International Journal of Information Security (2025) 24:74
https://doi.org/10.1007/s10207-025-00988-3

REGULAR CONTRIBUTION

Security analysis of the Wi-Fi Easy Connect

George Chatzisofroniou[1] · Panayiotis Kotzanikolaou[1]

Abstract
Wi-Fi Easy Connect is a protocol introduced by the Wi-Fi Alliance, as the core replacement of the Wi-Fi Protected Setup (WPS). It aims to facilitate user-friendly provisioning methods, such as scanning a QR code, or leveraging a short-range wireless protocol like Near-Field Communication and Bluetooth. In this paper, we thoroughly examine the security and privacy properties of Wi-Fi Easy Connect (version 3.0); an exhaustive assessment that has not been previously conducted to the best of our knowledge. In addition to uncovering security issues, we identified key aspects of the specification's design that surprisingly may increase, rather than decrease the attack surface for malicious actors, when compared to its predecessor, WPS. All our findings have been shared with the Wi-Fi Alliance, and the responses regarding action items or risk acceptance have been considered in our analysis. Finally, we analyzed *hostapd*, the most popular software implementation of Wi-Fi Easy Connect, and we uncovered an implementation issue that allowed an attacker to subvert future connections, highlighting the risks when implementations do not fully adhere to the protocol's design specifications. Our analysis illustrates the danger of introducing security and privacy vulnerabilities in protocols, when protocol design favors usability versus security.

Keywords Wi-Fi · Security · Authentication · Provisioning · Cryptography · Vulnerabilities

1 Introduction

The widespread adoption and utilization of wireless technology led to a significant increase in the use of Wi-Fi networks. Wi-Fi, adheres to the IEEE 802.11[1] specification, offering a convenient and efficient method for internet connectivity and wireless data sharing. Wi-Fi's adaptable nature positions it as an optimal solution for diverse applications, ranging from personal use to enterprise environments. It has become the standard for wireless home networking, as well as for network access on public or guest networks. In addition, businesses, educational institutions, and other organizations heavily depend on Wi-Fi to provide seamless connectivity.

One of the security protocols that is widely used alongside Wi-Fi is the Wi-Fi Protected Setup (WPS) [1]. WPS is a network security standard that was created by Cisco in 2006 and aims to make it easy for home users to set up Wi-Fi Protected Access (WPA) without having to understand the complexities of wireless security. However, a major security vulnerability was revealed in December 2011 which affects wireless routers that have the WPS PIN feature enabled by default [2]. This vulnerability allows a remote attacker to recover the WPS PIN in a few hours through a brute-force attack. Once the WPS PIN is recovered, the attacker also has access to the network's WPA/WPA2 pre-shared key (PSK). As a result of this vulnerability, users have been advised to turn off the WPS PIN feature, although this may not be possible on some router models.

Wi-Fi Easy Connect was introduced by the Wi-Fi Alliance in June 2018 along with WPA-3, as the core replacement for the WPS protocol. Being the replacement of WPS, it is expected to see extensive deployment across millions of devices globally in the coming years. The underlying protocol of Wi-Fi Easy Connect, named Device Provisioning Protocol [3] (DPP),[2] aims to facilitate user-friendly Wi-Fi provisioning methods. In DPP, bootstrapping and authentication can be configured in various user-friendly ways including among others, scanning a quick response (QR) code, short-range wireless protocols like Near-Field Communication (NFC) and Bluetooth Low Energy (BLE).

[1] https://www.ieee802.org/11/.

✉ George Chatzisofroniou
sophron@latthi.com

[1] SecLab, Department of Informatics, University of Piraeus, Piraeus, Greece

[2] The terms "Device Provisioning Protocol", "DPP" and "Wi-Fi Easy Connect" are used interchangeably throughout this paper.

Published online: 07 February 2025

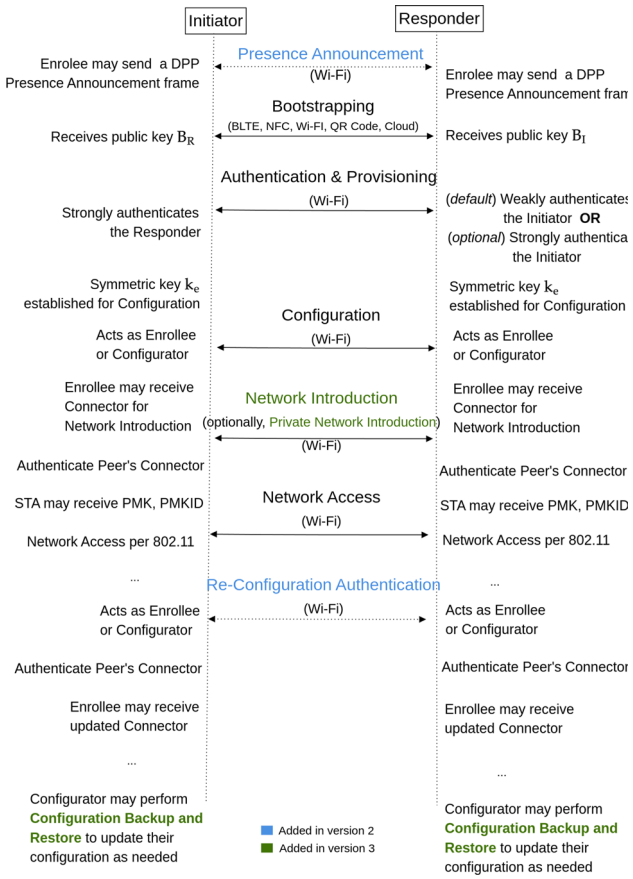

Fig. 1 High level overview of DPP

At the time of writing this paper, there is a growing trend of vendors implementing the DPP protocol annually. According to the Wi-Fi Alliance's Product Finder [4], there are currently 23 Wi-Fi Easy Connect^{TM} certified devices in the market from 6 different vendors, including major ones such as MediaTek, Sagemcom and Qualcomm. Additionally, some vendors have implemented part of the Wi-Fi Easy Connect specification. For example, Android only supports DPP in Initiator mode. Also, popular open-source software such as hostapd, wpa_supplicant, and iwd have already implemented a majority of the Wi-Fi Easy Connect specification. The DPP specification is subject to ongoing development, having undergone three releases since its initial deployment, with the present iteration being version 3.0. Each successive release incorporates substantial enhancements to the specification, while also ensuring compatibility with previous versions.

