Analysis of VoWiFi deployments: An ePDG server security study

Riccardo Fantasia, Leonardo Pantani

1 Introduction

Voice over Wi-Fi (VoWiFi) is emerging as a viable alternative to traditional cellular network calls, offering coverage and cost advantages, especially in areas with poor cellular signal reception. VoWiFi traffic is routed through an IPsec tunnel established between the user device (User Equipment, UE) and the ePDG (Evolved Packet Data Gateway), a key element of the mobile network operator's infrastructure. The security of this tunnel is therefore crucial to ensure the confidentiality and integrity of voice communications.

The initial phase of IPsec tunnel negotiation, managed by the Internet Key Exchange (IKE) protocol, in its IKEv1 [10] and IKEv2 [1] versions, is crucial for overall security. During this phase, the UE and ePDG agree on the security parameters to be used, including the symmetric encryption algorithm, the hashing algorithm and the Diffie-Hellman group for key exchange. Inadequate configuration of the cryptographic parameters, using outdated algorithms or weak parameters, can affect the security of the entire system, making communications vulnerable to interception, decryption and manipulation attacks.

This study aims to systematically analyse the security configurations of the ePDGs of an extensive sample of mobile network operators, in order to assess the level of adoption of appropriate security practices and to identify any critical issues. For our purposes, particular attention was paid to the different Diffie Hellman configurations that the various operators support.

2 Network architecture and role of ePDG in VoWiFi

Analysing the security implications of Voice over Wi-Fi (VoWiFi) requires a timely understanding of the underlying network architecture and the specific role of the Evolved Packet Data Gateway (ePDG). This section introduces the essential architectural concepts, with a focus on the routing of VoWiFi traffic and the functionality of the ePDG within 4G LTE and 5G NR mobile networks.

2.1 Contextualization of VoWiFi in mobile network architecture

VoWiFi is a service that enables voice and video calls over IEEE 802.11 compliant WLAN (Wireless Local Area Network) networks, relying on the infrastructure of a mobile network operator. This service is classified as 'non-3GPP access' as it does not use the 3GPP-standardised radio access network (EUTRAN or NG-RAN).

The key element in enabling VoWiFi is the ePDG, a gateway located at the border between the operator's network and external networks. Its primary function is to terminate IPsec tunnels established by UEs (User Equipment) for VoWiFi traffic, ensuring its confidentiality and integrity.

2.2 ePDG functionalities and interfaces

The ePDG performs the following functions:

1. **IPsec Tunnel Termination**: The ePDG is the termination point for IPsec tunnels established by VoWiFi compatible UEs. It manages the negotiation of security parameters via the IKE (Internet Key Exchange) protocol and the establishment of IPsec SAs (Security Associations).

2. **Authentication and authorisation**: The ePDG, interacting with the AAA servers and the HSS (Home Subscriber Server) via the Diameter protocol, performs authentication and authorisation of UEs requesting access to the VoWiFi service. This process may use IMSI (International Mobile Subscriber Identity) credentials or X.509 digital certificates.

3. **Traffic routing**: Following authentication and establishment of the IPsec tunnel, the ePDG routes VoWiFi traffic to the IMS (IP Multimedia Subsystem), the infrastructure of the Core Network responsible for managing multimedia services.

In terms of interfaces, the ePDG connects to the core network's Packet Data Network Gateway (PGW) via the S2b interface, based on the GPRS Tunneling Protocol (GTP) in 4G LTE environments. The PGW, in turn, acts as an anchor point for data traffic and an interface to external networks.

