Theme Article: Special Section on Novel Security Paradigms for Consumer Technologies

Evolution of Wi-Fi Protected Access: Security Challenges

Songhui Kwon and Hyoung-Kee Choi
Sungkyunkwan University.

***Abstract*—Security for Wi-Fi networks is now being upgraded to a new version, WPA3, after vulnerabilities and weaknesses in the previous versions were correctly patched. The most critical upgrades include 1) data traffics already sent remain a secret even if a preshared password of the Wi-Fi network is compromised by an adversary, and 2) weak passwords are immune to online and offline guessing attacks. This article explains in detail where in the previous versions these weaknesses originated and how in the new version they are rectified. Further, this article checks if there is still room for improvement, especially in security algorithms introduced in the new version.**

After 14 years of serving as a widespread security standard, Wi-Fi Protected Access 2 (WPA2) is about to be retired by the new standard WPA3.[1] Security upgrades and bug fixes to WPA2 include improvements in authentication, encryption, and strong default settings for robustness and resilience. WPA3 stages additional protections against new vulnerabilities for personal and enterprise networks. Users in the personal network receive increased protections from password guessing attempts, while enterprise users can take advantage of high-level security algorithms for handling and delivering sensitive data and internal information. An important part of WPA3 is that security is increased while complexity is not.

Consequently, network administrators in WPA3 may choose passwords that are easy to remember for their network users without being concerned about online or offline password guessing attacks. Data traffics that are already sent are protected from any password compromises in the future by using an ephemeral secret key.

For old security mechanisms developed for old versions of WPA and have remained in the current version and adapted security mechanisms

Digital Object Identifier 10.1109/MCE.2020.3010778
Date of publication 22 July 2020; date of current version 4 December 2020.

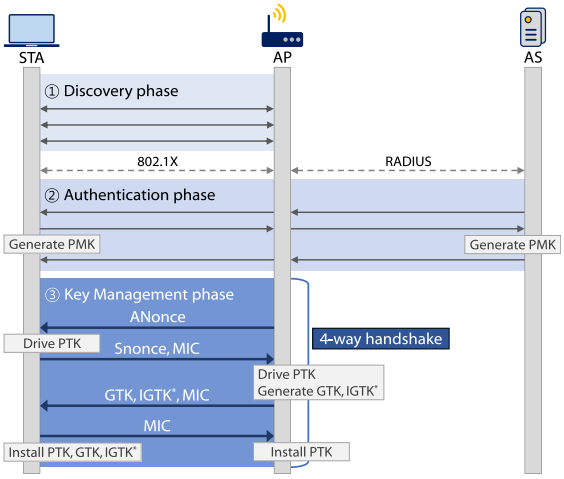

Figure 1. Three phases in the WPA2-Enterprise mode. The four-way handshake is a part of the key management phase. IGTK in the third message in the four-way handshake is optional for the PMF.

originated from other security protocols and were adapted for WPA3, we will trace back through a history of versions to see if any existence of security vulnerabilities may succeed into the current version without being rectified.

We will examine new mechanisms thoroughly to see if security upgrades can be retrofitted to incumbent security versions and cause any security violations in commercial fields.

OVERVIEW OF WI-FI PROTECTED ACCESS

WPA is an authentication and key management protocol developed by the Wi-Fi alliance. Until a new version, WPA3 is introduces it had two versions, which are WPA and WPA2. WPA was an interim version set up for suiting this protocol for being backward compatible with the vulnerable WEP until the IEEE 802.11i was officially available. The WPA2 is equivalent to IEEE 802.11i.[2] Furthermore, each version has two modes of operations, which are preshared key (PSK) and enterprise modes. In the PSK mode, the access point (AP) authenticates a station (STA) based on a password shared in advance. On the other hand, the enterprise mode the AP and STA authenticate mutually with the help of an authentication server (AS).