Motivation. To the best of our knowledge, no thorough security analysis of the Wi-Fi Easy Connect protocol has been conducted prior to this study. Considering that this protocol is specifically designed to streamline the provisioning of devices in contemporary networks and is anticipated to become a widely accepted standard, conducting a thorough security assessment is critical. Detecting and mitigating potential vulnerabilities in its early stages can enhance the protocol's robustness and support its safe implementation, thereby safeguarding users and networks globally.

Contribution. In this paper we provide a comprehensive security and privacy analysis of DPP, the fundamental protocol of Wi-Fi Easy Connect. Specifically:

- We conducted a thorough security analysis of the DPP protocol unveiling security vulnerabilities that can be exploited over the network. These vulnerabilities enable attackers to bypass or downgrade DPP security, escalate permissions over other peers, and compromise the privacy of honest devices.
- We thoroughly examined and highlighted areas that introduce new risks in comparison to its predecessor, the WPS protocol. These emerging risks indicate a shift in potential vulnerabilities and challenges that were not relevant in the previous WPS protocol.
- Besides the protocol specification itself, protocol implementation may also affect security. In this context, we performed code auditing of the hostapd implementation of DPP, revealing an implementation issue that allows attackers who successfully associate using DPP to manipulate future connections. We provide the technical details into this issue to aid other implementations in avoiding similar pitfalls.

The discovered attacks target various sub-protocols or security features within the Wi-Fi Easy Connect specification, which were introduced in different versions of the DPP protocol. However, all the discovered security issues are applicable as of the latest released version 3.0. Our findings demonstrate the danger of introducing novel security and privacy vulnerabilities in modern protocols when usability is over-prioritized in contrast to security.

As part of our responsible disclosure process, we communicated our findings on vulnerabilities within the DPP to the Wi-Fi Alliance. Several conclusions emerged from this interaction. The Wi-Fi Alliance acknowledged certain issues, such as the Configurator Impersonation Attack (described in Sect. 3.2) and the Group Downgrade Attack (see Sect. 3.3), for further discussion and potential mitigation strategies. However, other vulnerabilities, including the Private Introduction Protocol Downgrade (see Sect. 3.4), were considered by Wi-Fi Alliance as acceptable risks. Our disclosure helped highlight areas of potential improvement while ensuring transparency in addressing security concerns.

Structure of the Paper. In Sect. 2, we provide the necessary background on Wi-Fi Easy Connect (DPP). In Sect. 3, we present the results of our security analysis, highlighting the novel attacks and exploits. We then focus on an implementation-specific bug that we have uncovered in Sect. 5. In Sect. 6 we briefly examine the related work on

Table 1 Main entities and roles in DPP

Roles	Description
STA (Station)/AP (Access Point)	These are the basic roles in IEEE802.11. The STA receives WiFi services facilitated by the AP. Either the Enrollee or the Configurator may act as AP
Initiator /Responder	These roles define which entity initiates the DPP protocol
Enrollee /Configurator	These roles define which entity provides the authentication configuration and which entity receives the configuration information. Either the Initiator or the Responder may act as the Configurator

Wi-Fi security and compare our work with existing studies. Finally, Sect. 7 provides discussion and conclusions.

2 Background

In DPP, all Wi-Fi devices use public key-based identities to ensure the authenticity of other devices.

2.1 Protocol notation

We will follow the symbols and notation of the Wi-Fi Easy Connect specification [3]. Following the terminology of the specification, the two main entities of the IEEE 802.11 protocol are the *Station* (STA) that represents a device with Wi-Fi access capabilities, and the *Access Point* (AP), that represents the device that provides Wi-Fi connectivity. As shown in Table 1 STA and AP may also obtain additional authentication roles regarding the DPP sub-protocols. A *Configurator* is a logical entity with capabilities to enroll and provision devices for device-to-device communication or Infrastructure communication. Usually the AP has the role of the Configurator. In contrast, an *Enrollee* is a device that is enrolled in a Wi-Fi network via a Configurator.

2.2 Phases of the DPP

As shown in Table 1, based on the initiation capabilities of the devices, they may act as *Initiator* or *Responder*. A device acts as an Initiator if it initiates the DPP Authentication protocol, while it acts as a Responder if it responds to the initiation of the DPP Authentication protocol by another Initiator. Either the Configurator or the Enrollee can take the role of Initiator and the Responder and vice versa. Using the notation defined by DPP, let I (resp. R) represent the Initiator (resp. the Responder) of the protocol. We briefly describe the main phases of the protocol. Table 2 summarizes the long-term keys used in Wi-Fi Easy Connect, while we refer to the specification [3] for a complete description.

Table 2 Long-term credentials used in DPP

Type	Abbreviation	
Bootstrapping keys	Public: B_I, B_R	Private: b_I, b_R
Privacy protection key	Public: Ppk	Private: ppk
Passphrase	PSK	
Digital envelope password	P	

Let (B_I, b_I) (resp. (B_R, b_R)) denote the long-term identity public/private key pair of the Initiator (resp. of the Responder), called the *bootstrapping keys*. As defined in the protocol specification, a bootstrapping key is a public key that is obtained through a bootstrapping method. From a high-level view DPP involves the following phases or sub-protocols (see Fig. 1).

