Wi-Fi Calling

Revealing Downgrade Attacks and Not-so-private Private Keys

Gabriel K. Gegenhuber, Florian Holzbauer, Philipp É. Frenzel, Edgar Weippl, Adrian Dabrowski

The Speakers

Gabriel Gegenhuber
Bachelor's and Master's from TU Wien
Researcher at SBA Research
PhD Candidate at University of Vienna

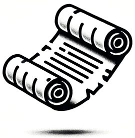
Adrian Dabrowski
PhD from TU Wien
PostDoc at University of California, Irvine
PostDoc at CISPA Helmholtz Center
Faculty at University of Applied Sciences, FH Campus Wien

Cellular Research Challanges

Different Access Technologies

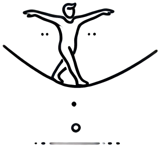
Radio: 2G, 3G, 4G, 5G

Voice: legacy and CSFB, VoLTE



Legacy Protocols

USSD, OTA, Proactive SIM, WAP



Corner Cases

Roaming

Zero-rating

Geo-blocked Services

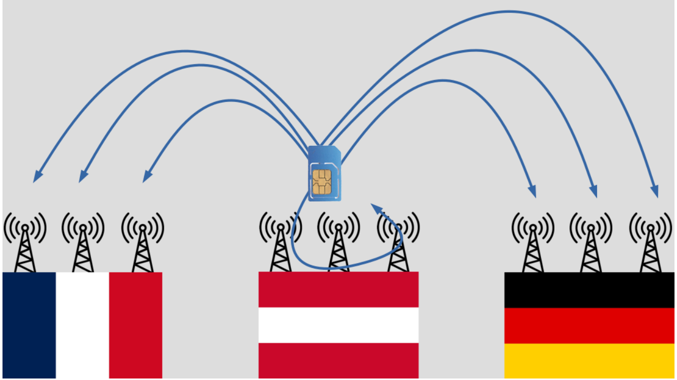
Geography

Strict confinement through frequency licensing

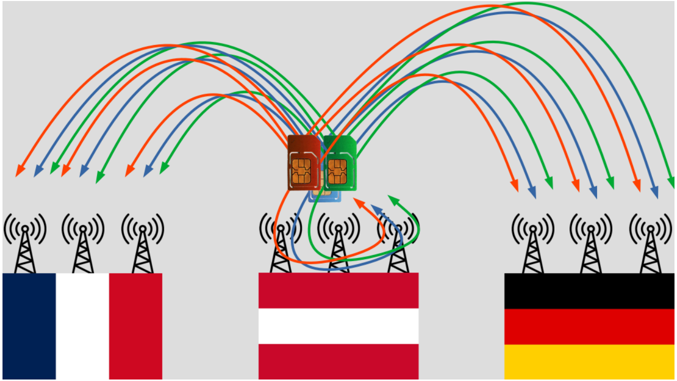
2-4 bare metal opterators per country

Large-scale / International Measurement in Radio Access Networks

Example: Measuring One Operator in Three Countries



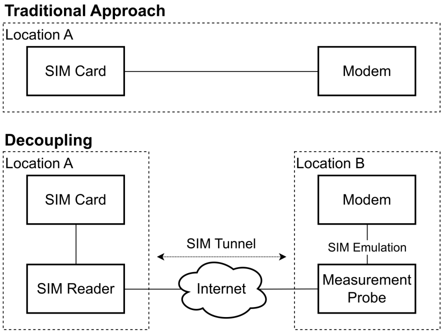
Example: Measuring Three Operators in Three Countries



Example: (6+1) $\times$ 3 Operators $\times$ 3 Plans $\times$ 3 Territories = 189

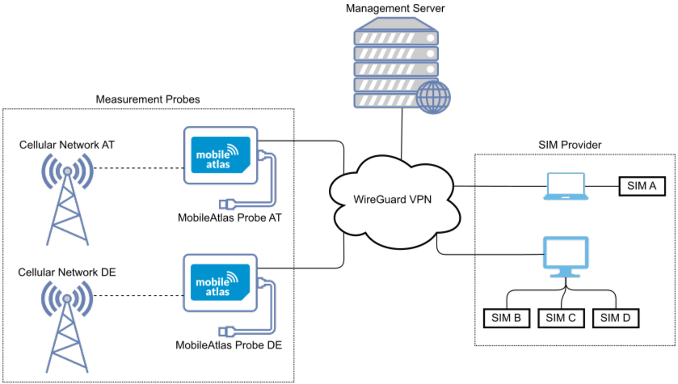
Geographically Decoupling Modem and SIM Card

- Traditionally modem and SIM card are seen as an indivisible unit
- We execute a **relay** attack on the **communication** between SIM card and modem
  - Modem is at location/country A
  - SIM card can be at location/country B
- **"Virtual Circuit"**: APDU over TCP connection
- SIM Tunnel interface $<$ 10 USD



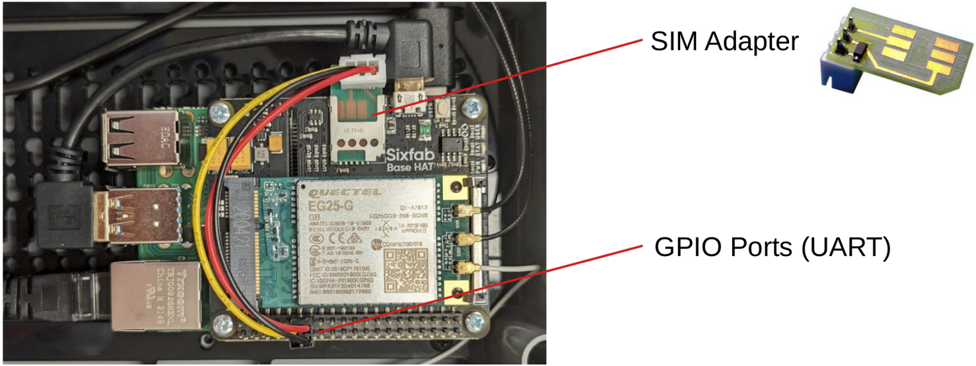
MobileAtlas

- Scalable, cost-efficient test framework for cellular networks
- Flexible roaming measurements
- Versatile measurement capabilities
- Controlled measurement environment