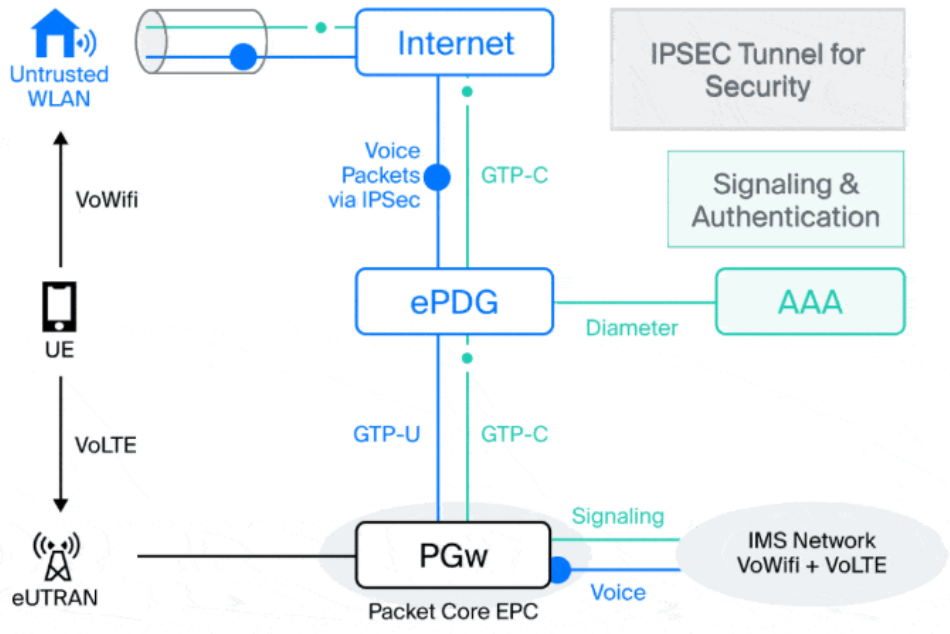


Figure 1: VoWiFi traffic flow and interfaces involved

2.3 Architecture Evolution with5G

Although the VoWiFi paradigm remains conceptually unchanged in the transition to 5G, the network architecture undergoes an evolution. In the 5G Core (5GC), the equivalent of the ePDG is the Non-3GPP InterWorking Function (N3IWF), which performs similar functions of terminating IPsec tunnels for non-3GPP access. This architecture is shown in Figure 2.

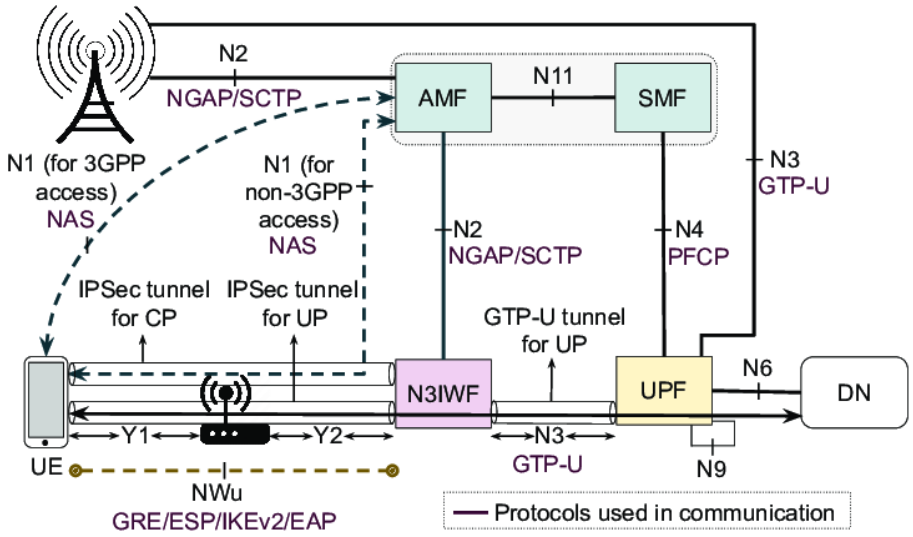


Figure 2: 5G Architecture with N3IWF for VoWiFi

3 VoWiFi Security and IKE protocol

The security of VoWiFi communications rests on several pillars: authentication, confidentiality and data integrity. The IPsec protocol, and in particular IKE, provides the necessary mechanisms to guarantee these security requirements.