During the *Bootstrapping phase*, the Initiator obtains the public key of the Responder B_R; in cases when mutual authentication is performed, the Responder may also obtain the public key of the Initiator B_I. DPP supports various methods of transferring a public key, such as: (a) scanning a QR code that contains an encoded version of the key, (b) exchanging the key wirelessly using the Public Key Exchange (PKEX) protocol [3], (c) using another short-range communication protocol, such as NFC and BLE, or (d) utilizing other proprietary methods, such as those that utilize the cloud. Regardless of the chosen method, the bootstrapping phase results in the Initiator, and optionally the Responder, obtaining the public key of a supposed trusted device. It is worth mentioning that these methods are not without their limitations. The physical security constraints in BLTE and NFC, such as proximity and line-of-sight, have been shown to be weak in the past against relay attacks and skimming [5]. The security level desired by a user may vary depending on the selected bootstrapping method for DPP, however, this flexibility can be difficult for less experienced users to navigate, potentially leaving them vulnerable to attacks.

In the *Authentication and Provisioning phase*, the long-term bootstrapping public key(s) B_R (and optionally B_I), are utilized to establish a temporary, authenticated connection for the exchange of credentials. The Responder is strongly authenticated to the Initiator by providing proof of ownership of the private key b_R. On the other hand, the Initiator can choose between two methods of authentication (see Table 3). The default option is a weak authentication, where the Initiator simply proves knowledge of the Responder's public key B_R as a means of confirming prior bootstrapping. Alternatively, mutual authentication can be enabled, allowing the Initiator to prove ownership of b_I and provide strong authentication to the Responder. According to the specification, by enabling strong mutual authentication both entities can be certain that the authenticated connection they established in the bootstrapping can be carried over in later phases

Table 3 DPP authentication methods

Specification requirement	Authentication method	
Responder authenticates Initiator	Initiator proves knowledge of B_R (Weak—Default)	Initiator proves knowledge of b_I (Strong—Enforced)
Initiator authenticates Responder	Responder proves ownership of b_R	
Enrolee (Configurator) authenticates Configurator (Enrollee)	Enrollee or Configurator proves knowledge of an element signed with ppk (i.e. a Connector)	
AP authenticates STA	STA proves knowledge of PSK	

of the protocol (e.g., the Configuration and Network Access phases). In some cases, depending on the bootstrapping method used, this means carrying over the authentication they performed in a different communication channel (i.e., from BLTE to Wi-Fi). For example, a mobile phone (Initiator) uses the BLTE method to exchange keys with another phone (Responder). After finishing with the bootstraping phase, the two devices wish to proceed with the authentication phase which occurs over Wi-Fi. The goal of mutual authentication is for both devices to ensure that the other endpoint is the entity they trusted over BLTE.

The outcome of this phase is the exchange of a symmetric key k_e, which is utilized in the next phase, the *Configuration phase*, to establish the actual communication keys, known as the connector keys (Connector-I and Connector-R respectively). The connectors are then utilized in the *Network Access phase*, to establish the actual network keys through Elliptic Curve Diffie-Hellman (ECDH) exchange, creating a Pairwise Master Key (PMK) for normal network access.

In version 2 of the Wi-Fi Easy Connect specification, two new features were added to the protocol. The first one is the introduction of the DPP *Presence Announcement phase*, which allows Enrollees to signal to potential Configurators that they are ready to engage in a DPP exchange. This frame contains a hash that includes the Enrollee's public bootstrapping key and can be broadcasted by devices that aim to initiate the DPP Authentication exchange regardless of whether they act as Initiators, by forcing Configurators to proceed with the authentication protocol in the channel on which they received the DPP Presence Announcement frame. The second feature is the inclusion of the DPP *Re-Configuration Authentication phase*, which allows for mutual authentication between an Enrollee and a known Configurator. This protocol involves a 3-way message exchange that generates a shared secret and an authenticated key, using the Configurator's connector and the Enrollee's connector issued during a previous configuration exchange.

In version 3 of the Wi-Fi Easy Connect specification, additional enhancements have been introduced to further augment the protocol's functionality and security. The *Network Introduction Protocol* and the *Private Introduction Protocol* facilitate communication between the provisioned Enrolles within the DPP network controlled by the Configurator, offering options for network introduction with or without privacy considerations. Moreover, a novel protocol has been incorporated to enable the backup and restoration of configuration information for DPP Configurators. This protocol, named *Configuration Backup and Restore*, mandates the storage of a DPP digital envelope, with storage and retrieval methods being vendor-specific. It places the onus on the owner to manage the password safeguarding the content-encryption key, ensuring the integrity and confidentiality of the configuration data. In essence, the protocol facilitates the distribution of the privacy protection key (Ppk, ppk), an authentication credential that is possessed only by authorized Configurators within the network.

3 Security analysis of DPP

We conducted a comprehensive security analysis of the DPP protocol, identifying three notable security vulnerabilities exploitable by attackers:

Configurator Impersonation: A vulnerability in the *DPP Re-Configuration Protocol* enables enrolled peers (Enrollees) to elevate their privileges to Configurators through offline brute-forcing.
PKEX Group Downgrade: A vulnerability in the *PKEX Bootstrapping* method allows an attacker to exploit the ECDH group selection process, forcing a downgrade to a less-desirable cryptographic group in certain scenarios.
Private Introduction Protocol Downgrade: An attacker can exploit a vulnerability to forcefully downgrade the connection from the *Private Introduction Protocol* to the less private *Network Introduction Protocol*.

The remainder of this section offers a detailed analysis of the three identified attacks, along with proposed remediation plans, following the description of the corresponding threat model.