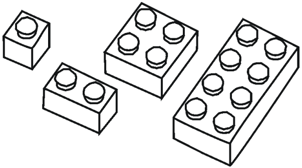
MobileAtlas: Probe & SIM Provider

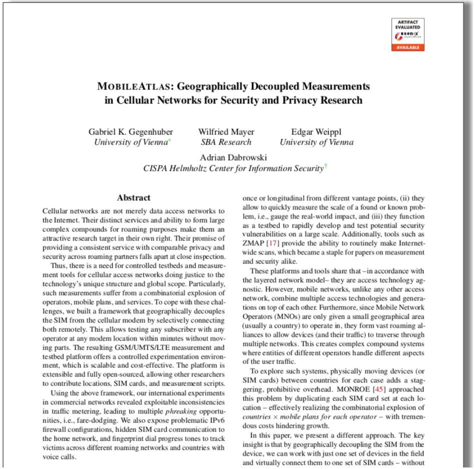
SIM Tunneling: Low-Cost Implementation



Measurement Cases

- Ringback tone fingerprinting
  - Leaking country/operator of target
- Proactive SIM: covert binary SMS to operator
- Zero-rating and free-riding





MOBILEATLAS: Geographically Decoupled Measurements in Cellular Networks for Security and Privacy Research

Gabriel K. Gegenhuber
University of Vienna[*]

Wilfried Mayer
SBA Research

Edgar Weippl
University of Vienna

Adrian Dabrowski
CISPA Helmholtz Center for Information Security[†]

Abstract

Cellular networks are not merely data access networks to the Internet. Their distinct services and ability to form large complex compounds for roaming purposes make them an attractive research target in their own right. Their promise of providing a consistent service with comparable privacy and security across roaming partners falls apart at close inspection.

Thus, there is a need for controlled testbeds and measurement tools for cellular access networks doing justice to the technology's unique structure and global scope. Particularly, such measurements suffer from a combinatorial explosion of operators, mobile plans, and services. To cope with these challenges, we built a framework that geographically decouples the SIM from the cellular modem by selectively connecting both remotely. This allows testing any subscriber with any operator at any modem location within minutes without moving parts. The resulting GSM/UMTS/LTE measurement and testbed platform offers a controlled experimentation environment, which is scalable and cost-effective. The platform is extensible and fully open-sourced, allowing other researchers to contribute locations, SIM cards, and measurement scripts.

Using the above framework, our international experiments in commercial networks revealed exploitable inconsistencies in traffic metering, leading to multiple *phreaking* opportunities, i.e., fare-dodging. We also expose problematic IPv6 firewall configurations, hidden SIM card communication to the home network, and fingerprint dial progress tones to track victims across different roaming networks and countries with voice calls.

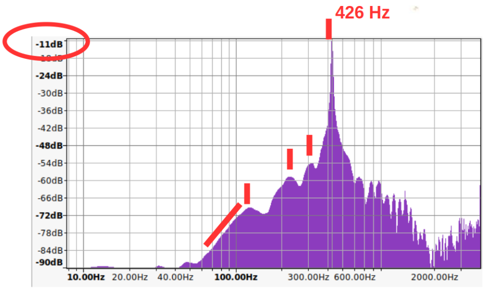
once or longitudinal from different vantage points, (ii) they allow to quickly measure the scale of a found or known problem, i.e., gauge the real-world impact, and (iii) they function as a testbed to rapidly develop and test potential security vulnerabilities on a large scale. Additionally, tools such as ZMAP [17] provide the ability to routinely make Internet-wide scans, which became a staple for papers on measurement and security alike.

These platforms and tools share that –in accordance with the layered network model– they are access technology agnostic. However, mobile networks, unlike any other access network, combine multiple access technologies and generations on top of each other. Furthermore, since Mobile Network Operators (MNOs) are only given a small geographical area (usually a country) to operate in, they form vast roaming alliances to allow devices (and their traffic) to traverse through multiple networks. This creates complex compound systems where entities of different operators handle different aspects of the user traffic.

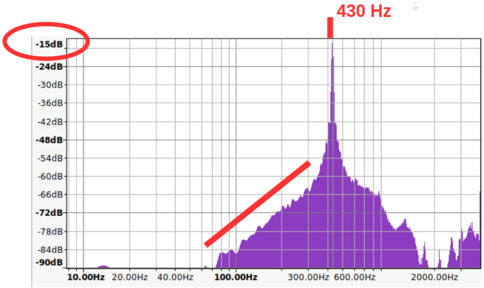
To explore such systems, physically moving devices (or SIM cards) between countries for each case adds a staggering, prohibitive overhead. MONROE [45] approached this problem by duplicating each SIM card set at each location – effectively realizing the combinatorial explosion of *countries* $\times$ *mobile plans for each operator* – with tremendous costs hindering growth.

In this paper, we present a different approach. The key insight is that by geographically decoupling the SIM from the device, we can work with just one set of devices in the field and virtually connect them to one set of SIM cards – without

Ringback Tones Examples

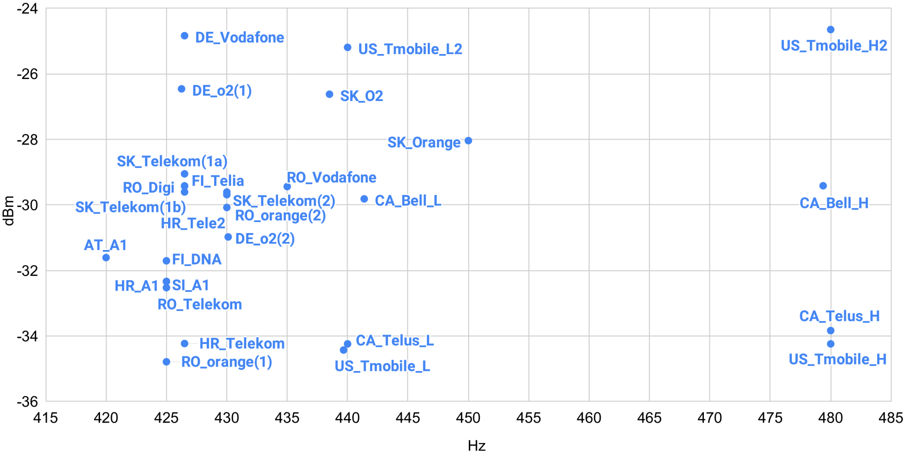


O2, Germany

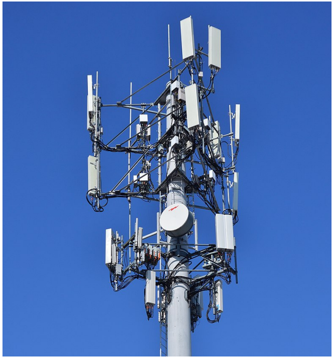


Vodaphone, Romania

Voice: Ringback Tones



Voice & Messaging: Two Access Technologies for 4G/5G

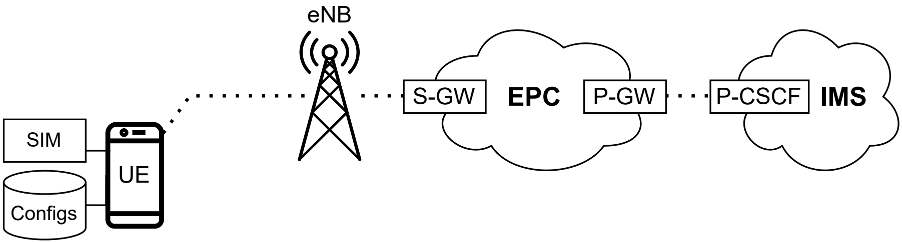


© Raysonho @ Open Grid Scheduler [CC0]