3.1 IPsec and the role of IKE

IPsec is a protocol suite standardised by the Internet Engineering Task Force (IETF) that operates at the network layer (layer 3 of the OSI model) and provides security services such as authentication, confidentiality, integrity and anti-replay [2]. IKE, in its two versions (IKEv1 and IKEv2), is the protocol in charge of negotiating Security Associations (SAs) between the user device (UE) and the ePDG. An SA defines the security parameters that will be used to protect a specific connection, including symmetric encryption algorithms, hashing algorithms, authentication method, Diffie-Hellman group for key exchange and SA lifetime [3].

The negotiation of the AS via IKE takes place in several stages. The initial phase, shown in Figure 3, involves the exchange of messages for the configuration of a secure communication channel, through which authentication and cryptographic key exchange take place. This phase is the same regardless of the authentication method that will be used.

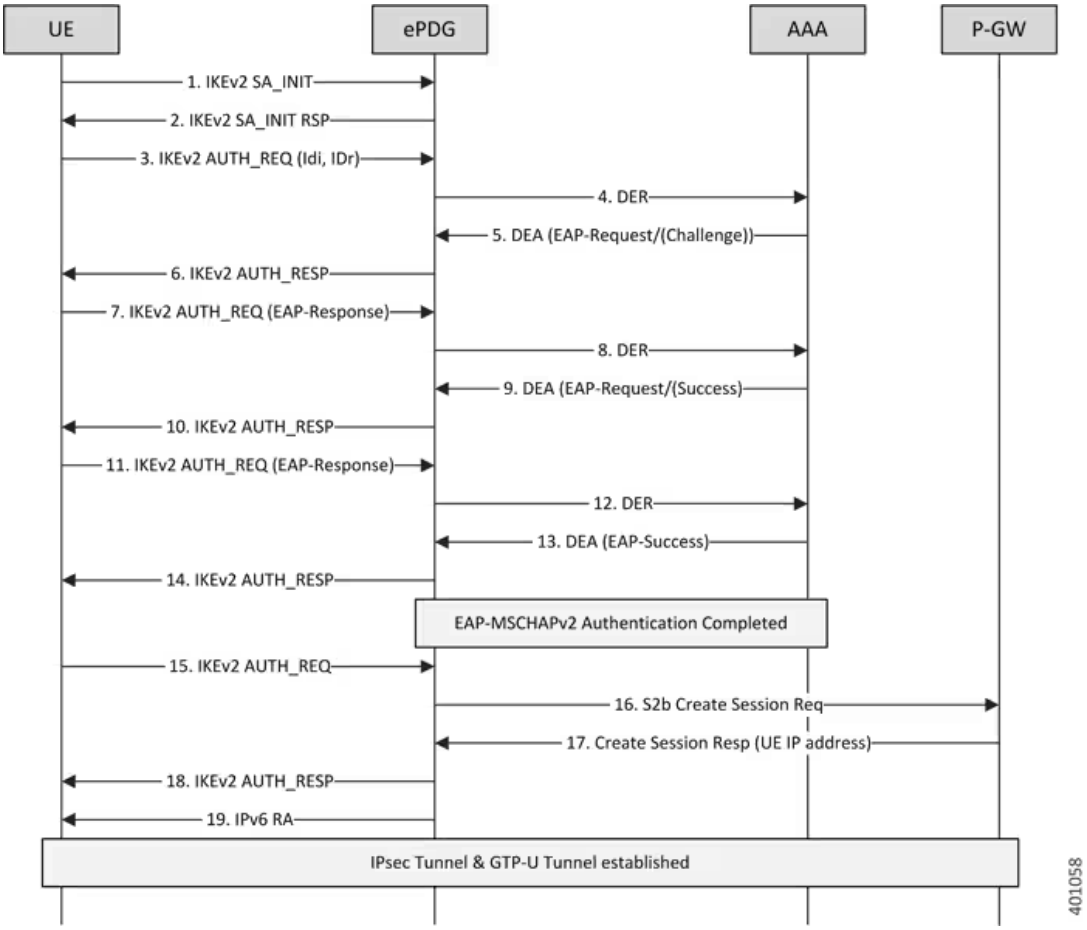


Figure 3: IKEv2 negotiation flow with EAP-MSCHAPv2 authentication

As illustrated in Figure 3, after the initialisation of the IKEv2 exchange (messages 1 and 2), the authentication phase can based either on the EAP-MSCHAPv2 protocol or the EAP-AKA protocol (for IMSI provided devices), with which the UE, via the ePDG, communicates with an AAA (Authentication, Authorisation, Accounting) server. This message exchange (messages 3-14) allows the user's identity to be validated, ensuring that only authorised entities can establish the IPsec connection. The ePDG interfaces with the P-GW for the creation of the session (messages 16 and 17), and upon completion of authentication, the secure IPsec tunnel and the GTP-U tunnel (message 19) are established for the transport of data traffic.