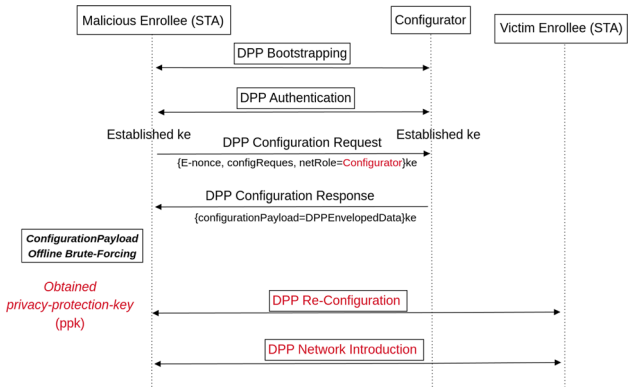

Fig. 2 Configurator impersonation attack

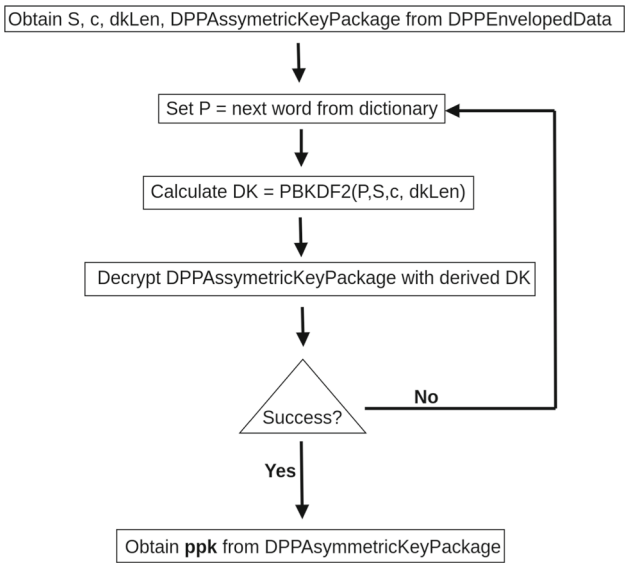

Fig. 3 Offline brute-force on `DPPEnvelopedData`

3.1 Threat model

The threat model defined in the Wi-Fi Easy Connect specification, considers three types of attackers: (i) passive adversaries capable of intercepting transmitted information during provisioning or subsequent operations, (ii) active adversaries with the ability to conduct association attacks and divert devices to unauthorized networks, and (iii) active adversaries capable of disrupting provisioning services without user notification [6]. In addition, it is assumed that the attacker consistently remains within the wireless proximity of the target and in some instances, is able to respond to wireless frames faster than the original recipient.

The attacks presented in this section conform to the above threat model. To clarify the particular prerequisites for each attack, the 'Exploitability' subsection presented within each attack further elucidates the necessary conditions for a successful attack, covering the specific parameters and constraints under which the discussed vulnerabilities can be effectively exploited.

3.2 Configurator impersonation attack in the DPP re-configuration phase

Although the protocol considers common threats like offline brute-force attacks in several areas of the specification (including the PKEX exchange), the same degree of focus has not been given to the Configuration Backup and Restore sub-protocol introduced in the third version. In this sub-protocol, the DPP digital envelope (denoted as `DPPEnvelopedData` in Fig. 2) is protected with the privacy-protection-key (denoted as `ppk`). This key, in turn, is encrypted with a password set by the end user.

Reliance on a password represents a common pitfall in the design of wireless protocols, as passwords are inherently susceptible to brute-force attacks. By using a password-based approach for protecting the `ppk`, the protocol inadvertently introduces a significant weakness, enabling malicious actors to systematically attempt all possible combinations of characters until the correct password is discovered.

According to the specification, a new Configurator can be enabled and configured during the *DPP Configuration protocol* (as described in Sect. 2), where the new Configurator acts as an Enrollee and sets the `netRole` to "Configurator" in the DPP Configuration Request frame (see Fig. 2). Additionally, if the parameter `netRole` in the DPP Configuration request has the value "Configurator", the `configurationPayload` shall consist of one instance of `DPPEnvelopedData`.

While the protocol effectively authenticates Enrollees and verifies their possession of the proper bootstrapping key, it lacks provisions for authorizing the Enrollee's request. This oversight allows malicious Enrollees to potentially exploit the system by requesting to become a new Configurator, thereby assuming the role of a malicious Configurator capable of hijacking future connections. Upon receiving a request from an Enrollee, the Configurator merely acknowledges the Enrollee's request *without evaluating its legitimacy* or verifying whether the Enrollee's intention aligns with the network's security policies. Consequently, a malicious Enrollee can exploit this loophole to pose as a legitimate candidate for Configurator status, without undergoing any scrutiny of its intentions or qualifications.

The attack's first steps include capturing the `DPPEnvelopedData` from the DPP Configuration Request (Fig. 2) and performing an offline password attack (see Fig. 3). The attacker first obtains a captured `DPPEn- velopedData`, which contains the encrypted payload along with the necessary parameters. Then, the attacker attempts an offline password attack (e.g., brute-force or dictionary attack on the password). In a password attack scenario against a cap-

tured DPPEnvelopedData, the attacker aims to recover the underlying password value P used in the key derivation process. This password is used for deriving the key DK required to decrypt the DPPEnvelopedData and obtain the DPPAsymmetric- KeyPackage that includes the private key-pair of a provisioned Configurator.

Note that the password attack can be performed *offline*, giving the attacker a significant advantage to successfully reveal the password. With each derived key DK (see Fig. 3), the attacker attempts to decrypt the captured DPPEnvelopedData using the underlying encryption scheme. If the decryption operation fails, the attacker moves on to the next password guess. If decryption is successful, the attacker has recovered the DPPAsymmetricKeyPackage, indicating a successful compromise of the encrypted data.

Upon attaining the role of a Configurator, a malicious actor gains the ability to disseminate unauthorized configurations. These configurations can instruct network stations to associate with the malicious actor's device posing as an AP serving the desired SSID. This manipulation allows the malicious actor to intercept and potentially manipulate network traffic. Such actions could lead to data interception, or the insertion of malicious payloads into the network traffic flow.

Exploitability. The attacker needs access to the DPP network as a valid Enrollee. Achieving this heavily depends on the bootstrapping methods used by the network administrators, as well as the distribution of bootstrapping keys. Furthermore, the success of the attack is strongly influenced by the entropy of the password. High-entropy passwords substantially elevate computational complexity, making brute-force attempts impractical.