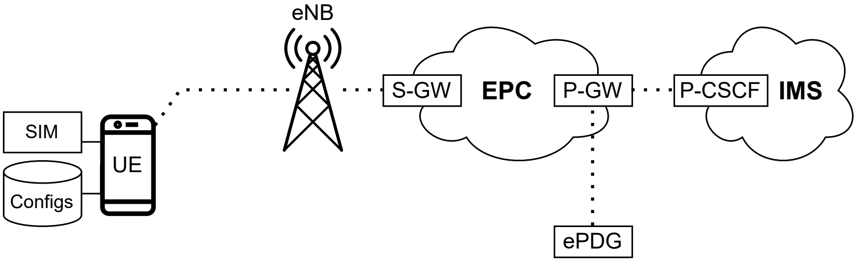
- VoLTE via **RAN / Celltower**
  - Also VoNR, Vo5G

- VoWiFi via **WiFi Access Point (AP)**
  - Also Wi-Fi Calling
  - Usually the preferred channel for call and message termination

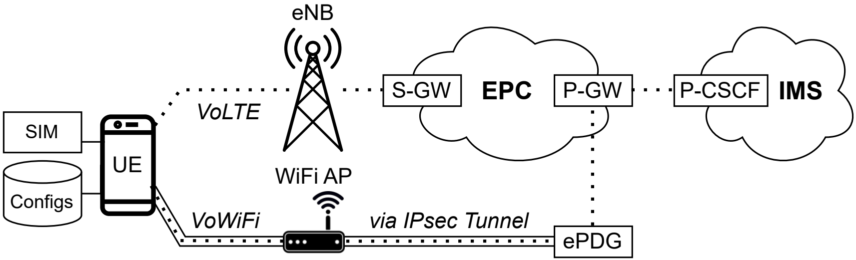
Recap: Measurement over RAN



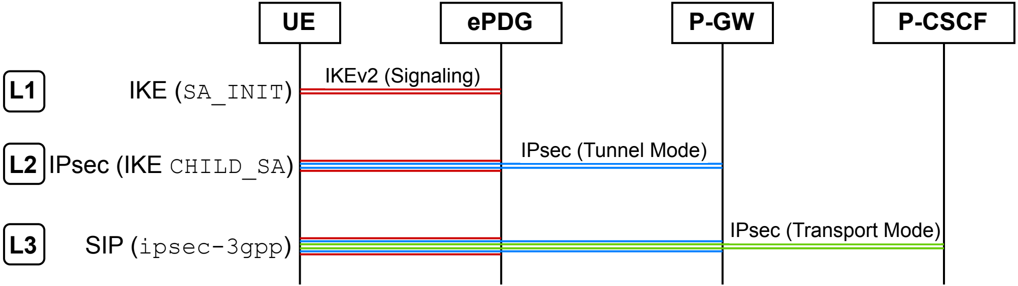
Recap: Measurement over RAN



Recap: Measurement over RAN (VoWiFi)



VoWiFi Requires Multiple IPSec Tunnels



Practical Example: `IKE_SA_INIT` Packet

```
▾ Internet Security Association and Key Management Protocol
    Initiator SPI: f85103b83df2b1b3
    Responder SPI: 0000000000000000
    Next payload: Security Association (33)
  ▸ Version: 2.0
    Exchange type: IKE_SA_INIT (34)
  ▸ Flags: 0x08 (Initiator, No higher version, Request)
    Message ID: 0x00000000
    Length: 360
  ▸ Payload: Security Association (33)
  ▾ Payload: Key Exchange (34)
      Next payload: Nonce (40)
      0... .... = Critical Bit: Not critical
      .000 0000 = Reserved: 0x00
      Payload length: 136
      DH Group #: Alternate 1024-bit MODP group (2)
      Reserved: 0000
      Key Exchange Data: e29f064510b80d6add0480f35e4ecb46d13c30095115930a66a5508f1065fe381d3f7802…
```

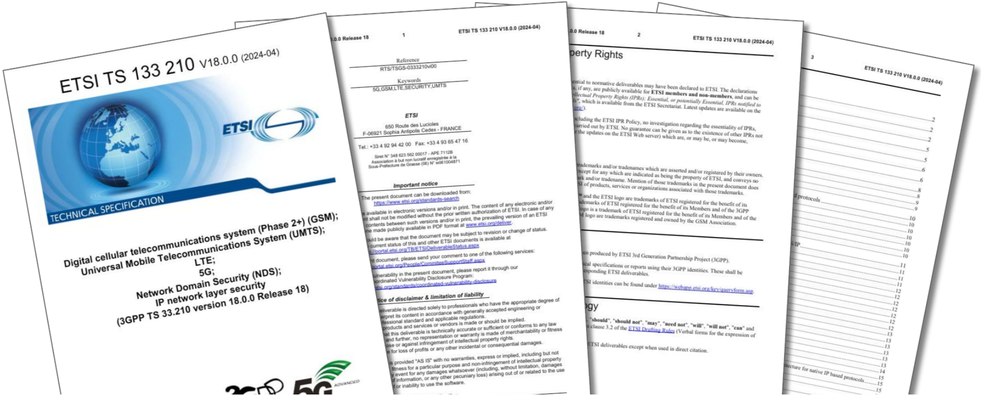
Practical Example: `IKE_SA_INIT` Packet

- DH2 (1024-bit MODP) might not be the best choice
- *Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice* (CCS 2015):
  "We further estimate that
  - *an academic team can break a 768-bit prime*
  - *a nation-state can break a 1024-bit prime."*
- Since 2015 computers got faster, cracking power got cheaper (AWS)

