universität wien

SBA Research

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

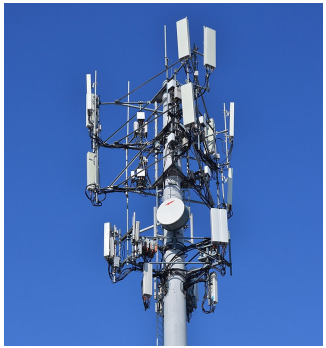
Diffie-Hellman Picture Show

Key Exchange Stories from Commercial VoWiFi Deployments

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

usenix THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

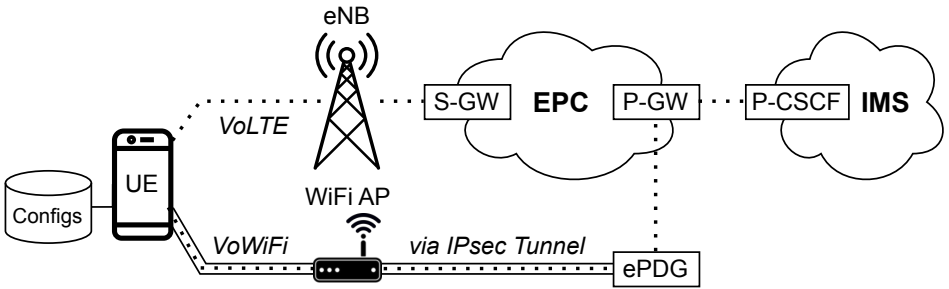
Two Access Technologies in 4G/5G



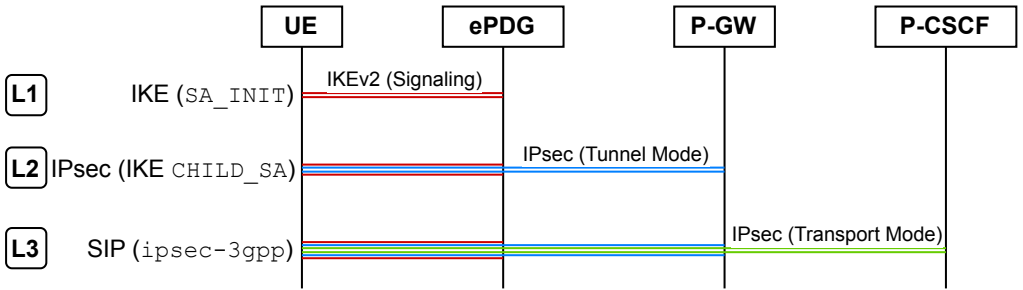
© Raysonho @ Open Grid Scheduler [CC0]

- VoLTE via **Celltower**
  - Also VoNR, Vo5G
- VoWiFi via **WiFi Access Point (AP)**
  - Also Wi-Fi Calling
  - Usually the preferred channel for call and message termination

VoWiFi in 4G/5G: Complementing Radio Access with WiFi APs



VoWiFi Requires Multiple IPSec Tunnels



Practical Example: IKE_SA_INIT Packet

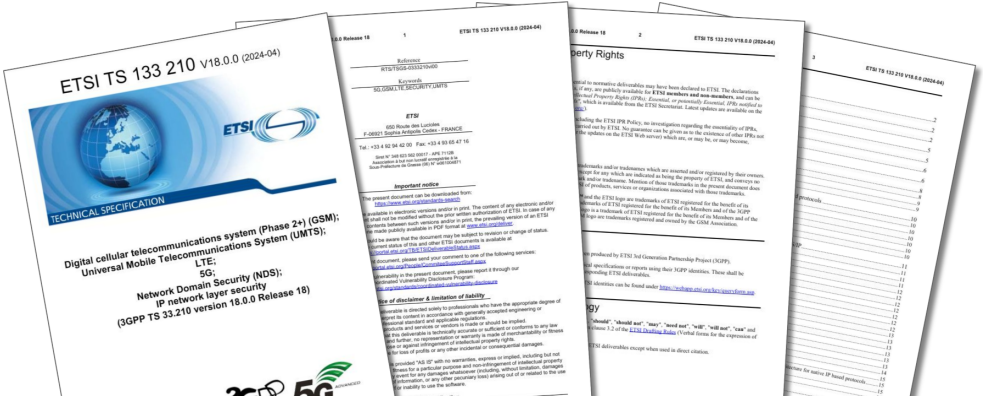
```
▾ Internet Security Association and Key Management Protocol
    Initiator SPI: f85103b83df2b1b3
    Responder SPI: 0000000000000000
    Next payload: Security Association (33)
  ▸ Version: 2.0
    Exchange type: IKE_SA_INIT (34)
  ▸ Flags: 0x08 (Initiator, No higher version, Request)
    Message 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…
```

universität wien SBA Research CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