Impact. The attacker will gain access to ppk, the privacy-protection-key which is shared among Configurators, including both retired ones and newly provisioned ones. After escalating their role to a Configurator, the attacker can distribute rogue configuration files that will allow the attacker to potentially intercept and manipulate wireless network's traffic in its totality.

Wi-Fi Alliance Response. "Wi-Fi Alliance will consider allowing for other methods of protecting the DPPEnvelopedData, in addition to the password method which is considered an acceptable risk."

Proposed Remediation. Unfortunately, the Wi-Fi Alliance's mitigation strategy does not fully resolve the issue, as the password-based method remains valid, and alternative methods of protecting DPPEnvelopedData may still be vulnerable to other attacks. To address this flaw in the protocol, several remediation measures can be implemented:

a. Introduction of authorization checks for the Configurators: This would involve the implementation of robust authorization checks within the DPP Configuration protocol to evaluate the legitimacy of Enrollees' requests to become Configurators. In this way the Enrollee's identity would be verified against predefined security policies before granting Configurator privileges.
b. Unique Key per Configurator: Another possible solution would be to use a cryptographic key that is unique to each Configurator, rather than using a single shared key for all Configurators. This ensures that even if one Configurator's key is compromised, the security of other Configurators remains intact. Employing individualized keys for each Configurator enhances the overall resilience of the system against attacks targeting Configurator credentials.

3.3 Lack of cryptographic verification in PKEX bootstrapping group negotiation

As explained in Sect. 2, PKEX is one of the bootstrapping methods supported by DPP. As per the 802.11 standard, stations have the ability to prioritize ECDH groups in a user-configurable order. For example, a user may avoid certain ECDH groups because they may not be supported by certain devices or software, or due to a threat model.

The goal of the PKEX group negotiation is to identify the most preferred common group between the two parties. The protocol favors the Initiator as it is the entity that proposes the first group. According to the specification, the Responder is only allowed to propose a different group if the group proposed by the Initiator is not supported. More specifically, the protocol starts with the Initiator sending its desired group in a PKEX Exchange Request frame. The Responder receives the message and if it does not support this group, it replies with a STATUS_BAD_GROUP along with a new offered group (see Fig. 4).

However, it is at this point that an attacker intercepting the channel can block the original message and send a bogus PKEX Exchange Response frame that includes the weakest option from all the alternative options for the Responder, as illustrated in Fig. 4. In this example, the Initiator first sends a PKEX Exchange Request frame requesting group 26 (curve P-224). The Responder receives the message and since it does not support the requested group (26), it generates a PKEX Exchange Response with the DPP Status set to STATUS_BAD_GROUP and proposes group 30 (EC_BRAIN-POOLP512R1) as an alternative. However, the attacker blocks the PKEX Exchange Response frame and sends a PKEX Exchange Request frame proposing group 27 (ECC_BRAINPOOLP224R1) instead. The Initiator accepts group 27, which is weaker than the group originally offered by the Responder. Since this negotiation process is not cryptographically validated, it is vulnerable to this type of attack.

It's important to note that while the established group (group 27) is "stronger" than what was originally requested

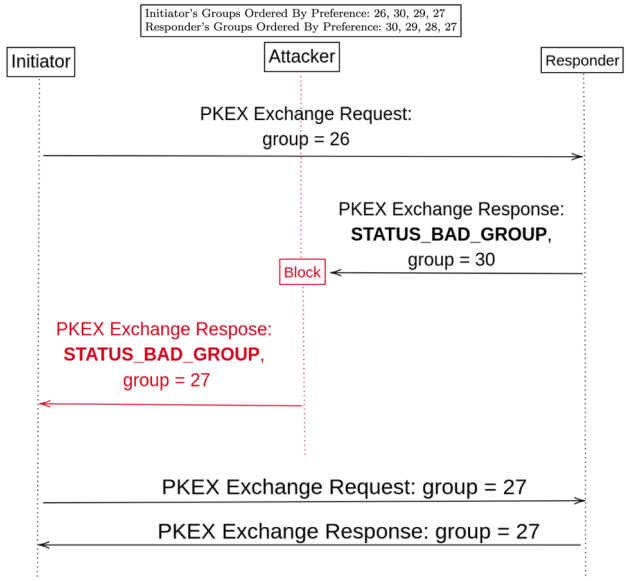

Fig. 4 DPP PKEX group downgrade attack

(group 26), a user's choice of elliptic curve groups may involve factors beyond just the prime length. For example, a cautious user might avoid certain groups and their associated parameters due to concerns about possible vulnerabilities or backdoors, as seen for example with Curve1174 [7].

Exploitability. The attack is applicable in cases where the Initiator requests for a group that is not supported by the Responder. Since group's preference for elliptic curves might involve considerations beyond just the length of the prime, the group the Initiator is requesting must be lower than the Responder's proposed alternative. In addition, The attacker must be within the wireless range of both the Initiator and Responder and have the ability to intercept the communication between the two. The attacker also needs knowledge of the supported groups of both endpoints in order to determine which groups can be agreed upon by both entities (this information can easily be obtained by intercepting traffic from the two entities, even in other associations with other clients). Finally, an attacker can use readily available software to block the Initiator's PKEX Exchange Request message.

Impact. The above attack underscores that the negotiation process lacks the cryptographic protection found in SAE's group negotiation as specified in 802.11. Although the scenario described in the Exploitability subsection is unlikely in most default settings, should it occur, the two entities will agree upon a less preferred ECDH setting. In the given example, this results in the entities agreeing on their least favored group. From the perspective of the Initiator, the agreed group is at least considered stronger than the original request, even though it may be the least favorite choice. On the other hand, from the perspective of the Responder, the resulting cyclic group was never influenced by the Responder's preferred order. The agreed group may provide less security for the established connection, as the group may have a known vulnerability. This can lead to a weaker encryption and a higher likelihood of successful attacks on the connection. This attack is similar to the group downgrade attack identified in the WPA3 specification [8, 9].

Wi-Fi Alliance Response. "Wi-Fi Alliance will take this matter under discussion and decide a course of action regarding cryptographic protection of group negotiation."