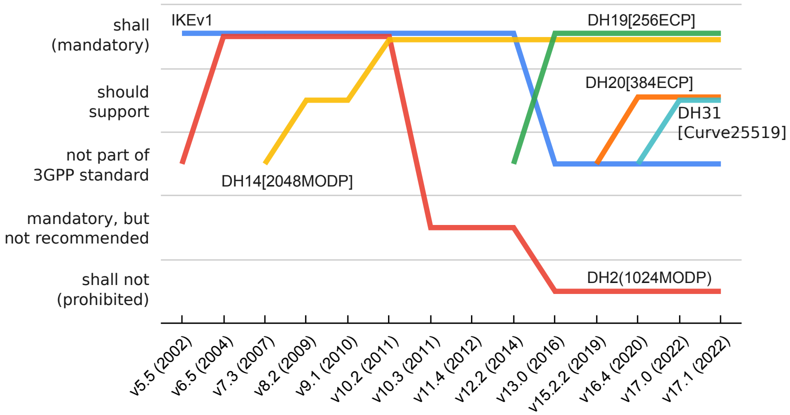
VoWiFi Security: Key Exchange vs. Security Associations

- IKE **key exchange is crucial** for residual connection (and other layers)
  - Used SAs (Security Associations) do not matter if weak key exchange is used
- Our wireshark example looks suspicious
  - We want to get the **global picture** at commercial operators
  - Standardization vs. status quo

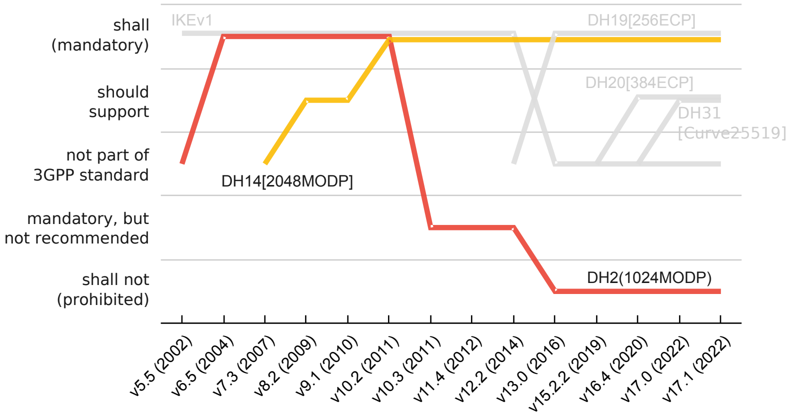
ETSI/3GPP Specification



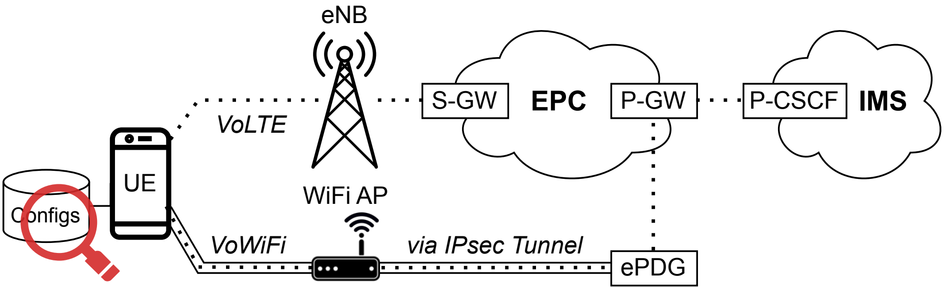
ETSI/3GPP Specification Over Time



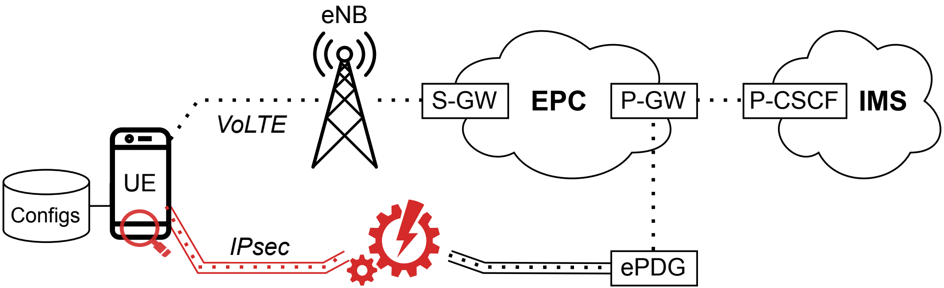
ETSI/3GPP Specification Over Time



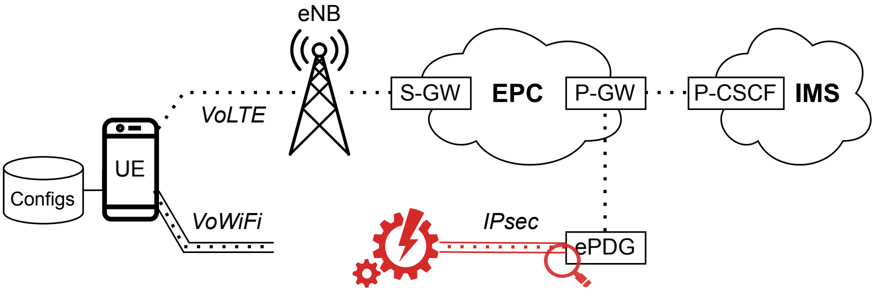
Flank I: Analyze Pre-loaded Configs at the Client-Side

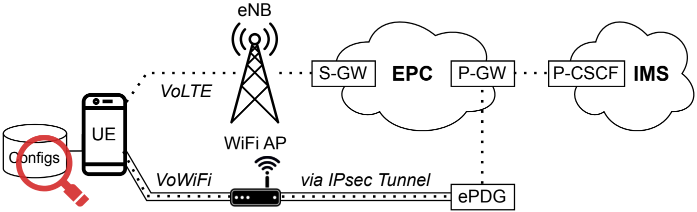


Flank II: Analyze IPsec Client on the UE



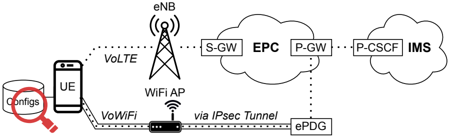
Flank III: Analyze Server Side Configurations





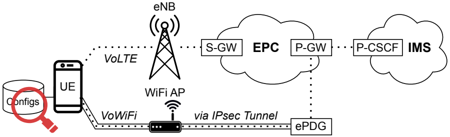
Flank I: Client-Side Pre-loaded Configurations