These two versions share a common stage of a three-phased initial setup. The three phases that were as illustrated in Figure 1 are 1) discovery, 2) authentication, and 3) key management. The first discovery phase has three message exchanges (① in Figure 1). The STA associates with the AP by advertising security capabilities and negotiating cipher suites.

In the second authentication phase, the STA and AP agree on the master key (MK) and derive the pairwise master key (PMK) based on the MK (② in Figure 1). The MK is either derived from the preshared password in the PSK mode or generated by the AS and delivered securely to the AP and STA, respectively, using the RADIUS and 802.1X in the enterprise mode.

Once the STA and AP share the PMK, these two parties proceed to the Key Management phase (③ in Figure 1). Both parties derive the pairwise temporal key (PTK) and confirm the possession of the same PTK by using the four-way handshake. The PTK is fresh in each association as it is derived from the PMK and two random numbers, respectively, chosen by each party for a single association.

SECURITY GOALS OF WI-FI NETWORKS

Threat Model

An adversary's ultimate goal in the Wi-Fi networks is to compromise communication channels between STAs and an AP. The adversary cannot only monitor and overhear the victim's messages in a passive fashion but also the adversary can intercept, inject, and manipulate packets for impersonation, session replay, message modification, and denial of services in an active fashion.

A rogue AP[3] is one of the active attacks where an adversary deploys an AP with the same service set identifier (SSID) as the target network. Once an STA is connected to the rogue AP, the adversary can control the victim's entire connections including disclosure of any network-level information.

Coffee shops and public places offer Wi-Fi networks to guests and visitors. Security for the Wi-Fi network prefers the personal mode to the enterprise mode because the enterprise mode incurs high costs and management overheads. A password in the personal mode must be shared by all guests and visitors. In case the password

is known to the public, which is perhaps of the case for most coffee shops, anyone can decrypt other guests' network traffic with the public password.

Security Requirements

A security goal in Wi-Fi networks is mainly to accommodate operationally secure services. Security requirements for Wi-Fi networks include security requirements for the general network protocol, which is confidentiality and integrity of data and mutual authentication of entities.

An STA would not succumb to the attachment of rogue APs if the attachment points were authenticated in advance by the STA. False AP or authentication servers could send forged messages to the STA to waste the resources in victims. This threat can be alleviated if mutual authentication is a prerequisite for any other operations in an STA. Illegal copying and modification of messages would not be easy once messages are authenticated and encrypted.

Future sessions will remain in secrecy even if a secret key in the current session is compromised. Under the circumstance that any messages, other than the exchanged in the specific session protected by the key, should not be affected by such compromise. This type of secrecy, referred to as perfect forward secrecy (PFS) in our subject, can be achieved by generating a unique secret key for every session.

FEATURES IN WPA3

Dragonfly, a Defend Against Offline Password Guessing Attack

A session key in WPA2 is computed from a preshared password and some publicly known values. In other words, one STA can snoop any other STA's sessions if the preshared password is known. The snooping becomes quite easy in cafés or restaurants where passwords are publicly available.

Even if the password is not public information yet, an adversary can still guess a password candidate and verify its guessed password.[4] This verification is possible because a hash value computed from the true password is available during the four-way handshake. WPA2 produces a 384-bit secret key called PTK. The first 128-bit

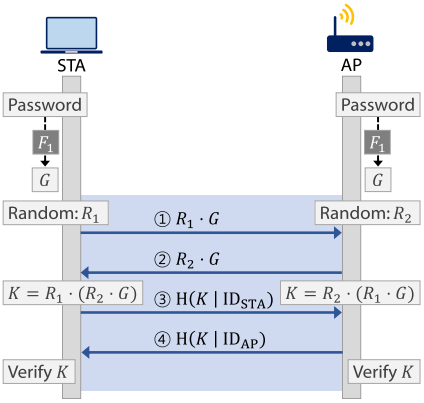

Figure 2. Dragonfly protocol resistant to offline guessing attack. The protocol satisfies PFS.

of the PTK is used as a key to generate secure hash values. The hash value gives an assurance of one's PTK possession to the other. The guess is correct if the hash value computed from the guess matches with the target hash value.