3.1.1 Typically used and recommended algorithms

- **AES (Advanced Encryption Standard)**: Adopted by the National Institute of Standards and Technology (NIST) in 2001, AES is considered the reference algorithm for symmetric encryption [6]. It supports keys of length 128, 192 and 256 bits. The implementation of AES with 128-bit keys is generally considered adequate for many purposes, while the use of 192- or 256-bit keys offers a higher level of security.

- **Hashing Algorithms of the SHA-2 Family (Secure Hash Algorithm 2)**: The SHA-256, SHA-384 and SHA-512 algorithms are considered secure and widely recommended for ensuring data integrity [7]. These algorithms produce hashes of length 256, 384 and 512 bits respectively. NIST recommends the use of SHA-256 or higher.

3.1.2 Vulnerable or obsolete Algorithms

- **DES (Data Encryption Standard)**: Standardised in 1977, DES uses a 56-bit key. Due to its short key length, it is considered obsolete and vulnerable to brute force attacks with modern hardware. NIST advises against its use [11].

- **3DES (Triple DES)**: Variant of DES that applies the DES algorithm three times with two or three separate keys. Although it provides a higher level of security than DES, it is computationally burdensome and, due to a key length below current standards, is considered obsolete. NIST recommends migration to AES [11].

- **MD5 (Message Digest 5)**: The inclusion of this hashing algorithm in this analysis is motivated by the fact that it is often used in combination with symmetric encryption algorithms and its weakness can compromise the integrity of the system. MD5 produces a 128-bit hash and is known to be vulnerable to collision attacks. NIST advises against its use, recommending hashing algorithms such as SHA-256 or higher.

- **SHA-1 (Secure Hash Algorithm 1)**: Although widely used in the past, SHA-1 (which produces a 160-bit hash) is now considered insecure due to its vulnerability to theoretical and, in some cases, practical collision attacks. NIST has been advising against its use since 2011 and recommends migrating to algorithms of the SHA-2 family. Its presence in VoWiFi implementations is therefore to be considered critical.

3.2 Diffie-Hellman key exchange and groups

Diffie-Hellman key exchange is a cryptographic method that allows two parties to establish a shared secret key over an insecure channel. The security of this mechanism is based on the computational difficulty of the discrete logarithm problem in a finite group. Diffie-Hellman groups, defined in IKE, specify the mathematical parameters used for key exchange, namely the modulus (a prime number p) and the generator (g) [12]. The size of the modulus p determines the security of the group: the larger the size of p, the greater the difficulty of calculating the discrete logarithm.

Given the criticality of key exchange within IpSEC, we concentrated our analysis on the different versions that the various devices and operators support.

The Diffie-Hellman groups, defined in IKE, specify the mathematical parameters used for key exchange, namely the modulus (a prime number p) and the generator (g). The size of the modulus p determines the security of the group: the larger the size of p, the more difficult it is to calculate the discrete logarithm.

Diffie-Hellman groups standardised for use in IKE are identified by a number. The summary Table 3.2 can be seen where the relative module size and NIST recommendations are shown for each group.