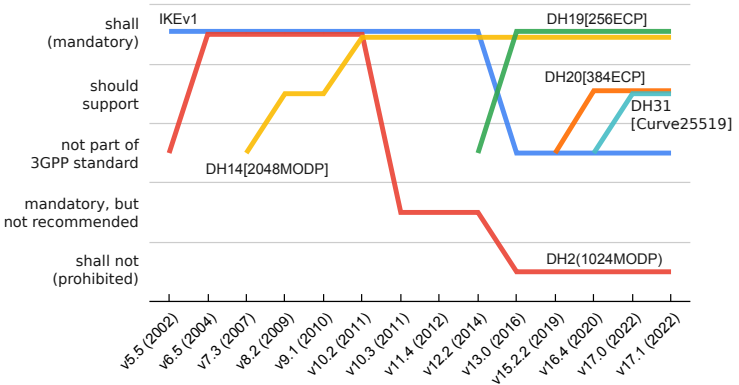
Practical Example: `IKE_SA_INIT` Packet

- 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)

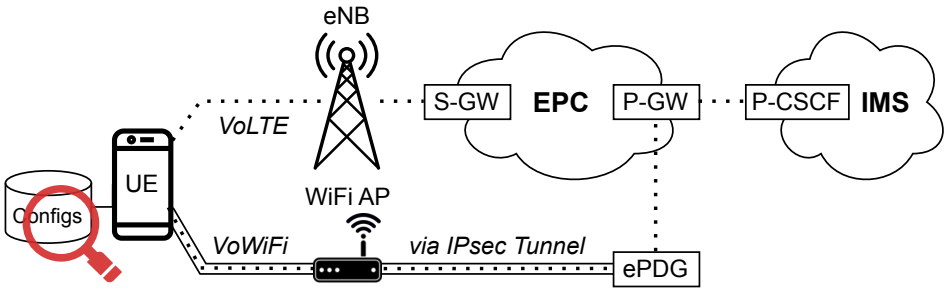
ETSI/3GPP Specification



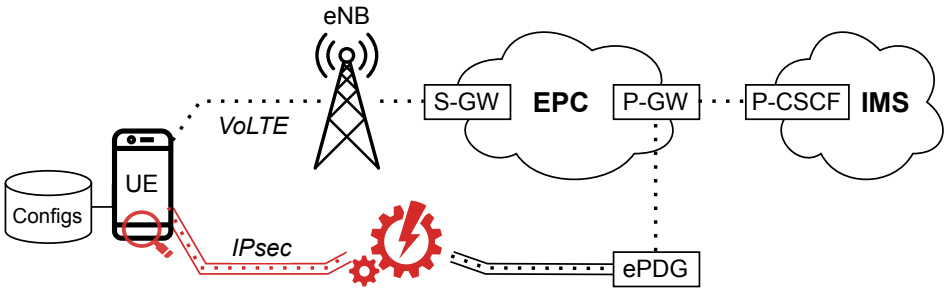
ETSI/3GPP Specification Over Time



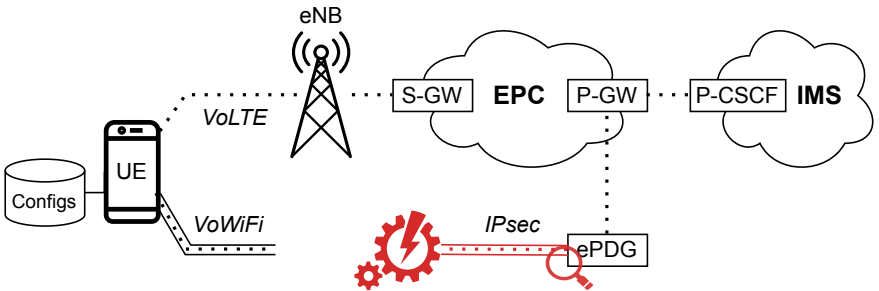
Step I: Analyze Pre-loaded Configs at the Client-Side

