An ePDG Server Security Study

Riccardo Fantasia
and
Leonardo Pantani

Introduction and Objectives

Voice over Wi-Fi (VoWiFi) enables voice calls over WLAN, leveraging IPsec tunnels to connect the user device (UE) with an **ePDG (Evolved Packet Data Gateway)**. Security heavily depends on the IKE negotiation phase, which defines cryptographic parameters like encryption and hashing algorithms, and Diffie-Hellman groups.

Goal of This Study:

- Investigate how ePDGs are configured worldwide by major mobile operators.
- Identify to what extent strong or weak algorithms are used.
- Focus on the adoption of recommended Diffie-Hellman group sizes.

Network Architecture and ePDG Role

VoWiFi is considered a non-3GPP access (using Wi-Fi instead of LTE/NR radio). The **ePDG** is the main gateway for terminating IPsec tunnels from end users and ensuring secure transit of packets into the operator's core network.

Key Functions of the ePDG:

- IPsec tunnel termination (via IKE).
- UE authentication and authorization (through AAA and HSS).
- Routing voice traffic to the IMS (IP Multimedia Subsystem).

Security in VoWiFi: IKE and IPsec

IPsec is a framework that provides authentication, confidentiality, and integrity at the network layer. **IKE** (Internet Key Exchange) is the protocol responsible for negotiating the **Security Associations (SAs)** between the UE and ePDG.

IKEv2 Negotiation Phases (simplified):

- Exchange of cryptographic proposals (encryption, hashing, DH groups).
- Authentication of the user (EAP-based methods).
- Establishment of the final IPsec tunnel.

Common Cryptographic Algorithms (Recap)

Recommended:

- **AES** (128, 192, 256-bit keys) for encryption.
- **SHA-2** family (SHA-256, SHA-384, SHA-512) for data integrity.

Outdated or Vulnerable:

- **DES, 3DES** (short key length or computational overhead).
- **MD5, SHA-1** (collision vulnerabilities).

Diffie-Hellman Groups

Diffie-Hellman (DH) allows two parties to derive a shared secret over an insecure channel. Groups specify the modulus size; larger means more secure. NIST recommends at least **2048-bit** modulus.

Examples:

- DH1: 768 bits (obsolete)
- DH2: 1024 bits (deprecated)
- DH14: 2048 bits (sufficient)
- DH19: elliptic curve, strong equivalent

Methodology for ePDG Analysis

Domain Generation: For each operator (MCC/MNC), we constructed the domain name in the format `epdg.epc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org`.

DNS Resolution: A Python script performed recursive DNS lookups (A, AAAA, CNAME) to collect IPv4/IPv6 addresses.

IKEv2 Probing: Using **Scapy**, the script sent IKEv2 requests to ports 500/4500, iterating over different combinations of:

- Symmetric ciphers (AES, DES, 3DES)
- Hashing (SHA-1, SHA-256, MD5)
- Diffie-Hellman groups (DH1 to DH19)

Experimental Results: ePDG

Global Findings:

- Many operators ($\approx 48\%$) still allow DH < 2048 bits (e.g., DH2 at 1024 bits).
- Some ePDGs accept DES or MD5 despite official deprecation.
- A notable subset prefers weaker groups if the client proposes them.

Such misconfigurations or backward-compatibility modes can severely weaken the IPsec tunnel, making it susceptible to interception or downgrade attacks.