Besides, the adversary can expedite an entire verification by processing it offline. Even worse, the adversary can extrapolate a victim's future secret keys based on the current compromise. Secret keys in the WPA2 personal mode are subject to an offline guessing attack due to exposure of the hash value directly computed with the password.

WPA3's defense against the offline guessing attack is not to expose any derivatives of the preshared password. The preshared password is transformed into generator G by the known function as shown in Figure 2. The STA and AP exchange random numbers R_1 and R_2, respectively, after securing them in $R \cdot G$ (① and ② Figure 2). The secret key K is computed to $R_2 \cdot R_1 \cdot G$. Both parties confirm that they have the same secret key by comparing the hash value of the secret key (③ and ④ Figure 2). These additional exchanges of four messages are referred to as the Dragonfly handshake.[5] Notice that the Dragonfly variant used in WPA3 is also known as the simultaneous authentication of equals (SAE).

The offline guessing attack is not applicable in WPA3-SAE[1] because one cannot compute a secret key (K in Figure 2) from the password guess without knowing two random values. Even if the password is public information, compromising the secret key is quite difficult due to the ignorance of random values.

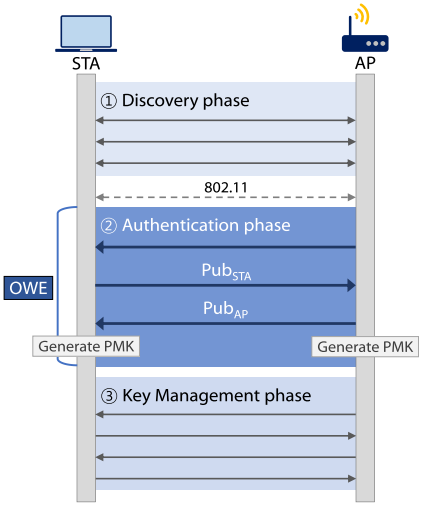

Figure 3. OWE overlaid over the authentication phase generates an ephemeral secret key for confidentiality.

Imagine that one can find a secret key from the hash value (③ and ④ in Figure 2) with brute force attacks. This finding does not help secret key compromises for future sessions as a secret key is derived from independently unique values in each session. In this sense, the Dragonfly handshake is considered to satisfy the PFS.

Enhanced Open Wi-Fi Networks

Network administrators often face situations where sharing secrets in advance is not affordable. If this is the case, open Wi-Fi networks in WPA2 is an option. This mode of operation dispenses with any encryption or authentication putting network users in the exposure of any security threats. A resolution approached in the WPA3 is the provision of message confidentiality based on an ephemeral secret key. This new approach is referred to as the enhanced open Wi-Fi network, it is also called the opportunistic wireless encryption (OWE).[6]

As shown in Figure 3, the enhanced open is overlaid over the authentication phase, where two messages carry public keys of the STA and AP. Based on these public keys, using the Elliptic Curve Diffie-Hellman (ECDH) algorithm, both parties derive an ephemeral secret key that becomes the PMK. The four-way handshake immediately follows for setting up secret keys for an incoming session. The STA and AP may decide to cache the PMK for a period to avoid expensive ECDH computation for possible reassociation in the near future.

For confidentiality, the enhanced open network requires the AES CCMP encryption method with a 128-bit key and does not allow any old and broken methods like TKIP or even WEP. A shared yet insecure PSK may lead to information disclosures to other users, while OWE is resistible to such threats. Due to its encryption-only nature, OWE is most useful in a coffee shop or anywhere that encryption is necessary, but authentication is not. Consequently, OWE is vulnerable to man-in-the-middle attacks. Further, it is vulnerable to denial-of-service (DoS) attacks in that an adversary may send deassociation or deauthentication messages in the discovery phase to interrupt the handshake.

Device Provisioning Protocol

The Wi-Fi protected setup (WPS)[7] is a feature in WPA2 for a convenient and fool-proof setup for accessing the Wi-Fi network. The feature is most helpful for home users who know little about Wi-Fi network security or for devices with limited or no display interfaces to user inputs.