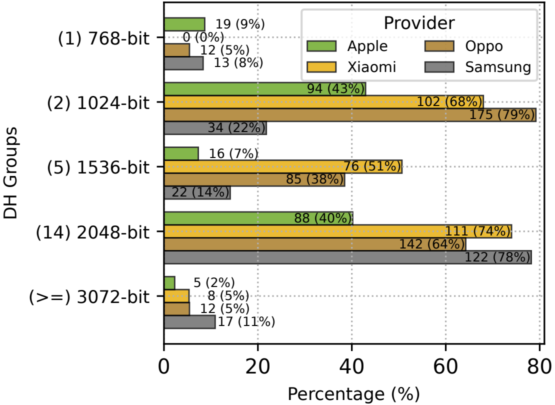
Methodology I: Pre-loaded Configs at the Client-Side



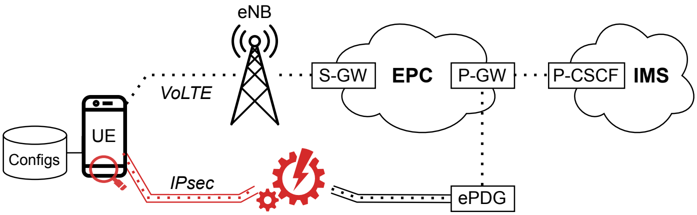
- Every phones comes with their own PRE-LOADED database
  - 3GPP ecosystem lacks auto-configuration, even on IETF protocols
- Evaluated **different manufacturers and devices**
  - Apple: IPCC Carrier Profiles
    - `https://github.com/mrlnc/ipcc-downloader`
  - Samsung: XML Config File
    - `/system/etc/epdg_apns_conf.xml`
  - Xiaomi, Oppo: Qualcomm MBN File
    - `https://github.com/sbaresearch/mbn-mcfg-tools`
  - Google Pixel uses default values (hardcoded in source code)

Results I: Pre-loaded Configs at the Client-Side



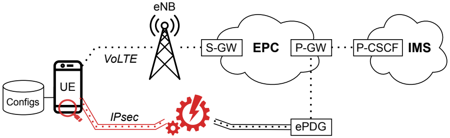


- Results for Apple, Samsung, Xiaomi, Oppo
- DH2 (1024-bit MODP) is very popular ϟ
- DH Groups > 2048-bit barely used



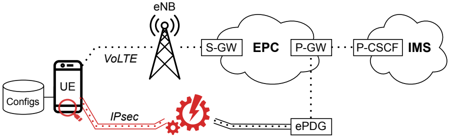
Flank II: IPsec Client Implementation on the UE

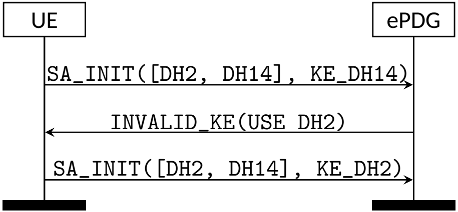
Methodology II: Analyze IPsec Client on the UE



- VoLTE/VoWiFi **implementation depends on manufacturer/device**
  - Managed by the modem (e.g., Qualcomm)
  - Managed in the userspace (e.g., strongSwan binaries for Samsung, MediaTek)
- Investigated whether **downgrade attacks** are possible

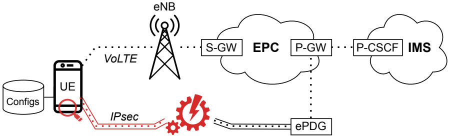
Results II: (Protocol Conform) Downgrade Procedure

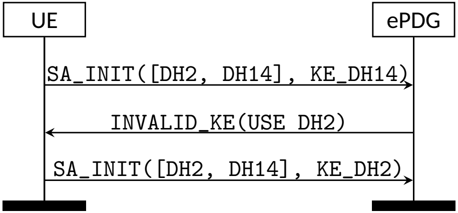




- Client selects **preferred DH group**, but also signals support for **other groups**
  - Server can request **switch to other group** via `INVALID_KE` packet
  - Client starts over, respecting the server's choice

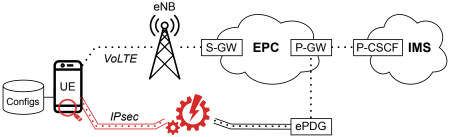
Results II: (Protocol Conform) Downgrade Vulnerability

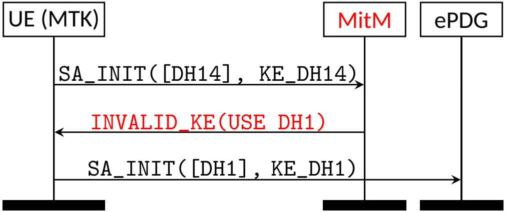




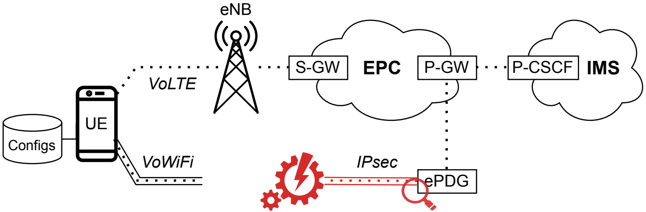
- Client selects **preferred DH group**, but also signals support for **other groups**
  - Server can request **switch to other group** via `INVALID_KE` packet
  - Client starts over, respecting the server's choice
- A malicious **interceptor** could **inject a downgrade packet**
  - Could be mitigated by servers always demanding strongest group
  - However, 41% of servers **tolerate weak client choices** ϟ

Results II: Downgrade Vulnerability at MediaTek Clients



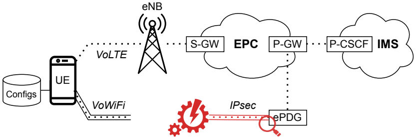


- MediaTek chipsets allow **downgrade to arbitrary DH group** ϟ
  - Even when the group was not part of the client's proposal
  - Can always downgrade to weak groups (DH1, DH2) if target server supports it



Flank III: Analyze Server Side Configurations

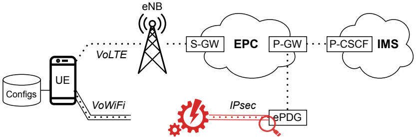
Methodology III: Supported DH Groups at the Server-Side



- Goals
  - What parameters (DH groups) do MNOs actually support?
  - How will ePDGs react, if client prefers weaker DH-groups than mutually supported?
- Each operator is identified by MCC + MNC
- ePDG domain: `epdg.epc.mnc⟨id⟩.mcc⟨id⟩.pub.3gppnetwork.org`
- Two steps