Group	**Modulo size (bit)**	**State**
DH1	768	Obsolete
DH2	1024	Obsolete
DH5	1536	Deprecated
DH14	2048	Sufficient
DH15	3072	Recommended
DH16	4096	Recommended
DH17	6144	Recommended
DH18	8192	Recommended
DH19	256 (Elliptic Curves)	equivalent to 3072 bit

4 Methodology

4.1 ePDG data collection

In order to conduct a comprehensive analysis of the security configurations of ePDGs, a Python script was developed to automate the process of identifying IP addresses and the subsequent sending of IKEv2 packets. The starting basis for the identification of ePDGs is a list of Mobile Country Codes (MCC) and Mobile Network Codes (MNC), which are unique identifiers for mobile network operators globally. For each pair (MCC, MNC), a domain name was generated according to the standardised format `epdg.epc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org`, in accordance with the 3GPP specification [8].

4.1.1 Recursive DNS resolution

The script implements a recursive DNS resolution for each generated domain name, with the goal of obtaining all associated IPv4 and IPv6 addresses. This functionality was implemented using the `dnspython` library. Queries of type 'A' (for resolving IPv4 addresses), 'AAAA' (for IPv6 addresses) and 'CNAME' (for alias management) are performed. In the presence of CNAME records, resolution continues recursively on the referenced domain name, until the final IP addresses are obtained. This process also guarantees the detection of ePDGs not directly reachable via the original domain name, but 'hidden' behind a chain of aliases. An example of recursive resolution is illustrated below:

```
epdg.epc.mnc001.mcc001.pub.3gppnetwork.org. -> CNAME ->
epdg-alias.example.com. -> A -> 192.168.1.1
```

4.1.2 IKEv2 scan

To evaluate security configurations, the script sends IKEv2 (Internet Key Exchange version 2) packets to UDP ports 500 and 4500, standard for the IKEv2 protocol, of the IP addresses obtained. The creation and sending of IKEv2 packets are handled by the `Scapy` library [9], which allows careful control over individual packet fields. The generated network traffic was captured, for analysis and verification purposes, using the `tcpdump` tool, which requires **sudo** permissions.

4.2 Configurations analysis

For each ePDG identified, an IKEv2 negotiation was initiated, simulating different client configuration scenarios. In particular, multiple IKEv2 packets were sent, with different configurations, defined within the Python script presented in the appendix. This was made possible through the use of a custom IKE library developed from Scapy [9] and based on the code of [16] and [18]. For each ePDG, the following configurations were tested, defined in the script's `TEST_CONFIG`:

- Support for different symmetric encryption algorithms: AES (with 128-, 192- and 256-bit keys), DES, 3DES.
- Support for different hashing algorithms: SHA-1, SHA-256, SHA-384, SHA-512, MD5.
- Support for several Diffie-Hellman groups: DH1 (768 bits) to DH18 (8192 bits), and DH19 (elliptic curve).
- Checking the acceptance of connections with parameters considered weak or insecure: DES, 3DES, MD5, SHA-1 and Diffie-Hellman groups of less than 2048 bits.

These configurations were tested by adopting an iterative approach: starting from the weakest to the strongest configuration, the ePDGs' responses were recorded, analysing the accepted or rejected parameters. Given the absence of a valid and registered IMSI (International Mobile Subscriber Identity) for each operator, the analysis was limited to the IKE SA INIT negotiation phase, which was sufficient to determine the cryptographic parameters supported by the ePDG, reducing the number of requests made.

5 Analysis of phone configurations

It should be mentioned at the outset that, due to limitations related to the availability of the necessary hardware and software tools, and the impossibility of accessing a complete set of mobile devices, it was not possible to conduct an exhaustive analysis of the security configurations of all phones on the market. Therefore, we relied on information already analysed and available online on the main vendors and operating systems. This information, although not the main basis of our research, allowed us to obtain an overview, albeit partial, of the security configurations adopted by the main mobile device manufacturers. We emphasise that this analysis was purely advisory in nature.

5.1 Analysis Results

5.2 Apple iOS

Analysis of the `.ipcc` (iPhone Carrier Bundle) configuration files used by Apple devices revealed that out of 745 operator-specific configurations, 219 include VoWiFi settings. A worrying aspect is that, for 94 operators (representing 43% of the 219 with VoWiFi configurations and 12.6% of the total 745 operators analysed), the only Diffie-Hellman group supported is DH1 (768 bits), an obsolete group not specified in any 3GPP document. In general, Apple's VoWiFi configurations were rather uniform, with only one setting available for each parameter, such as a single encryption algorithm, a single hashing algorithm and a single DH group.