The WPS-enabled AP carries a button or an eight-digit personal identification number (PIN). An STA's user simply pushes the button or enters the PIN to establish secure channels. The WPS automatically configures the wireless network name (SSID) and PMK. The WPS replaces authentication in the WPA by ensuring that the STA is near the AP and confirming that the STA can access information on the AP. However, WPA security was compromised due to rather a short PIN number and an insecure mechanism for key generation.[8]

The device provisioning protocol (DPP)[9] is an authentication protocol in WPA3 for improving convenience and security over the WPS. The DPP is composed of eight messages in four phases as shown in Figure 4. It has no central authority to coordinate an entire procedure. Rather, provisioning in the DPP allows a trusted relay to bootstrap unauthenticated devices by gaining trust in a device's public keys through out-of-band channels (Bootstrapping in Figure 4). The relay binds the public key to the device's identifier once the device proves possession of a matching private key. This completes the device's authentication

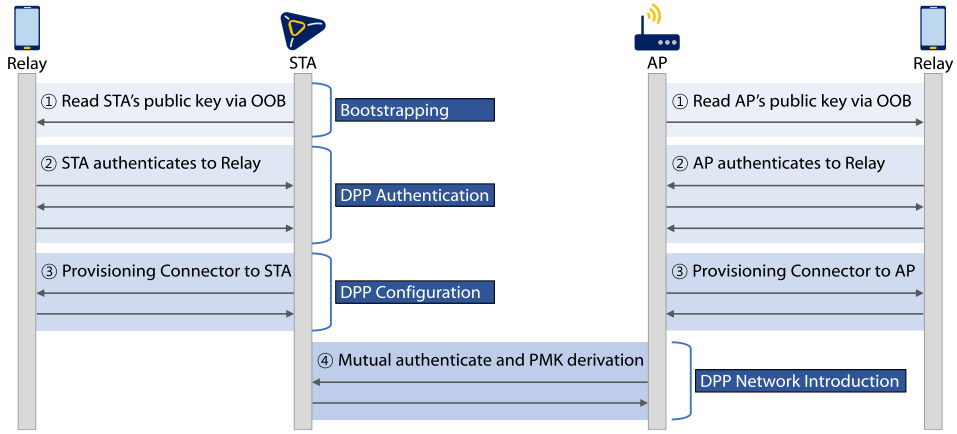

Figure 4. DPP is composed of eight messages in four phases. The two devices authenticate mutually and agree on the PMK for network access.

to the relay (Authentication in Figure 4). After authentication, the relay returns a token, called a connector, to the device. The token includes an authentication blob signed by the relay and the relay's ephemeral public key (Provisioning in Figure 4).

For a network access, a DPP-provisioned device exchanges an authentication blob with another DPP-provisioned device. Mutual authentication happens at this stage when one device proves a signature in the connector with the relay's public key. These devices derive the PMK by implementing an ECDH key exchange (Network introduction in Figure 4). The PMK is fresh in each provisioning as it is based on the ephemeral public keys chosen by both devices.

Security Upgrade in Enterprise Mode

An STA can connect to an AP with varying degrees of security options, such as ciphers, hash functions, key exchanges, and authentication methods. One of the issues in the WPA2-enterprise mode was too many options, some of which turn out to be insecure. For instance, using a TLS cipher suite that performs an RSA key exchange with a 1024-bit certificate would undermine the strength of security significantly. Such issues are caused by the STA's intractability on parameters negotiated at the time of initiation, offering a possibility for STAs to forcibly choose the least secure options.

The WPA3-enterprise mode requires a minimum length encryption key of 256-bit and use of Commercial National Security Algorithms (CNSA) approved cipher suites.[1] For instance, 384-bit hashed message authentication mode (HMAC-SHA384) for hashing, NIST's p384 elliptic curve for key establishment and digital signatures, and AES-GCM-256 for data encryption and authentication. With CNSA, the EAP method must be EAP-TLS. It is not possible to employ mix-and-match algorithms in an insecure manner not to enforce cipher downgrades.

