc. 2017 ACM SIGSAC Conf. Comput. and Commun. Secur.*, pp. 1313-1328, Dallas, USA, Oct. 2017.

[3] M. Vanhoef and F. Piessens, “Release the kraken: New KRACKs in the 802.11 standard,” in *Proc. 2018 ACM SIGSAC Conf. Comput. and Commun. Secur.*, pp. 299-314, Toronto, Canada, Oct. 2018.

[4] D. Harkins and J. Malinen, *Addressing the issue of nonce reuse in 802.11 implementations*(2017), Retrieved May, 31, 2019, from https://mentor.ieee.org/802.11/dcn/17/11-17-1602-03-000m-nonce-reuse-prevention.docx.

[5] D. Harkins, *Release Davy Jones*(2018), Retrieved May, 31, 2019, from https://mentor.ieee.org/802.11/dcn/18/11-18-1990-05-000m-kill-the-kracken.docx.

[6] C. Kohlios and T. Hayajneh, “A comprehensive attack flow model and security analysis for Wi-Fi and WPA3,” *Electronics*, vol. 7, no. 11, pp. 1-28, Oct. 2018.

[7] Wi-Fi Alliance, “*WPA3 specification* v1.0,” Apr. 2018.

[8] Wi-Fi Alliance, “*Wi-Fi 6: High performance, next generation Wi-Fi*,” Oct. 2018.

[9] High efficiency wireless LAN task group, *Status of project IEEE 802.11ax*, Retrieved Jul., 31, 2019, from http://www.ieee802.org/11/Reports/tgax_update.htm.

[10] Wi-Fi Allance, *Wi-Fi Alliance introduces Wi-Fi CERTIFIED WPA3 security*(2018), Retrieved Jul., 27, 2019, from https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-certified-wpa3-security.

[11] H. M. Sun, B. T. Hsieh, and H. J. Hwang, “Secure e-mail protocols providing perfect forward secrecy,” *IEEE Commun. Lett.*, vol. 9, no. 1, pp. 58-60, Jan. 2005.

[12] C. P. Kohlios and T. Hayajneh, “A comprehensive attack flow model and security analysis for Wi-Fi and WPA3,” *Electronics*, vol. 7, no. 11, pp. 1-28, Oct. 2018.

[13] O. Nakhila, et al., “Parallel active dictionary attack on WPA2-PSK Wi-Fi networks,” in *Proc. 2015 IEEE MILCOM*, pp. 665-670, Tampa, USA, Oct. 2015.

[14] S. Viehbock, *Brute forcing Wi-Fi protected setup*(2011), Retrieved May, 31, 2019, from

http://warxezz.free.fr/direct/PDFs/PIN_wps_viehboeck.pdf.

[15] A. Sari and M. Karay, "Comparative analysis of wireless security protocols: WEP vs WPA," *Int. J. Commun., Netw. and Syst. Sci.*, vol. 8, no. 12, pp. 483-491, Dec. 2015.

[16] Wi-Fi Alliance, "*Wi-Fi certified Wi-Fi protected setup*," Mar. 2014.

[17] Z. Chi, et al., "EMF: Embedding multiple flows of information in existing traffic for concurrent communication among heterogeneous IoT devices," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, pp. 1-9, Atlanta, USA, May 2017.

[18] IEEE, "*IEEE 802.11w-2009 - IEEE standard for information technology – Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements. Part 11: Wireless LAN medium access control(MAC) and physical layer(PHY) specifications amendment 4: Protected management frames*," Sep. 2009.

[19] K. Bauer, H. Gonzales, and D. McCoy, "Mitigating evil twin attacks in 802.11," in *Proc. 2008 IEEE Int. Performance, Computing and Commun. Conf.*, pp. 513-516, Austin, USA, Dec. 2008.

[20] Wi-Fi Alliance, "*Wi-Fi certified WPA3 technology overview*," Jun. 2018.

[21] D. Harkins, "*Dragonfly key exchange*," IRTF RFC 7664, Nov. 2015.

[22] D. Harkins, "Simultaneous authentication of equals: A secure, password-based key exchange for mesh networks," in *Proc. 2008 2nd Int. Conf. Sensor Technol. and Appl. (sensorcomm)*, pp. 839-844, Cap Esterel, France, Aug. 2008.

[23] Wi-Fi Alliance, "*Wi-Fi certified enhanced open technology overview*," Jun. 2018.

[24] D. Harkins and W. Kumari, "*Opportunistic wireless encryption*," IETF RFC 8110, Mar. 2017.

[25] Wi-Fi Alliance, "*Device provisioning protocol specification v1.1*," Dec. 2018.

[26] IEEE, "*IEEE 802.11-2016 - IEEE standard for information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN medium access control(MAC) and physical layer(PHY) specifications*," Dec. 2016.

[27] H. Krawczyk and P. Eronen, "*HMAC-based extract-and-expand key derivation function (HKDF)*," IETF RFC 5869, May 2010.

[28] M. S. Ahmad and S. Tadakamadla, "Short paper: Security evaluation of IEEE 802.11 w specification," in *Proc. fourth ACM WiSec*, pp. 53-58, Hamburg, Germany, Jun. 2011.

[29] M. Vanhoef and E. Ronen, *Dragonblood: A security analysis of WPA3's SAE handshake* (2019), Retrieved May 31, 2019, from https://papers.mathyvanhoef.com/dragonblood.pdf.

[30] B. Bertka, "802.11w security: DoS attacks and vulnerability controls," in *Proc. Infocom*, Orlando, USA, Mar. 2012.

[31] C. He and J. C. Mitchell, "Analysis of the 802.11i 4-way handshake," in *Proc. 3rd ACM Workshop on Wireless Secur.*, pp. 43-50, Philadelphia, USA, Oct. 2004.

[32] Y. D. Kim, A. Perrig, and G. Tsudik, "Communication-efficient group key agreement," in *Proc. IFIP Int. Inf. Secur. Conf.*, vol. 65, pp. 229-244, Paris, France, May 2001.

남 지 현 (Ji-Hyun Nam)

2019년 2월 : 성신여자대학교 융합보안학과 학사
2019년 3월~현재 : 성균관대학교 전자전기컴퓨터공학과 석사과정
<관심분야> 보안공학, 네트워크 보안, 컴퓨터공학
[ORCID:0000-0002-3612-5409]

이 주 엽 (Ju-yeop Lee)

2014년 2월 : 성균관대학교 컴퓨터공학과 학사
2019년 3월~현재 : 성균관대학교 소프트웨어플랫폼학과 석사과정
<관심분야> 컴퓨터공학, 보안공학
[ORCID:0000-0003-4173-6260]

권 송 희 (Song-hui Kwon)

2019년 8월 : 성균관대학교 수학과 학사
2019년 9월~현재 : 성균관대학교 전자전기컴퓨터공학과 석사과정
<관심분야> 네트워크 보안, 보안공학
[ORCID:0000-0002-2875-7502]

최 형 기 (Hyoung-Kee Choi)

1992년 2월 : 성균관대학교 전자공학과 학사
1996년 2월 : Polytechnic Uni-versity in Brooklyn, NY 석사
2001년 2월 : Georgia Institute of Technology in Atlanta, GA 박사
2001년 1월~2004년 12월 : Lancope 근무
2004년 3월~현재 : 성균관대학교 소프트웨어대학 교수
<관심분야> 네트워크 보안, 리버스 엔지니어링
[ORCID:0000-0002-5342-5913]