5.2.1 Android devices

Qualcomm (Xiaomi, Oppo) The analysis of `.mbn` configuration files for Android devices based on Qualcomm chipsets (in particular Xiaomi and Oppo) showed greater variability than for Apple. For Xiaomi, out of 150 `.mbn` files analysed, 68% supported the DH2 group (1024 bits), always in combination with other groups. For Oppo, out of 377 `.mbn` files analysed, the DH2 group is supported in 8% of cases, again in combination with other groups.

Samsung In Samsung devices, VoWiFi configurations are contained in a specific file: the `/system/etc/epdg_apns_conf.xml` file, accessible with **root permissions**. Interestingly, only one operator, T-Mobile Germany, configures its Samsung devices to support an elliptic curve group, DH19. In the default configuration, Samsung only supports the DH2 group (1024 bits).

Google Pixel Google Pixel devices, starting with the Pixel 6 with Tensor SoC, consolidate VoWiFi configurations in the general Android settings. Analysis of these configurations suggests that VoWiFi-specific settings may not be used in practice. Many Pixel devices therefore seem to fall back on the defaults, which include support for DH2 (1024 bits), DH5 (1536 bits) and DH14 (2048 bits).

5.3 General considerations on phone configurations

The advisory analysis, even with its limitations, points to an alarming trend: many mobile devices, from different manufacturers, support obsolete or deprecated Diffie-Hellman

groups (such as DH1, DH2, DH5), in some cases as the only available option (as for some operators on Apple devices). This support, although not always exploited in practice, could be used by an attacker capable of influencing IKE negotiation to reduce the security level of VoWiFi connections. The variability of configurations between manufacturers also points to a lack of de facto standardisation in client-side VoWiFi security settings.

6 Experimental Results

In this section, we present the results of our analysis, conducted on all ePDGs of mobile network operators globally. Unfortunately, it should be noted that not all ePDGs responded to our requests. This lack of response can be attributed to several reasons, including:

- **Firewalls and Security Mechanisms:** Many mobile network operators implement firewalls and other security mechanisms to protect their infrastructure. These systems may have blocked our scanning requests, interpreting them as potential attacks [13].
- **ePDG configuration not publicly accessible**. Some ePDGs may not be directly accessible from the Internet, but may be protected by a NAT (Network Address Translation) layer or be reachable only via a private network of the operator [14]. In these cases, direct scanning is not possible.
- **Number of requests and throttling** To prevent abuse, ePDGs may implement rate limiting or throttling mechanisms, which limit the number of requests accepted in a given time frame [15]. If the frequency of our scans exceeded these thresholds, subsequent requests may have been ignored.
- **configuration or maintenance problems ePDG:** Some ePDGs may be temporarily unavailable due to configuration problems, scheduled maintenance or hardware/software failures.
- **IKE non-standard implementations:** Some ePDGs may implement the IKE protocol in a non-standard way, making it difficult to negotiate with our custom library.
- **Geographical Blocking:** Some ePDGs may be configured to respond only to requests from certain geographical areas, excluding our scans.

The analysis focused on verifying support for obsolete or insecure encryption and hashing algorithms, as well as the use of Diffie-Hellman (DH) groups of inadequate size. The results are summarised in Tables 1, 2 and 3, which show the support for different cryptographic parameters, both globally and for Italian operators.