Transition Mode in OWE and SAE

WPA3 provides transition modes in OWE and SAE, respectively, for allowing a gradual migration to new versions.[16] An AP in the transition mode for OWE is configured to create two SSIDs with separate beacons. One is an open SSID for the legacy open network. The other is a hidden SSID for OWE. OWE-capable STAs first connects to the open SSID. In the beacon, the STA will learn to look for beacons from the hidden SSID advertising OWE capabilities. Legacy STAs simply ignore new options in the beacon.

The SAE transition mode runs WPA3-SAE and WPA2-PSK on the same basic service set (BSS) with the same SSID. The password is the same in both modes. STAs with the WPA3 capacity connect to a network by using the WPA-SAE mode, while legacy STAs connect to a network by using the WPA2-Personal mode.

A transition mode for the WPA3 enterprise mode is not available because this mode is not backward compatible. Because of this incompatibility deploying, the WPA3-Enterprise mode

requires a flag day to switch a security level to a higher strength.

SECURITY ANALYSIS OF WPA3

Downgrade Attack for Dragonfly

WPA2-PSK and WPA3-SAE can be operated on the same BSS in the transition mode. To avoid STA's confusions, the standard has decided to use the same password for both modes.

Mathy Vanhoef and Eyal Ronen[11] demonstrated a downgrading attack for WPA3-SAE called the "Dragonblood." This attack forces to downgrade a protocol to a vulnerable version in the WPA3-SAE transition mode. An adversary may install a rogue AP or an evil-twin AP with the same SSID of the target AP. The rogue AP opts out the WPA3-SAE mode and only advertises the WPA2-PTK mode. A victim STA is forced to choose the WPA2-PSK mode. As discussed elsewhere, a weak password in the WPA2-PSK mode is subject to an offline dictionary attack. A countermeasure suggested that an STA should remember if a network supports the WPA3-SAE mode. In this way, the STA never connects this visited network by using a weaker handshake even though the first visit may still be vulnerable.

An attacker who determines the password can access Wi-Fi networks irrespective of the WPA's mode. In addition, even if an attacker is in the WPA3-SAE mode, other STAs that connect the same SSID as the attacker still benefit from forward secrecy because the secret key remains unknown to the attacker.

This attack has a limitation in that an adversary must play an AP role in running the four-way handshake. The downgrade attack toward an AP by an adversary playing an STA role should fail because of an adversary's incapability of generating the hash value demanded in the guessing attack. Such critical hash values derived from the PTK are contained in the second and third messages in the four-way handshake. An adversary as an STA not being aware of the password cannot generate the hash value in the second message, thus the victim AP must reject the handshake after verifying a wrong hash value. In contrast, an adversary as an AP does not have any problems in getting the hash value from the victim.

Weaknesses in Protected Management Frame

Management frames are used by the STA or AP for initiating new sessions or tearing down on-going sessions. Since these frames must be heard and understood by all STAs, they must be transmitted as unencrypted. However, they must be protected from misuses if an attacker could spoof management frames to disrupt on-going sessions.

The IEEE 802.11w[10] suggests protected management frame (PMF) prevents such DoS attacks. The PMF is optional in WPA2, while it is mandatory in WPA3. The benefit reaped by the PMF is a replay protection and message integrity for unicast and broadcast management frames.

Integrity group temporal key (IGTK) is a secret key generated by an AP and delivered to STA in the third message during the four-way handshake (see Figure 1). The AP uses IGTK to generate a hash value by using AES-128 in the CMAC mode for the protection of management frames. Both the AP and STA maintain an IGTK Packet Number (IPN). The IPN is used as a sequence number to protect packets from being replayed. For unicast management frames, PMF uses the same secret key as any other data frames.