1. **DNS discovery**
   – Done via mass DNS resolution
2. **IKE handshake**
   – Reimplemented IKE handshake via scapy

Results III: Supported DH Groups at the Server-Side



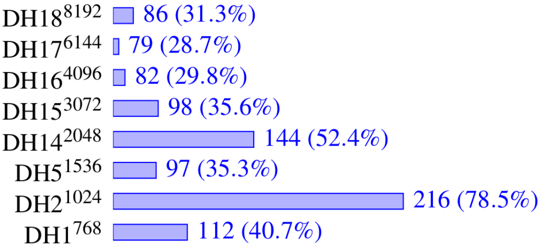
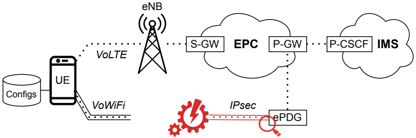


Figure 7: Number of MNOs per supported DH group

- Active probing of ePDG servers
  - 423 domain entries found, 275 responsive ePDGs
- DH2 (1024-bit MODP) most popular ϟ
- DH1 (768-bit MODP) supported by 40% of servers ϟ

Results III: Supported DH Groups at the Server-Side



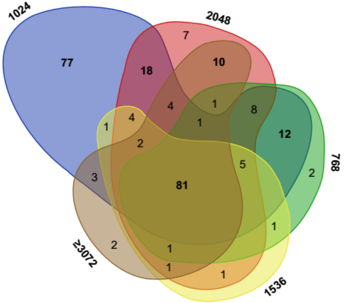


Figure 8: Number of MNOs that support a specific combination of DH key exchange groups. 3072-8192 bit groups are combined because of their low diversity.

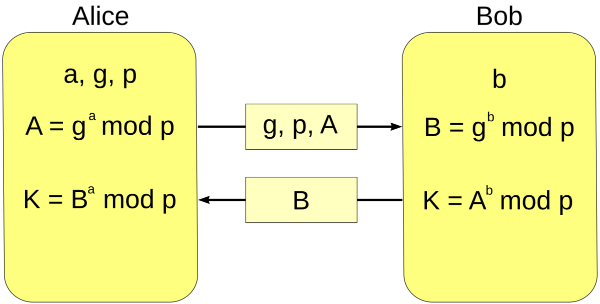
- Client indicated weaker DH group than mutually supported
  - 41% MNOs accepted the less secure method
  - 12% returned error without proposal
  - 42% desired an upgrade by the UE
    - ½ choose DH18 (8192),
    - Others DH14 (2048)
  - 4% indicate a downgrade to DH1 (768)

Result III: Repeating Public Keys

```
6.193: no ikev2 resp
6.9: no ikev2 resp
6.65: no ikev2 resp
3.4: successfull key exchange, group: 2, ke: 5ec39b6e39a340b7b46c8945db2d369abfb6274e803ce5160578e6365c67aa4c210d86ca9c
5.4: successfull key exchange, group: 2, ke: 5ec39b6e39a340b7b46c8945db2d369abfb6274e803ce5160578e6365c67aa4c210d86ca9c
5.4: successfull key exchange, group: 2, ke: 3956b7611cd573607b20294d34420d9f82d714b6ae5f7fd3e0bf7bab47c14f8676fa4d4475
3.4: successfull key exchange, group: 2, ke: edfdd0a3b7348bf4d2e37f38b5ab896e6e8be8bbe8a6cdf3dc9bd3275b61058d1011e5c736
133: no ikev2 resp
.208: no ikev2 resp
.82: no ikev2 resp
.137: successfull key exchange, group: 2, ke: 78a293a79fc2087adff64afc8d970cbbcbdcc3ec378b20a794b847a2bf4adf95113dca582
.14: successfull key exchange, group: 2, ke: 283b0ca2e9dfb01b1d0848b1dc14b868929e0c60b11bd7cba443e446e557f3ed904fc2f7ad
.26: successfull key exchange, group: 2, ke: b179cd529c3ffd1041cc9df08b5a6b444e3844ce59a30ba532629d3450a1e54007003adcb0
102: successfull key exchange, group: 2, ke: 5ec39b6e39a340b7b46c8945db2d369abfb6274e803ce5160578e6365c67aa4c210d86ca9c
166: successfull key exchange, group: 2, ke: 310fd2f9078860039eca1da3a91c775a7688cd5f1f0d39abdf4616f761bca02d3a5e609af9
.252: successfull key exchange, group: 2, ke: c2c3bf563416db1d83c034a3008d6615d971e01cad31d4009c6197ac53ea16c0ded1bc709
.252: successfull key exchange, group: 2, ke: 04f4c38d95d898ab99c8fb103f72c83c12ebfa7088aa1e34159e657c4426a2683017e9046
: successfull key exchange, group: 2, ke: 44d4813bed8d09c96e9664144495ca92d61e88f1df9e4ea0301f1a311cdb41eebdb3a585de124
: successfull key exchange, group: 2, ke: 5ec39b6e39a340b7b46c8945db2d369abfb6274e803ce5160578e6365c67aa4c210d86ca9ccbe
1: no ikev2 resp
```

5ec39b6e39a340b7b46c8 Aa ab .* 8 of 8

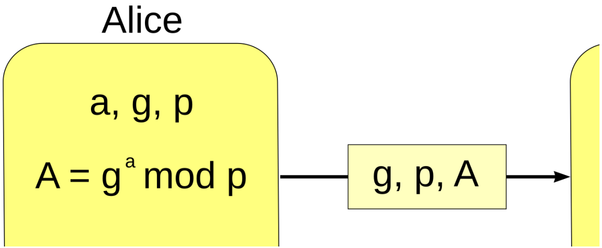
Short Excursion: Diffie-Hellman Key Exchange



$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$

- a: private key Alice
- b: private key Bob
- p: public prime number (DH group)
- g: public integer smaller than p (DH group)
- A: public key Alice
- B: public key Bob
- K: secret session key between Alice and Bob

Short Excursion: Diffie-Hellman Key Exchange



a: private key Alice

b: private key Bob

p: public prime number (DH group)

g: public integer smaller than p (DH group)