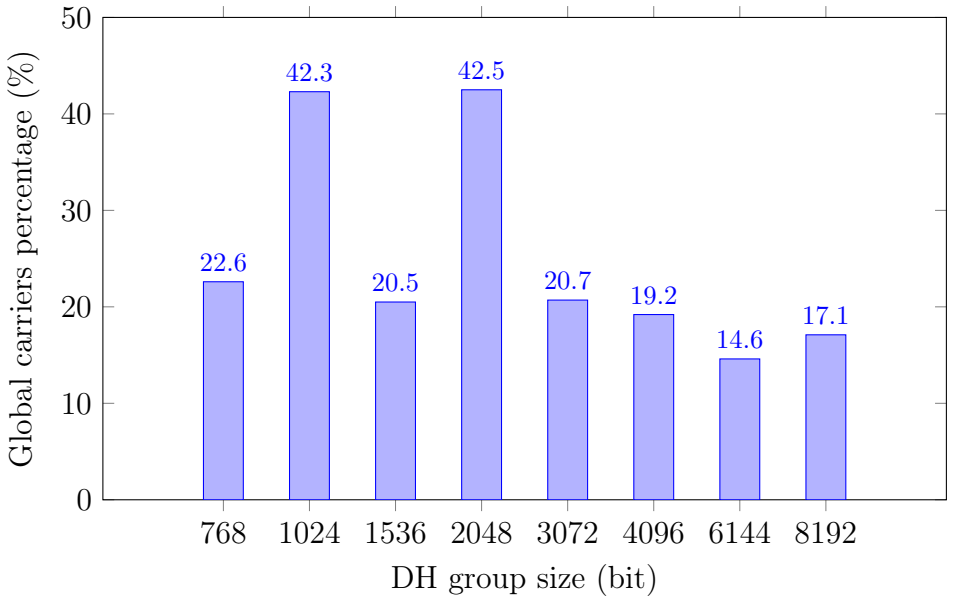
6.1 Support for Diffie-Hellman groups

Table 1 shows support for Diffie-Hellman groups. Globally, it shows that 250 operators (out of a total of 522) support DH groups with a module size of less than 2048 bits, which are considered insecure according to NIST recommendations. Of these, 183 support the DH2 group (1024 bits) despite also supporting more robust groups. In contrast, 252

operators support DH groups with a module size of at least 2048 bits. In Italy, the situation is mixed, with 2 operators supporting DH groups of less than 2048 bits and 4, of those who responded, supporting groups of an appropriate size.

Table 1: Diffie Hellman Support

Category	Carriers Total	Italian Carriers	Global percentage (%)
DH $<$ 2048 bit	250	2	47.89
DH $\geq$ 2048 bit	252	4	48.28
DH 1024 bit	183	0	35.06



6.2 Support for weak or obsolete algorithms

Tables 2 and 3 summarise support for hashing and encryption algorithms that are considered weak or obsolete.

Table 2: Integrity Algorithms Support

Category	Carriers Total	Italian Carriers
DH 1024 bit with MD5 (no encryption)	22	0
DH 1024 bit with MD5 (AES_128)	29	0
DH 1024 bit with SHA1 (AES_128)	70	0

Regarding Italian operators, Table 3 shows that 1 operator supports DH2 in combination with DES and 1 operator uses 3DES.

6.3 Tolerance toward weak parameters

A critical issue that emerged from the analysis is that, in some cases, ePDGs, while supporting robust DH groups, select the weakest group among those proposed by the

Table 3: Encryption Algorithms Support

Category	Carriers Total	Italian Carriers
No encryption	17	0
DH 1024 bit with DES	109	1
3DES as encryption	130	1

client, even when the client supports more secure groups. This behavior, observed in 183 operators globally for DH2 group, could be due to misconfiguration or a deliberate choice to favor backward compatibility at the expense of security. This practice, however, exposes communications to significant risk, as an attacker could exploit this weakness to force the use of a vulnerable DH group and compromise communication confidentiality.

7 Conclusions

This study extensively analyzed the security configurations of ePDGs of mobile network operators globally. The findings point to a critical situation, with widespread adoption of outdated or weak cryptographic parameters that expose VoWiFi communications to significant risks.

In particular, we found that a considerable number of operators still support Diffie-Hellman groups with a module size of less than 2048 bits, which are considered insecure according to NIST recommendations. In addition, many ePDGs agree to negotiate IPsec connections using outdated encryption and hashing algorithms such as DES, 3DES, MD5, and SHA-1, despite the availability of more robust alternatives such as AES and SHA-2.

Note the unwarranted tolerance for weak parameters, where ePDGs, while supporting more secure configurations, often select the weakest Diffie-Hellman group among those proposed by the client.