Diffie-Hellman Group Usage

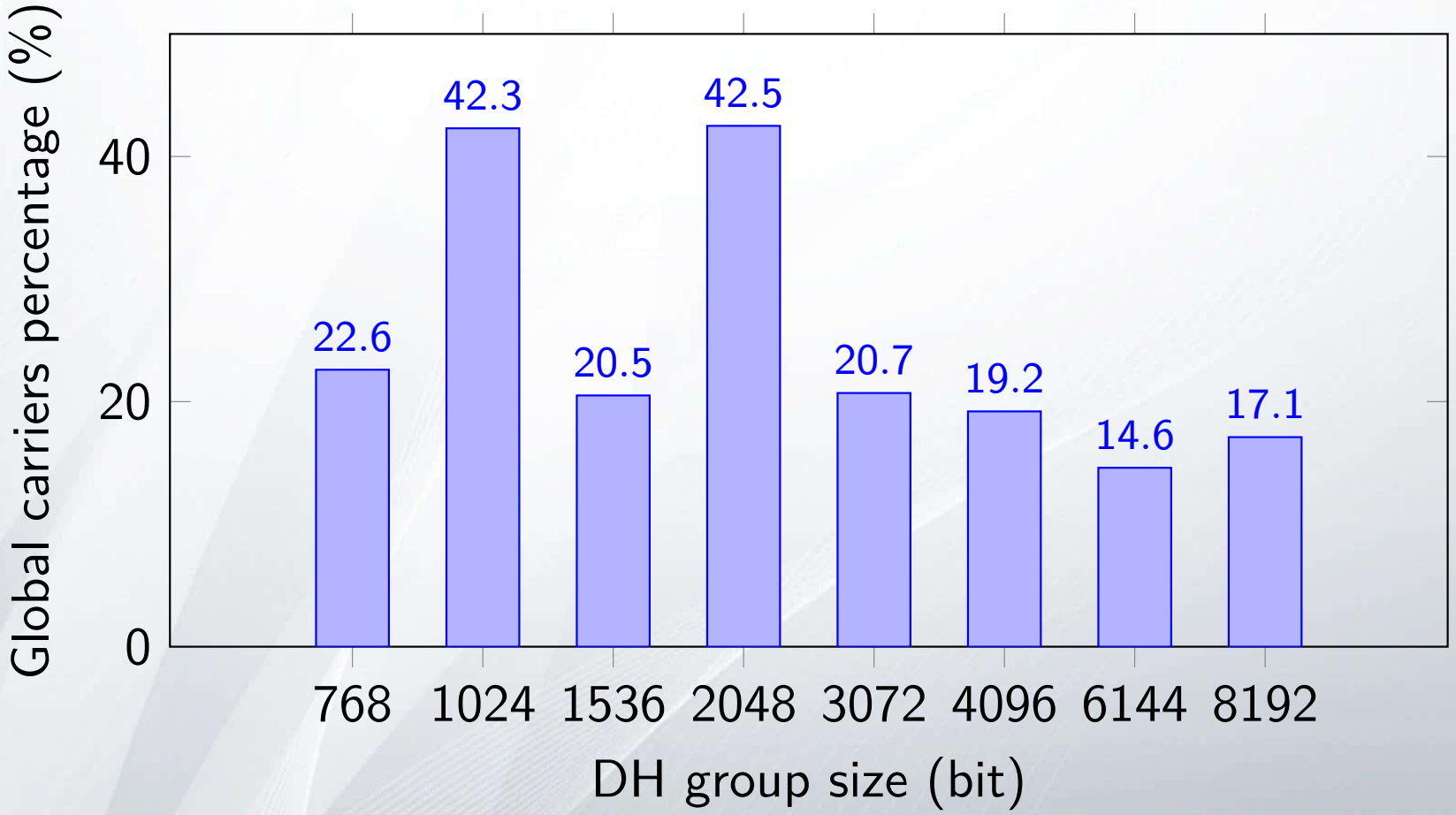

Figure: Percentage of global carriers using specific DH group sizes.

Phone Configurations

The study also examined phone-side settings in carrier bundles (e.g., .ipcc on iOS, .mbn on Qualcomm-based Android devices):

- Some carriers only allow a single Diffie-Hellman group (often 768 or 1024 bits).
- Samsung defaulting to DH2 (1024 bits) in many configurations.
- Only T-Mobile Germany used an elliptic curve group (DH19) in specific Samsung settings.
- Apple configurations frequently lock in a single group, sometimes DH1 (768 bits).

Observations and Weak Parameters

Weak parameters are still widely supported, even in situations where stronger ones are available. Operators often select the lowest common denominator, leaving IPsec vulnerable.

Potential Attacks:

- **Downgrade Attacks:** Attackers can force the connection to use weak DH groups or ciphers.
- **Brute-Force or Cryptanalysis:** Small key sizes (like 768 or 1024 bits) are more easily broken with sufficient computing resources.

Conclusions

Key Takeaways: Operators should discontinue the use of DES, 3DES, MD5, and SHA-1. They must enforce **2048-bit or larger** Diffie-Hellman groups and robust ciphers (AES, SHA-2). Mandatory selection of the strongest mutually supported parameters during IKE negotiation is crucial.

Future Work: Encourage wider collaboration among operators and device manufacturers to ensure consistent and secure default configurations for VoWiFi, minimizing weak fallback options.