A: public key Alice

B: public key Bob

K: secret session key between Alice and Bob

10 public keys

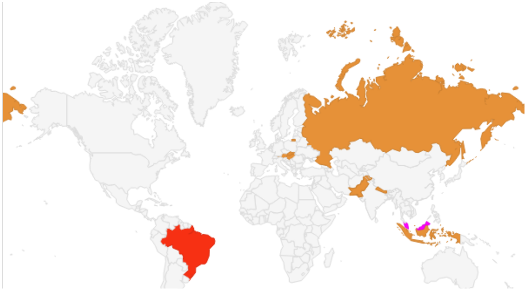
→

10 private keys

(world-wide)

Result III: (Not-so) Private Keys

- Identical key exchange value -> **identical private-keys**
  - Inter MNO key sharing: private-key collisions with unrelated MNOs
- 16 operators **spread across the world**: e.g., Austria, Brazil, Indonesia, Malaysia, Nepal, Russia, etc.
  - Estimation: 140 million subscribers affected
  - Anyone having access to the private keys can decrypt the VoWiFi traffic
- Affected operators all use ZTE equipment for their core network



Responsible Disclosure I: CVE-2024-20069

- MediaTek: CVE-2024-20069, severity high
  - Fixed via Android Security Update (June 2024)
  - Dimensity SoC MT6833, MT6853, MT6855, MT6873, MT6875, MT6875T, MT6877,MT6883, MT6885, MT6889, MT6891, MT6893, MT8675, MT8771,MT8791T, MT8797
  - NR15 modem
  - Not much more details

Responsible Disclosure II: CVE-2024-22064, CVD-2024-0089

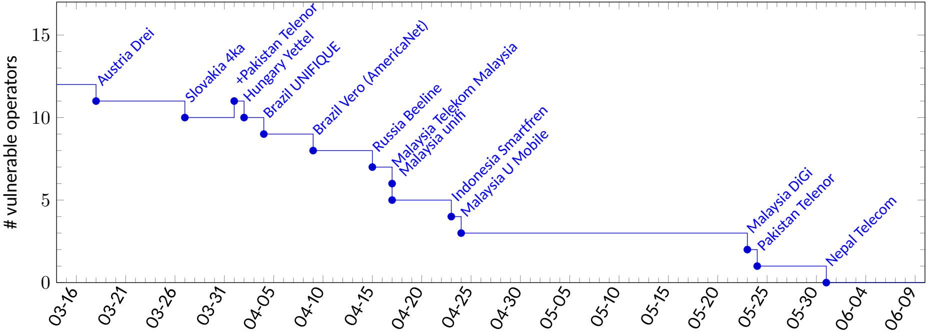
- Responsible disclosure was coordinated by GSMA
  - Initial report in February 2024
  - CVD-2024-0089
- ZTE: CVE-2024-22064, severity high
  - Private keys are leftovers from integration testing
  - Accidentally slipped into production images
  - affected: ZXUN-ePDG $<$ V5.20.20
  - Some of those operational since 2016

Table 5: Static IPSec keys: Vulnerable Operators.

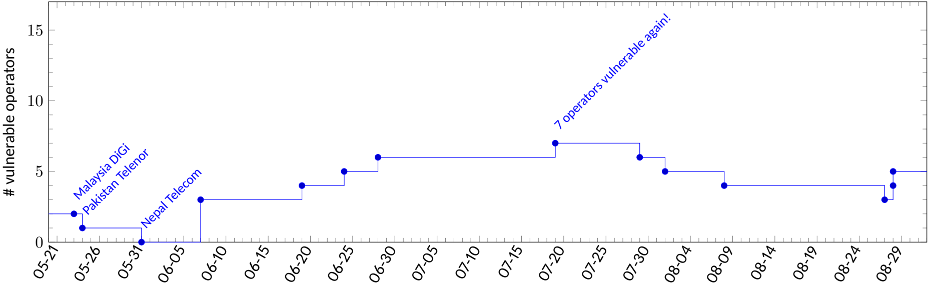
MCC-MNC	Country	Operator	Subscribers(M)		Remediation[b]
232-05, 232-10	Austria	Drei	4.1	[1]	2024-03-18
231-03	Slovakia	4ka	0.6	[12]	2024-03-27
216-01	Hungary	Yettel	3.7	[3]	2024-04-02
724-29	Brazil	UNIFIQUE	< 0.5	[2]	2024-04-04
724-26	Brazil	Vero (AmericaNet)	< 0.5	[2]	2024-04-09
250-99	Russia	Beeline	44	[11]	2024-04-15
502-11	Malaysia	Telekom Malaysia	2	[6]	2024-04-17
502-153	Malaysia	unifi	0.8	[8]	2024-04-17
510-09, 510-28	Indonesia	Smartfren	36	[4]	2024-04-23
502-18	Malaysia	U Mobile	8.5	[7]	2024-04-24
502-16	Malaysia	DiGi	20.6	[5]	2024-05-23
410-06[a]	Pakistan	Telenor	(44)	[10]	2024-05-24
429-01	Nepal	Nepal Telecom	20	[9]	-
Total			> 140.3 Mio		

[a] Vulnerability introduced April 2nd 2024. [b] Cut-off date: May 31th 2024

ZTE: Remediation Timeline

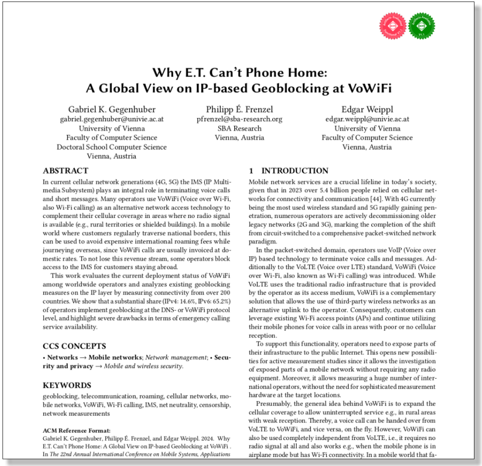


ZTE: Remediation Timeline Part II - The Return



Limited Coverage due to VoWiFi Geoblocking

- **Potentially** even **more vulnerable operators** out there
- Many operators employ **geoblocking** at VoWiFi
  - Especially common within Europe and Asia
  - Shown in related paper *Why E.T. Can't Phone Home*



Why E.T. Can't Phone Home: A Global View on IP-based Geoblocking at VoWiFi

Gabriel K. Gegenhuber
gabriel.gegenhuber@univie.ac.at
University of Vienna
Faculty of Computer Science
Doctoral School Computer Science
Vienna, Austria

Philipp É. Frenzel
pfrenzel@sba-research.org
SBA Research
Vienna, Austria

Edgar Weippl
edgar.weippl@univie.ac.at
University of Vienna
Faculty of Computer Science
Vienna, Austria

ABSTRACT

In current cellular network generations (4G, 5G) the IMS (IP Multimedia Subsystem) plays an integral role in terminating voice calls and short messages. Many operators use VoWiFi (Voice over Wi-Fi, also Wi-Fi calling) as an alternative network access technology to complement their cellular coverage in areas where no radio signal is available (e.g., rural territories or shielded buildings). In a mobile world where customers regularly traverse national borders, this can be used to avoid expensive international roaming fees while journeying overseas, since VoWiFi calls are usually invoiced at domestic rates. To not lose this revenue stream, some operators block access to the IMS for customers staying abroad.