The analysis of phone configurations, while advisory, revealed that many mobile devices still support outdated Diffie-Hellman groups, in some cases as the only available option. This situation, combined with the tolerance for weak parameters of ePDGs, creates a chain of vulnerabilities that jeopardize the security of VoWiFi communications.

The need for action by mobile network operators to improve the security level of their infrastructure is highlighted. It is essential that these:

- **Disable support for obsolete and weak algorithms**. DES, 3DES, MD5, and SHA-1 should be removed from ePDG configurations.
- **Adopt secure Diffie-Hellman groups:** DH groups with a module size of at least 2048 bits (DH14 or higher) must be used.
- **Prioritize security on backward compatibility:** ePDGs should be configured to always select the most robust security parameters from those supported by the client.

- **Promote the adoption of secure configurations:** Operators should work with mobile device manufacturers to ensure that phones support and use appropriate security configurations.

References

[1] Internet Engineering Task Force (IETF). *RFC 7296: Internet Key Exchange Protocol Version 2 (IKEv2)*. October 2014. https://www.rfc-editor.org/rfc/rfc7296

[2] Internet Engineering Task Force (IETF). *RFC 4301: Security Architecture for the Internet Protocol*. December 2005. https://www.rfc-editor.org/rfc/rfc4301

[3] National Institute of Standards and Technology (NIST). *NIST Special Publication 800-57 Part 1 Revision 5: Recommendation for Key Management - Part 1: General*. May 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf

[4] National Institute of Standards and Technology (NIST). *NIST Special Publication 800-52 Revision 2: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*. March 2019. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf

[5] National Institute of Standards and Technology (NIST). *NIST Special Publication 800-175B: Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms*. January 2021. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175B.pdf

[6] National Institute of Standards and Technology (NIST). *FIPS PUB 197: Advanced Encryption Standard (AES)*. November 2001. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

[7] National Institute of Standards and Technology (NIST). *FIPS PUB 180-4: Secure Hash Standard (SHS)*. March 2012. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

[8] 3rd Generation Partnership Project (3GPP). *TS 33.402: 3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses*. https://www.3gpp.org/DynaReport/33402.htm

[9] Philippe Biondi. *Scapy: a powerful interactive packet manipulation program*. https://scapy.net/

[10] Internet Engineering Task Force (IETF). *RFC 2409: The Internet Key Exchange (IKE)*. November 1998. https://www.rfc-editor.org/rfc/rfc2409

[11] National Institute of Standards and Technology (NIST). *NIST Special Publication 800-131A Revision 2: Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*. November 2019. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf

[12] Internet Engineering Task Force (IETF). *RFC 6951: Additional Diffie-Hellman Groups for Use in IKEv2*. May 2013. https://www.rfc-editor.org/rfc/rfc6951

[13] Internet Engineering Task Force (IETF). *RFC 8200: Internet Protocol, Version 6 (IPv6) Specification*. July 2017. https://www.rfc-editor.org/rfc/rfc8200

[14] Internet Engineering Task Force (IETF). *RFC 2663: IP Network Address Translator (NAT) Terminology and Considerations*. August 1999. https://www.rfc-editor.org/rfc/rfc2663

[15] Cisco Systems. *Cisco ASR 5000 Series ePDG Administration Guide, Release 21.13.6.7*. 2021. https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-13_6-7/ePDG-Admin/21-13-ePDG-Admin_chapter_01.html

[16] Spinlogic. (2024). *epdg_discoverer* [Software]. GitHub. Retrieved from https://github.com/Spinlogic/epdg_discoverer (Accessed: 2024-12-31)

[17] G. K. Gegenhuber, F. Holzbauer, P. É. Frenzel, E. Weippl, and A. Dabrowski, "Diffie-Hellman Picture Show: Key Exchange Stories from Commercial VoWiFi Deployments," in *33rd USENIX Security Symposium (USENIX Security 24)*, 2024.

[18] aatlasis. (2024). *yIKEs* [Software]. GitHub. Retrieved from https://github.com/aatlasis/yIKEs/blob/main/crypto.py