The IGTK is not available until the four-way handshake. Management frames transmitted before the handshake remain unprotected against the deauthentication attack.[12] In this attack, the adversary floods the victim STA and/or the legitimate AP spoofed deauthentication and deassociation frames. Once the victim's on-going session is disconnected by the deauthentication attack, the adversary launches the evil-twin AP attack.

To defend against the deauthentication attack, OWE mandates the PMF for protections of management frames. However, the PMF is not effective for an entire lifetime of STA and AP association. An adversary can still launch the deauthentication attack when management frames remain unprotected.

Performances Overhead by Security Upgrade

Priority in WPA3 security is to support PFS. By providing PFS STA can isolate the key compromise within that session so that this compromise is not epidemic to future sessions. In addition, the WPA3 accommodates transparency in accessing Wi-Fi networks. Devices without any user

Table 1. Security Capabilities of WEP, WPA/WPA2, and WPA3 in Default Setting.

Capabilities		WEP	WPA/WPA2	WPA3	References
Year in released		1997	2004	2018	[1][2][14]
En/Decryption	Personal	RC4	TKIP/AES-CCMP	AES-CCMP	
	Enterprise		TKIP/AES-CCMP	AES-GCMP	
Integrity	Personal	No	CCMP 64-bit MIC	CCMP 64-bit MIC	
	Enterprise			GCMP 128-bit MIC	
Key length	Personal	40-bit or 104-bit	128-bit	128-bit	
	Enterprise		128-bit	256-bit	
Pre-shared key		PSK	PSK	SAE	[1][5][14]
Open network encryption		Open	Not supported	OWE	[6][14]
Easy connect		Not supported	WPS	DPP	[7][9]
PMF		Not supported	Optional	Mandatory	[1][10]
Offline dictionary attack		Vulnerable	Vulnerable	Invulnerable	[4][15]

interfaces can still access Wi-Fi networks without undergoing long and complex procedures.

WPA3 trades off security and transparency with delay and performance. The number of messages in WPA3 has been increased by four compared with the one in WPA2. This increase is caused by the exchange of ECDH public keys in Dragonfly and Enhanced Open. At the same time, this exchange has also increased a round-trip time. The Diffie–Hellman implementation for a key exchange levy a significant amount of computational burdens especially if STA is a device without or a limited user interface, such as an IoT device.

Additional resources are required to OWE for message confidentiality. Confidentiality is met by encrypting every message by using AES CCMP (Counter with CBC-MAC Protocol) with a 128-b secret key. It takes about roughly 32 ms to encrypt 500 B.[13] Although this amount is small to nil, still the extra overhead introduces the lesser imperative amendments to the existing clients.

Security Capabilities of Different Versions

Table 1 illustrates the security capabilities of different Wi-Fi versions. By 1999, the first version of Wi-Fi security was known as the Wireless equivalent privacy (WEP). It was easily overcome by unsophisticated attacks because of a short key length. WPA and WPA2 soon followed WEP to compensate for shortcomings. A support of the message integrity code (MIC) was added for data integrity and message authentication. Changes in confidentiality are mainly the encryption algorithm and key size. The algorithm was changed from RC4 to AES, while the key size was increased to 128-b.

In WPA3, STA can choose a key size for encryption between 128 and 256-b. Furthermore, a hash size of message integrity is also increased up to 384-b.

CONCLUSION

Our daily usage and reliance on Wi-Fi networks have changed considerably since WPA2 was released. However, the security of the Wi-Fi networks was compromised by unsophisticated attacks, where some were quite critical. WPA3 addresses the shortcomings of WPA2 and adds functionalities, which were not available in WPA2. WPA3 protects data traffic even if a password is compromised after the data was transmitted. WPA3 will be further fortified by addressing some of the immediate concerns regarding resilience against DoS attacks, validation of Wi-Fi security implementations, and consistency in security configurations.

ACKNOWLEDGMENTS

This work was supported by Institute for Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea Government (MSIT) (2019-0-01343, Regional strategic industry convergence security core talent training business).