This work evaluates the current deployment status of VoWiFi among worldwide operators and analyzes existing geoblocking measures on the IP layer by measuring connectivity from over 200 countries. We show that a substantial share (IPv4: 14.6%, IPv6: 65.2%) of operators implement geoblocking at the DNS- or VoWiFi protocol level, and highlight severe drawbacks in terms of emergency calling service availability.

CCS CONCEPTS

• **Networks → Mobile networks**; *Network management*; • **Security and privacy** → *Mobile and wireless security*.

KEYWORDS

geoblocking, telecommunication, roaming, cellular networks, mobile networks, VoWiFi, Wi-Fi calling, IMS, net neutrality, censorship, network measurements

ACM Reference Format:
Gabriel K. Gegenhuber, Philipp É. Frenzel, and Edgar Weippl. 2024. Why E.T. Can't Phone Home: A Global View on IP-based Geoblocking at VoWiFi . In *The 22nd Annual International Conference on Mobile Systems, Applications*

1 INTRODUCTION

Mobile network services are a crucial lifeline in today's society, given that in 2023 over 5.4 billion people relied on cellular networks for connectivity and communication [44]. With 4G currently being the most used wireless standard and 5G rapidly gaining penetration, numerous operators are actively decommissioning older legacy networks (2G and 3G), marking the completion of the shift from circuit-switched to a comprehensive packet-switched network paradigm.

In the packet-switched domain, operators use VoIP (Voice over IP) based technology to terminate voice calls and messages. Additionally to the VoLTE (Voice over LTE) standard, VoWiFi (Voice over Wi-Fi, also known as Wi-Fi calling) was introduced. While VoLTE uses the traditional radio infrastructure that is provided by the operator as its access medium, VoWiFi is a complementary solution that allows the use of third-party wireless networks as an alternative uplink to the operator. Consequently, customers can leverage existing Wi-Fi access points (APs) and continue utilizing their mobile phones for voice calls in areas with poor or no cellular reception.

To support this functionality, operators need to expose parts of their infrastructure to the public Internet. This opens new possibilities for active measurement studies since it allows the investigation of exposed parts of a mobile network without requiring any radio equipment. Moreover, it allows measuring a huge number of international operators, without the need for sophisticated measurement hardware at the target locations.

Presumably, the general idea behind VoWiFi is to expand the cellular coverage to allow uninterrupted service e.g., in rural areas with weak reception. Thereby, a voice call can be handed over from VoLTE to VoWiFi, and vice versa, on the fly. However, VoWiFi can also be used completely independent from VoLTE, i.e., it requires no radio signal at all and also works e.g., when the mobile phone is in airplane mode but has Wi-Fi connectivity. In a mobile world that fa-

Lessons Learned & Takeways

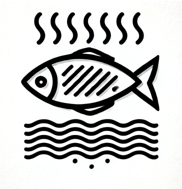
Remove Code

... and not just the handshake advertisement.

Attackers might find a way to activate it.

Deprication Path

Built-in from the first version of a standard



Key Freshness

Algorithmically or statistically

Thank you

Contact

- gabriel.gegenhuber@univie.ac.at
  @GGegenhuber
  @ggegenhuber.bsky.social
- adrian.dabrowski@fh-campuswien.ac.at
  @Atrox_at @atrox.at

github.com/sbaresearch/vowifi-epdg-scanning

Diffie-Hellman Picture Show:
Key Exchange Stories from Commercial VoWiFi Deployments

Gabriel K. Gegenhuber[1,2], Florian Holzbauer[1,2], Philipp É. Frenzel[3], Edgar Weippl[1,4], and Adrian Dabrowski[5]

[1]University of Vienna, Faculty of Computer Science, [2]UniVie Doctoral School Computer Science, [3]SBA Research, [4]Christian Doppler Laboratory for Security and Quality Improvement in the Production System Lifecycle (CDL-SQI), [5]CISPA Helmholtz Center for Information Security

Abstract

Voice over Wi-Fi (VoWiFi) uses a series of IPsec tunnels to deliver IP-based telephony from the subscriber's phone (User Equipment, UE) into the Mobile Network Operator's (MNO) core network via an Internet-facing endpoint, the Evolved Packet Data Gateway (ePDG). IPsec tunnels are set up in phases. The first phase negotiates the cryptographic algorithm and parameters and performs a key exchange via the Internet Key Exchange protocol, while the second phase (protected by the above-established encryption) performs the authentication. An insecure key exchange would jeopardize the later stages and the data's security and confidentiality.

In this paper, we analyze the *phase 1* settings and implementations as they are found in phones as well as in commercially deployed networks worldwide. On the UE side, we identified a recent 5G baseband chipset from a major manufacturer that allows for fallback to weak, unannounced modes and verified it experimentally. On the MNO side –among others– we identified 13 operators (totaling an estimated 140 million subscribers) on three continents that all use the same globally static set of ten private keys, serving them at random. Those *not-so*-private keys allow the decryption of the shared keys of every VoWiFi user of all those operators. All these operators

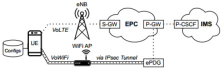


Figure 1: VoLTE compared to VoWiFi over an untrusted Internet connection – as relevant for this paper

adoption as *Voice over Wi-Fi* (VoWiFi), also called *Wi-Fi Calling* or *Voice over WLAN* (VoWLAN). For the end user, it often provides better coverage, and for the operator, it provides a way to externalize the last mile's costs while keeping the full revenue.

On iPhone and Android, by default, VoWiFi is the preferred call termination channel when available.

At its core, *untrusted non-3GPP access* works by setting up at least one IPsec tunnel to the operator's Evolved Packet Data Gateway (ePDG). It uses the Internet Key Exchange (IKE) protocol [34] and relies heavily on predefined Diffie-Hellman (DH) groups, some of which are known to be weak. For example, since 2015 [15], $DH1^{768\ bits}$ is assumed to be