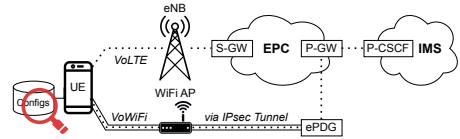


Step II: Analyze IPsec Client on the UE

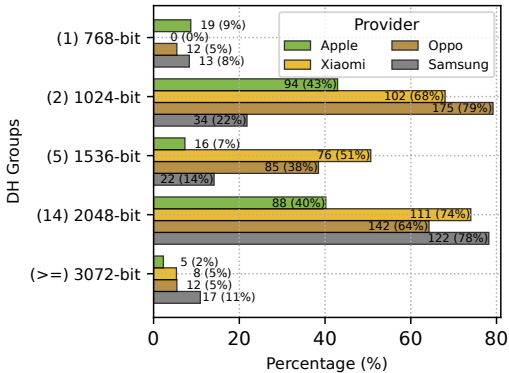


Step III: Analyze Server Side Configurations

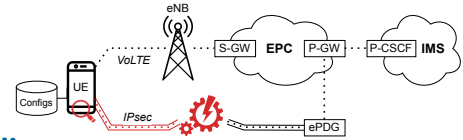




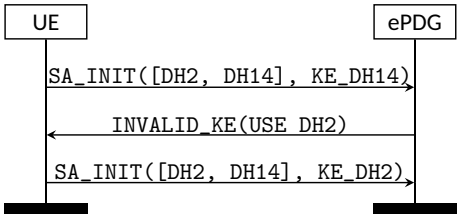
Results I: Pre-loaded Configs at the Client-Side



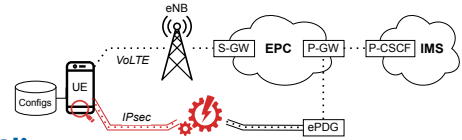
- Evaluated **different manufacturers and devices**
  - Apple: IPCC Carrier Profiles
  - Samsung: XML Config File
  - Xiaomi, Oppo: Qualcomm MBN File
- DH2 (1024-bit MODP) is very popular ϟ
- DH Groups > 2048-bit barely used



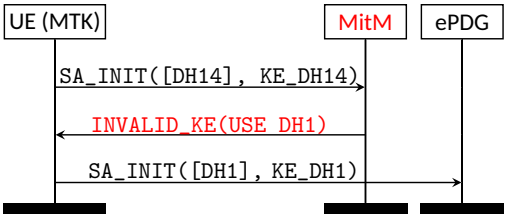
Results II: (Protocol Conform) Downgrade Possibility



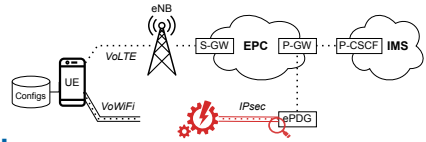
- Client selects **preferred DH group**, but also signals support for **other groups**
  - Server can request **switch to other group** via `INVALID_KE` packet
  - Client starts over, respecting the server's choice
- A malicious **interceptor** could **inject a downgrade packet**
  - Could be mitigated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



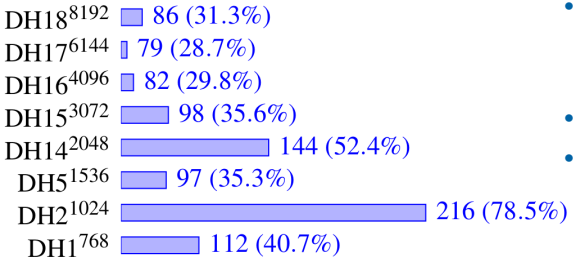
Results II: Downgrade Vulnerability at MediaTek Clients



- 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



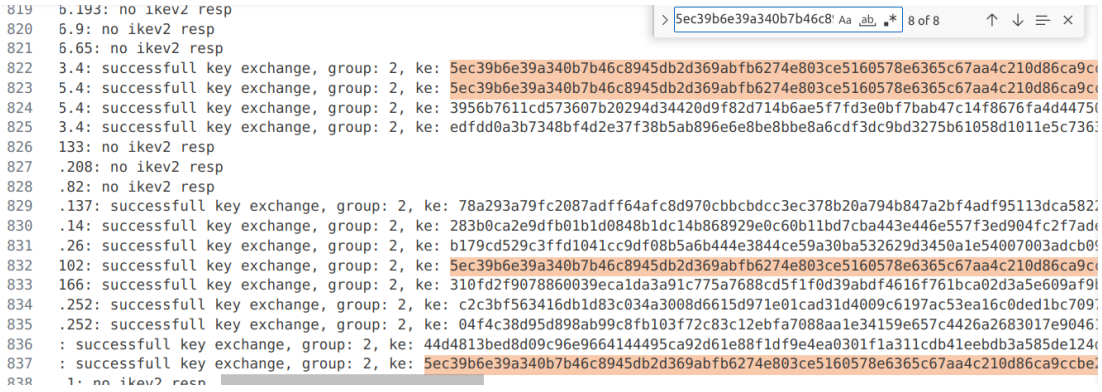
Results III: Supported DH Groups at the Server-Side