REFERENCES

1. G. O. Wi-Fi Alliance, "WPA3 specification," Version 2.0, Dec. 20, 2019. [Online]. Available: https://www.wi-fi.org/download.php?file=/sites/default/files/private/WPA3_Specification_v2.0.pdf
2. A. H. Adnan *et al.*, "A comparative study of WLAN security protocols: WPA, WPA2," in *Proc. Int. Conf. Adv. Elect. Eng.*, 2015, pp. 165–169.
3. M. Waxid, S. Zeadally, and A. K. Das, "Mobile banking: Evolution and threats: Malware threats and security solutions," *IEEE Consum. Electron. Mag.*, vol. 8, no. 2, pp. 56–60, Mar. 2019.
4. O. Nakhila, A. Attiah, Y. Jin, and C. Zou, "Parallel active dictionary attack on WPA2-PSK Wi-Fi networks," in *Proc. IEEE Military Commun. Conf.*, 2015, pp. 665–670.
5. D. Harkins, "Dragonfly key exchange," IETF RFC 7664, Nov. 2015.
6. Wi-Fi Alliance, "Opportunistic wireless encryption specification," Version 1.0, Apr. 9, 2018. [Online]. Available: https://www.wi-fi.org/file/opportunistic-wireless-encryption-specification
7. Wi-Fi Alliance, "Wi-Fi CERTIFIED Wi-Fi protected setup: Easing the user experience for home and small office Wi-Fi networks," Mar. 2014. [Online]. Available: https://www.wi-fi.org/download.php?file=/sites/default/files/private/wp_Wi-Fi_CERTIFIED_Wi-Fi_Protected_Setup_20140409.pdf
8. D. Bongard, "Offline bruteforce attack on WiFi protected setup," *presented at the PasswordsCon*, Dec. 2014.
9. Wi-Fi Alliance, "Device provisioning protocol specification v1.1," Dec. 3, 2018. [Online]. Available: https://www.wi-fi.org/file/device-provisioning-protocol-specification
10. K. K. Raju and V. V. Kumari, "Formal verification of IEEE 802.11w authentication protocols," *J. Netw.*, vol. 8, no. 4, pp. 769–778, Apr. 2013.
11. M. Vanhoef and E. Ronen, "Dragonblood: Analyzing the Dragonfly handshake of WPA3 and EAP-pwd," in *Proc. IEEE Symp. Secur. Privacy*, 2020, pp. 517–533.
12. B. Bertka, "802.11w security: DoS attacks and vulnerability controls," in *Proc. IEEE Int. Conf. Comput. Commun.*, 2012. [Online]. Available: http://blogs.ubc.ca/computersecurity/files/2012/04/BBertka_bbertka_571B_final.pdf
13. S. Tripathy and J. Mathew, "Design and evaluation of an IoT enabled secure multi-service ambulance tracking system," in *Proc. IEEE Region 10 Conf. TENCON*, 2016, pp. 2209–2214.
14. A. H. Lashkari, M. Mansoor, and A. S. Danesh, "Wired equivalent privacy (WEP) versus Wi-Fi protected access (WPA)," in *Proc. Int. Conf. Signal Process. Syst.*, 2009, pp. 445–449.
15. T. Newsham, "Cracking WEP keys," *presented at the Black Hat USA 2001*, Jul. 2001.

Songhui Kwon is currently working toward the Master's degree in electrical and computer engineering at Sungkyunkwan University, Seoul, South Korea. Her research interests include authentication, secure messaging protocol and reverse engineering. She received the Bachelor's degree in mathematics and computer science from Sungkyunkwan University, in 2019. Contact her at songhee@o365.skku.edu.

Hyoung-Kee Choi is a Professor with the Department of Software, Sungkyunkwan University, Seoul, South Korea. His research interests include network security and vulnerability assessment. He received the Ph.D. degree in electrical and computer engineering from Georgia Institute of Technology, Atlanta, GA, USA, in 2001. He is the corresponding author of this article. Contact him at meosery@skku.edu.