Possible Remediation. An easy way to mitigate the attack is by adding cryptographic verification of the groups that were originally sent in the PKEX Exchange phase of the protocol. During the Commit-Reveal phase, the Responder should also include their supported groups in the commitment that they sign and send to the Initiator. The Initiator will calculate its own version of the commitment, which includes the Responder's MAC address, public bootstrapping key, ephemeral keys, and supported groups. If the commitment received from the Responder does not match the one calculated by the Initiator, it indicates that the information used to calculate the hash was tampered with, which could be due to a group downgrade attack. In this case, the Initiator should abort the connection. This approach ensures that the groups that were agreed upon in the PKEX Exchange phase are cryptographically verified before proceeding with the rest of the protocol.

3.4 Private introduction protocol downgrade

The *Private Introduction Protocol* was introduced in the third version of the WiFi Easy Connect specification as shown in Fig. 1, and allows a DPP client in an infrastructure network to establish a connection with the AP while prioritizing privacy. This protocol encrypts the device's connector while transmitting it to the AP. Initially, the device issues a `Private Peer Introduction` message, which can be sent directly to the AP or broadcasted to discover APs on the current channel. Upon receiving this message, the AP responds with a `Private Peer Introduction Notify` message containing transaction details and its own connector. The receiving device, say device B then validates the received connector and proceeds with key establishment. The protocol continues with device B wrapping the connectors and sending an update to the sending device A, which completes the protocol by unwrapping and validating the connector. The successful termination of the Private Introduction Protocol ensures a secure connection setup.

A privacy issue arises from the potential jamming or destruction of the `Private Peer Introduction` message by adversaries. If disrupted, the affected device is forced to abandon the secure Private Introduction Protocol and resort to the less secure Network Introduction Protocol.

Impact. An attacker may gain insight into the DPP device's attempts to connect to a specific network, including its SSID. This exposure affects the device owner's privacy and potentially facilitates the execution of association attacks [10].
WiFi Alliance Response. "Wi-Fi Alliance considers the attack an acceptable risk. Inducing the abandonment of the Private Introduction Protocol and forcing the use of Network Introduction Protocol is merely privacy-exposing as it will expose the non-AP STA's connector to a passive attacker. There is no compromise of confidentiality or integrity of communication by using the Network Introduction Protocol."
Possible Remediation. To address this kind of privacy risk, future iterations of the specification should implement countermeasures to validate the STA's preferences from the AP in subsequent exchanges. By verifying the legitimacy and integrity of the STA's preferences during ongoing communication sessions, the AP can detect and mitigate potential attacks aimed at disrupting the Private Introduction Protocol.

4 Security considerations of the DPP threat model

The transition from WPS to DPP in modern Wi-Fi networks introduces new security challenges. Although not constituting explicit vulnerabilities within the protocol, the design of DPP inherently introduces certain security weaknesses compared to its predecessor, which we will highlight in this section. According to Wi-Fi Alliance, these weaknesses are considered acceptable within the established threat model.

DPP operates independently of traditional authentication protocols such as WPA2/WPA3, relying on public-key cryptography rather than shared passphrases for device provisioning. While this offers advantages in terms of security and ease of use, it also creates new attack vectors and management complexities that are discussed below. Specifically, we highlight two security concerns regarding mixed authentication modes and key management, as well as recommendations that may reduce the attack surface associated with these areas.

4.1 Mixed authentication modes

Not all devices fully support the DPP, as many vendors implement only certain aspects of it. For example, some may support only QR code provisioning. As a result, network administrators must maintain multiple provisioning methods, creating a mixed authentication mode. For instance, in a DPP network that needs to accommodate various devices, regardless of their specific DPP implementation, it may support both PKEX and QR code provisioning methods simultaneously. However, this flexibility introduces a potential security issue: the system could default to the weaker of the two methods-in this case, the QR code method, which relies on single-factor authentication as opposed to mutual authentication. This allows devices to bypass the stronger mutual authentication by opting for the weaker provisioning method, if enabled.
Wi-Fi Alliance Response. "The DPP protocol certification requires an Enrollee to be able to do mutual authentication as well as non-mutual authentication but it is not required to perform non-mutual in the event that mutual is not available. This is a policy decision for the deployed Enrollee."
Proposed Security Enhancement. While the Wi-Fi Alliance appears to have designed this flexibility intentionally, we believe that, given the vulnerabilities inherent to Wi-Fi-such as the ease of client spoofing-as well as the lack of security awareness among many network operators, the protocol specification should not support mixed authentication modes. If strong mutual authentication is enabled, all connections should be required to use this method to ensure a consistent security level. In a "mutual-auth only" mode, the Responder would always authenticate the Initiator. While it's possible that certain DPP implementations will enforce this, it remains uncertain unless explicitly specified in the standard.

4.2 Privacy-protected keypair management

As discussed earlier, at the core of the DPP is the DPP Configurator, a central entity responsible for provisioning devices onto the network. Unlike WPS the DPP Configurator retains ongoing control over network access, even when network credentials such as WPA2 or WPA3 are changed. This is because it operates through the Privacy-Protected Keypair (Ppk/ppk), which is independent of those credentials.

However, the DPP specification lacks mechanisms for revoking or updating this crucial keypair. This contradicts security policies that may require regular rotation of sensitive cryptographic keys. Since the ppk allows continuous access to the network even if the network settings are modified, a compromised ppk could grant an attacker permanent access.

The vulnerability described in 3.2 serves as an example of an attack that allows attackers to gain access to the critical keypair, with recovery being exceptionally difficult as it require restarting the entire protocol and invalidating all distributed bootstrapping keys.
Proposed security enhancement To revoke access for compromised Configurators or PPK keypairs, revocation mechanisms must be put in place to update the sensitive keypair [11]. A similar approach is employed in Enterprise Wi-Fi networks utilizing the EAP-TLS protocol that rely on the Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP) to invalidate compromised certificates, preventing unauthorized access to the network [12].