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

Figure 7: Number of MNOs per supported DH group

Result III: (Not-so) Private Keys



universität wien SBA Research CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Result III: (Not-so) Private Keys

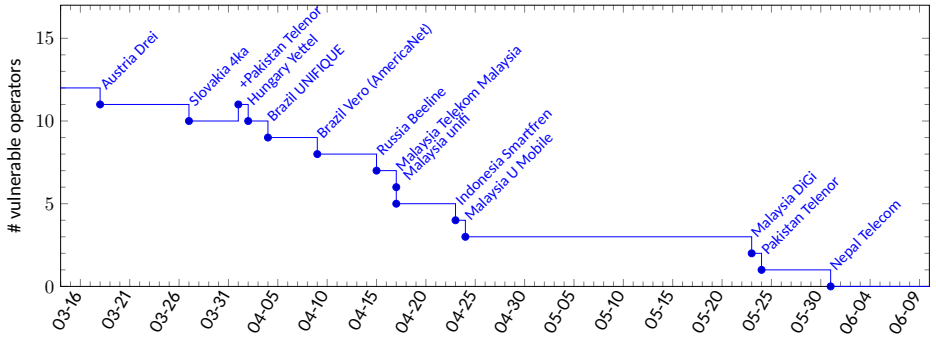
- Identical key exchange value -> **identical private-keys**
  - Inter MNO key sharing: private-key collisions with unrelated MNOs
- 16 operators **spread across the world**: e.g., Austria, Brazil, Indonesia, Malaysia, Nepal, Russia, etc.
  - Estimation: 140 million subscribers affected
  - Anyone having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

universität wien SBA Research CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

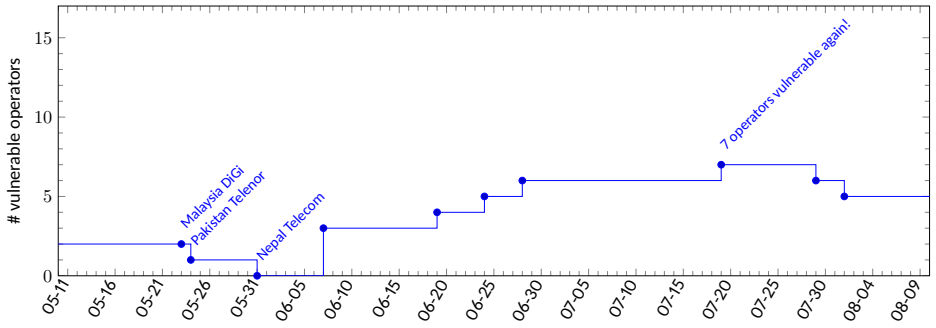
Responsible Disclosure and Remediation

- Responsible disclosure was coordinated by GSMA
  - Initial report in February 2024
  - CVD-2024-0089
- MediaTek: CVE-2024-20069, severity high
  - Fixed via Android Security Update (June 2024)
- ZTE: CVE-2024-22064, severity high
  - Private keys are leftovers from integration testing
  - Accidentally included into production images

ZTE: Remediation Timeline



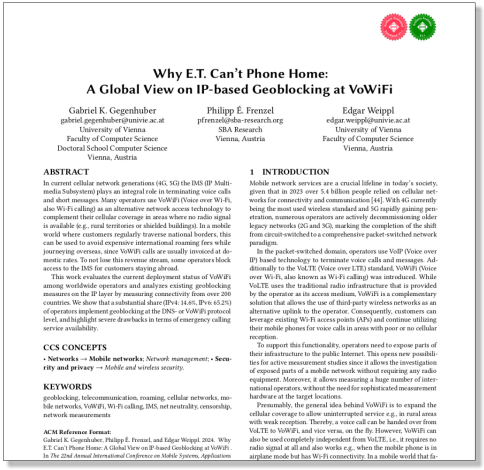
ZTE: Remediation Timeline Continued :|



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*

github.com/sbaresearch/scanywhere



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-

universität wien | SBA Research | CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Questions?

- Research artifacts on Github
  - Client side configuration extraction
  - Server side ePDG probing
- Contact
  - Mail: gabriel.gegenhuber (at) univie.ac.at
  - Twitter: @GGegenhuber

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]