5 Analysis of the DPP implementation in Hostapd

In addition to the security analysis at a protocol level that lead to the identification of weaknesses that are implementation-agnostic, we also examined a specific software implementation of DPP, to explore for possible implementation-specific vulnerabilities. For this purpose, we chose *hostapd* which is a popular software used for access point and authentication server implementations. It is widely used in a variety of settings, including home networks, public Wi-Fi hotspots, and enterprise networks. For our code audit of the DPP implementation in hostapd, we thoroughly analyzed the source code to identify potential implementation vulnerabilities. The goal of this code audit analysis of DPP implementations was to explore the potential for additional vulnerabilities induced on top of protocol-wide weaknessess and not to serve as an exhaustive code analysis of DDP implementations.

Re-using the PKEX code. According to the Wi-Fi Easy Connect specification [3], the PKEX protocol utilized in DPP, is vulnerable to threats if public keys and codes (passwords) are reused. For example, if an entity has successfully bootstrapped public keys in the past and uses the same code with multiple keys, they could potentially subvert a future bootstrapping by passively observing the keys. To mitigate this risk, once the PKEX protocol is completed successfully and both the device and peer have each other's trusted public key, the code should be irreversibly deleted. However, our code audit of the PKEX implementation in hostapd revealed that the dpp_pkex_build_exchange_req function found in the file "./src/common/dpp_pkex.c" generates a new public key for every exchange request transmitted, and the pkex code remains active even after a successful PKEX association. This can potentially lead to an automatic association attack, as the attacker can impersonate a Configurator and use the same code, to trick new Enrollees into connecting to the attacker instead of the legitimate Configurator. Following responsible disclosure, we immediately notified the hostapd developers, who were able to address the issue. A Common Vulnerability and Exposure identifier (CVE-2022-37660) was assigned to the vulnerability [13]. The identified vulnerability serves as an example of an implementation mistake that can lead to severe impact, highlighting the importance for vendors to conduct thorough code audits when implementing the specification.

6 Related work and comparison

The increasing popularity of Wi-Fi brings significant security challenges for the design of wireless protocols [14]. In the literature, several attacks and vulnerabilities of Wi-Fi protocols have been reported. We briefly summarize some of the key findings, along with a comparison with this work.

Vanhoef et al. [15] uncovered Key Reinstallation Attacks (KRACK) in WPA2. By exploiting flaws in the four-way handshake they managed to force nonce reuse, thus verifying critical vulnerabilities in the widely used WPA2 protocol, long after its deployment. The same researchers identified weaknesses in the Dragonfly handshake of WPA3, including side-channel leaks and downgrade attacks, termed "Dragonblood" [9]. More recently [16] they demonstrated a time-memory trade-off attack on the Simultaneous Authentication of Equals authentication and key exchange method of WPA3 (WPA3-SAE), highlighting that even modern protocol designs can remain vulnerable to sophisticated attacks.

Some works examine the use of fuzzing techniques against the authentication process of WPA2 and WPA3. Marais et al. [17] proposed a fuzzing strategy called WPA3Fuzz, based on which three vulnerabilities that may be exploited to DoS attacks are discovered. In addition, Kambourakis et al. [18] proposed an extensible open-source Wi-Fi fuzzer tool, which covers the IEEE 802.11 management and control frame types, as well as the WPA3-SAE. The fuzzer can be used to detect vulnerabilities potentially existing in wireless Access Points under WPA3 and WPA2.

Chatzoglou et al. [18, 19] demonstrated the feasibility of Denial-of-Service (DoS) attacks on WPA3-SAE, emphasizing the susceptibility of the protocol to resource exhaustion and de-authentication techniques, as well as the need for comprehensive security mechanisms that may ensure the reliability and robustness of the respective protocols.

Other works on Wi-Fi security focus on Wi-Fi association attacks [10, 20], through which attackers may gain man-in-the-middle position, by tricking unsuspecting clients into connecting to a rogue network. These attacks often exploit Wi-Fi features that, while related to the 802.11 specification, are not explicitly defined by any published standard, allowing for varied and potentially insecure custom implementations.

Concerning Wi-Fi provisioning protocols, the Pixie Dust attack [21] against the WPS protocol, the predecessor of Wi-Fi Easy Connect, has been known for nearly a decade, and it may have been actively exploited even before that. The attack demonstrates how static, predictable values in the protocol can allow attackers to brute-force the key offline. Interestingly, the vulnerability arises from fundamental design choices inherent to the protocol, making any mitigation at the protocol level challenging without compromising compatibility with millions of devices already in use.

In summary, the related work highlights the importance of identifying and addressing security flaws in Wi-Fi protocols at the earliest stage possible, as timely mitigation is crucial for protecting millions of devices. Although existing works have revealed various attacks and vulnerabilities in WPA2/WPA3 handshake and authentication[9, 15, 16, 18], DoS attacks on

WPA3 [18, 19], attacks on the WPS provisioning protocol [21] and Wi-Fi association attacks [10, 20], to the best of our knowledge an analysis of the Wi-Fi Easy Connect specification has not been conducted prior to this study. Despite the different protocols or security fields of Wi-Fi security examined in the related work, a common ground is that Wi-Fi protocols and specifications should prioritize security from the outset and include thorough peer reviews before they are widely deployed. This work aims to assist in this direction, concerning the Wi-Fi Easy Connect specification.

7 Discussion and conclusions

Wi-Fi Easy Connect is a powerful technology that aims to streamline the process of connecting devices to Wi-Fi networks. However, as our analysis has shown, several weaknesses in DPP can be exploited by attackers. The protocol design-specific attacks that we described cannot be solved without updating the protocol itself. The impact of these attacks can be particularly severe given the huge number of expected users of DPP.

The migration from WPS to DPP clearly shifts the burden of risk management significantly toward the network operator, who must make critical decisions about which provisioning methods to support. Operators are thus faced with the complex task of balancing the need for robust security against the demand for user-friendly provisioning processes. Operators who lack education in information security may find it challenging to manage these trade-offs.

Overall, while DPP offers sophisticated security capabilities compared to its predecessor, it simultaneously requires careful deployment and meticulous management to prevent the erosion of the very protections it is designed to strengthen.

Our analysis reveals that the usability features added in the newer versions of DPP (v2 and v3) have introduced additional security vulnerabilities, such as the risk of connected users impersonating the Configurator and distributing malicious files to other devices.

The identified weaknesses serve as additional evidence, of the need to carefully consider the security implications of user-friendliness features in new protocols (such as the use of mixed authentication modes or reconfiguration capabilities).

The results highlight the importance of thoroughly analyzing new Wi-Fi protocols that are anticipated to be widely adopted. It is a call for rigorous scrutiny and evaluation to ensure the robust and secure integration of these advanced technologies into our digital infrastructure.

Funding This work was supported in part by the University of Piraeus Research Centre.

Declarations

Conflict of interest The authors have no relevant financial or non-financial interests to disclose.

References

1. Wi-Fi Alliance. Wi-Fi Protected Setup (WPS) Specification version 1.0h. 2006. https://www.wi-fi.org/discover-wi-fi/wi-fi-protected-setup (2015)
2. Viehbck, S.: Wi-Fi Protected Setup online pin brute force vulnerability (2011)
3. Wi-Fi Alliance. Device provisioning protocol (dpp) specification, Technical Specification, Wi-Fi Alliance, Latest Version. https://www.wi-fi.org/discover-wi-fi/device-provisioning-protocol (2025). Accessed 02 Jan 2025
4. Wi-Fi Alliance. Wi-Fi Alliance product finder. https://www.wi-fi.org/product-finder. Accessed 07 Jan 2023
5. Group, N.: Ble proximity authentication vulnerable to relay attacks. Available: https://www.nccgroup.com/us/research-blog/technical-advisory-ble-proximity-authentication-vulnerable-to-relay-attacks/ (2023). Accessed 02 Jan 2025
6. Nobles, P.: Vulnerability of IEEE802.11 WLANs to MAC layer DoS attacks. In: IET Conference Proceedings, pp. 14–14(1). https://digital-library.theiet.org/content/conferences/10.1049/ic.2004.0670 (2004)
7. Bernstein D.J., Hamburg, M., Krasnova, A., Lange, T.: Elligator: elliptic-curve points indistinguishable from uniform random strings. In: Proceedings of the 2013 ACM SIGSAC conference on Computer & Communications Security, pp. 967–980 (2013)
8. WiFi Alliance: WPA3 specification version 1.0. Available: https://www.wi-fi.org/file/wpa3-specifica-tion-v10
9. Vanhoef, M., Ronen, E.: Dragonblood: analyzing the dragonfly handshake of WPA3 and EAP-pwd. In: IEEE Symposium on Security & Privacy (SP). IEEE (2020)
10. Chatzisofroniou, G., Kotzanikolaou, P.: Association attacks in IEEE 802.11: exploiting WiFi usability features. In: Proceedings of the International Workshop on Socio-Technical Aspects in Security and Trust (STAST). Springer , pp. 107–123 (2019)
11. National Institute of Standards and Technology (NIST): A closer look at revocation and key compromise in public key infrastructures. National Institute of Standards and Technology, Tech. Rep. https://www.nist.gov/publications/closer-look-revocation-and-key-compromise-public-key-infrastructures (2023). Accessed 02 Jan 2025
12. IEEE Standard for Local and Metropolitan Area Networks–Port-Based Network Access Control, IEEE Std. 802.1X-2010. https://standards.ieee.org/standard/802_1X-2010.html (2010)

13. Common Vulnerability and Exposure database: CVE-2022-37660. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37660 (2022)
14. Rondon, L.P., Babun, L., Aris, A., Akkaya, K., Uluagac, A.S.: Survey on enterprise internet-of-things systems (e-iot): a security perspective. Ad Hoc Networks, vol. 125, p. 102728. https://www.sciencedirect.com/science/article/pii/S1570870521002171 (2022)
15. Vanhoef, M., Piessens, F.: Key reinstallation attacks: Forcing nonce reuse in wpa2. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, ser. CCS '17. ACM, New York, NY, USA, pp. 1313–1328. http://doi.acm.org/10.1145/3133956.3134027 (2017)
16. Vanhoef, M.: A time-memory trade-off attack on wpa3's sae-pk. In: Proceedings of the 9th ACM on ASIA Public-Key Cryptography Workshop, ser. APKC '22, pp. 27–37. Association for Computing Machinery, New York, NY. https://doi.org/10.1145/3494105.3526235(2022)
17. Marais, S., Coetzee, M., Blauw, F.: Simultaneous deauthentication of equals attack. In: Wang, G., Chen, B., Li, W., Di Pietro, R., Yan, X., Han, H. (eds.) Security, Privacy, and Anonymity in Computation, Communication, and Storage, pp. 545–556. Springer, Cham (2021)
18. Kampourakis, V., Chatzoglou, E., Kambourakis, G., Dolmes, A., Zaroliagis, C.: Wpaxfuzz: sniffing out vulnerabilities in wi-fi implementations. In: Cryptography, vol. 6, no. 4. https://www.mdpi.com/2410-387X/6/4/53 (2022)
19. Chatzoglou, E., Kambourakis, G., Kolias, C.: How is your WiFi connection today? DoS attacks on WPA3-SAE. J. Inf. Secur. Appl. **64**, 103058 (2022)
20. Chatzisofroniou, G., Kotzanikolaou, P.: Exploiting WiFi usability features for association attacks in IEEE 802.11: attack analysis and mitigation controls. J. Comput. Secur. **30**(3), 357–380 (2022)
21. Bongard, D.: Offline bruteforce attack on WPS: The pixie dust attack. Presentation at Hack.lu 2014. https://archive.hack.lu/2014/Hacklu2014_offline_bruteforce_attack_on_wps.pdf (2014). Accessed 02 Jan 2025